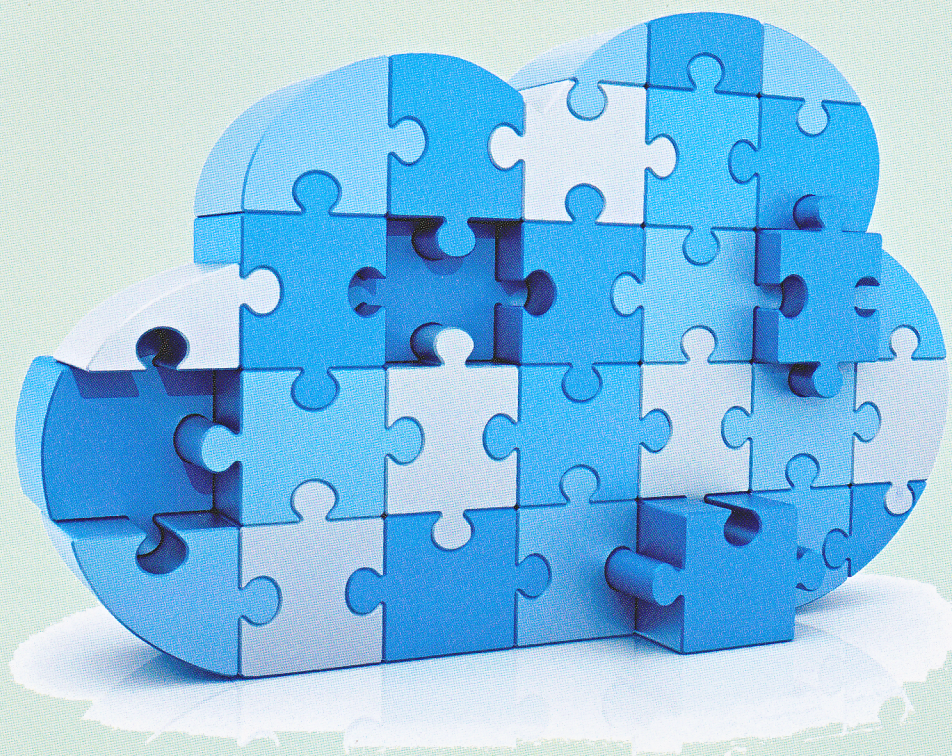


**РУМЕН ТРИФОНОВ • КАМЕН СПАСОВ
ПЛАМЕН ВАЧКОВ • СЛАВЧО МАНОЛОВ
РАДОСЛАВ ЙОШИНОВ • ЛЮБОМИР БЛАГОЕВ**

ОПЕРАТИВНА СЪВМЕСТИМОСТ НА ИНФОРМАЦИОННИ СИСТЕМИ



София • 2016

РУМЕН ТРИФОНОВ • КАМЕН СПАСОВ
ПЛАМЕН ВАЧКОВ • СЛАВЧО МАНОЛОВ
РАДОСЛАВ ЙОШИНОВ • ЛЮБОМИР БЛАГОЕВ

ОПЕРАТИВНА СЪВМЕСТИМОСТ НА ИНФОРМАЦИОННИ СИСТЕМИ



ОПЕРАТИВНА СЪВМЕСТИМОСТ НА ИНФОРМАЦИОННИ СИСТЕМИ

© Доц. Румен Трифонов, Автор, 2016

© Доц. Камен Спасов, Автор, 2016

© Доц. Пламен Вачков, Автор, 2016

© Доц. Славчо Манолов, Автор, 2016

© Доц. Радослав Йошинов, Автор, 2016

© Инж. Любомир Благоев, Докторант, Автор, 2016

ISBN 978-619-160-721-1

Издателство Авангард Прима

София 2016

Настоящата книга „Оперативна съвместимост на информационни системи“ е учебно помагало за Софийския университет и Технически университет – София. Тя е полезна за всички, компютърни и софтуерни инженери, студенти и докторанти в областта на математика и информатика, компютърни науки, компютърни системи и технологии, компютърно и софтуерно инженерство, електронно управление и информационни технологии.

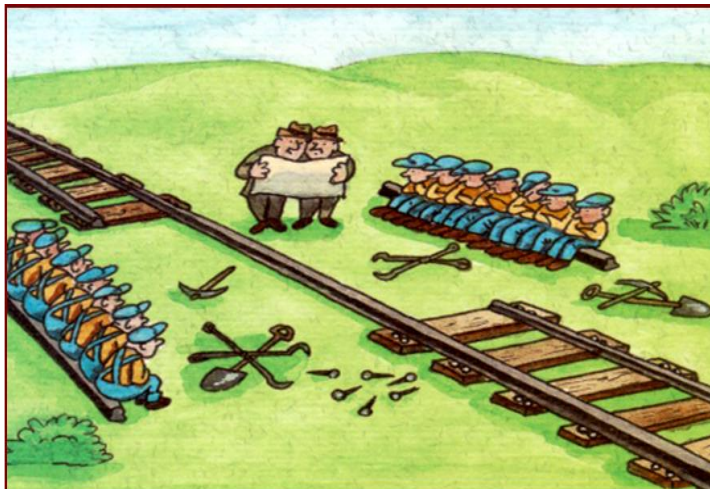
СЪДЪРЖАНИЕ

ОПЕРАТИВНА СЪВМЕСТИМОСТ НА ИНФОРМАЦИОННИ СИСТЕМИ.....	1
ЧАСТ 1	1
Фундаментален характер на оперативната съвместимост	1
ЧАСТ 2	10
ЕВРОПЕСКИ АСПЕКТИ	10
ГЛАВА 2.1	10
НОРМАТИВНА РЕГУЛАЦИЯ И СТАНДАРТИЗАЦИЯ НА ОПЕРАТИВНАТА СЪВМЕСТИМОСТ	10
ГЛАВА 2.2	25
ЕВРОПЕЙСКИ ИНИЦИАТИВИ	25
ГЛАВА 2.3	32
БЪЛГАРСКОТО РАЗВИТИЕ.....	32
ЧАСТ 3	35
ОПЕРАТИВНА СЪВМЕСТИМОСТ НА Е-ПРАВИТЕЛСТВО СЪГЛАСНО ЗАКОНА ЗА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ И НАРЕДБИТЕ КЪМ НЕГО	35
ГЛАВА 3.1	35
ЗАКОН ЗА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ	35
ГЛАВА 3.2	44
ОПЕРАТИВНА СЪВМЕСТИМОСТ	44
ЧАСТ 4	48
ТЕХНОЛОГИЧНА РЕАЛИЗАЦИЯ.....	48
ГЛАВА 4.1	48
ВЪВЕДЕНИЕ.....	48
ГЛАВА 4.2	50
РЕГИСТЪР НА СТАНДАРТИТЕ	50
ГЛАВА 4.3	61
РЕГИСТРИ НА ИНФОРМАЦИОННИТЕ ОБЕКТИ И НА ЕЛЕКТРОННИТЕ УСЛУГИ	61
ГЛАВА 4.4	75
ЕДИННА СРЕДА ЗА ОБМЕН НА ЕЛЕКТРОННИ ДОКУМЕНТИ (ЕСОЕД).....	75
ГЛАВА 4.5	86
СПИСЪЦИ НА АКРЕДИТИРАНИТЕ ЛИЦА И СЕРТИФИЦИРАНИТЕ СИСТЕМИ	86
ЧАСТ 5	88
СТРУКТУРА И ФУНКЦИОНАЛНОСТИ НА АДМИНИСТРАТИВНА ИНФОРМАЦИОННА СИСТЕМА (АИС)	88

ГЛАВА 5.1	88
АДМИНИСТРАЦИЯТА КАТО ОБЕКТ НА АВТОМАТИЗАЦИЯ. ОБЩА СХЕМА НА ВЪТРЕШНАТА АРХИТЕКТУРА НА АДМИНИСТРАТИВНАТА ИНФОРМАЦИОННА СИСТЕМА	88
ГЛАВА 5.2	95
СРЕДИЩНО ПОЛОЖЕНИЕ НА АДМИНИСТРАТИВНАТА ИНФОРМАЦИОННА СИСТЕМА.	95
ГЛАВА 5.3	98
ИЗИСКВАНИЯ КЪМ УПРАВЛЕНИЕТО НА ЖИЗНЕНИЯ ЦИКЪЛ В АИС ПРИ СЪВМЕСТНО ИЗПОЛЗВАНЕ НА ЕЛЕКТРОННИ И ДОКУМЕНТИ НА ХАРТИЕН НОСИТЕЛ.	98
ГЛАВА 5.4	108
ВЪЗЛАГАНЕ И ОТЧИТАНЕ НА ЗАДАЧИ ЧРЕЗ ИЗПОЛЗВАНЕТО НА ЕЛЕКТРОННИ ДОКУМЕНТИ. КОНТРОЛ НА ДЕЙНОСТТА ЧРЕЗ АИС.	108
ЧАСТ 6	123
СТАНДАРТИ ЗА ЕЛЕКТРОНЕН ОБМЕН НА ДАННИ.....	123
ЧАСТ 7	146
ОЦЕНКА НА СЪОТВЕТСТВИЕТО.....	146
ГЛАВА 7.1	146
ИЗПЪЛНЕНИЕ НА ДЕЙНОСТИТЕ ПО ОСИГУРЯВАНЕ НА ОПЕРАТИВНА СЪВМЕСТИМОСТ И ИНФОРМАЦИОННА СИГУРНОСТ СЪГЛАСНО ИЗИСКВАНИЯТА НА ЗЕУ	146
ГЛАВА 7.2	194
КОНТРОЛ НА ОПЕРАТИВНАТА СЪВМЕСТИМОСТ	194
ГЛАВА 7.3	196
СЕРТИФИКАЦИЯ	196
ИЗПОЛЗВАНА ЛИТЕРАТУРА	199

ЧАСТ 1

Фундаментален характер на оперативната съвместимост



Фигура 1-1

Глобализацията на “Информационното общество” поставя проблема за оперативната съвместимост на преден план.

Натрупаните несъответствия, неунифицирани подходи и технологии вече доведоха до т.н. “Цифрова анархия”, при което според Gartner Group от 40 до 80 % от стойността на информационните системи отива за приспособяване към съществуващите системи и към хетерогенната обкръжаваща среда. Според същия анализ около 2 % от глобалния брутен вътрешен продукт (над 1 трилион USD годишно) се губи от неефективността, предизвикана от системната несъвместимост, ръчното прехвърляне на информация с неизбежните грешки, информационен излишък и затруднените процеси на вземане на решения.

Това с особена сила важи за публичните системи, контактуващи с многообразни потребители.

Трябва, преди всичко, да стане ясно, че „оперативна съвместимост въобще“ не съществува. Това понятие винаги има контекст и се отнася до определени процеси и явления.

В нашия случай (и относно електронното управление, и относно електронния бизнес) става въпрос за информационно-ориентирана оперативна съвместимост. Това изключва от нашето внимание. При това, физическите и механични аспекти на оперативната съвместимост, като конектори за окабеляване, електрически контакти, винтове и гайки и пр. остават извън нашето внимание.

Между различните модификации на информационно-ориентираната оперативна съвместимост ние ще се фокусираме на тези, свързани с приложенията на електронното управление и електронния бизнес.

В същото време, трябва да се подчертае, че не трябва да се ограничаваме само с техническите аспекти на оперативната съвместимост. Областта на разглеждане трябва да включи съвместимост на правната уредба, организационната достъпност, съвместимостта

на моделирането на бизнес-процесите, възможностите за възприемане от потенциалните потребители и пр.

Дефиниции на оперативната съвместимост

Гледна точка	Дефиниция
Създаване на технически системи	Способност да се комуникира, да се изпълняват програми и да се обменят данни през различни функционални устройства по начин, който предполага потребителите да не познават уникалните характеристики на тези устройства
Специфициране природата на системите и компонентите	Способност на две или повече системи или компоненти да обменят информация и да използват информацията, която са обменили.
Включване концепцията за „процес“	Способност на система или процес да използва информация и/или функционалност от друга система или процес чрез спазване на общи стандарти.
Специфициране природата на процесите	Способност на ИКТ-системите и на бизнес-процесите, които те поддържат, да обменят данни и да позволяват да бъдат споделени информация или знание
Специфициране нивата на оперативната съвместимост	Способност на системите и машините да обменят, обработват и коректно да интерпретират информацията. Това е преди всичко техническо предизвикателство, но също включва правни, организационно и семантични аспекти на третираните данни

Тблица 1-1

Посочените дефиниции позволяват да се направят изводи за главните общи характеристики на оперативната съвместимост:

- че е способност на ИКТ-системите и бизнес-процесите, които те поддържат;
- че тази способност е свързана с обмен, обработка, правилно тълкуване, използване и споделяне на информация;
- че това включва технически, правни, организационни и семантични аспекти на третираните данни;
- че манипулацията с информацията се подчинява на общи стандарти.

Програмата MODINIS дефинира оперативната съвместимост в контекста на е-Правителство и специфицира ИКТ-системите и бизнес-процесите на публичните администрации, като изтъква обстоятелствата, свързани с обмена на информация. Според нея оперативната съвместимост е способността на ИКТ-системите и бизнес-процесите да споделят информация и знания вътре и извън организационните граници с цел да подобрят предоставянето на публични услуги, както и на публични политики и демократични процеси.

В същото време, дефиницията, приета от Европейската комисия и цитирана в Европейската рамка за оперативна съвместимост, определя, че оперативната съвместимост, в контекста на предоставянето на европейски обществени услуги, е способността на различни и разнообразни организации да си взаимодействат за постигане на взаимно изгодни и съгласувани общи цели, което включва обмен на информация и знания между организациите чрез бизнес-процесите, които те поддържат, посредством обмен на данни между съответните им ИКТ-системи.

Поради множество причини ние считаме, че дефиницията на Европейската комисия на оперативна съвместимост, обявена в "Европейската рамка за оперативна съвместимост на европейските обществени услуги", както следва:

"Оперативната съвместимост е способността на информационните системи и бизнес-процесите, които те поддържат, да обменят данни и да интегрират информация и знание", не е напълно подходяща в общия контекст на нашите цели.

Препоръчително е да се придържахме към по-широка дефиниция, която включва човешки, социални и организационни фактори

Добър пример е дефиницията на Австралийското правителство:

"Оперативната съвместимост не е точно технически начин за свързване на компютърни мрежи. Тя включва също споделяне на информация между мрежи и редизайн на бизнес процеси, който осигурява подобряване на резултатите и ефективността, както и поддържане на „безшевно“ предоставяне на електронни услуги.

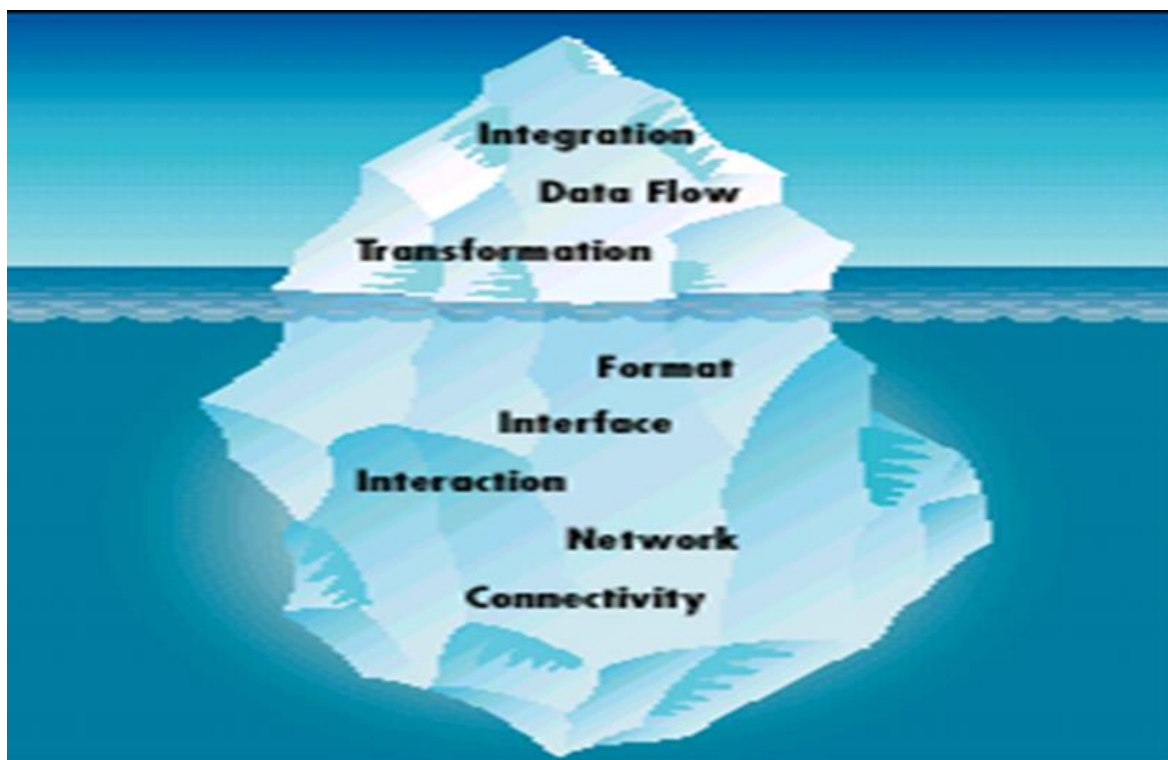
Оперативната съвместимост е важен елемент от предоставянето на е-Услуги и интеграционни инициативи. В този контекст, трябва да е ясно, че:

- оперативната съвместимост не е цел сама по себе си, но благоприятна възможност;
- стандартите са необходими, но не са достатъчни за постигане на оперативна съвместимост;
- от съществено значение е разбирането на икономическия, социалния, политическия и културния контекст на организациите;

- за да бъде оперативно съвместима, организацията трябва да се включва активно в непрекъснатия процес на гарантиране, че нейните системи, процеси и персонал се управляват по начин, който увеличава възможностите за вътрешен и външен обмен и повторно използване на информацията;

- организационни граници не трябва да стоят на пътя на решенията, които осигуряват високо качество на услугата. "Interoperability is an important element in the delivery of e-Service and integration initiatives. Within this context, it should be understood that:

„Айсбергът“ на системната интеграция



Фигура 1-2

Разликата между понятията “системна интеграция” и “оперативната съвместимост”

Разликата между “системна интеграция” и “оперативна съвместимост” е доста тънка. Съгласно дефинициите, възприети в Европейския съюз:

Оперативна съвместимост е способността на информационните системи и бизнес-процесите, които те поддържат, да обменят данни и да интегрират информация и знание.

Системната интеграция се дефинира като способност на функционалните поведения на различните системи, както и данните, върху които те се базират, да се интегрират в нови бизнес-процеси.

Системната интеграция предполага съвместно използване на компоненти, модули и процеси. При това, терминът “интегриран достъп до информация” предполага наличието

на външна (обхващаща) система, която комбинира множеството индивидуални механизми за достъп и осигурява единна интерпретация на представяната информация.

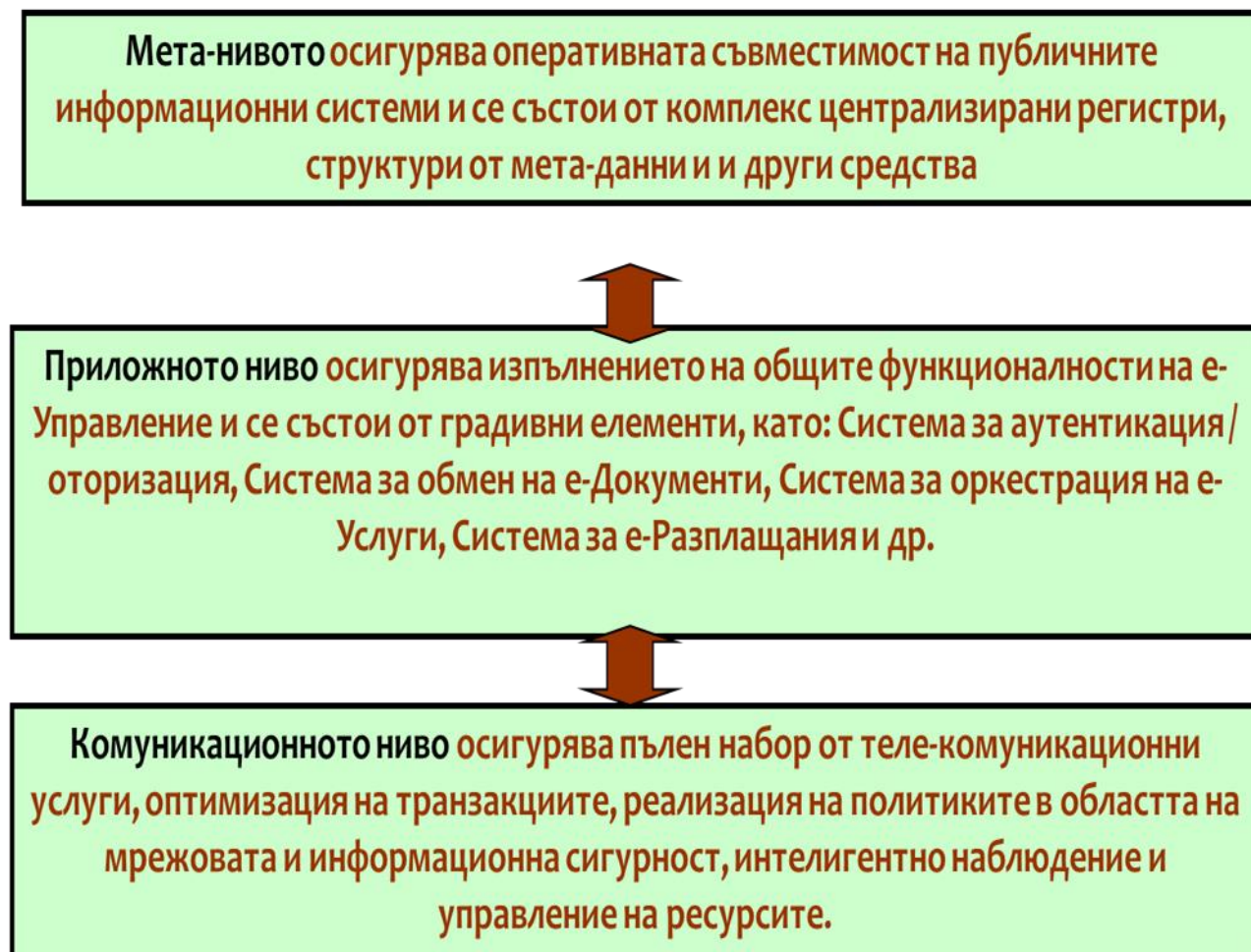
По принцип, системната интеграция преобладава в комплексните системи, обслужващи една институция. В сложните разпределени системи на разнообразни институции, като правило, става въпрос за оперативна съвместимост.

Електронното правителство е особено чувствително към проблемите на оперативната съвместимост поради многообразието и взаимовръзките на своите подсистеми



Фигура 1-3

Основни нива на Единната информационно-комуникационна среда за е-Управление



Фигура 1-4

Някои особености при е-Търговия

Оперативната съвместимост на електронната търговия има някои специфични особености в сравнение с другите сфери на електронното управление и информационно общество.

Те са свързани, преди всичко, с:

- идентификацията и класификацията на продукти и компоненти;
- синхронизацията и обмена на каталози и каталожни данни.

необходимост от строго спазване на отраслови стандарти (такива, като международните банково-финансови стандарти, регламентиращи електронните разплащания).

Освен това, съществуват съществени различия при прилагането на принципите на оперативната съвместимост в т.н. “мулти-секторна среда”, отколкото само в определен сектор.

Обща черта на новите подходи към проблема за оперативна съвместимост е необходимостта от систематизация на моделирането на бизнес-процесите. В съответствие с това, бизнес-мениджърите трябва да се фокусират върху изискванията и стандартните методологии за описание и управление на бизнес-процесите.

Основни аспекти на оперативната съвместимост

Оперативната съвместимост има три основни аспекта: организационен, семантичен и технически, които трябва да бъдат взети под внимание при разработването на информационните системи.

Организационният аспект на оперативната съвместимост произтича от различията в бизнес процесите и вътрешните структури на организациите, които участват в създаването и предоставянето на обществени услуги и трябва да си сътрудничат за постигане на взаимно изгодни и съгласувани европейски цели, свързани с обществените услуги,. Поради това, целта на постигането на организационна оперативна съвместимост е да се преодолеят всички организационни пречки, така че по този начин е да се създадат съответните интра-и интер-организационни работни потоци. На практика организационната оперативна съвместимост означава интегриране на бизнес процеси и свързаните с тях обмени на данни. Организационната оперативна съвместимост има за цел също така да способства на информационните системи да отговарят на изискванията на потребителската общност чрез предоставяне на услуги, лесно разпознаваеми, достъпни, и потребителски ориентирани.

Семантичният аспект на оперативната съвместимост произхожда от различните езикови, културни, правни и административни среди в държавите-членки, в частност и от многоезичието в Европейския съюз. Основните семантични конфликти са свързани със структурата на данните и смисъла на данните, например, различни термини се използват за един и същ смисъл (например значението "чужденец" в една база данни може да означава, че лицето не е гражданин на страната, , докато в друга база данни, то може да означава, че лицето не е гражданин на ЕС), различен формат за представяне на едни и същи данни, различни мерни единици (напр. сантиметри в една база данни и в инчове в друга), и т.н.

Ето защо, семантична оперативна съвместимост е предназначена за управлението на всички семантични конфликти между различните системи в напълно автоматизиран начин и възможност за добавяне на нови системи или премахване съществуващи по всяко време. Семантичната оперативна съвместимост дава възможност на организациите да обработват информация от външни източници по съдържателен начин и гарантира разбирането и запазването на точното значение на обменената информация. Разрешаване на семантични конфликти могат да бъдат постигнати чрез използването на договорен език за представяне на данните. С други думи, необходимо е да се разработи обща таксономия, речник на използваните термини или каталог за приобщаване на данните, които допълнително трябва да бъдат предоставени на разположение на информационни системи.

Техническият аспект на оперативната съвместимост е свързан със способността за обмен на информация между хетерогенни компютърни мрежи, приложения и техни

компоненти. Техническата оперативна съвместимост се занимава с всички технически въпроси (технологии, стандарти, политики), за да се гарантира, че техническите компоненти на информационните системи на сътруднящите си органи ще могат да работят заедно. Поради това, техническата оперативна съвместимост обхваща техническите аспекти на свързването на информационните системи. Следва да се отбележи, че техническата оперативна съвместимост обхваща не само технологии за връзка на физическо ниво (като мрежови протоколи, например), но също и с технологии, които поддържат организационния и семантичния слоеве. Тя включва аспекти като интерфейсни спецификации, услуги за взаимно свързване, за интеграция на данни и услуги, представяне на данните при обмен, и т.н. Тя е най-очевидният аспект на оперативната съвместимост, защото компютърните системи са изградени и развити с използване на инженерната техника и за всеки технически проблем е възможно да се намери подходящо решение.

Ползи и бенефициенти на оперативната съвместимост

Оперативната съвместимост е както предпоставка, така и улесняващ фактор за ефективното предоставяне на европейски обществени услуги. Тя включва необходимостта от:

- сътрудничество между публичните администрации, за да се урегулират обществените услуги;
- обмен на информация между публичните администрации за изпълнение на правните изисквания или политическите ангажименти;
- споделяне и повторно използване на информация между публичните администрации за повишаване на административната ефективност и намаляване на затрудненията за гражданите и бизнеса.

При това се постигат следните резултати:

- подобро предоставяне на публични услуги на гражданите и бизнеса, чрез осигуряване "обслужване на едно гише" за предоставянето на обществени услуги;
- по-ниски разходи за публичните администрации, бизнеса и гражданите, благодарение на ефикасното предоставяне на публични услуги. В рамките на програмата MODINIS, бяха определени следните пет различни направления, в които предимствата на оперативна съвместимост на ИКТ-системи са очевидни;
- между различните услуги, насочени се към един и същ потребител, а именно „групирани“ услуги (например, според събитията от живота или проблемните сценарии), които икономисват ресурси и подобряват качеството на услугите (правителство „на едно гише“);
- в различните етапи от веригата за добавена стойност на дадена услуги, когато доставчикът на услугата се нуждае от данни, администрирани от други доставчици, и има нужда от обмен на тези данни с тях. При това е необходима оперативна съвместимост между данните и работните процеси в двете организации;

- между отделните агенции в различни географски области, а именно оперативна съвместимост, отнасяща се до прякото прехвърляне на данни от системата на една администрация в системата на друга администрация (главно, пространствени данни);
- между директории на услуги или документи, а именно оперативна съвместимост между местните директории, общи метаданни за услугите, както и алгоритми за намиране на съответния администратор на данните. Този важен въпрос изисква създаването на общи дескриптори за услуги и доставчици;
- допълнителни услуги (управление на идентичността, валидация на подписани електронни документи и т.н.).

Следващата таблица обобщава основните бенефициенти на оперативната съвместимост, както и ползите, които те получават от оперативно съвместимите публични услуги.

Бенефициент	Полза
Публична администрация на страна членка и ЕК	<ul style="list-style-type: none"> - повишаване на ефективността при установяване на европейски обществени услуги; - повишаване на информираността за риска от създаване на нови електронни бариери, ако бъдат избрани за обществени услуги решения, които не са оперативно съвместими на равнище Европейски съюз; - сътрудничество, което улеснява обмена, споделянето и повторната употреба на информация..
Граждани и бизнес	<ul style="list-style-type: none"> - ефикасна и ефективна доставка на публични услуги на гражданите и бизнеса, независимо от границите и секторите; - намаляване на разходите; - избягване дублирането на материални разходи и човешки труд; - намаляване на административните тежести.
Европейският съюз като цяло	<ul style="list-style-type: none"> - принос за постигането на целите на Лисабонската стратегия за превръщане на Европа в най-динамичната и конкурентноспособна, основана на знанието икономика чрез подобряване на качеството на живот на гражданите и чрез намаляване на административната тежест върху предприятията; - по-ефективно прилагане на политиките и инициативите на Европейския съюз; - насърчаване на укрепването на общия пазар чрез четирите свободи; - подкрепа на икономическата интеграция на страните и на консолидирането на вътрешния пазар.

Таблица 1-2

ЧАСТ 2

ЕВРОПЕСКИ АСПЕКТИ

ГЛАВА 2.1

НОРМАТИВНА РЕГУЛАЦИЯ И СТАНДАРТИЗАЦИЯ НА ОПЕРАТИВНАТА СЪВМЕСТИМОСТ

Барieri пред оперативната съвместимост

Има много препятствия, които могат да пречат на напредъка по реализирането на концепцията за електронно правителство, призната за приоритет в рамките на Европейския съюз чрез различни свързани директиви, комуникета и изследователски инициативи. Съществените правни, политически, административни, социални, институционални и културни различия между държавите-членки и регионите в ЕС предизвикват необходимостта от систематизиране на основните пречки пред електронното правителство, които препятстват електронизацията на важни обществени услуги в ЕС през националните и регионалните граници (например: за електронни обществени поръчки, за електронно здравеопазване, за подкрепа на трудовата мобилност и пр.). Бързото технологично развитие също създава проблеми.

Европейските документи определят седем основни категории барieri, които могат да блокират или ограничават напредъка на електронното правителство:

1. Неуспешно ръководство -. Бавен и неравномерен напредък на електронното правителство като резултат от липсата на адекватна лидерство по време на всеки етап в инициирането, изпълнението, популяризирането и продължаващата подкрепа на развитието му.

2. Финансови задръжки - неадекватни анализи на разходите и ползите могат да провалят или задръжат притока на инвестиции в нивата, необходими за подкрепа на развитието на електронното правителство.

3. Цифрово неравенство – неравностойност в: уменията, достъпа до съответните системи, знанията и мотивационната подкрепа. Това може да се ограничи и фрагментира навлизането на електронното правителство.

4. Лоша координация - липсата на координация и хармонизация може да бъде спирачка за създаването на подходящи за електронно правителство мрежи и услуги, които пресичат административните и географски граници.

5. Липса на организационна гъвкавост - широката реализация на ползите от електронното правителство може да бъде ограничена или блокирана от закостенялост в отговор на необходимостта от извършване на необходимите промени в практиките на публичната администрация, на процесите и организационните структури, които да позволяват ефективното използване на възможностите на електронните мрежи и улесняването на обмена на информация и предоставянето на услуги.

6. Липса на доверие - повишените страхове за недостатъчни гаранции за сигурност и защита на личните данни в електронните мрежи може да подкопае доверието в приложенията на електронното правителство.

7. Лошо техническо проектиране - блокажите за оперативната съвместимост, причинени от несъвместимост между ИКТ системи или трудни за използване интерфейси за услуги на електронното правителство илюстрират вида на практическите недостатъци, които могат да станат сериозни оперативни пречки за навлизане на e-Government системи.

Правните измерения на основните категории бариери подчертават доколко законите и наредбите са основните фундаменти за политиките, засягащи електронното правителство в рамките на и между европейските държави-членки и на регионално ниво.

Например, директивите на ЕС, свързани с електронното правителство, включват:

- Директива 1999/93 / ЕО на Съвета относно електронните подписи;
- Директива 2001/29 / ЕО относно хармонизирането на някои аспекти на авторското право и сродните му права в информационното общество;
- Директива 2002/58 / ЕО на Съвета относно неприкосновеността на личния живот и електронни комуникации и;
- Регламент 2014/910 / ЕО относно електронната идентификация.

В тези директиви са предвидени осем ключови правни измерения:

- Административно право;
- Аутентикация и идентификация;
- Права на интелектуална Собственост;
- Отговорност;
- Личен живот и защита на данните;
- Прозрачност в държавната администрация;
- Отношения между публичните администрации, гражданите и други участници в областта на ИКТ и
- Повторна употреба на информацията в общественния сектор.

Цифровият дневен ред на Европейския съюз

На 19 май 2010 г. европейският комисар по информационно общество г-жа Нели Крос представи новата европейска програма в областта на информационните технологии. т.н. “A Digital Agenda for Europe”.

Този програмен документ дефинира осем основни направления за действие, едното от които е “Оперативна съвместимост и стандарти”. В документа се казва: „Необходима ни е действителна оперативна съвместимост между продуктите и услугите на информационните технологии (ИТ), за да



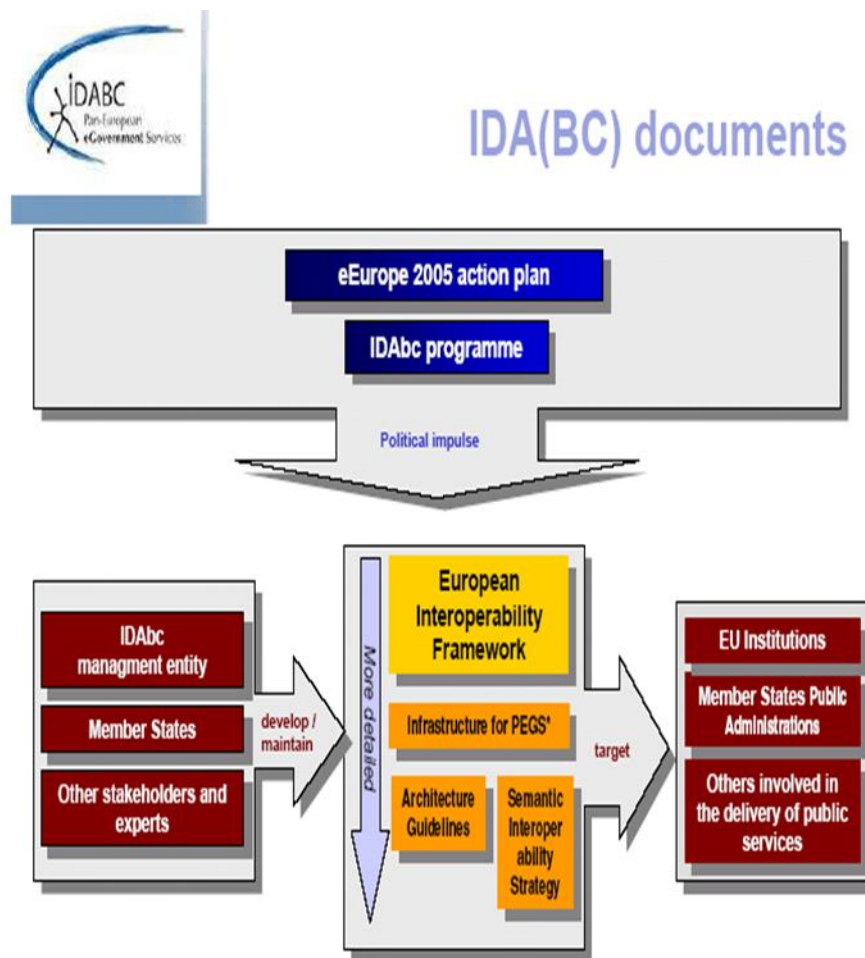
изградим истинско информационно общество.

Интернет е най-добрият пример за мощта на техническата оперативна съвместимост . Неговата отворена архитектура предостави оперативно съвместими устройства и приложения на милиарди хора в цял свят. Но за пълно оползотворяване на предимствата на ИКТ трябва още да се повиши оперативната съвместимост между устройствата, приложенията, хранилищата на данни, услугите и мрежите.

Европейска “пътна карта” за постигане на оперативна съвместимост

Съгласно “пътната карта” на Програмата на Европейската комисия IDABC (Interoperable Delivery of European e-Government Services to public Administrations, Businesses and Citizens), разработката на пан-Европейската среда, осигуряваща системната интеграция и оперативна съвместимост на информационните системи, преминава през следните основни етапи:

- създаване на “Рамка за оперативна съвместимост на информационните системи”;
- разработване на конкретни правила за системна интеграция и оперативна съвместимост на приложения, свързани с електронното правителство;
- разработване на “Препоръки за архитектурата на информационните системи”;
- създаване на централно хранилище на информационни ресурси, необходими за постигане на оперативна съвместимост;
- създаване на “пан-Европейска административна ориентационна карта”.

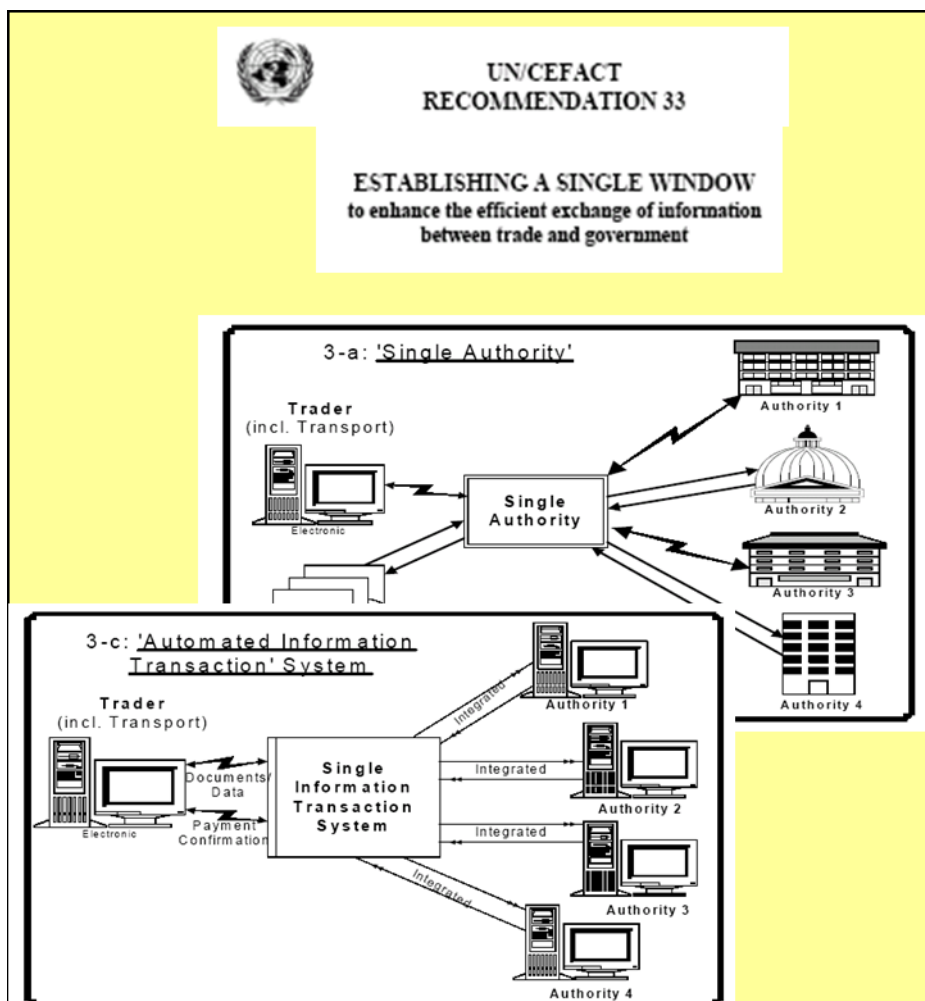


Фигура 2-1

Международни документи, регламентиращи оперативната съвместимост.



Фигура 2-2



Фигура 2-3

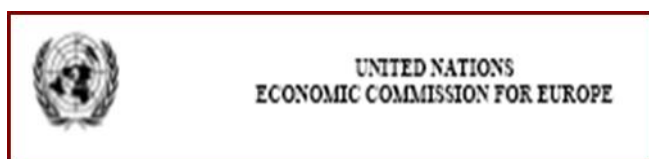
Препоръка № 35 на UN/CEFACT от 2010 г. за правните основи на “единния прозорец”

В контекста на тази Препоръка “единният прозорец” се определя като механизъм, позволяващ на страните, участващи в търговски и транспортни операции да представят стандартизирана информация и документи с използване на единен пропускателен канал с цел изпълнение на всички регулиращи изисквания, засягащи импорта, експорта и транзита.

Ако информацията е в електронен вид, то отделните елементи на данните трябва да се представят само един път.

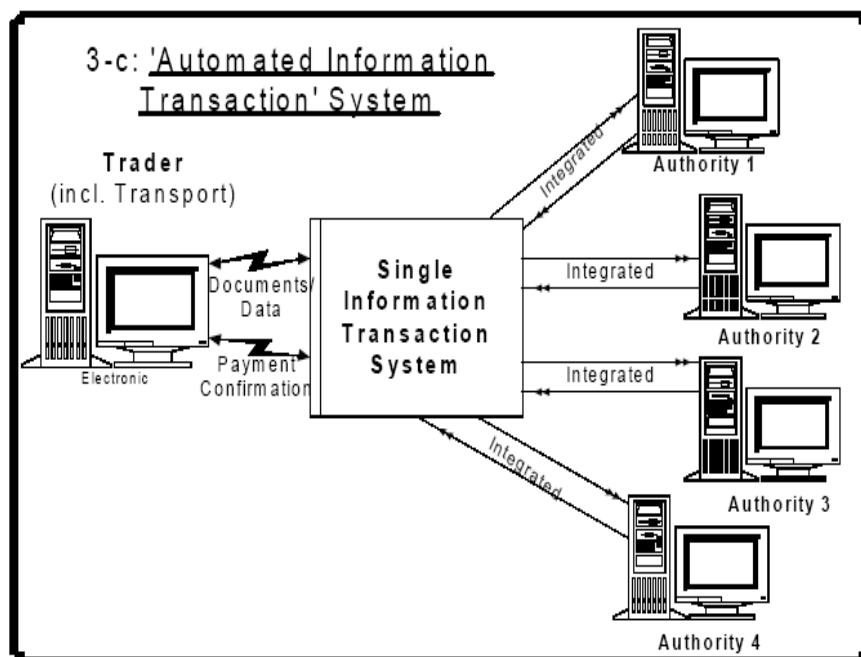
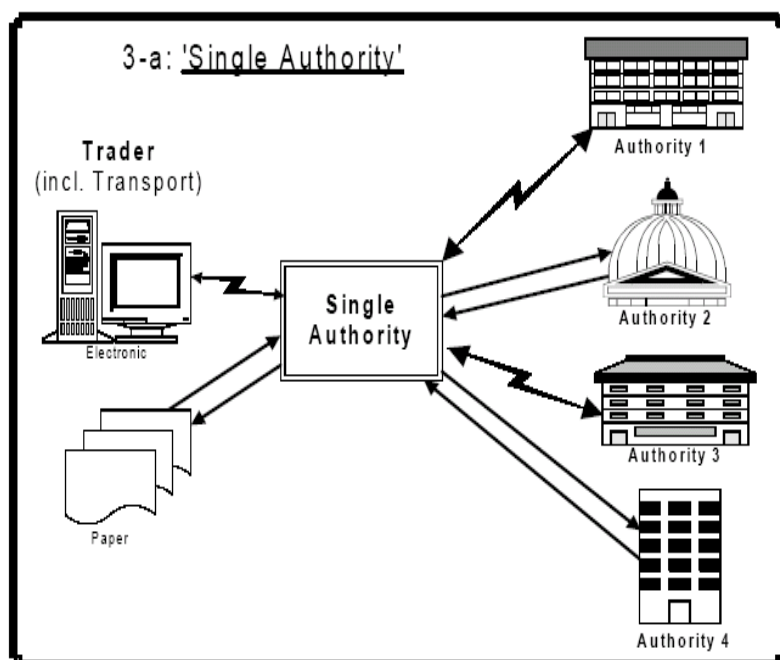
От практическа гледна точка “единният прозорец” е призван да опрости и ускори информационните потоци между фирмите и държавните органи и да донесе значителни изгоди за всички страни, участващи в транс-граничната търговия. “Единният прозорец”, като правило, се управлява от централизирана организация, което осигурява на съответните държавни органи и учреждения възможност за получаване на актуална информация за техните цели. Освен това, държавните органи и учреждения могат да координират техните мерки за контрол.

При определени условия “единният прозорец” може да осигури възможност за заплащане на съответните данъци, такси, мита, акцизи и т.н.



UN/CEFACT
RECOMMENDATION 33

ESTABLISHING A SINGLE WINDOW
to enhance the efficient exchange of information
between trade and government



Фигура 2-4

Създаването на “единен прозорец” често изисква изменение на действащите закони и подзаконови актове, например законите за електронно представяне на документите, за електронните подписи, за потвърждаване на потребителя и на съобщенията, за обмен на данните, за осигуряване на съхранението, унищожаването и архивирането на данните и електронните потвърждения.

Разбира се, системата на “единния прозорец” може да се създаде и без съществени изменения на националните законодателства. Във всеки случай, действащите понастоящем нормативни актове и практика, които регламентират движението на търговската информация, въздействат на избора на организационния и технологичния модели на системата за “единен прозорец”. Затова, съвременният анализ на съществуващите и на потенциалните юридически препятствия, свързани с обмена на търговски данни, представлява първата важна крачка към създаването и настройването на “единния прозорец”. Такъв анализ трябва да отчита възможно най-широкия контекст на международната търговия, в която ще функционира “единният прозорец”..

За всички операции на “единния прозорец” е крайно важна прозрачността и безопасността на обмена на търговски данни. Надеждният правов режим, който прави възможни събирането на данните, достъпа до тях, тяхното разпределение и уточнява режима на конфиденциалност и отговорност, позволява да се създаде надеждна основа за функциониране на такъв механизъм и установява отношения на доверие между всички заинтересовани страни.

В тези случаи, когато се разглежда внедряването на електронна система за “единен прозорец” за организатора на този процес е важно да анализира общите законодателни рамки в сферата на електронната търговия, включително електронния обмен на данни и електронните подписи. Това е целесъобразно не само за системата на “единния прозорец” в търговията, но също така и с цел развитие на електронните инструменти за взаимодействие извън рамките на системата на “единния прозорец”. Трябва да се отговори на въпросите:

- а) изучена ли е юридическата основа за реализацията на системата за “единен прозорец”?
- б) избрана ли е съответната организационна структура?
- в) създадени ли са съответните процедури за идентификация, удостоверяване на истинността и за санкциониране?
- г) кой има пълномощия да изисква данни от “единния прозорец”?
- д) кога и как данните могат да се използват съвместно, в какви обстоятелства и с какви органи на страната и на други страни?
- е) създадени ли са съответните механизми за защита на данните?
- ж) кой носи отговорност за осигуряване на точност и цялостност на данните?
- з) създадени ли са механизми за регулиране на споровете?
- и) създадени ли са процедури за електронно архивиране и система от контролни записи?
- к) разгледани ли са въпросите относно интелектуалната собственост и собствеността на базите данни?

Европейска стратегия за оперативната съвместимост

Европейската стратегия за оперативна съвместимост и Европейската рамка за оперативна съвместимост, която допълва и детайлизира постановките на стратегията, се

считат за два ключови елемента в „Цифровия дневен ред за Европа“ и служат за основа на бъдещи дейности, насочени към подобряване на оперативната съвместимост за предоставяне на Европейския обществени услуги.

Прилагането на Европейската стратегия за оперативна съвместимост изисква следното разделение на ролите:

1. Европейската комисия ще осигури:

- прилагане на Европейската стратегия за оперативна съвместимост чрез подходящи инструменти, като Програма ISA (Interoperability Solutions for European public Administrations) и Програма ICT-PSP (Information and Communication Technologies Policy Support Programme) ;
- организиране на тясно сътрудничество между държавите-членки и други заинтересовани страни в областта на изграждане на електронно правителство;
- привеждане на вътрешните стратегии за оперативна съвместимост с Европейската стратегия за оперативна съвместимост чрез инициативи на комисията;
- гарантиране на включването на Европейската рамка за оперативна съвместимост при прилагането на ново законодателство и създаването на нови европейски обществени услуги;
- осигуряване на управлението на Европейската стратегия за оперативна съвместимост и на свързаните с нея глобални и секторните дейности за оперативна съвместимост, в тясно сътрудничество с държавите-членки.

2. Държавите-членки ще осигурят:

- - привеждане на националните стратегии за оперативна съвместимост в съответствие с Европейската стратегия за оперативна съвместимост, както и национални инициативи и действия, със съответните инициативи и действия на ниво Европейски съюз;
- - взаимодействие помежду си и с Европейската комисия относно прилагането на Европейската стратегия за оперативна съвместимост, при наблюдение на напредъка и въздействието на свързаните с тях действия на национално ниво;
- привеждане на националните рамки за оперативна съвместимост в съответствие с Европейската рамка за оперативна съвместимост;
- - вземане предвид на европейското измерение на ранен етап в развитието на всяка публична услуга, която може да стане част от европейските обществени услуги в бъдеще;
- - допринасяне за управлението на Европейската стратегия за оперативна съвместимост и на свързаните с него дейности за оперативна съвместимост.

Европейската стратегия за оперативна съвместимост е разработена от Генералната дирекция на Европейската комисия за информатика в споразумение за сътрудничество с държавите-членки и е приета през 2010 година. Стратегията беше подготвена в изпълнение на Програмата IDABC (Interoperable Delivery of pan-european services for

Administration, Businesses and Citizens) и финализирана след обществено допитване в рамките на последвалата я Програма ISA.

За да се постигне общоевропейско ефективно и ефикасно предоставяне на публични услуги, дейностите на Европейския съюз и на ниво „държава-членка“ следва да бъдат координирани. Освен това, следва да се установи управление на оперативната съвместимост на ниво Европейски съюз. Европейската стратегия за оперативна съвместимост е в горната част на пирамидата на управление на оперативната съвместимост и тя определя общ, последователен подход и предоставя основа за организационна, финансова и оперативна рамка в подкрепа на трансграничната и междусекторна оперативна съвместимост. Европейската стратегия за оперативна съвместимост има за цел да предостави насоки и да се даде приоритет на необходими действия за подобряване на взаимодействието, обмена и сътрудничеството между европейските публични администрации през границите и между отделните сектори, за предоставянето на европейски обществени услуги.

Дейностите, съдържащи се в Европейската стратегия за оперативна съвместимост следват определен набор от принципи, които са описани в таблицата по-долу.

Принцип	Обяснение
Повторна употреба	Дейностите на Европейската стратегия за оперативна съвместимост трябва да бъдат приспособени за повторна употреба въз основа на устойчиви подходи
Прозрачност	Дейностите на Европейската стратегия трябва да са прозрачни и да предлагат възможност за проследяване
Отвореност и иновации	Дейностите на Европейската стратегия трябва да са отворени, съответстващи на стандартите, платформено-независими и да позволяват бъдещо развитие и усъвършенстване
Непрекъснато подобряване	Дейностите на Европейската стратегия трябва да се базират на непрекъсната оценка и подобряване
Общ интерес	Дейностите на Европейската стратегия трябва да почиват на общия интерес. Това може да бъде на различни нива: на експертната общност, на общността на публичните услуги, на цялата европейска общност
Доверие	Дейностите на Европейската стратегия трябва да се базират на взаимното доверие. Администрациите трябва да осигурят всички транзакции да са сигурни, надеждни и заслужаващи доверие

Тблица 2-1

Дейностите по оперативна съвместимост са специфицирани в Европейската стратегия три групи, описани в таблицата по-долу.

Главни компоненти	Цел	Специфични дейности
Сигурен информационен обмен	Да определи как трябва да се предава и обработва информацията, за да се постигне оперативна съвместимост	<ul style="list-style-type: none"> - да се работи с ограничено количество политически съгласувани и конкретни секторни проекти на ниво Европейски съюз или страни-членки; - да се осигури непрекъсната поддръжка на ключови елементи от оперативната съвместимост на европейско ниво (електронна идентификация, цифрови подписи и пр.); - да бъде осигурено продължение на подхода на проекта SEMIC (www.semic.eu) за семантична оперативна съвместимост - да се работи за създаването на отворени базови регистри, отчитайки добрите практики, възможните рискове и алтернативи, както и разнообразните желания и очаквания на всички участници; - да се работи по създаването на общи каталози на услугите, предоставяни от публичните администрации в Европейския съюз.

Тблица 2-2

Гл. компоненти	Цел	Специфични дейности
Архитектура на оперативната съвместимост	Да се определи как инфраструктурата може да осигури ОС	<ul style="list-style-type: none"> - да разработят обща визия за архитектурата на оперативната съвместимост, като първо се дефинира нейния обхват и потребностите от общи инфраструктурни услуги и общи стандарти на интерфейса; да дефинират насоки относно областите на архитектурата, в които държавите-членки имат общ интерес; - да гарантират системното повторно използване на архитектурни блокове при разработването на услуги, които да се използват от държавите-членки. Съществуващите компоненти на инфраструктурата на услуги заедно с общи приложения (системи за ранно предупреждение, управление на проекти и т.н.) могат да бъдат използвани отново и рационализирани. Освен това, да се създаде каталог на архитектурни блокове за повторно използване на разположение от държавите-членки

Таблица 2-3

Европейска рамка за оперативна съвместимост

Първата версия на Европейската рамка за оперативна съвместимост бе одобрена през октомври 2004 година. В момента реалната версия е втората версия на рамката, която бе одобрена през 2010 година. Европейската рамка за оперативна съвместимост се поддържа от Европейската комисия, чрез изпълнението на програмата ISA ([http://ec.europa.eu / МОС /](http://ec.europa.eu/MOC/)), в тясно сътрудничество със държавите-членки на ЕС.

Рамката за оперативна съвместимост представлява съгласуван подход за оперативна съвместимост за организации, които желаят да работят заедно за постигане на съвместно предоставяне на обществени услуги. В контекста на нейното приложно поле, в документа се посочва набор от общи елементи, като например: речник, понятия, принципи, политики, насоки, препоръки, стандарти, спецификации и практики.

Европейската рамка за оперативна съвместимост е всеобхватен набор от политики, стандарти и насоки, които описват начина, по който организациите са се споразумели, или трябва да се споразумеят, за да взаимодействат по електронен път един с друг.

Европейската рамка за оперативна съвместимост е нетехническо документ, разработен със следните основни цели:

- да насърчава и подкрепя предоставянето на европейски обществени услуги чрез насърчаване на трансграничната и междусекторна оперативна съвместимост;
- ориентиране на публичните администрации в тяхната работа, за да се предоставят пан-европейски транс-гранични публични услуги на бизнеса и гражданите;
- да се допълнят и свържат заедно различните национални рамки за оперативна съвместимост на европейско равнище.

В целевата аудитория на Европейската рамка за оперативна съвместимост се включват всички, които: - - участват в определянето, разработването и прилагането на европейски обществени услуги, например, мениджърите на проекти за електронно управление в държавите-членки, администрациите и органите на Европейския съюз, администрациите на държавите-членки, европейските институции и агенции и пр.

Европейската рамка за оперативна съвместимост се прилага, когато:

- се вземат на решения за европейски публични услуги, които подпомагат осъществяването на инициативи, свързани с политиката на Европейския съюз;
- изграждане на публични услуги, които в бъдеще могат да бъдат повторно използвани като част от европейските обществени услуги.

Европейската рамка за оперативна съвместимост обхваща следното съдържание:

- 25 препоръки за публичните администрации;
- 12 основни принципи;
- концептуалния модел за обществени услуги;
- 3 нива на оперативна съвместимост;
- концепция за споразумения за оперативна съвместимост;
- механизми за управление на оперативната съвместимост.

Основни принципи на Европейската рамка

Ето защо, семантична оперативна съвместимост е предназначена за управлението на всички семантични конфликти между различните системи в напълно автоматизиран начин и възможност за добавяне на нови системи или премахване съществуващи по всяко време. Семантичната оперативна съвместимост дава възможност на организациите да обработват информация от външни източници по съдържателен начин и гарантира разбирането и запазването на точното значение на обменената информация. Разрешаване на семантични конфликти могат да бъдат постигнати чрез използването на договорен език за представяне на данните. С други думи, необходимо е да се разработи обща таксономия, речник на използваните термини или каталог за приобщаване на данните, които

допълнително трябва да бъдат предоставени на разположение на информационни системи.

Техническият аспект на оперативната съвместимост е свързан със способността за обмен на информация между хетерогенни компютърни мрежи, приложения и техни компоненти. Техническата оперативна съвместимост се занимава с всички технически въпроси (технологии, стандарти, политики), за да се гарантира, че техническите компоненти на информационните системи на сътрудническите си органи ще могат да работят заедно. Поради това, техническата оперативна съвместимост обхваща техническите аспекти на свързването на информационните системи. Следва да се отбележи, че техническата оперативна съвместимост обхваща не само технологии за връзка на физическо ниво (като мрежови протоколи, например), но също и с технологии, които поддържат организационния и семантичния слоеве. Тя включва аспекти като интерфейсни спецификации, услуги за взаимно свързване, за интеграция на данни и услуги, представяне на данните при обмена, и т.н. Тя е най-очевидният аспект на оперативната съвместимост, защото компютърните системи са изградени и развити с използване на инженерната техника и за всеки технически проблем е възможно да се намери подходящо решение.

Оперативната съвместимост е както предпоставка, така и улесняващ фактор за ефективното предоставяне на европейски обществени услуги. Тя включва необходимостта от:

- сътрудничество между публичните администрации, за да се урегулират обществените услуги;
- обмен на информация между публичните администрации за изпълнение на правните изисквания или политическите ангажименти;
- споделяне и повторно използване на информация между публичните администрации за повишаване на административната ефективност и намаляване на затрудненията за гражданите и бизнеса.

При това се постигат следните резултати:

- подобро предоставяне на публични услуги на гражданите и бизнеса, чрез осигуряване "обслужване на едно гише" за предоставянето на обществени услуги;
- по-ниски разходи за публичните администрации, бизнеса и гражданите, благодарение на ефикасното предоставяне на публични услуги.

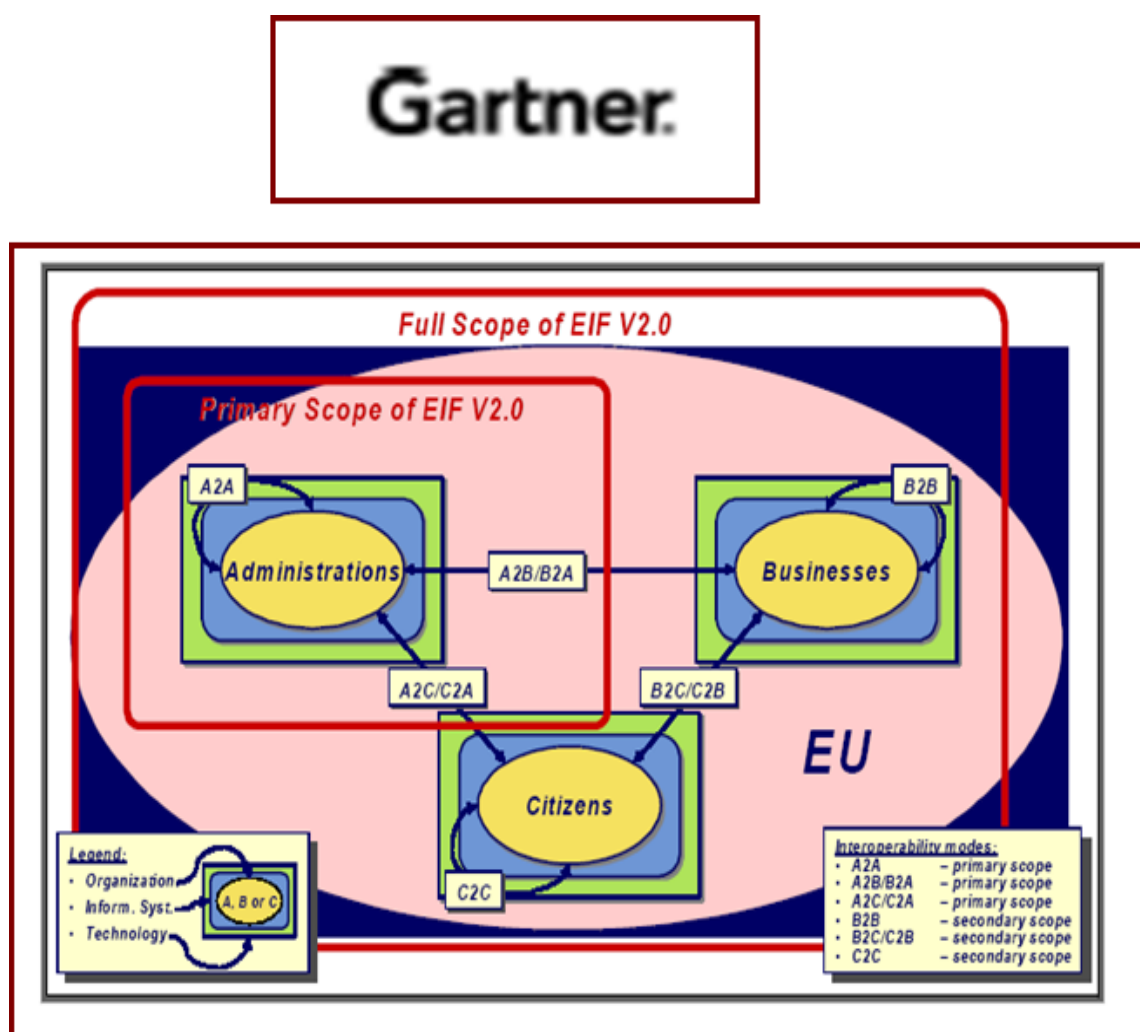
В рамките на програмата MODINIS, бяха определени следните пет различни направления, в които предимствата на оперативно съвместимите ИКТ - системи са очевидни:

- между различните услуги, насочени се към един и същ потребител, а именно „групирани“ услуги (например, според събитията от живота или проблемните сценарии), които икономисват ресурси и подобряват качеството на услугите (правителство „на едно гише“);
- в различните етапи от веригата за добавена стойност на дадена услуги, когато доставчикът на услугата се нуждае от данни, администрирани от други доставчици, и има нужда от обмен на тези данни с тях. При това е необходима оперативна съвместимост между данните и работните процеси в двете организации;

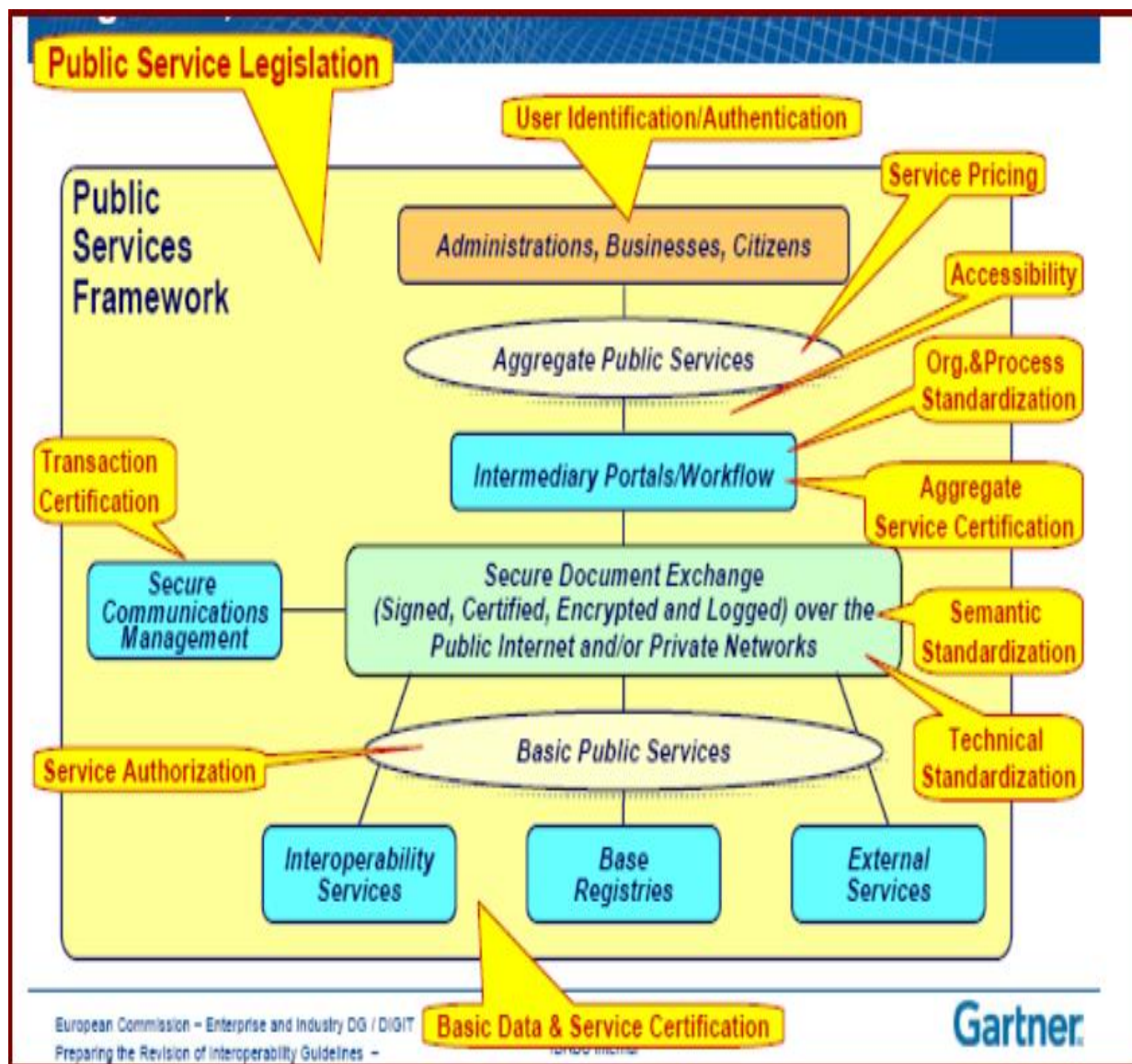
- между отделните агенции в различни географски области, а именно оперативна съвместимост, отнасяща се до прякото прехвърляне на данни от системата на една администрация в системата на друга администрация (главно, пространствени данни);
- между директории на услуги или документи, а именно оперативна съвместимост между местните директории, общи метаданни за услугите, както и алгоритми за намиране на съответния администратор на данните. Този важен въпрос изисква създаването на общи дескриптори за услуги и доставчици;
- допълнителни услуги (управление на идентичността, валидация на подписани електронни документи и т.н.).

Следващата таблица обобщава основните бенефициенти на оперативната съвместимост, както и ползите, които те получават от оперативно съвместимите публични услуги.

Разработка на версия 2,0 на Европейската рамка за оперативна съвместимост



Фигура 2-5



Фигура 2-6

През 2006 г. известната фирма Gartner Group спечели обявения от Европейската комисия търг за усъвършенстване на Европейската рамка за оперативна съвместимост и на Изискванията към архитектурата за пан-Европейски електронни услуги.

В работата на Експертната група взе участие и представител на България.

ГЛАВА 2.2

ЕВРОПЕЙСКИ ИНИЦИАТИВИ

Европейски програми

Европейските програми: IDA (Interchange of Data Between Administrations), IDA II, IDABC (Interoperable Delivery of European e-Government Services to Public Administrations, Business and Citizens) и ISA (Interoperability Solutions for European Public Administrations) представляват верига от последователни усилия, насочени към подобряване на сектора на публичната администрация в Европейския съюз. Съществена част от тези програми е посветена на оперативната съвместимост.

Подобно на тях, програмата ICT PSP (2007-2013) и нейният предшественик eTEN (2000-2006) развиват редица аспекти на е-Правителство и, в частност, на оперативната съвместимост. В техния състав се разработват редица значими пилотни проекти в различни отрасли, като: e-CODEX (e-justice Communication Via Online Data Exchange (2010-2013)), epSOS (European Patients – Smart Open Services (2008-2013)), PEPPOL (Pan-European Public Procurement Online (2008-2012)), SPOCS (Simple Procedures Online For Cross-Border Services (2009-2012)), STORK (Secure Identity Across Borders Linked (2008-2012)).

Друга програма от съществено значение е MODINIS (Monitoring of the e-Europe 2005 action plan, Dissemination of good practices and the improvement of Network and Information Security), която изследва добрите практики на е-Правителство (в т.ч. оперативната съвместимост) в страните-членки на ЕС, и дава практически препоръки за разпространение на положителния опит.

Програмата MODINIS има следните цели:

- да следи за качеството на оперативната съвместимост в рамките на държавите-членки и да я сравнява с най-добрите в света, като се използват, когато е възможно, официални статистически данни;
- да подкрепя усилията на държавите-членки на национално, регионално или местно равнище, като се анализират добри практики и създаване на механизъм за обмен на опит;
- да се анализират икономическите и социалните последици от информационното общество, с оглед улесняване на политическите дискусии, особено по отношение на конкурентоспособността на промишлеността и сближаване, както и по отношение на социалното включване;
- да извършва подготовка за изграждането на бъдещата структура на мрежовата и информационна сигурност на европейско равнище.

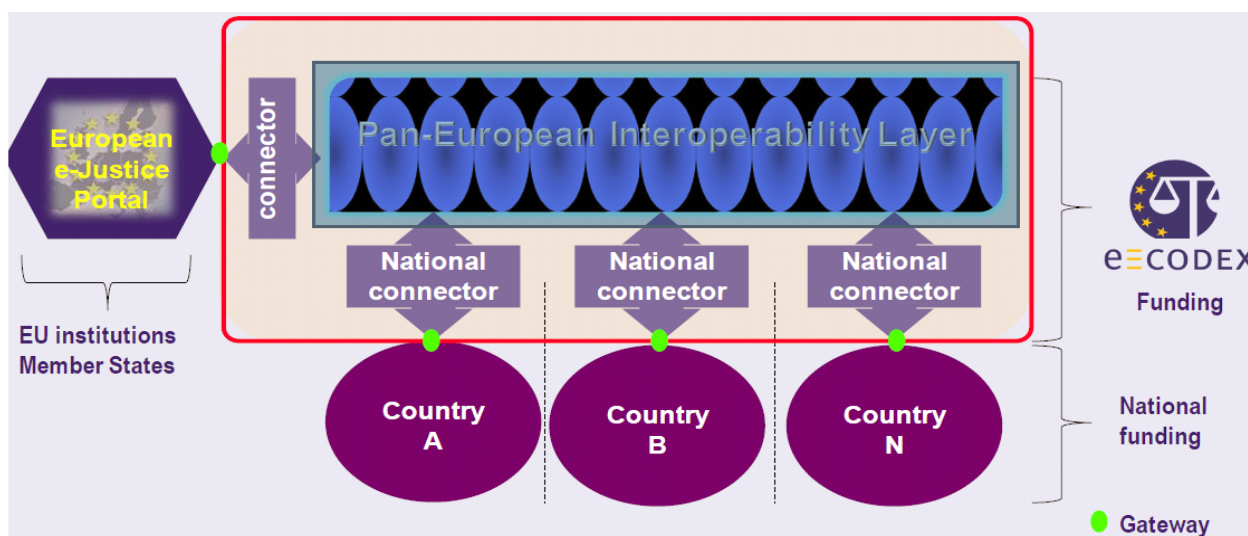
Съдейки по работните програми, може да се види, че всяка година се реализират дейности и действия, свързани с електронното правителство. Резултатите от проекта могат да бъдат групирани в три основни области:

- обмен на опит и примери от практиката;
- местно и регионално проучване на оперативна съвместимост;

- разпространяване и насърчаване на напредъка и на възприемането на оперативна съвместимост.

Програма e-CODEX (e-justice Communication via Online Data EXchange)

Целта на проекта е да се подобри трансграничния достъп на гражданите и бизнеса до съдебните ресурси в Европа, както и да се подобри оперативната съвместимост между съдебните власти в рамките на ЕС. e-CODEX разработва градивни елементи, които могат да бъдат използвани от държавите-членки в подкрепа на трансгранична операция на процесите в областта на правосъдието. Тези решения са в различни области: от безопасно транспортиране на идентичността и правата на управление на достъпа до стандарти за документи. Те следва да създадат безопасна среда за потребителите (вариращи от гражданите и бизнеса до различните юридически професии) да получат достъп до широк спектър от правни услуги в цяла Европа и ще допринесат за създаване на паневропейско ниво за обмен на информация в областта на правосъдието. Една от целите на проекта е да се постигне оперативна съвместимост между съществуващите национални правни системи.



Фигура 2-7

Проект „European patients – smart open services (epSOS)“

epSOS е европейски проект в областта на е-Здравеопазване, третиращ оперативна съвместимост съвместно финансиран от Европейската комисия и партньорите. Той се фокусира върху подобряване на медицинското обслужване на гражданите при престой в чужбина, като предоставя на здравните специалисти необходимите данни за пациенти в сигурен електронен формат. По-специално, epSOS се стреми да предлага безпроблемна здравни грижи за европейските граждани чрез изграждане и оценка на инфраструктурна услуга.

Целта на проекта е да се проектира, изгради и оцени услуга, реализираща трансгранична оперативна съвместимост между системите за електронни здравни досиета в Европа. Тя се концентрира върху разработването на практическа рамка на електронното здравеопазване и ИКТ инфраструктура, която позволява сигурен достъп до болнична информация между различните европейски системи за здравеопазване. От правна и нормативна гледна точка е важно да се отбележи, че epSOS услуги ще се предлагат чрез

пилотен проект. Като пилотен, основната му цел е да се събере информация и доказателства, за да се улесни последващо пълно разгръщане. Мисията на проекта е да се гарантира, че предизвикателствата, които са от решаващо значение за реализацията на ерSOS в реалните житейски ситуации, са надлежно признати и адресирани. Тази работа трябва да подкрепя и насочва страните-участнички в ерSOS в прехвърлянето на тези знания на национално равнище и ще подпомогне по-тясно сътрудничество с органите за защита на данните на всички участващи страни.

Проект „pan-European public procurement online (PEPPOL)“

Проектът PEPPOL се стреми към разширяване на пазарната и оперативна съвместимост между системите за електронни обществени поръчки. Проектът дава достъп до своята базирана на ИТ стандарти транспортната инфраструктура чрез точки за достъп, и предоставя услуги за електронни обществени поръчки със стандартизирани формати за електронни документи (на базата на UBL и CEN / BII). Той се фокусира конкретно върху оперативната съвместимост на електронните обществени поръчки.

PEPPOL не се опитва да осигури интегрирана платформа. Той предлага вместо това модулен набор от ИТ спецификации, както и свързани с отворен код оперативни съвместими софтуерни решения, които всяка организация може лесно да инсталира на своите съществуващи ERP системи, за да си взаимодействат с други системи чрез обмен на специфични бизнес документи. Целта на PEPPOL- решенията е да улеснят трансграничните сделки и да се намалят пречките за малките и средни предприятия.

В сърцето на PEPPOL е електронната транспортна инфраструктура, която позволява на правителствата и компаниите да свържат своите ИТ системи и надеждно да обменят данни и бизнес документи.

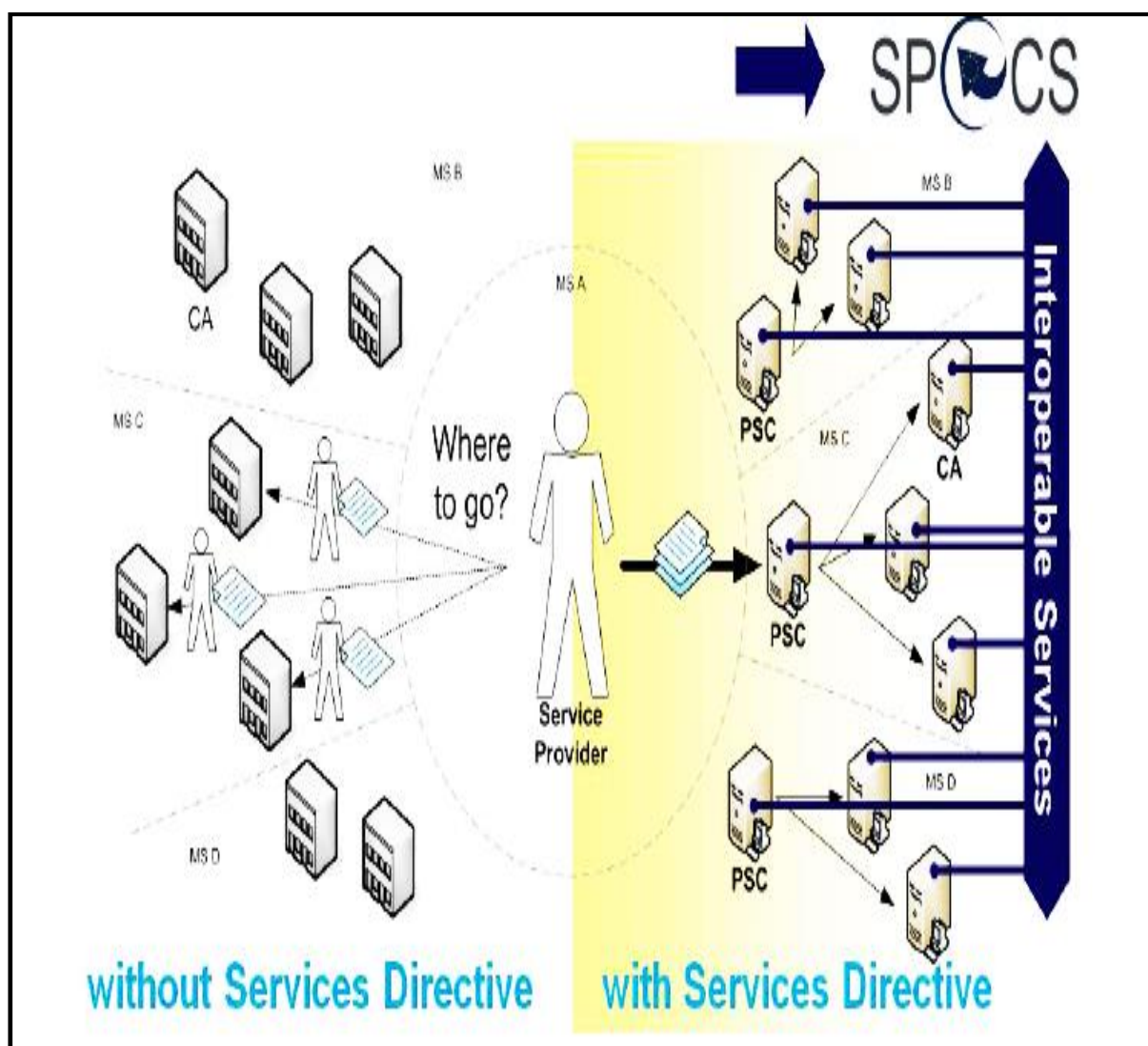
Проект „Simple procedures online for cross-border services (SPOCS)“

Проектът е тясно свързан с Директивата за услугите, която призовава за създаването на единни звена за контакт (ЕЗК). ЕЗК действат като посредници между доставчиците на услуги и националните публични администрации. SPOCS има за цел да изгради следващото поколение на онлайн портали, които всяка европейска държава сега има на разположение, чрез процедури за трансграничен електронен обмен.

Целта на SPOCS е да се разработи слой оперативна съвместимост, за да се насърчи икономиката на услугите в Европа чрез улесняване на доставчиците на услуги. Прилагат се единни звена за контакт. Друга цел е да се покаже, че градивните елементи, разработени в рамките на проекта, съставляващи този слой оперативна съвместимост наистина функционират в реалния живот.

Процесът, следван в рамките на SPOCs, цели да постигне реално изпитване на:

- - Определянето на градивните елементи на SPOCs (синдикация, електронни документи, електронна доставка, e-Safe и електронни услуги);
- - Разработване на градивните елементи на SPOCs въз основа на техните спецификации;
- - Разполагане и пилотни изпитания на елементите в страните-участнички в SPOCs;
- - Оценка на резултатите и итеративно адаптиране на спецификациите и модулите, както е необходимо;
- - Мащабиране и съхранение на градивните елементи на SPOCs.



Фигура 2-8



Фигура 2-9

Проект „Secure identity across borders linked (STORK)“

Целта на проекта STORK е да създаде оперативно съвместима платформа за електронна самоличност, която ще даде възможност на гражданите да създават нови електронни връзки зад граница, само като представят своята национална електронна самоличност. Трансграничното удостоверяване на потребителя за такива електронни отношения са приложени и изпитани от проекта с помощта на пет пилотни под-проекти, които използват съществуващите правителствени служби в страните-членки на ЕС.

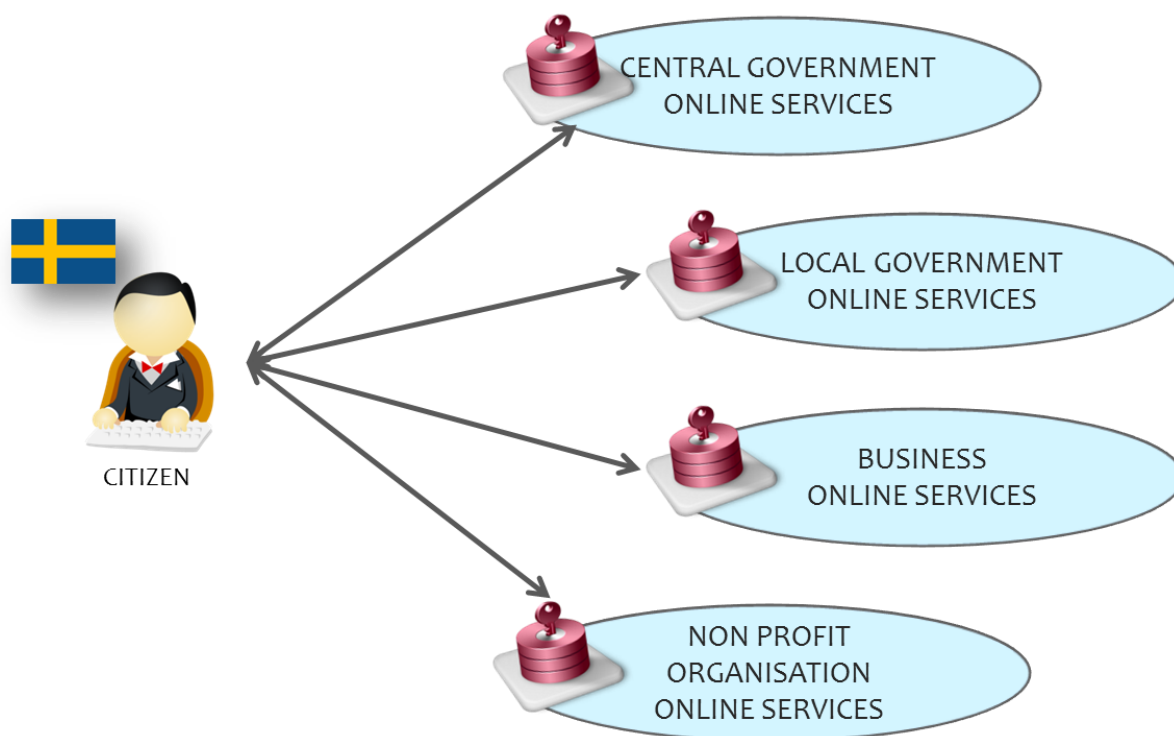
Проектът STORK ще направи по-лесен достъп до онлайн обществени услуги през граница за гражданите и бизнеса чрез разработване и изпитване на общи спецификации за взаимно признаване на националната електронна самоличност между страните-участнички.

Това се реализира чрез:

- разработване на общи правила и спецификации за подпомагане на взаимното признаване на електронни самоличности отвъд националните граници;
- тестване в реалния живот на среди за сигурни и лесни за използване решения за електронна самоличност за гражданите и бизнеса;
- взаимодействие с други инициативи на ЕС, за да бъдат услугите за електронна самоличност максимално полезни.

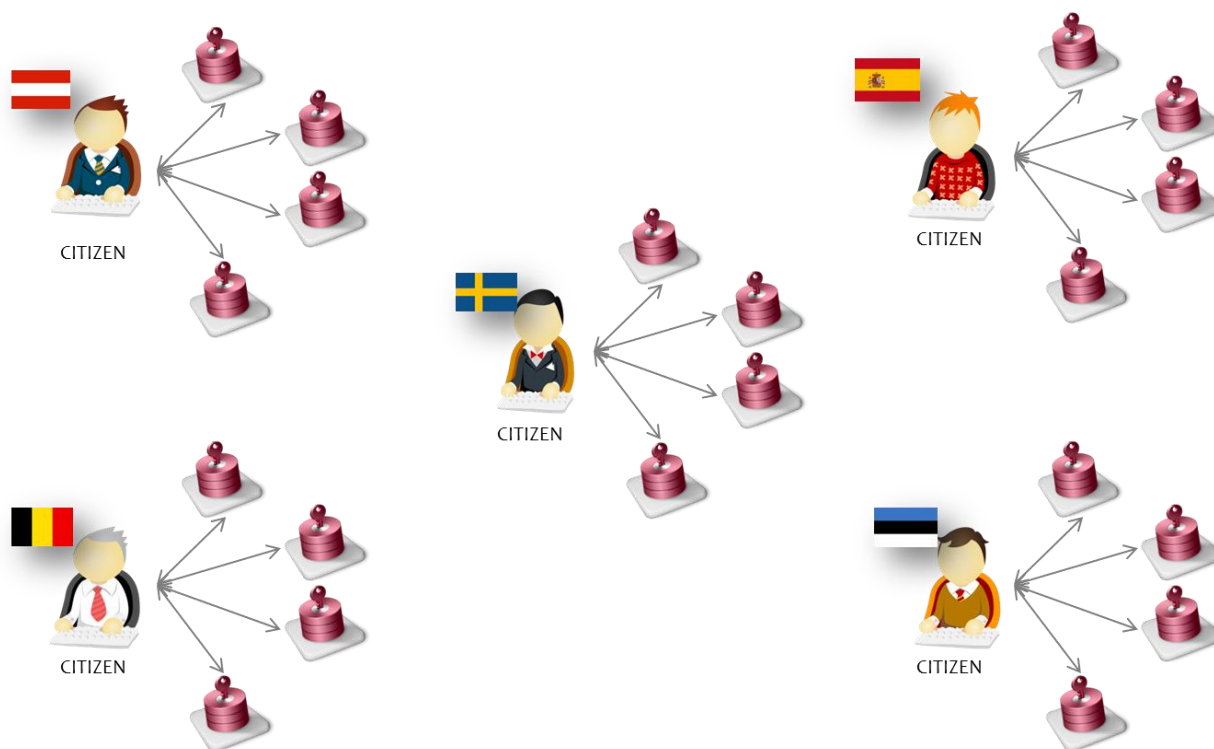
STORK се фокусира върху прагматични решения за оперативна съвместимост на електронната самоличност, върху изпълнението на няколко пилотни трансгранични услуги за електронна самоличност, избрани въз основа на тяхното високо въздействие върху всекидневния живот.

Национални „он-лайн“ услуги с Eid



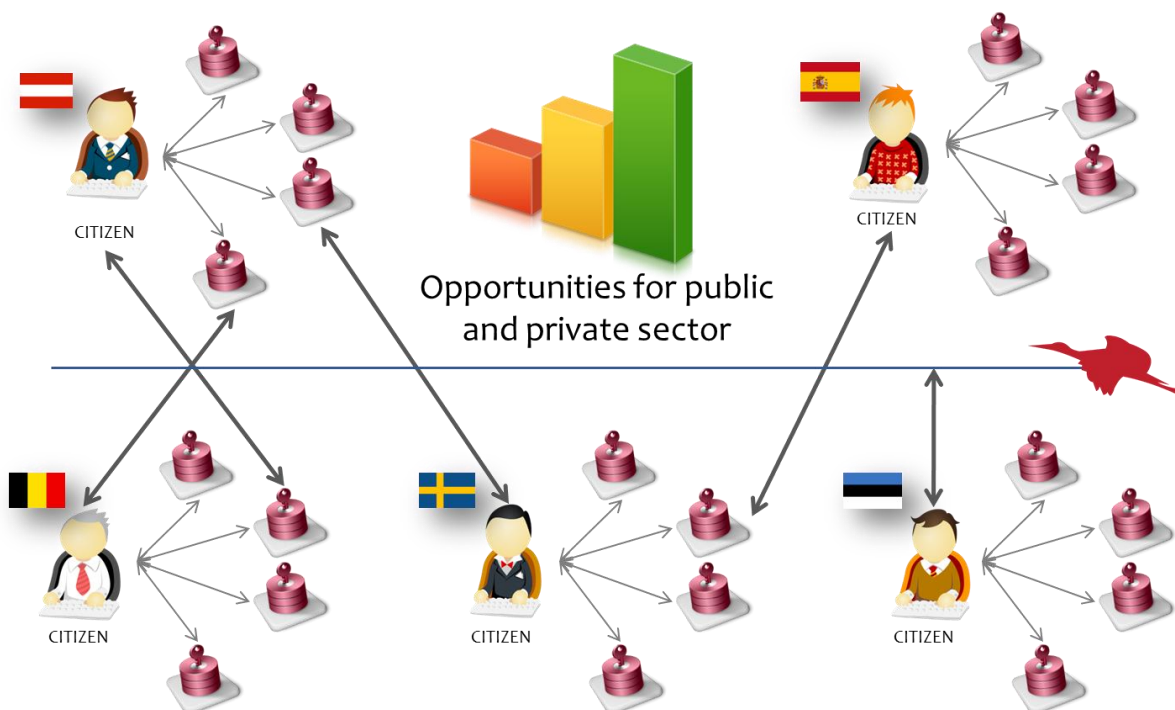
Фигура 2-10

Множество национални eID инфраструктури



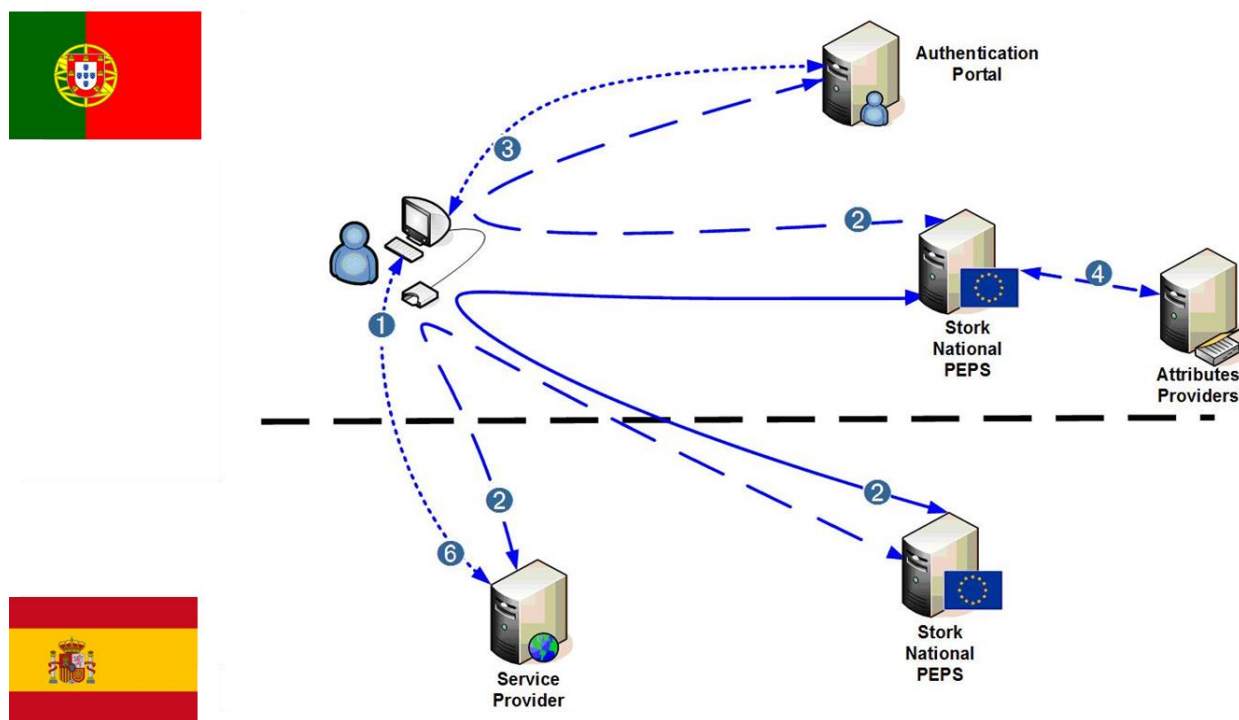
Фигура 2-11

Възможност за транс-гранични е-Услуги



Фигура 2-12

STORK: Комуникационна структура



Фигура 2-13



Фигура 2-14

ГЛАВА 2.3

БЪЛГАРСКОТО РАЗВИТИЕ

Малко история



1. През м. юли 2004 година група ентузиасты, организирани от КЦИКУТ, представиха за обществено обсъждане документа “Основни принципи за постигане на оперативна съвместимост на информационните системи в състава на е-Правителство”.

2. С любезното съдействие на Майкрософт България работната група на два пъти беше консултирана от водещия експерт Стивън Мак-Гибън, който оцени високо разработката

3. В края на 2004 г. Европейската комисия публикува “Европейската рамка за оперативна съвместимост за пан-Европейски услуги на е-Правителство” версия 1,0

4. На база на Европейската рамка работната група подложи на преработка горепосочения документ и през м. юни 2005 г. внесе в Министерския съвет “Българска национална рамка за оперативна съвместимост на информационните системи в изпълнителната власт”

5. Поради смяната на Правителството процесът на приемане се забави, проектът беше внесен отново от Министъра на държавната администрация и административната реформа

6. На 28 юни 2006 г. Министерският съвет прие с Решение № 482 Българската национална рамка за оперативна съвместимост

7. До края на м. ноември 2006 г. Министърът на държавната администрация и административната реформа и Председателят на Държавната агенция за информационни технологии и съобщения утвърдиха четирите инструкции, съпровождащи и конкретизиращи Националната рамка

8. В същото време Министърът на държавната администрация и административната реформа със съдействието на Държавната агенция за информационни технологии и съобщения внесе в Министерския съвет проект на Закон за електронното управление

9. Законът беше приет от Народното събрание и публикуван в “Държавен вестник” на 12 юли 2007 година, влезе в сила на 12 юли 2008 г.

10. Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност беше приета от Министерския съвет и публикуван в “Държавен вестник” на 25 ноември 2008 г.

Виж Приложение 1.

Българската национална рамка

В основата на Националната рамка е заложен подход, съчетаващ: а) класическия Реферативен модел на отворения разпределен процесинг (стандарт ISO/IEC 1076 / 1998 г.,

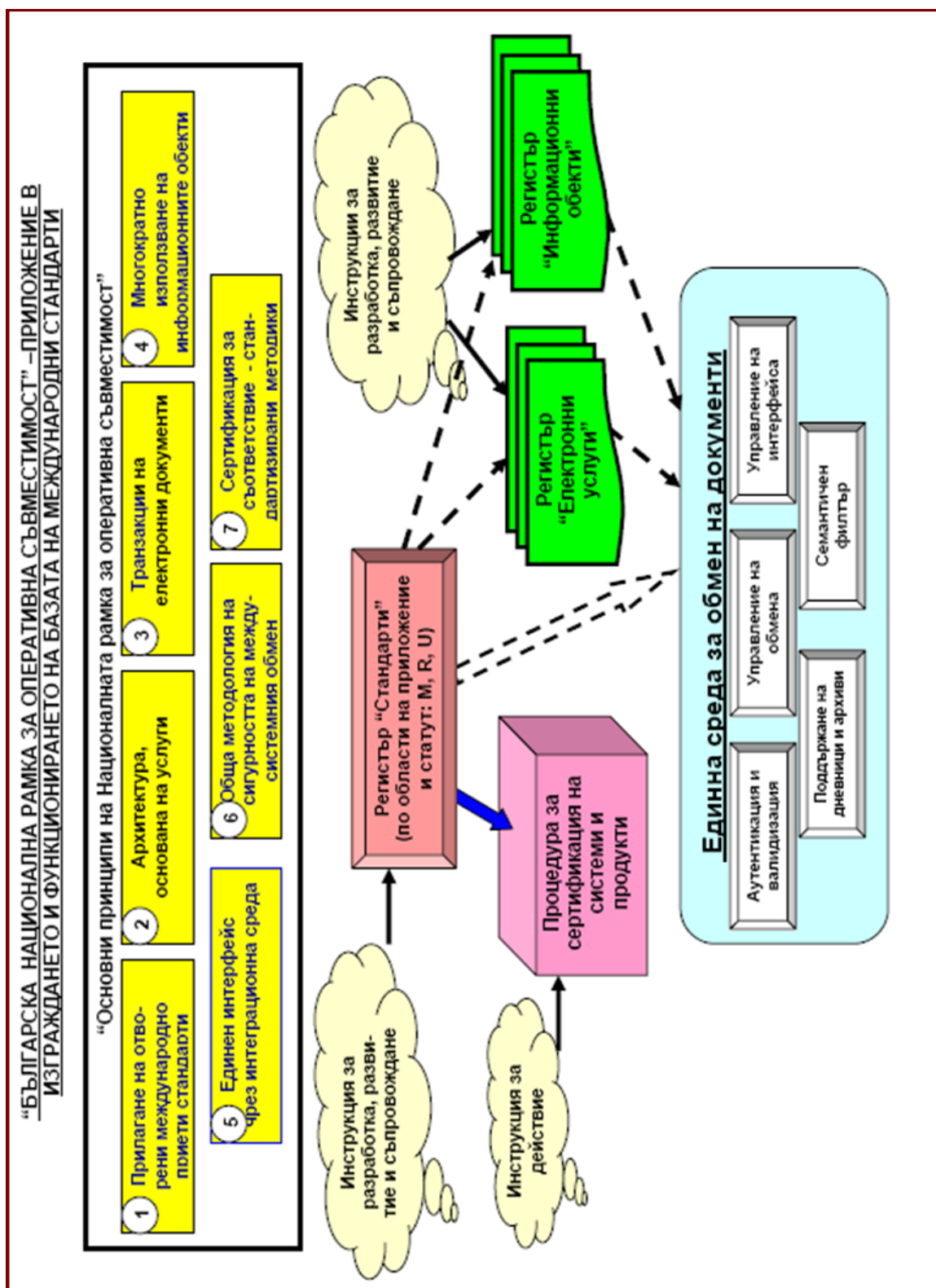


Фигура 2-15

който дефинира инфраструктурата за реализация на разпределени процеси за обработка на информация между хетерогенни технологични ресурси и многочислени организационни домейни; б) последното ниво в еволюцията на стандартите за системна интеграция – т.н “Архитектура, ориентирана към услуги (SOA) ”.

Стандартизацията на Електронното правителство в областта на системната интеграция и оперативна съвместимост обхваща по-широка област от тази на т.н. “формални хармонизирани стандарти”, утвърждавани от официалните между-правителствени стандартизационни органи (като ISO, ITU на глобално ниво или CEN, CENELEC, ETSI – на европейско ниво). Тя включва също така неформални и хибридни стандартизационни процеси - продукцията на секторни консорциуми, като: OASIS, IETF, W3Consortium, UN/CEFACT, OMG и др.

Обща схема на действието на Националната рамка за оперативна съвместимост



Фигура 2-16

ЧАСТ 3

ОПЕРАТИВНА СЪВМЕСТИМОСТ НА Е-ПРАВИТЕЛСТВО СЪГЛАСНО ЗАКОНА ЗА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ И НАРЕДБИТЕ КЪМ НЕГО

ГЛАВА 3.1

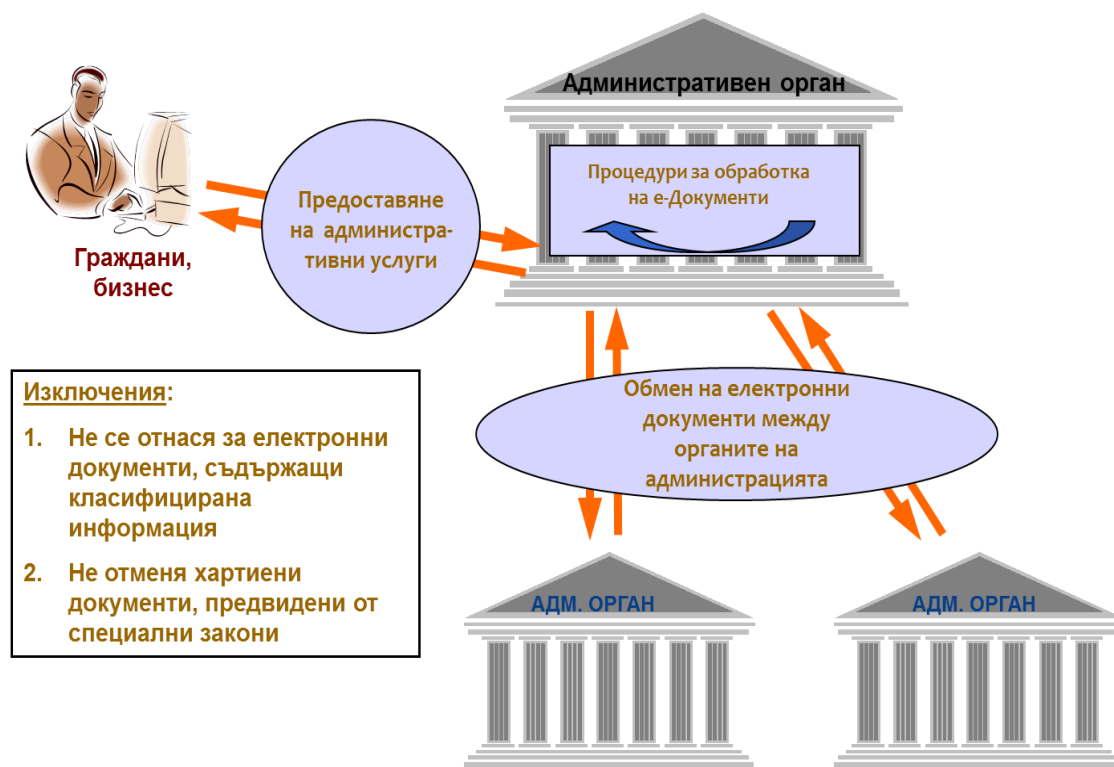
ЗАКОН ЗА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

Законът за електронното управление, приет на 12.06.2007 г. и влязъл в сила след едногодишен подготвителен период, урежда дейността на административните органи при работа с електронни документи, предоставянето на административни услуги по електронен път и обмена на електронни документи между административните органи.

В глава четвърта “Оперативна съвместимост и информационна сигурност” Законът ясно регламентира изискванията за постигане на оперативна съвместимост в информационни системи на административните органи.

В същата глава Законът посочва държавния орган, отговорен за разработването и провеждането на политиката в областта на оперативната съвместимост, включително за упражняването на контрол – Министерството на транспорта, информационните технологии и съобщенията.

Сфера на действие на Закона за електронно управление



Фигура 3-1

Защо е това особено внимание към оперативната съвместимост?

За разлика от преобладаващата понастоящем практика на автономно развитие на информационните системи във всяка отделна администрация, изискването на Закона за еднократно въвеждане на данни от гражданите и фирмите предизвиква необходимост от интензивен информационен обмен между административните системи.

В общия случай, всяка електронна административна услуга изисква такъв обмен и необходимостта от оперативна съвместимост за целите на този обмен е очевидна.

Предстоящото включване на българската администрация в системите за пан-Европейски транс-гранични електронни услуги също е свързано с тези условия.

Затова Законът и наредбите към него предвиждат изисквания и мерки за постигането им.

Определение

Съгласно т. 13 от Допълнителните разпоредби към Закона за електронното управление „Оперативна съвместимост” е “способността на информационните системи да обработват, съхраняват и обменят електронни документи и данни помежду си, използвайки единни технологични стандарти и процеси”.

Състав на оперативната съвместимост

Съгласно Препоръка № 3 на Европейската рамка за оперативна съвместимост, последната съдържа три аспекта:

- технически – позволяващ обмен между приложните системи в различни компютри;
- семантичен – осигуряващ едно и също смислово съдържание на обменяните данни;
- организационен – създаващ организация по управление на процесите за обмен и обработка на данните между различни организационни структури.

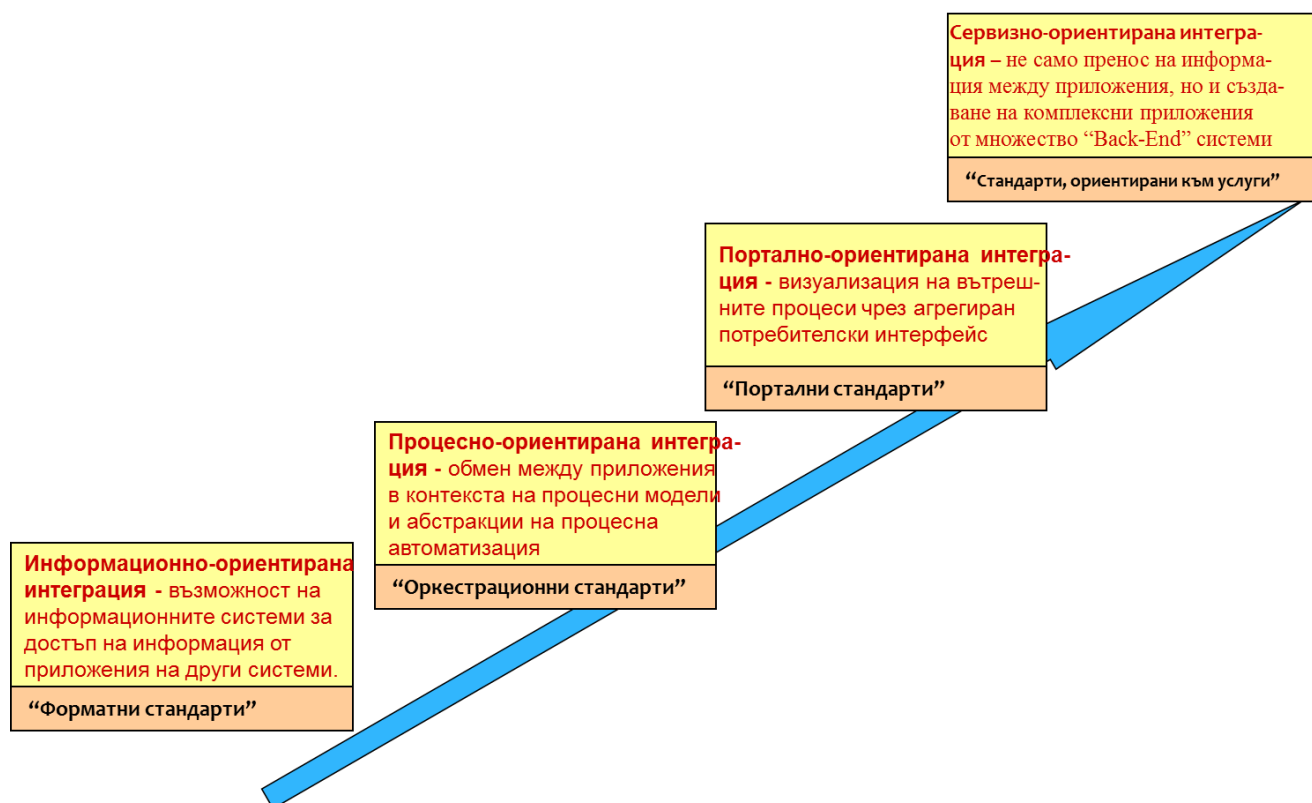
При това техническата оперативна съвместимост се разпространява върху:

- методите за представяне на данните;
- методите на достъп;
- методите за интеграция на данните;
- архитектурите за разпределени приложения;
- протоколите за обмен на съобщения и файлове;
- мрежовите услуги;
- услугите по сигурността на обмена и съхраняването на съобщенията.

Семантичната оперативна съвместимост се основава на специфични информационни ресурси от два типа:

- ресурси, осигуряващи морфологична съвместимост (номенклатури, тезауруси, онтологии и пр.);
- ресурси, осигуряващи синтактична съвместимост (XML-схеми, модели и схеми на мета-данни и пр.)

Еволюцията на стандартизационния процес следва стъпките на еволюцията на системната интеграция



Фигура 3-2

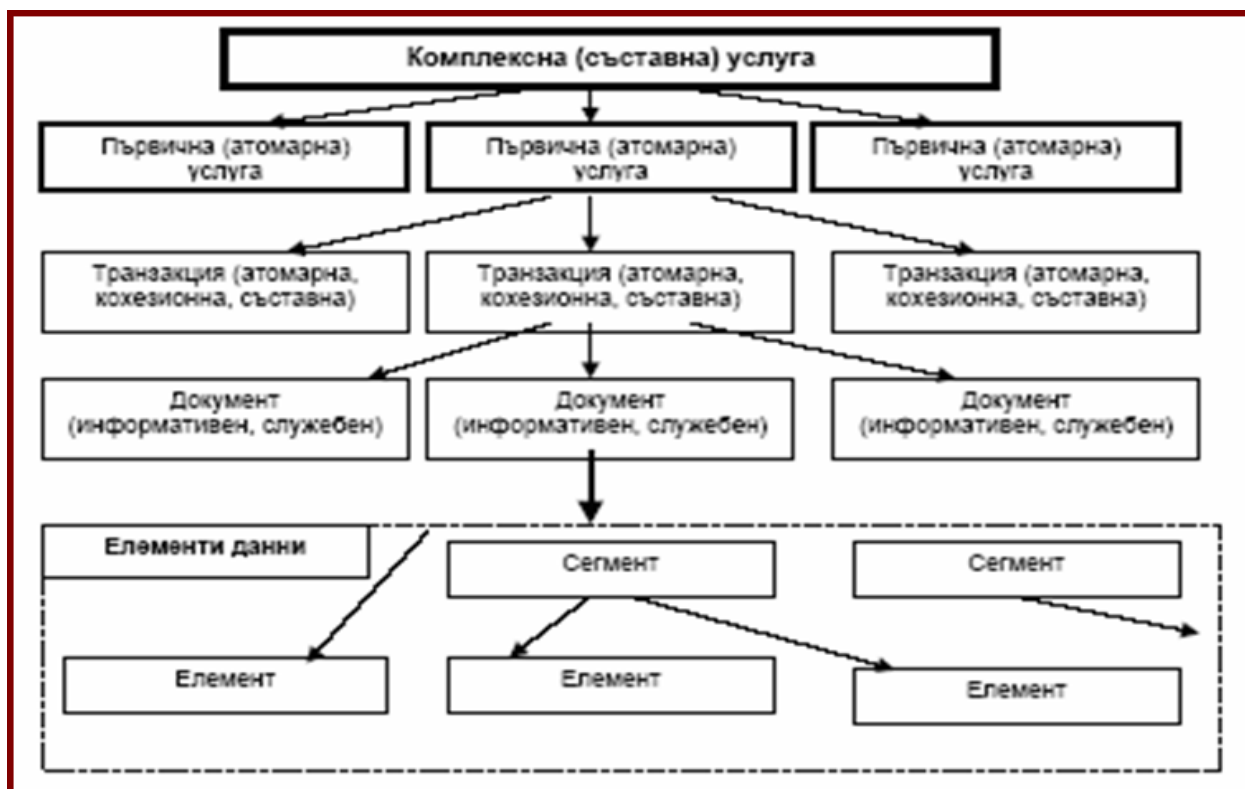
Същност на архитектурата, ориентирана към услуги

Всички функции се интерпретират като независими услуги с добре дефинирани извикваеми интерфейси, които могат да бъдат инициирани в последователност, оформяща определени процеси.

Основни особености:

- а) всички функции (собствено услуги, транзакции, системни услуги и пр.) се дефинират като е-Услуги;
- б) услугите работят като "черни кутии", при което външните компоненти знаят само очаквания резултат;
- в) извикваемият интерфейс не зависи от това дали е локален (вътре в системата) или отдалечен, каква

интерконектна схема или протокол предизвикват извикването, какви инфраструктурни компоненти са необходими за създаване на конкретната връзка.

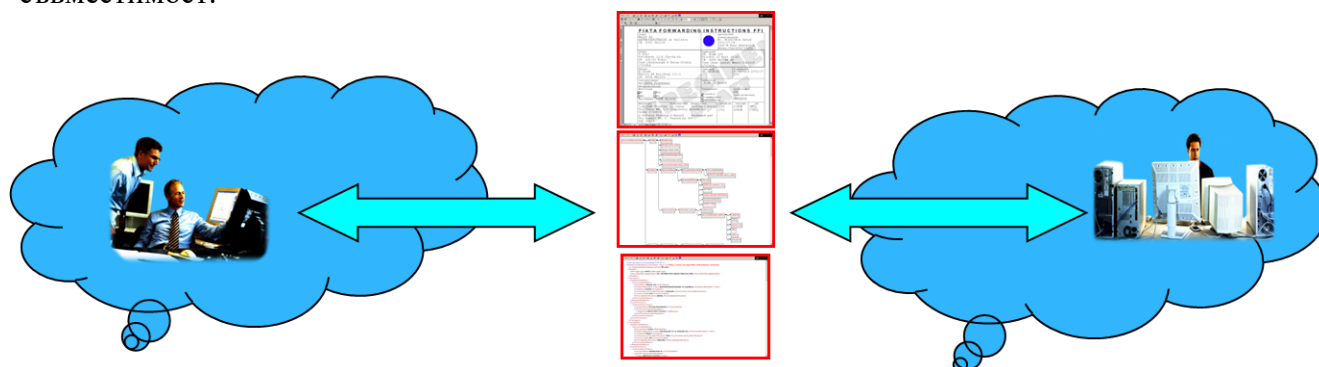


Фигура 3-3

Пасивна оперативна съвместимост

В някои приложения, основно базирани на стандартите от групата eBXML, се изхожда от предположението, че агенти от различни хетерогенни среди могат да постигнат оперативна съвместимост, като обменят стандартизирани съобщения чрез унифицирана технология за обмен. Това се дефинира като “Пасивна оперативна съвместимост”.

Практическите резултати, обаче, показват, че това е недостатъчно да бъдат покрити изискванията особено на семантичната и организационната съставляващи на оперативната съвместимост.



Фигура 3-4

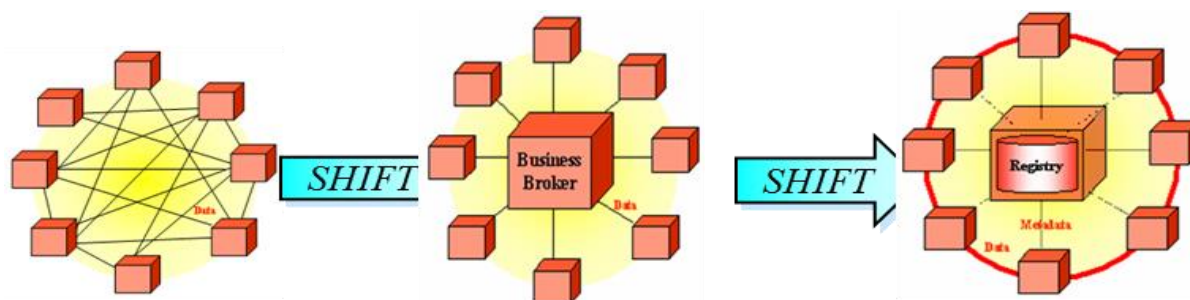
Полу-активна оперативна съвместимост

По-висока степен на оперативна съвместимост е т.н. “Полу-активна или регистрова оперативна съвместимост”.

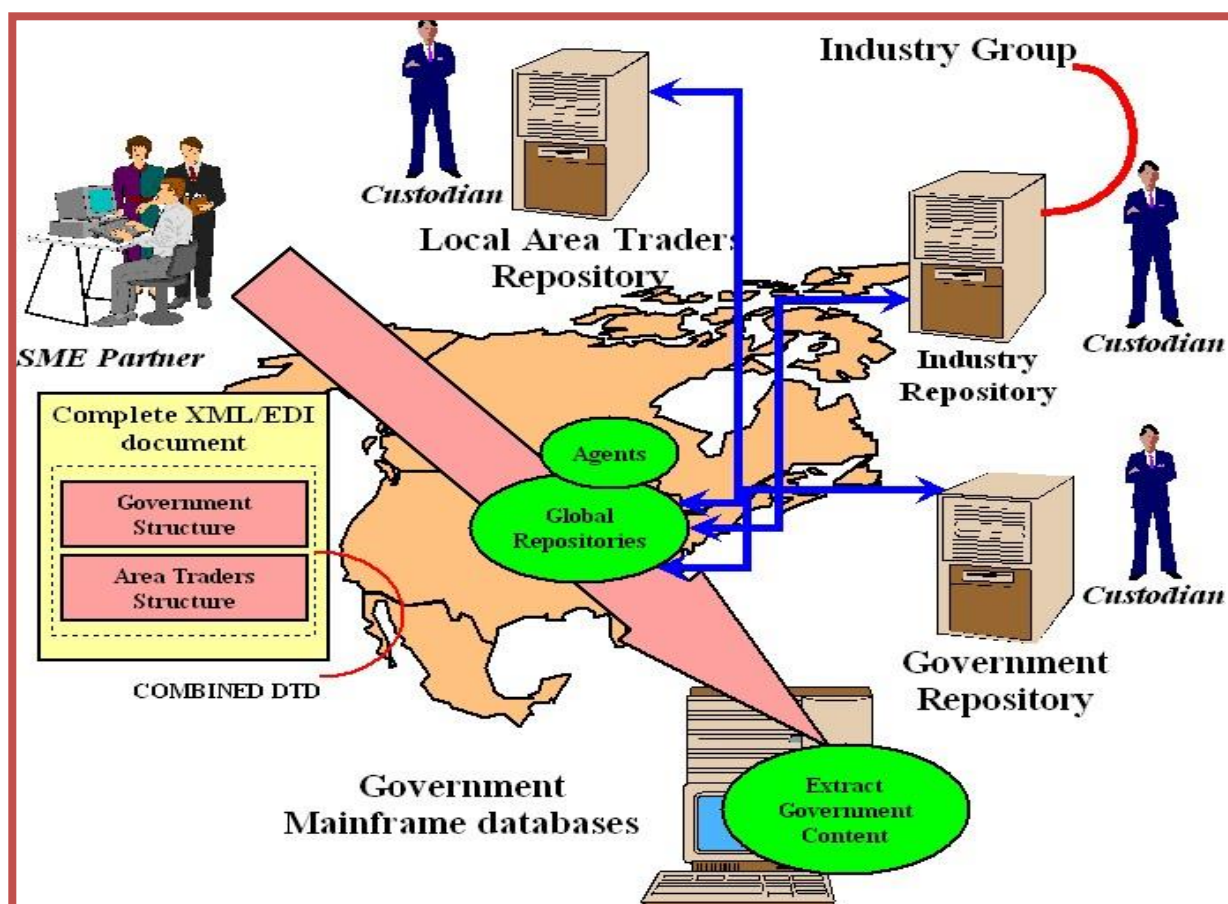
Съвременната стандартизационна концепция е “регистрово-ориентирана”.

В случая с “Българската национална рамка” това се постига чрез създаване и поддържане на :

1. Регистър на стандартите с четири класификационни схеми
2. Регистър на информационните обекти, включващ XML-, UML- и графично описание на структурите от електронни документи, сегменти и елементи
3. Регистър на електронните услуги, включващ XML- и графично описание на структурите на услугите, BPEL-описание на извикването им и точката на достъп и пр.



Фигура 3-5



Фигура 3-6

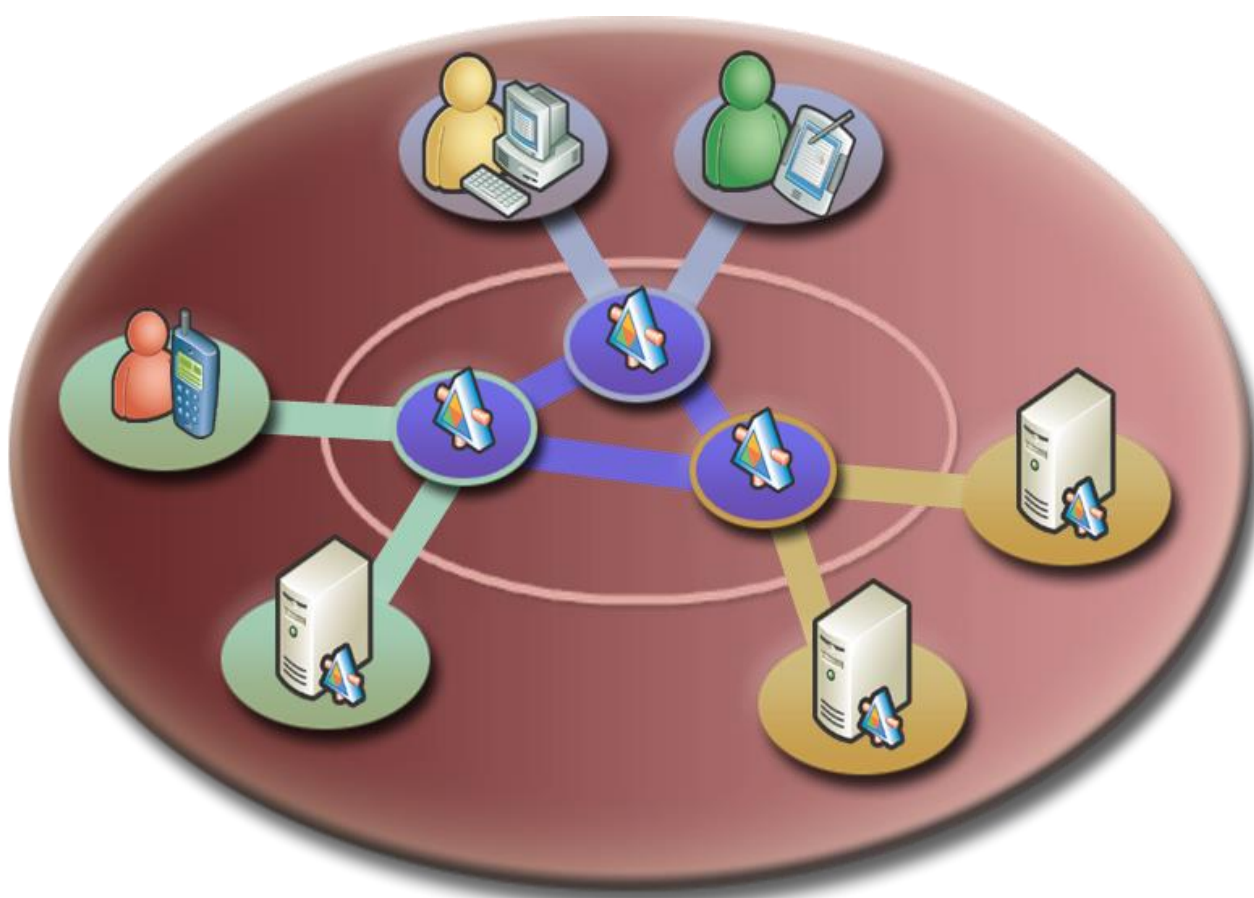
Активна оперативна съвместимост

Този подход се базира на следните препоръки от “Европейската рамка за оперативна съвместимост”:

- препоръка No 3, дефинираща трите аспекта на оперативната съвместимост;
- препоръка No 5, дефинираща необходимостта от подходящи “Business Interoperability Interfaces (BII)”.

От технологична гледна точка, “Активната оперативна съвместимост” предполага, че агенти от различни хетерогенни среди могат да постигнат оперативна съвместимост чрез посредничеството на хомогенна среда с вътрешен стандартизиран обмен.

Практически това се реализира чрез централизираните общосистемни решения, наричани обобщено “Единна среда за обмен на електронни документи (ЕСОЕД)”



Фигура 3-7

Основни особености на българския подход

1. Обхваща първите два етапа от Европейската “пътна карта”.
2. Базира се на “архитектура, ориентирана към услуги”.
3. Създава регистрово-базирана мета-среда.
4. Реализира “активна” съвместимост чрез хомогенна среда за обмен между слабо свързани хетерогенни системи.

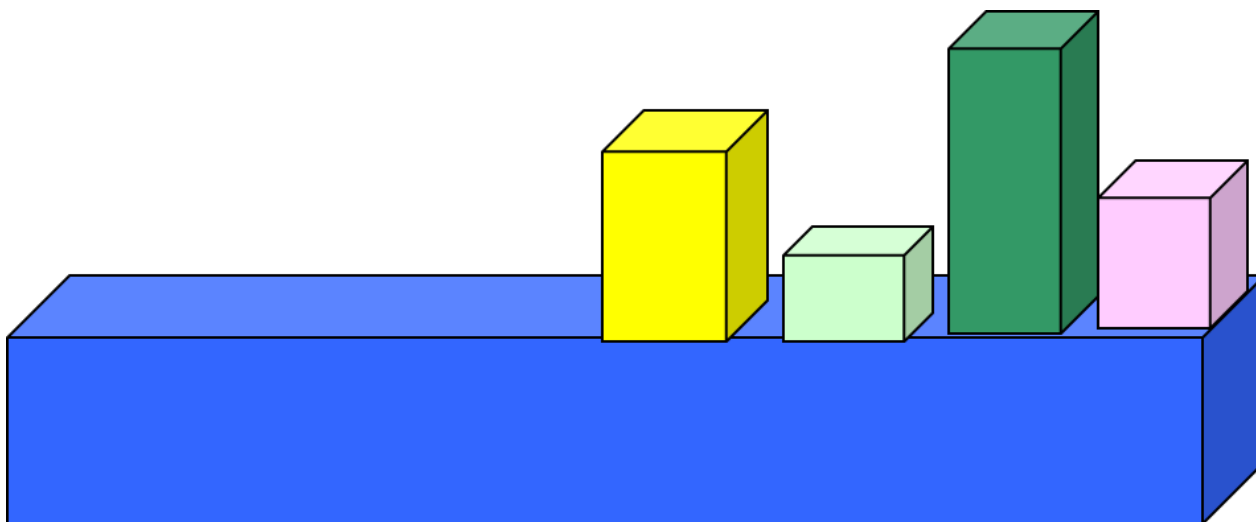
5. Предвижда задължителна оценка на съответствието (преди, сертификация от акредитирани органи)

Вертикални съставляващи на оперативната съвместимост

Всяка вертикална (или секторна) оперативна съвместимост се разглежда като надстройка над общата (или хоризонтална) оперативна съвместимост, представена чрез Националната рамка.

Примери:

- в е-Здравеопазване – стандартите, разработвани от CEN/TC 251, ISO/TC 215, HL7, DICOM и IEEE;
- в е-Банкиране - стандартите, разработвани от SWIFT, FIX, ISO 15022;
- в е-Образование - стандартите, разработвани от ADL (SCORM), IEEE-LTSC (LOM) и пр.



Фигура 3-8

Наредба за общите изисквания за оперативна съвместимост и информационна сигурност

Наредбата е разработена в изпълнение на чл. 43 ал. 2 от Закона за електронното управление. Законът задължава административните органи и лицата, изпълняващи публични функции, да използват единни стандарти и правила, установяващи технологични и функционални параметри, които се поддържат от информационните им системи за постигане на оперативна съвместимост и информационна сигурност.

Наредбата е разработена с отчитане на всички постановки на Българската национална рамка за оперативна съвместимост на информационните системи в изпълнителната власт, приета с решение на Министерския съвет № 482 от 28 юни 2006 година, на Европейската рамка за оперативна съвместимост, Комюнике COM (2006) 45 от 16 февруари 2006 година на Европейската комисия, озаглавено „Оперативна съвместимост на пан-Европейските услуги на Електронното правителство”, Комюнике COM (2006) 251 на Европейската комисия, озаглавено „Стратегия за сигурно информационно общество – диалог, партньорство и разширение на възможностите”, както и други европейски и международни препоръки, стандарти и добри практики.

Напълно контролируема оперативна съвместимост

За разлика от Националната рамка за оперативна съвместимост, която има действително “рамков” характер, Наредбата за оперативна съвместимост и информационна сигурност въвежда слой от изисквания, подлежащи на еднозначна обективна проверка и залегнали в процедурите за сертификация на информационните системи и продуктите.

Изпълнението на тези изисквания се обективизира и вследствие на функционирането на системите от т.н. “мета-ниво” на е-Правителство:

- Единната среда за обмен на електронни документи (ЕСОЕД) и
- шестте регистъра, съставлящи “Националния модел на данните в администрацията”.

Слой от директивни изисквания

Освен споменатите изисквания, които са включени в процедурите за сертификация, наредбите дефинират и редица изисквания, които подлежат на субективен контрол. Такъв характер има и Регистъра на стандартите.

Пример за подобни изисквания са тези за:

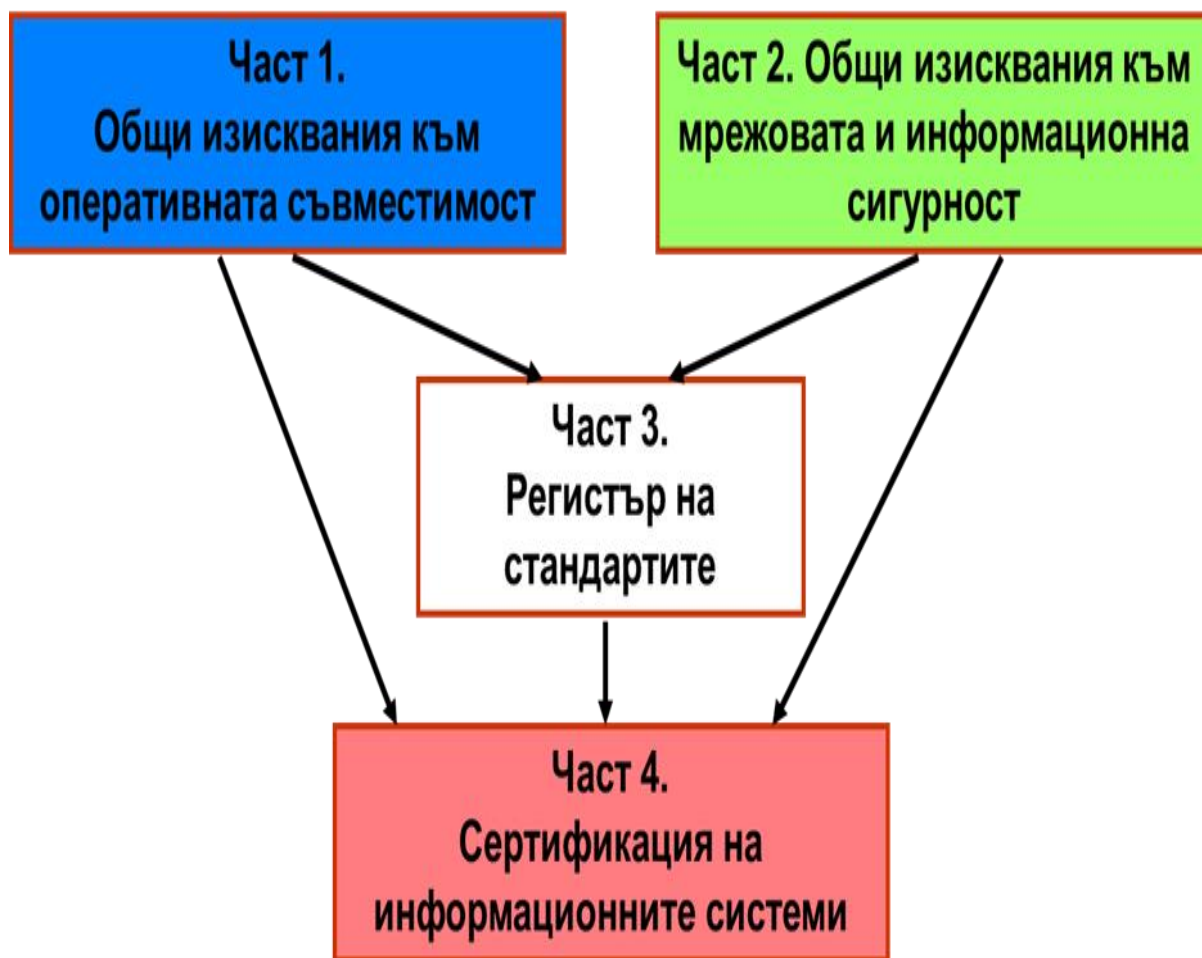
- достъпността и използваемостта на потребителския интерфейс от Наредбата за е-Услуги;
- начините за подаване на е-Документи към доставчика на е-Услуги и обратното изпращане на е-Документи към получателя на услугата;
- създаването на вътрешни правила за мрежова и информационна сигурност в административните органи и т.н.

Контрол на изпълнението на изискванията

Както е посочено в Наредбата “Гаранцията за спазването на изискванията за оперативна съвместимост и мрежова и информационна сигурност се осъществява чрез:

1. Оценка на съответствието (преди, сертификация) на информационните системи и продукти в съответствие с глава шеста от наредбата;
2. Функционалността на единната среда за обмен на документи (ЕСОД), която допуска обмен само на видове документи, вписани в регистъра на информационните обекти;
3. Сертификация и одит на администрациите по отношение на система за управление на информационната сигурност в съответствие с международния стандарт ISO 27001:2005;
4. Контрол от страна на Министъра на ТИТС, в изпълнение на чл. 60 от Закона за електронното управление и в съответствие с утвърдена от него Методика за текущ контрол на оперативна съвместимост и мрежова и информационна сигурност.”

Структура на Наредбата



Фигура 3-9

ГЛАВА 3.2

ОПЕРАТИВНА СЪВМЕСТИМОСТ

Тази част от Наредбата включва следните раздели:

1. Изисквания за свързаност (Interconnectivity) между информационните системи на административните органи;
2. Изисквания по отношение на данните;
3. Изисквания по отношение на електронните документи;
4. Изисквания по отношение на приложенията за визуализация/редактиране на електронни документи;
5. Изисквания към административните информационни системи.

Раздел 1. Изисквания за свързаност между информационните системи

Изискванията за свързаност между информационните системи на администрациите регламентират основната среда за връзка между системите (Единната среда за обмен на електронни документи (ЕСОЕД), изградена съгласно чл. 41 от Закона за електронното управление).

Раздел 2. Изисквания по отношение на данните

Изискванията за оперативна съвместимост по отношение на представянето и употребата на данните, преди всичко, фиксират необходимостта от използване само на унифицирани описания на данните.

Администрациите трябва да използват в своята дейност само унифицирани описания на данни, регистрирани в съответните раздели на регистъра на регистрите и данните, в съответствие с чл. 8 от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите, приета с Постановление № 101 на Министерския съвет от 2008 г. (обн., ДВ, бр. 48 от 2008 г.).

Еднократното въвеждане на данните и тяхното многократно използване, както и семантичната оперативна съвместимост между различните приложения в административните информационни системи се осигуряват чрез задължителното използване на Регистъра на информационните обекти.

Оперативна съвместимост на управлението на съдържанието

Под оперативна съвместимост на управлението на съдържанието се подразбира възможността за споделяне на съдържание между организации, опериращи с различни продукти за управление на съдържание.

Под управление на съдържанието се разбира процесът на събиране, управление и публикуване на информация в целеви публикации.

При това управляваното съдържание се състои от записи и файлове, съдържащи съдържателни компоненти, административни данни и мета-данни.

Раздел 3. Изисквания по отношение на електронните документи

Формализираните електронни документи, обменяни между администрациите и издавани от тях към други лица и организации трябва да бъдат с организация на данните в тях, съответстваща на вписаната в регистъра на информационните обекти.

Електронните документи трябва да съдържат валидни данни, съгласно вписаните изисквания за това в регистъра на информационните обекти.

Раздел 4. Изисквания по отношение на приложения за визуализация и / или редактиране на електронните документи

Изискванията за оперативна съвместимост по отношение на електронните документи и на приложения за визуализация и редактиране на електронни документи осигуряват т.н. „оперативна съвместимост, ориентирана към хората”, т.е. изображенията на електронните документи, предназначени за човешко възприемане, възпроизведени от информационните системи на всички участващи в обмена организации, да бъдат идентични.

Приложенията трябва да бъдат сертифицирани за съответствие с изискванията за оперативна съвместимост и информационна сигурност. Тези приложения, за които успешно е приключила процедура по сертификация, се вписват в списъка на сертифицираните информационни системи.

Приложенията, осигуряващи само визуализация на електронни документи трябва да визуализират съдържанието им като:

- . съдържанието на всички данни се визуализира съгласно указанията, вписани при тяхната регистрация в регистъра на информационните обекти;
- за всички данни се визуализира наименованието, с което те са вписани в регистъра на информационните обекти;
- за всички данни е осигурен достъп до текста на тяхното определение, с който те са вписани в регистъра на информационните обекти чрез подходящ интерфейс;
- за всички данни е осигурена индикация за наименованието на грешка съгласно тяхната регистрация в регистъра на информационните обекти, ако проверката за тяхната валидност е неуспешна;
- за всяка установена грешка е осигурен достъп до текста на нейното определение, с който тя е вписана в регистъра на информационните обекти чрез подходящ интерфейс.

Приложенията, осигуряващи редактиране на електронни документи, освен функциите по визуализация на съдържание на електронен документ, трябва да съдържат и функции за:

- запис и четене на файлово съдържание на електронен документ в и от средата на файлова система, намираща се пряко под контрол на потребителя на приложението за редактиране, включително разположена върху преносим физически носител;

- въвеждане, коригиране и изтриване на стойност за всички данни в електронен документ.;

Приложенията, трябва да осигуряват възможност за установяване на несъответствия в съдържанието на визуализиран или редактиран документ с регистрацията му в регистъра на информационните обекти. Те трябва да сигнализират за установените несъответствия чрез визуализация на съответната грешка, съгласно регистрацията на документа в регистъра на информационните обекти. Освен това, те трябва да позволяват извеждането на грешките по ал. 2 в съдържанието на документ от вида „Регистрирани грешки в съдържание на документ”, генериран от приложението.

Раздел 5. Изисквания по отношение на информационните системи

Тези изисквания се отнасят за административните информационни системи, съгласно чл. 4 и следващите от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите.

Освен това те засягат и специализираните информационни системи, осигуряващи изцяло или частично функциите на административна информационна система, доколкото създават електронни документи, регламентирани в горепосочената наредба.

При автоматично създаване на електронни документи от информационна система проверка за изпълнение на изискванията на раздел 3 се извършва по време на създаването. При неуспешна проверка, създаването се прекратява и за това се уведомява служителя, осъществяващ функции по обработка в неавтоматизиран режим или контролиращ автоматичното изпълнение на етап от услуга или процедура, при което се извършва създаването на документа.

Тази проверка се извършва от оценено за съответствие (преди, сертифицирано) приложение за проверка съвместимост на електронни документи, интегрирано в информационната система. Наличието на такова приложение е задължителна предпоставка за оценката на съответствие на информационната система.

Други изискванията за оперативна съвместимост по отношение на информационните системи засягат:

А. Възможностите за преносимост на всички съдържатели се в тях данни в случаи на непредвидени обстоятелства, при което данните се извеждат от тях в съдържанието на електронен документ от вида „Данни за пренос между информационни системи” и могат да се въвеждат в друга административна информационна система;

Б. Визуализацията на поддържаните от тях данни, като:

а) съдържанието на всяка данна се визуализира съгласно указанията, вписани при нейната регистрация в регистъра на информационните обекти;

б) за всяка данна се визуализира наименованието, с което тя е вписана в регистъра на информационните обекти;

в) за всяка данна е осигурен достъп до текста на нейното определение, с който тя е вписана в регистъра на информационните обекти чрез подходящ интерфейс.

Регистър на стандартите

Регистърът на стандартите е база от данни, управлявана от информационна система, съдържаща техническите стандарти и спецификации, които трябва да се прилагат

от административните органи за предоставяне на електронни услуги, както и за осигуряване на оперативна съвместимост и информационна сигурност.

Ще бъде описан подробно в следващия раздел.

Оценка за съответствие за оперативна съвместимост и информационна сигурност. Методика за оценката за съответствие

Администрациите са длъжни да използват само информационни системи и програмни приложения, които са сертифицирани за съответствие с установените със Закона за електронното управление и подзаконовите актове по прилагането му изисквания за оперативна съвместимост и информационна сигурност.

Процедурите по оценка за съответствие ще бъдат описани подробно в следващия раздел.

Списъци на оценените за съответствие системи и продукти

В списъците на оценените за съответствие системи и продукти се вписват обстоятелства относно оценените за съответствие информационни системи и продукти.

Тези списъци ще бъдат описани подробно в следващия раздел

The implementation of these requirements is objectified consequently the operation of the systems composing so called "Meta-level of e-Government":

Заклучение

Регламентирайки дейността на административните органи при работа с електронни документи, Законът за електронното управление и шестте наредби към него формулират от технологична гледна точка комплекс от нови изисквания към административните информационни системи и, по същество, създават една нова среда за тяхното действие.

Тези изисквания са насочени преди всичко към осигуряване на ефективен обмен на т.н. вътрешни електронни административни услуги и към създаване на възможност за включване на електронните административни услуги, предоставяни от отделните администрации, във вериги с добавена стойност, без допълнителни действия от страна на доставчиците.

ЧАСТ 4

ТЕХНОЛОГИЧНА РЕАЛИЗАЦИЯ

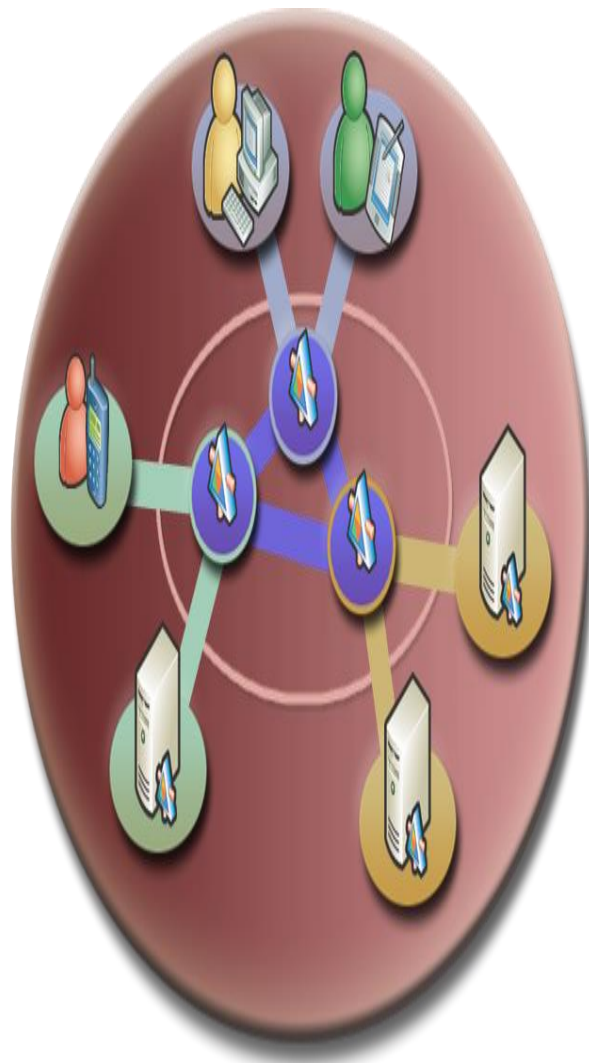
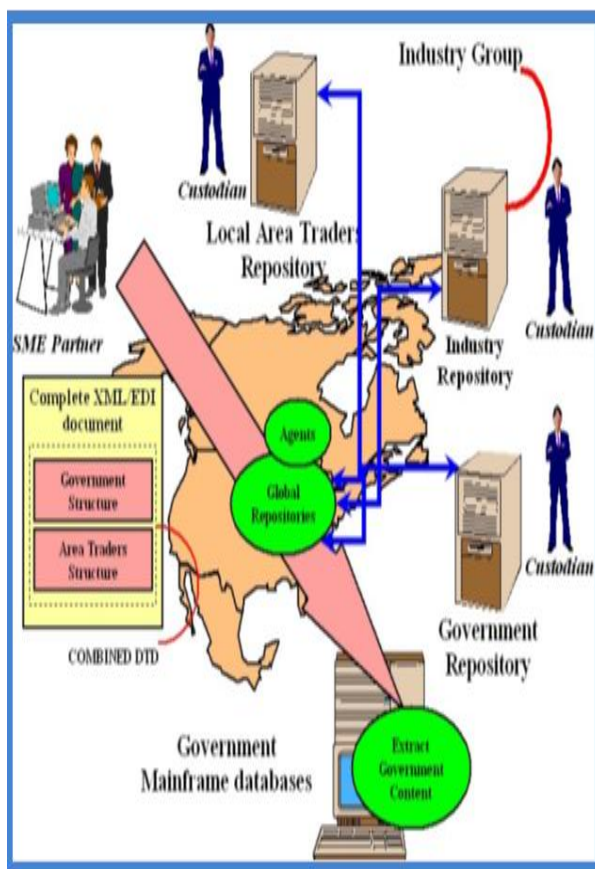
ГЛАВА 4.1

ВЪВЕДЕНИЕ

Активна оперативна съвместимост

Кокто беше посочено в предишния раздел, т.н. “Активната оперативна съвместимост” предполага, че агенти от различни хетерогенни среди могат да постигнат оперативна съвместимост чрез посредничеството на хомогенна среда с вътрешен стандартизиран обмен.

Освен това, тя включва и изискванията за “регистрово-ориентирана” инфраструктура на данните.



Фигура 4-1

Напълно контролируема оперативна съвместимост

За разлика от Националната рамка за оперативна съвместимост, която има действително “рамков” характер,

Наредбата за оперативна съвместимост и информационна сигурност въвежда слой от изисквания, подлежащи на еднозначна обективна проверка и залегнали в процедурите за сертификация на информационните системи и продуктите.

Изпълнението на тези изисквания се обективизира и вследствие на функционирането на системите от т.н. “мета-ниво” на е-Правителство:

- Единната среда за обмен на електронни документи (ЕСОЕД) и
- шестте регистъра, съставлящи “Националния модел на даннитев администрацията”.

Състав на централизираната инфраструктура

1. Инфраструктура за оперативна съвместимост – включва информационни системи за поддръжка на регистри и списъци за нуждите на е-Правителството, които се подразделят на две групи:

- регистри, поддържащи Националния модел на данни и процедури: регистър на регистрите и данните, регистър на информационните обекти, регистър на електронните услуги, списък с унифицираните наименования на административните услуги, национална номенклатура на видовете документи, национална номенклатура на делата;
- спомагателни регистри: регистър на стандартите, списъци на акредитираните лица и на сертифицираните системи и продукти.

2. Инфраструктура за мрежова и информационна сигурност

3. Инфраструктура на електронните услуги – включва:

- единна среда за обмен на електронни документи (ЕСОЕД);
- национален портал на електронното правителство;
- система за единно астрономическо време;
- национален портал за пространствени данни;
- система за електронни разплащания на електронното правителство.

ГЛАВА 4.2

РЕГИСТЪР НА СТАНДАРТИТЕ

Регламентация от Закона за електронното управление

За да осигури адекватното използване от административните органи на международните стандарти, свързани с оперативната съвместимост и информационната сигурност, Законът за електронното управление постановява следното:

„Към Министерството на транспорта, информационните технологии и съобщенията се води регистър на стандартите като единна централизирана електронна база данни, управлявана от информационна система, съдържаща техническите стандарти и тяхната приложимост.

В регистъра на стандартите се вписват техническите стандарти, които трябва да се прилагат от административните органи за предоставяне на електронни административни услуги и за осигуряване на оперативна съвместимост, информационна сигурност и автоматизиран обмен на информация и документи между административните органи.

Воденето, съхраняването и достъпът до регистъра на стандартите се уреждат с наредба”.

Подзаконово регулиране

В изпълнение на Закона, регистърът на стандартите се урежда с глава четвърта от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

Регистърът на стандартите е база от данни, управлявана от информационна система, съдържаща техническите стандарти и спецификации, които трябва да се прилагат от административните органи за предоставяне на електронни услуги, както и за осигуряване на оперативна съвместимост и информационна сигурност.

Под името „регистър” в Наредбата се подразбира както информационния ресурс, така и регистриращия орган по смисъла на БДС ISO/IEC 6523-2:2000.

Регистърът на стандартите е динамична структура, отразяваща актуалното състояние на стандартизационните процеси и възможностите за прилагането им в текущия момент.

Допълнителни функции

Министърът на транспорта, информационните технологии и съобщенията трябва да създаде организация за:

- а) разпространение на знание относно приложението на стандартите, осигуряващи оперативна съвместимост на информационните системи и информационна сигурност;
- б) предложения пред Българския институт по стандартизация за приемане на международни или европейски стандарти като Български държавни стандарти;
- в) предложения пред Българския институт по стандартизация за разработване на нови Български държавни стандарти.

Подбор на стандарти

Поради изключителното многообразие на стандарти и спецификации, свързани с оперативната съвместимост и мрежовата и информационна сигурност, от решаващо значение е изборът на фундаменталната стандартизационна платформа.

Еволюцията на стандартизационния процес по отношение на системната интеграция и оперативна съвместимост насочва този избор към архитектурата, ориентирана към услуги. Последната позволява не само пренос на информация от приложение към приложение в различни информационни системи, но и създаване на комплексни приложения чрез услуги, поддържани в отдалечени системи чрез разпределяне на обща бизнес-логика между приложенията.

Обхват на регистъра

Стандартизацията на административните информационни системи в областта на оперативната съвместимост и информационната сигурност обхваща по-широка област от тази на т.н. “формални хармонизирани стандарти”, утвърждавани от официалните междуправителствени стандартизационни органи (като ISO, ITU на глобално ниво или CEN, CENELEC, ETSI – на европейско ниво). Тя включва неформални и хибридни стандартизационни процеси - продукцията на секторни консорциуми, като: OASIS, IETF, W3Consortium, UN/CEFACT, OMG и др.

Въз основа на областите на приложение стандартите се подразделят на две основни групи:

- хоризонтални – с общо приложение (във всички области);
- вертикални – с приложение в специфицирана област (отрасъл и пр.). Като пример за целите на администрацията това могат да бъдат: медицинска информатика, банково дело, географски информационни системи, промишлени продуктови системи и т.н.

Критерии за избор на стандарти

Основните критерии за избор на стандартите са както следва:

- отвореност;
- ниво на приемане и поддържане;
- зрялост;
- потенциал;
- приложимост към националните условия.

В случай, че за определени цели, свързани с оперативната съвместимост, е прието действието само на част от даден стандарт, или действието на даден стандарт е ограничено само за някои специфични области, това се записва като отделно обстоятелство на дадения стандарт в Регистъра на стандартите.

При подбора и оценката на стандартите като ръководно начало се прилага „Общия метод за оценка на стандартите” (Common assessment method for standards and specifications - CAMSS), разработван в рамките на Програма IDABC на Европейската комисия.

Основни функции на Регистъра на стандартите

Регистърът на стандартите поддържа множество раздели и класификационни структури на регистрираните стандарти с цел:

- дефиниране на набори от изисквания, представени чрез регистрирани стандарти, намиращи се в подходящ статус, за обслужване на процеса на сертификация;
- отразяване на резултата от процедурни действия по поддръжка на статуса на регистрирани стандарти.

Регистърът на стандартите ще бъде инструмент за практическо създаване и поддържане на стандартизационната основа на всички дейности в състава на проекта за електронно правителство.

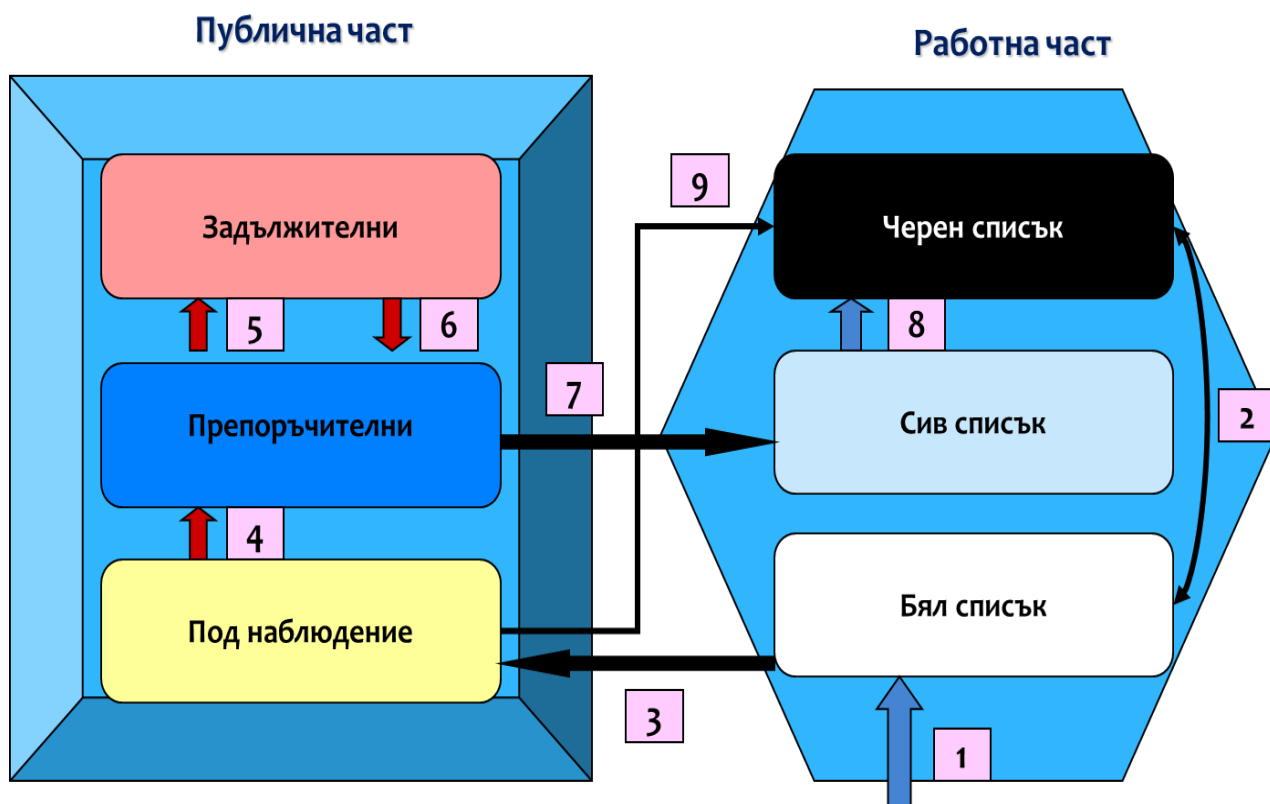
Регистърът има базов характер и не цитира данни от други регистри.

Атрибути на стандартите

На вписване в регистъра на стандартите подлежат следните обстоятелства:

- а) наименование;
- б) идентификатор;
- в) пояснение;
- г) версия;
- д) дата на приемане;
- е) организация, създава и поддържаща стандарта;
- ж) текст (ако е публикуван със свободен достъп);
- з) URL на публикация;
- и) степен на приложимост;
- к) тематична принадлежност;
- л) обхват на приложимост
- м) URI на партида.

Структура и динамика на процеса на поддържане на Регистъра на стандартите



Фигура 4-2

Класификация на международните стандарти, осигуряващи ОС на ИС

<p><u>Технологично-ориентирана класификация:</u></p> <ul style="list-style-type: none"> • моделиране на процеси и данни • клиентска част • презентация • интеграция на приложения • семантична ин-билност • мидълуеър • комуникации • управление на директории • връзка с "Back-End" • сигурност 	<p><u>Процесно-ориентирана класификация:</u></p> <ul style="list-style-type: none"> • свързаност • Web-услуги • интеграция на данни • управление на съдържание • управление на идентификатори • работни станции • други вериги 	<p><u>Сервизно-ориентирана класификация</u> - услуги по:</p> <ul style="list-style-type: none"> • архивиране на документи; • обмен на документи; • EDI; • Web; • вътрешния интерфейс; • трансфер на съобщения; • трансфер на файлове; • упр-ние на потоци задания; • управление на директории; • управление на мрежи; • управление на сигурността.
<p>Пример: ebXML Registry Information Model - ISO 15000-3</p> <p>V. 2.0 03.04.2002 ISO/IEC, OASIS http://www.oasis-open.org Статут: Под наблюдение</p>		
Интеграция на приложения	Управление на идентификатори	Услуги по вътрешния интерфейс

Фигура 4-3

Общ вид



Фигура 4-4

Описание на стандарт

Национален регистър на стандартите за оперативна съвместимост и информационна сигурност

Начална страница | Национален регистър на стандартите | Нормативна база | Същност на стандартите

Стандарти за комуникация и процедури за обмен

Стандарти за уеб-услуги

Стандарти за интеграция на данни

Стандарти за управление на съдържанието и дефиниции на метаданни

Стандарти за потребителски интерфейси

Стандарти за работни станции

Стандарти за вътрешна организация на дейността и работни процеси

Стандарти за управление на електронната идентичност

Стандарти за информационна сигурност

Post Office Protocol (POP3)

Моля, въведете дата към която е валиден стандарта: 2009-06-05

Потвърди

Наименование на стандарт: Post Office Protocol (POP3)

Идентификатор на стандарт: RFC 1939

Пояснение на стандарта: Пощенският протокол е предназначен за установяване на динамичен достъп на работната станция до пощенския сървър. Той позволява на работната станция да получи поща, която сървърът съхранява за нея.

Версия на стандарта: 3.0

Дата: 01.5.1995 г.

Организация: Internet Engineering Task Force (IETF)

URL на публикация: свободен достъп

Степен на приложимост: задължителен

Тематична принадлежност: комуникация и процедури за обмен

Обхват на приложимост: целия стандарт

URL на партидата: Post Office Protocol (POP3)

Време на вписване: 11.5.2009 г.

Текст

Описания на обстоятелствата

Фигура 4-5

Обстоятелства на стандарт



Национален регистър на стандартите за оперативна съвместимост и информационна сигурност

Начална страница | Национален регистър на стандартите | Нормативна база | Същност на стандартите | Действия за сайта

Преглед на цялото съдържание на сайта

Обстоятелства на стандартите

обстоятелство	време на вписване	заявител на вписване
идентификатор на стандарт	11.5.2009 г.	ДАИТС
наименование на стандарт	11.5.2009 г.	Йонко Божинов
версия на стандарта	11.5.2009 г.	Йонко Божинов
дата	11.5.2009 г.	Йонко Божинов
пояснение на стандарта	11.5.2009 г.	Йонко Божинов
организация	11.5.2009 г.	Йонко Божинов
URL на публикация	11.5.2009 г.	Йонко Божинов
степен на приложимост	11.5.2009 г.	Йонко Божинов
тематична принадлежност	11.5.2009 г.	Йонко Божинов
обхват на приложимост	11.5.2009 г.	Йонко Божинов
URL на партида	11.5.2009 г.	Йонко Божинов
текст на стандарта	11.5.2009 г.	Йонко Божинов

Кошче

Фигура 4-6

Конкретно обстоятелство

The screenshot shows a web browser window displaying a national registry for standards. The page title is "Национален регистър на стандартите за оперативна съвместимост и информационна сигурност". The main heading is "Post Office Protocol (POP3)". Below the heading is a table with details of the standard entry.

Navigation links: [Начална страница](#), [Национален регистър на стандартите](#), [Нормативна база](#), [Същност на стандартите](#), [Действия за сайта](#)

Actions: [Нов елемент](#), [Редактиране на елемент](#), [Изтриване на елемент](#), [Управление на разрешения](#), [Предупреждавай ме](#)

Наименование на стандарт	Post Office Protocol (POP3)
Заявител на вписване	Йонко божинов
УРИ на заявлението за вписване	URI-2238
Време на вписване	11.5.2009 г. 00:00
Служител извършил вписване	SERVER4\jonko
УРИ на регистър на стандартите	18
Номер на партида	76
Номер на вписване	596
УРИ на обстоятелство	3
Съдържание на обстоятелство	Пощенският протокол е предназначен за установяване на динамичен достъп на работната станция до пощенския сървър. Той позволява на работната станция да получи поща, която сървърът съхранява за нея.
Обстоятелство	пояснение на стандарта

Създадено в 11.5.2009 г. 14:30 от [Системен акаунт](#)
Последна промяна в 11.5.2009 г. 14:30 от [Системен акаунт](#)

Затвори

Фигура 4-7

Производство по вписване в регистъра

Производството по вписване започва със заявление, подадено от административен орган. Производство по вписване може да започне и по инициатива на Министъра на транспорта, информационните технологии и съобщенията по предложение на Съвета по стандартите за оперативна съвместимост и информационна сигурност.

Министърът на транспорта, информационните технологии и съобщенията предоставя следните електронни услуги, свързани с регистъра на стандартите:

- а) вписване на стандарт;
- б) вписване на промени в обстоятелствата за стандарт;
- в) справка за вписванията в регистъра на стандартите за отделен стандарт или за стандарти по определени критерии.

При това, Министърът на транспорта, информационните технологии и съобщенията утвърждава задължителни формуляри в електронна форма за:

- а) заявление за първоначално вписване на стандарт;
- б) заявление за вписване на допълнителни обстоятелства към вече вписан стандарт;
- в) заявление за справка за вписванията в регистъра на стандартите;
- г) справка за вписванията в регистъра на стандартите за отделен стандарт или за стандарти по определени критерии.

Формулярите се вписват в раздел „Документи” на регистъра на информационните обекти и се публикуват на Интернет-страницата на МТИТС.

Достъп до Регистъра на стандартите

Регистърът на стандартите се съхранява безсрочно. Министърът на транспорта, информационните технологии и съобщенията съхранява регистъра на стандартите в съответствие с изискванията на тази наредба, като система с клас на информационна сигурност 3 или А.

Регистърът на стандартите е достъпен чрез Интернет-страницата на МТИТС и по друг начин в зависимост от технологичната готовност.

Министърът на транспорта, информационните технологии и съобщенията осигурява възможност за преглед на актуалното състояние на партидите на стандартите към момента на проверката, както и на състоянието им към определена дата назад във времето.

Всеки може да иска и извършва справка за вписванията в регистъра чрез Интернет-страницата на МТИТС, като справките са безплатни.

Съвет по стандартите

Към Министъра на транспорта, информационните технологии и съобщенията се създава Съвет по стандартите за оперативна съвместимост и информационна сигурност. Той е помощен консултативен орган и включва експерти, определени със заповед на Министъра на транспорта, информационните технологии и съобщенията .

Съветът по стандартите за оперативна съвместимост и информационна сигурност взема решенията относно допустимостта и основателността за извършване на вписванията в регистъра на стандартите.

Приложение на регистъра на стандартите

Регистърът на стандартите дава практически насоки на възложителите, разработчиците и доставчиците на информационни системи и програмни продукти за административните органи, като ги ориентира в:

- а) минималното количество изисквания, които възложителят трябва да постави в своето задание;
- б) минималното количество изисквания, които възложителят трябва да постави към технологията на експлоатация и организиране на изпълнението на предоставяните от него услуги;
- в) насоките за изпълнителя какъв инструментариум да избере за разработка. Поставя се бариера пред изисквания, които по същество връщат разработките назад в технологично отношение.

Общи понятия за регистъра на стандартните данни

Целта на регистъра е събирането и поддържането на данни за всички регистри, списъци и други набори от данни, водени от административните органи в Република България, осигуряването на уникален индекс за всеки набор от данни или раздел от набор от данни, поддържането на определения на неунифицирани и унифицирани данни и унифицирани определения на етапи на административни услуги и процедури.

Регистърът се води от Министъра на транспорта, информационните технологии и съобщенията, чрез овластени от него лица.

Обекти, вписвани в регистъра

В регистъра се вписват следните видове обекти:

- обекти от вид „набор от данни”;
- обекти от вид „тип обстоятелство”;
- обекти от вид „унифицирана данна”;
- обекти от вид „пакет от данни”;
- обекти от вид „унифициран етап”;
- обекти от вид „лица по чл. 2, ал. 1 от ЗЕУ” .

Обект се вписва в съответния раздел само при условие, че заявката за вписване съдържа данни за всички подлежащи на вписване обстоятелства. Някои от обстоятелствата се вписват служебно въз основа на решение на Съвета по вписванията към Министъра на транспорта, информационните технологии и съобщенията.

Обект “Унифицирана данна”

Обстоятелствата за обекти от вид „унифицирана данна”, подлежащи на вписване в раздел „Унифицирани данни” са:

- наименование на унифицираната данна - вписва се наименованието на унифицираната данна, което трябва да е уникално по отношение на наименованията на останалите вписани унифицирани данни, които са със статус "използваем";
- определение на унифицираната данна – вписва се разширено текстово описание на унифицираната данна, позволяващо еднозначно ѝ отграничение от останалите вписани унифицирани данни;
- статус на информационен обект – вписва се указание относно възможността данната да се използва в нормативни актове, включително в определенията на други данни. Възможните стойности са "използваема" или "неизползваема";
- тип или състав на данна – ако данната е единична се вписва "единична", а ако е съставна, се вписва наборът от изграждащите я данни;
- лица с право на достъп до данната – въвежда се списък с административните органи, лицата, осъществяващи публични функции и организациите, предоставящи обществени услуги, които въз основа на закон обработват тази данна.

ГЛАВА 4.3

РЕГИСТРИ НА ИНФОРМАЦИОННИТЕ ОБЕКТИ И НА ЕЛЕКТРОННИТЕ УСЛУГИ

Законова регламентация

Законът за електронното управление изисква предоставянето на вътрешни електронни административни услуги и обменът на електронни документи между административните органи да се извършват в условията на оперативна съвместимост. Важна съставна част на последната е семантичната оперативна съвместимост, която осигурява едно и също смислово съдържание на обменяните данни.

Семантичната оперативна съвместимост на обмена на електронни документи между административните органи се осигурява чрез:

- уеднаквяване на именованията на данните, подлежащи на съхранение в бази данни или в регистри;
- формализиране на данните и на административните услуги за осигуряване на технологична възможност за автоматизиран обмен между административните органи и обработката на данни.

Законът постановява формализираните данни и формализираното описание на електронните административни услуги да се вписват в регистъра на информационните обекти, съответно в регистъра на електронните услуги. Тези регистри се водят от Министъра на транспорта, информационните технологии и съобщенията.

Подзаконова уредба

Условията и реда за воденето, съхраняването и достъпа до регистъра на информационните обекти и до регистъра на електронните услуги се уреждат в специална наредба.

Съгласно Наредбата за водене, съхраняване и достъп до регистъра на информационните обекти и до регистъра на електронните услуги тези регистри са бази от данни, управлявани от информационни системи и съдържаща формализирани технологични описания съответно:

- на информационните обекти, събирани, създавани, съхранявани и обработвани от административните органи в рамките на тяхната компетентност и
- на електронните административни услуги и вътрешните електронни административни услуги, предоставяни чрез единната среда за обмен на документи.

Регистрите се водят чрез поддържане на единна централизирана база от данни. В тях се поддържа история на вписванията.

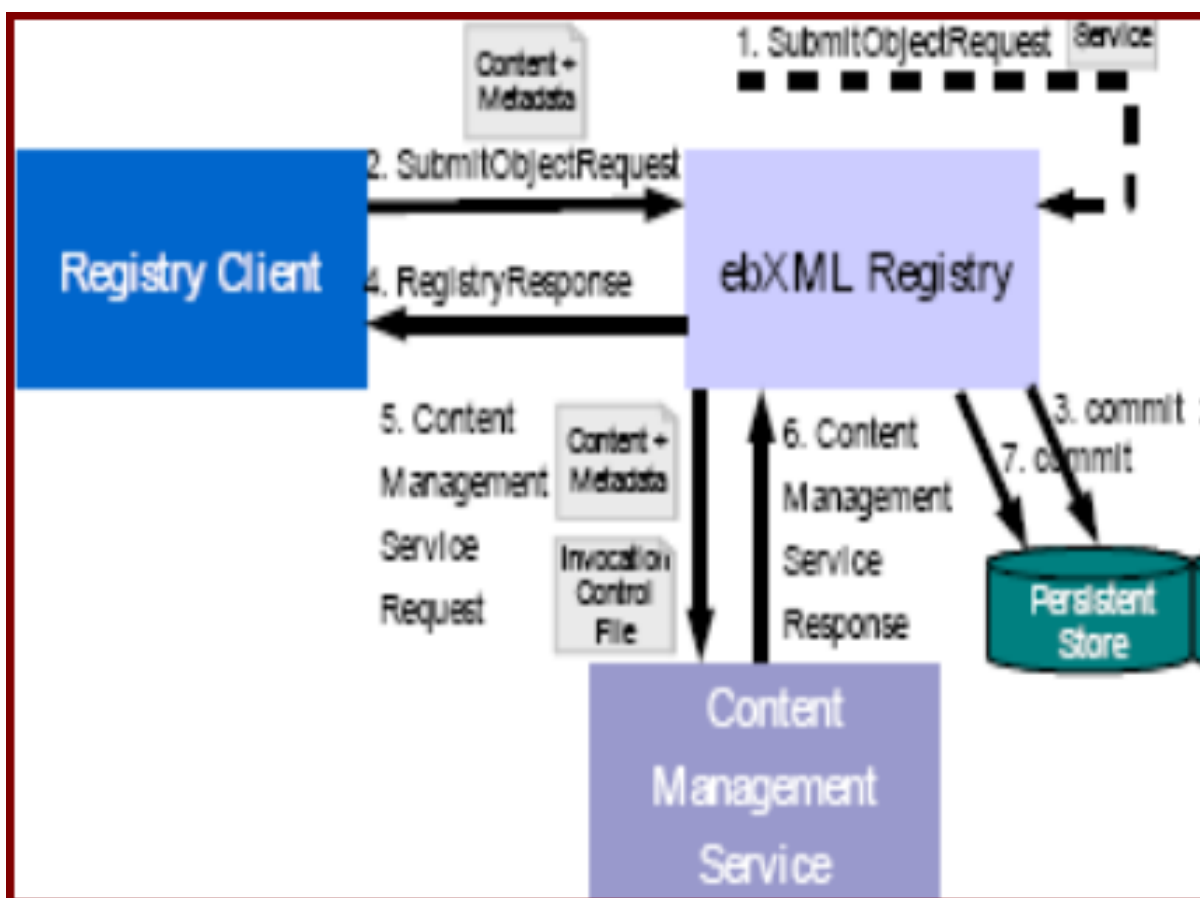
Информационни обекти

Информационните обекти са единични или съставни данни, събирани, създавани, съхранявани или обработвани от административните органи в рамките на тяхната компетентност.

Видовете информационни обекти от гледна точка на общия информационен модел на данните в администрацията са както следва:

- а) „термин” - понятие, което се интерпретира еднозначно от всички участници в административния процес;
- б) „номенклатура” - краен списък от тематично свързани термини, вписани в регистъра;
- в) „стойност” – представя величина и се описва с краен брой значения, зададени с формални ограничения;
- г) „сегмент” – структура, съставена от вече вписани в регистъра термини, номенклатури, стойности и/или други сегменти;
- д) „документ” - сегмент, за който е осигурено програмно приложение, даващо възможност за пълна, точна и вярна визуализация на съдържащите се данни.

Общи изисвания към организацията на регистрите в държавната администрация



Фигура 4-8

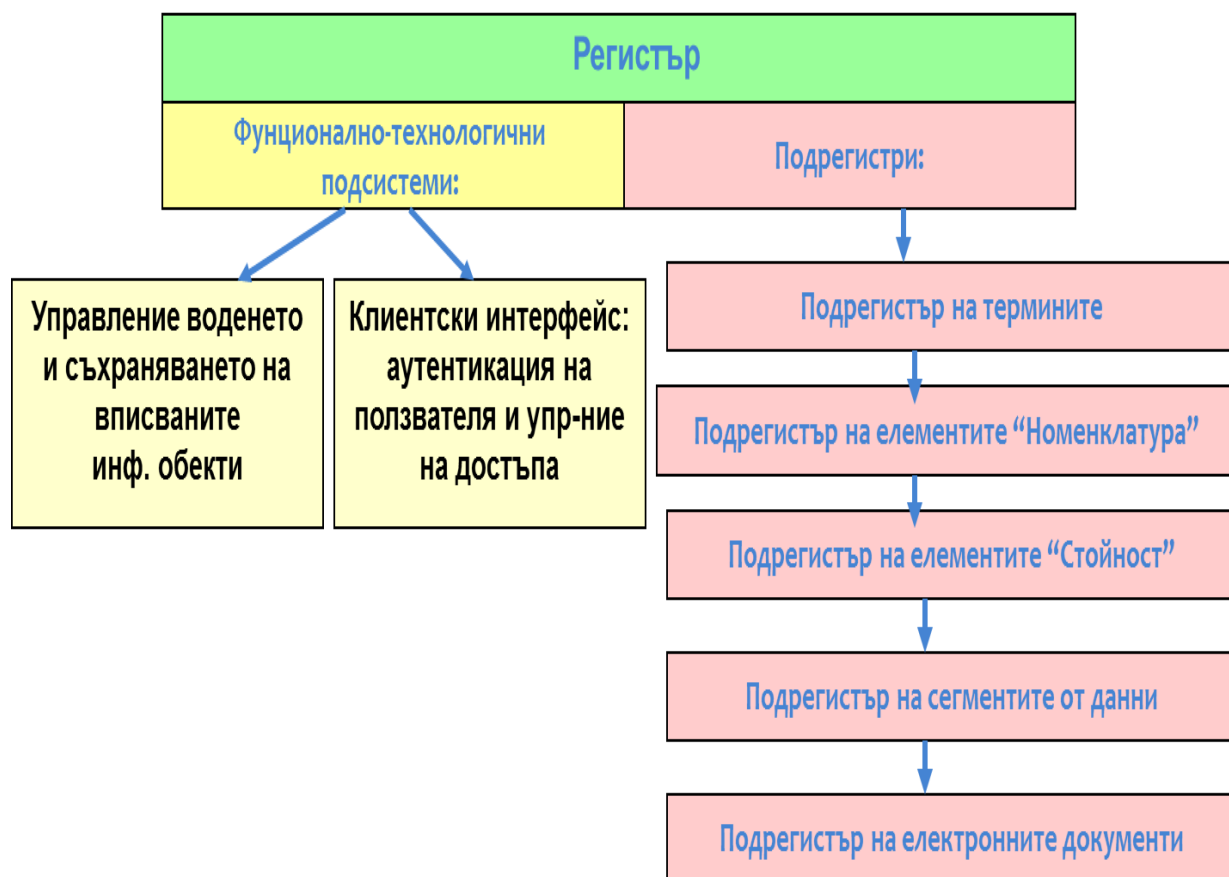
Информационните структури от типа “Регистри” функционират в две логически (виртуални) среди:

- средата на интегрираните данни, характеризираща се не само с техническа съвместимост (формати, процедури за обмен и обработка), но и със семантична съвместимост;
- средата на комплексните електронни услуги (по същество регистрите са източник на електронни услуги).

Това определя и основните изисквания към регистрите в държавната администрация:

1. Да отговарят на международните стандарти
2. Да осъществяват интерфейс с ползвателите като “е-Услуги” със съответна аутентификация / оторизация и пр.
3. Да осигурят взаимни връзки за осъществяване на принципа на еднократното подаване на данни:
 - А. При вписвания да не се иска данна, която първични се съхранява в друг регистър, а да се търси от там;
 - Б. При промяна на данната в “първичния за нея” регистър да се извърши автоматично и “он-лайн” промяна във всички други регистри.

Регистър на информационните обекти



Фигура 4-9

“Електронен документ” в контекста на “оперативната съвместимост” е: “логически завършена само-описваща се информационна структура, която може да бъде визуализирана и едновременно с това обработвана от информационните системи на Електронното правителство и без пряка човешка намеса. При това електронният документ съдържа механизми за безспорна автентикация и защита от неправомерен достъп”.

Пример – информационен обект тип „сегмент“

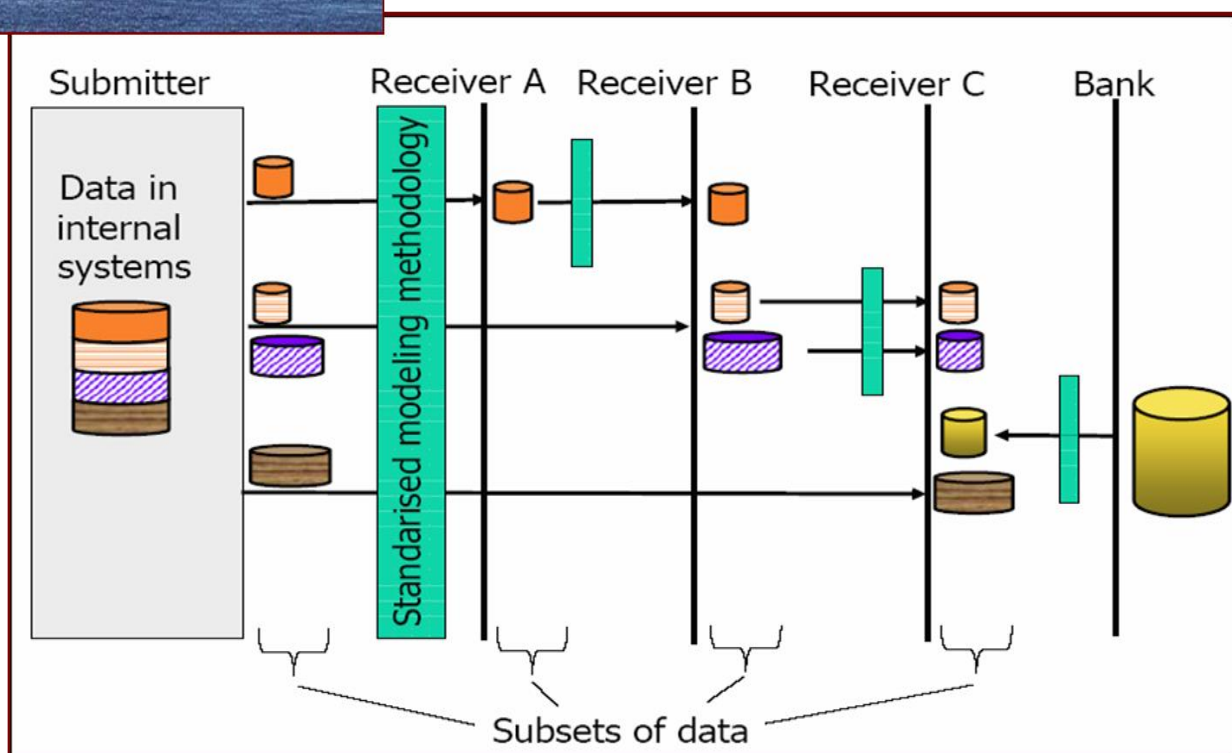
<ul style="list-style-type: none"> Термини Номенклатури Стойности Сегменти Документи 	<p>Обща информация</p> <p>УРИ 0009-000002</p> <p>Наименование Доставка на електронни административни услуги</p> <p>Предназначение Описва данни за доставчика на електронни административни услуги. Доставчикът е или юридическо лице, регистрирано по българското законодателство или лице, упражняващо свободна професия, регистрирано в регистър БУЛСТАТ</p> <p>Унифицирана данна 0003-000010 (Доставчик на електронни административни услуги)</p> <p>Статус използваем</p> <p>Интернет-страница на партията http://ereg.egov.bg/public/info/segment/view.rg?Uri=0009-000002</p> <p>Указания за Начин на визуализация: Данните за доставчика се визуализират с основни данни за юридическото лице, доставчик на електронната административна услуга и с обработка вида на доставчика. Начин на обработка При редактиране електронната форма трябва да даде възможност да се попълнят данните за доставчика с основни данни за юридическо лице и да се отбележи вида на доставчика.</p> <p>XML дефиниция</p> <pre><?xml version="1.0" encoding="UTF-8"?> <xsd:schema targetNamespace="http://ereg.egov.bg/segment/0009-000002" xmlns="http://ereg.egov.bg/segment/0009-000002" xmlns:ebd="http://ereg.egov.bg/segment/0009-000013" xmlns:espt="http://ereg.egov.bg/value/0008-000034" xmlns:xsd="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"> <xsd:import namespace="http://ereg.egov.bg/segment/0009-000013"/> <xsd:import namespace="http://ereg.egov.bg/value/0008-000034"/> <xsd:complexType name="ElectronicServiceProviderBasicData"> <xsd:annotation> <xsd:documentation xml:lang="bg">Доставчик на електронни административни услуги</xsd:documentation> </xsd:annotation> <xsd:sequence> <xsd:element name="EntityBasicData" type="ebd:EntityBasicData"/> <xsd:element name="ElectronicServiceProviderType" type="espt:ElectronicServiceProviderType"/> </xsd:sequence> </xsd:complexType> </xsd:schema></pre> <p>Указания за проверка на валидност Валидацията се извършва в съответствие с приложената в полето "XML дефиниция" XSD схема, като се прилагат правилата за проверка на елемента от тип "Основни данни за юридическо лице", когато наследява. В случай на несъответствие се извежда съобщението за грешка при валидация на основния елемент.</p> <p align="right">Към началото</p>
	<p>Списък от грешки</p> <p>Термин на грешка 0006-000069 (Невалидна структура на обекта съгласно XML дефиницията му, вписана в регистъра на информационните обекти)</p>

Фигура 4-10

Норвежкият пример

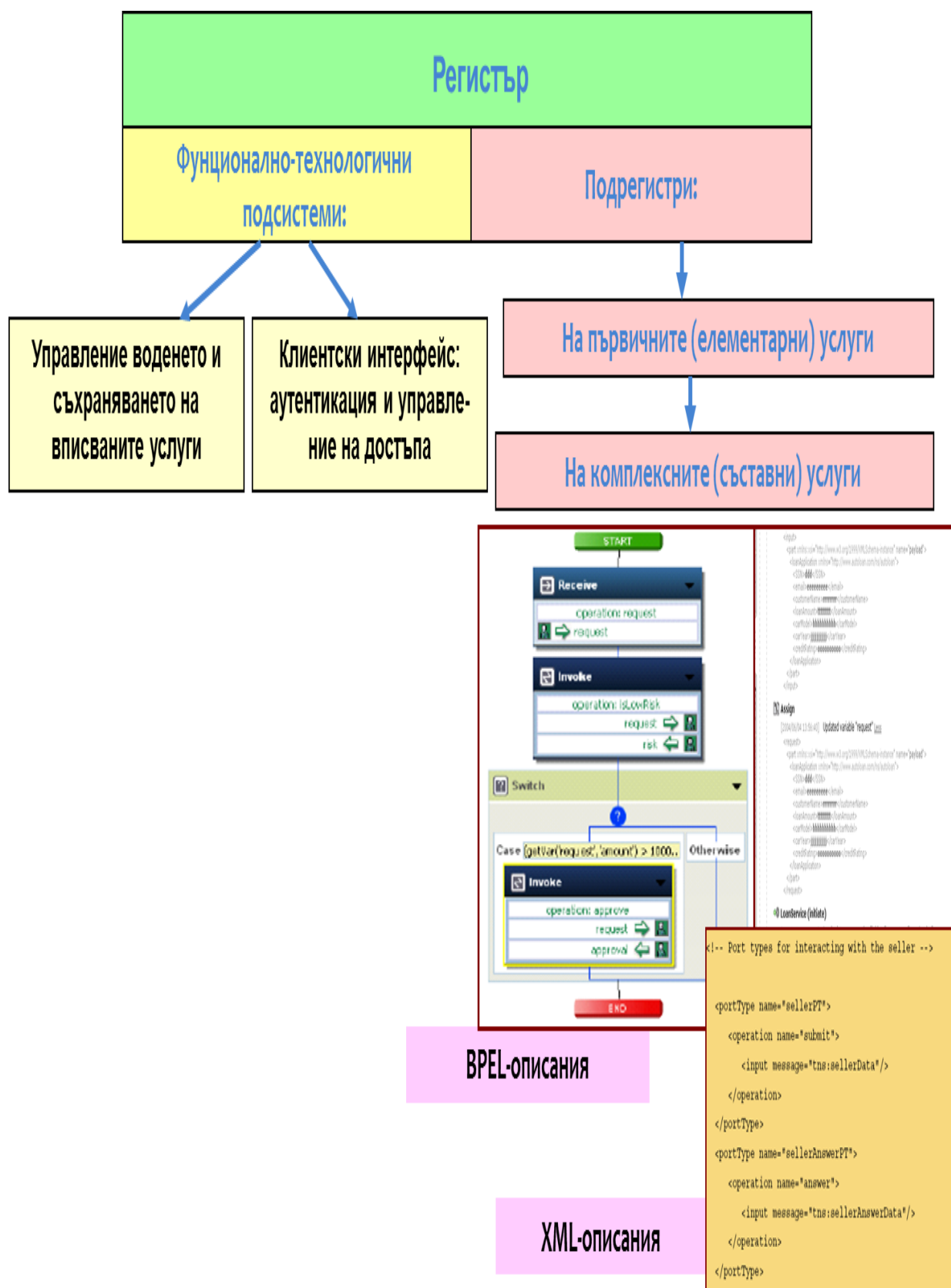


Норвежкият регистър “Oppgaverregisteret (the Register of Reporting Obligations of Enterprises)”, въведен със закон от 1999 г., съдържа понастоящем над 17 000 семантични единици, формиращи над 700 електронни документа, обменяни между бизнеса и държавата, над 260 лицензии и разрешителни.



Фигура 4-11

Регистър на електронните услуги



Фигура 4-12

Особености на Регистъра на електронните услуги

Функционирането на регистъра на електронните услуги е свързано с някои важни особености, например:

- обстоятелствата, свързани с вътрешна електронна административна услуга, включват списък на получателите - т.е. вписва се списък с данни за административните органи, организации, предоставящи обществени услуги и лица, осъществяващи публични функции, които съгласно нормативен акт имат право достъп до данните, предоставяни с вътрешната електронна административна услуга и условията, при които могат да ги получат;
- електронна услуга, която се предоставя от административен орган, може да се впише в регистъра само, ако е налице вписване за нея като административна услуга в списъка с унифицираните наименования на административните услуги, воден от Министъра на държавната администрация и административната реформа. В този случай обстоятелствата се вписват със съдържание, аналогично на вписаното в списъка с унифицираните наименования на административните услуги.

Производство по вписване

Производството по вписване в регистрите започва със заявление от административен орган. Лица, осъществяващи публични функции и организации, предоставящи обществени услуги могат да заявяват за вписване електронни услуги, които се предоставят чрез единната среда за обмен на документи и информационни обекти, които се събират, създават, съхраняват и обработват от тях при предоставяне на тези услуги.

Процедурата за вписване включва:

- а) приемане на заявлението за вписване;
- б) проверка дали заявлението е подадено от оправомощено лице и дали информационният обект, съответно електронната услуга подлежат на вписване;
- в) проверка дали са заявени всички изискуеми обстоятелства и дали те отговарят на изискванията на наредбата;
- г) проверка дали информационният обект, съответно електронната услуга не е вече вписана;
- д) извършване на вписването или издаване на мотивиран отказ за вписване;
- е) уведомяване на заявителя за извършеното вписване, съответно за отказа.

Съвет по вписванията

Посочените проверки се извършват от Съвета по вписванията. Последният е помощен консултативен орган и включва независими експерти в областта на информационните технологии, юристи, специалисти по административно обслужване и други експерти, определени със заповед на министъра на държавната администрация и административната реформа.

Съветът по вписванията дава становища относно допустимостта и основателността за извършване на вписванията в списъка с унифицираните наименования на

административните услуги, регистъра на регистрите и данните, регистъра за информационните обекти и регистъра на електронните услуги.

Електронни услуги, свързани с регистрите

Министърът на транспорта, информационните технологии и съобщенията предоставя следните електронни услуги, свързани с регистъра на информационните обекти и регистъра на електронните услуги:

- вписване на информационен обект;
- вписване на електронна услуга;
- вписване на промени в обстоятелствата за информационен обект;
- вписване на промени в обстоятелствата за електронна услуга;
- справка за вписванията в регистъра на електронните услуги за отделна електронна услуга или за всички електронни услуги;
- справка за вписванията в регистъра на информационните обекти за отделен информационен обект или за всички информационни обекти;
- справка за списъка на данните, съдържащи се в регистриран информационен обект от вид документ.

Достъп до регистрите

Регистрите на информационните обекти и на електронните услуги се съхраняват безсрочно.

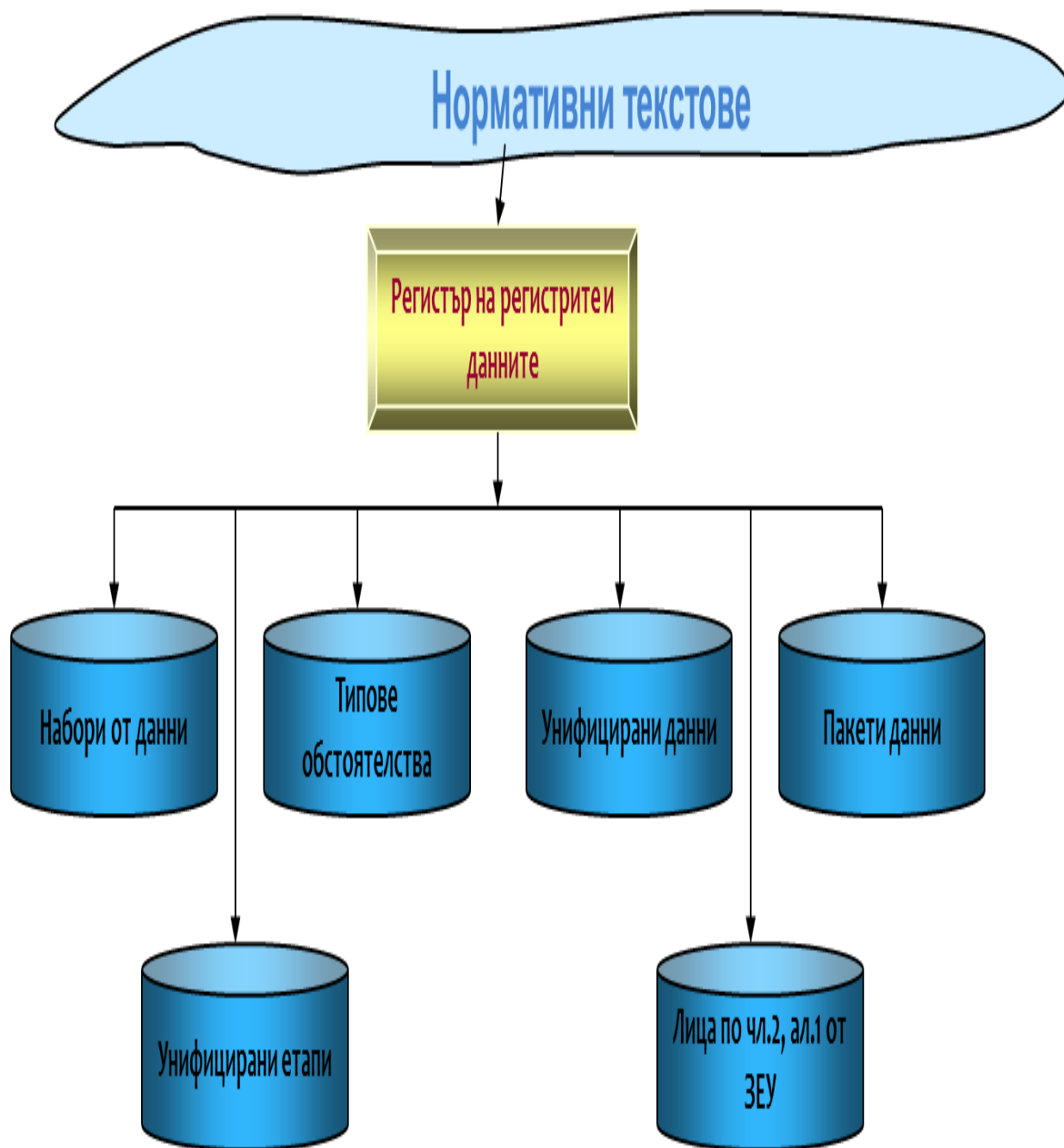
Министърът на транспорта, информационните технологии и съобщенията съхранява регистрите на информационните обекти и на електронните услуги в съответствие с изискванията на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност на Министерския съвет, като система с клас на информационна сигурност 3 или „А”.

Регистрите на информационните обекти и на електронните услуги са достъпни чрез интернет-страницата на Министерството на транспорта, информационните технологии и съобщенията и по друг начин в зависимост от технологичната готовност на министерството.

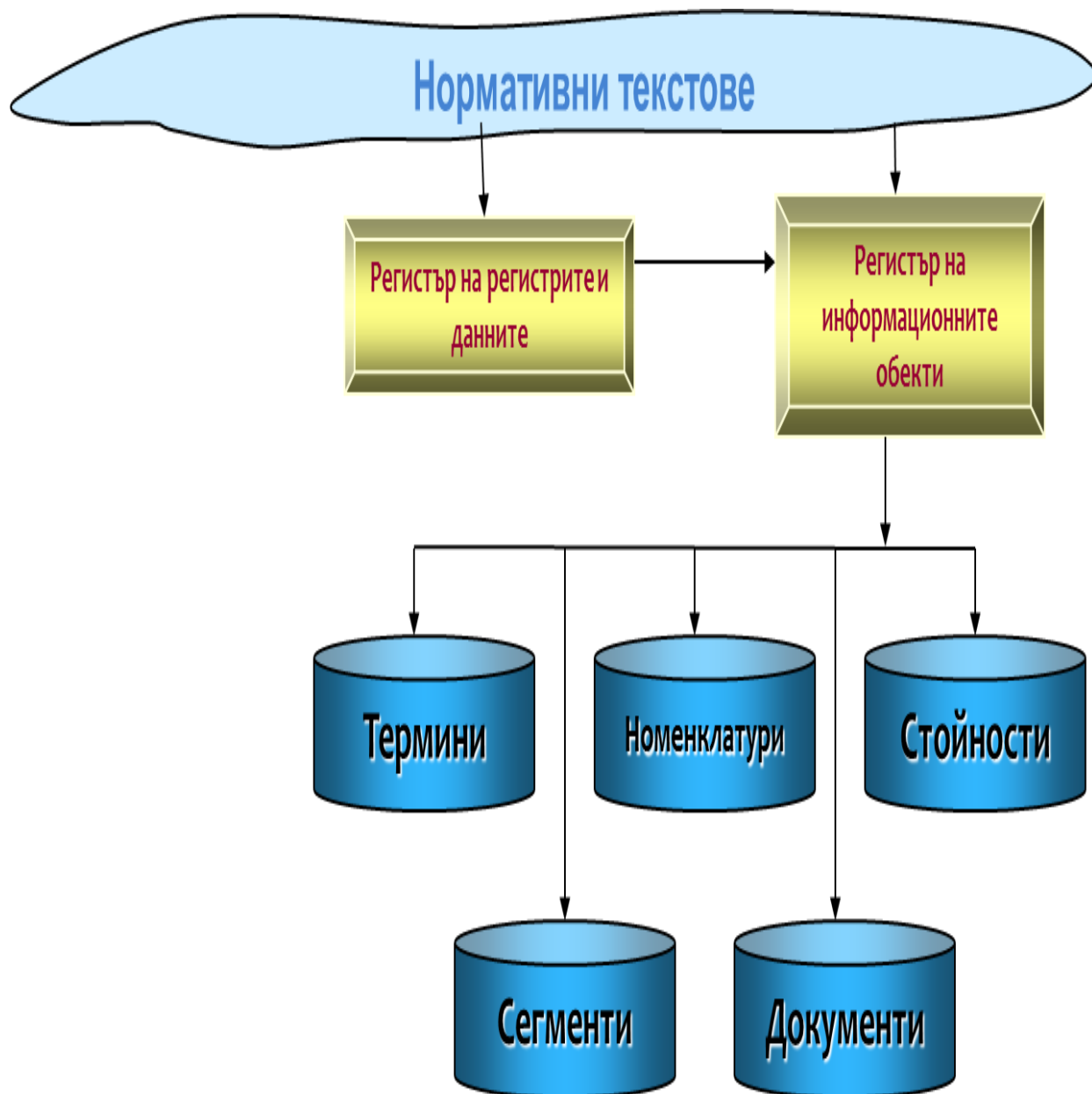
Министърът на транспорта, информационните технологии и съобщенията осигурява възможност за преглед на актуалното състояние на партидите на информационните обекти и на електронните услуги към момента на проверката, както и на състоянието им към определена дата назад във времето.

Всеки може да иска и извършва справка за вписванията в регистрите чрез интернет-страница на Министерството на транспорта, информационните технологии и съобщенията, като справките в регистрите са безплатни.

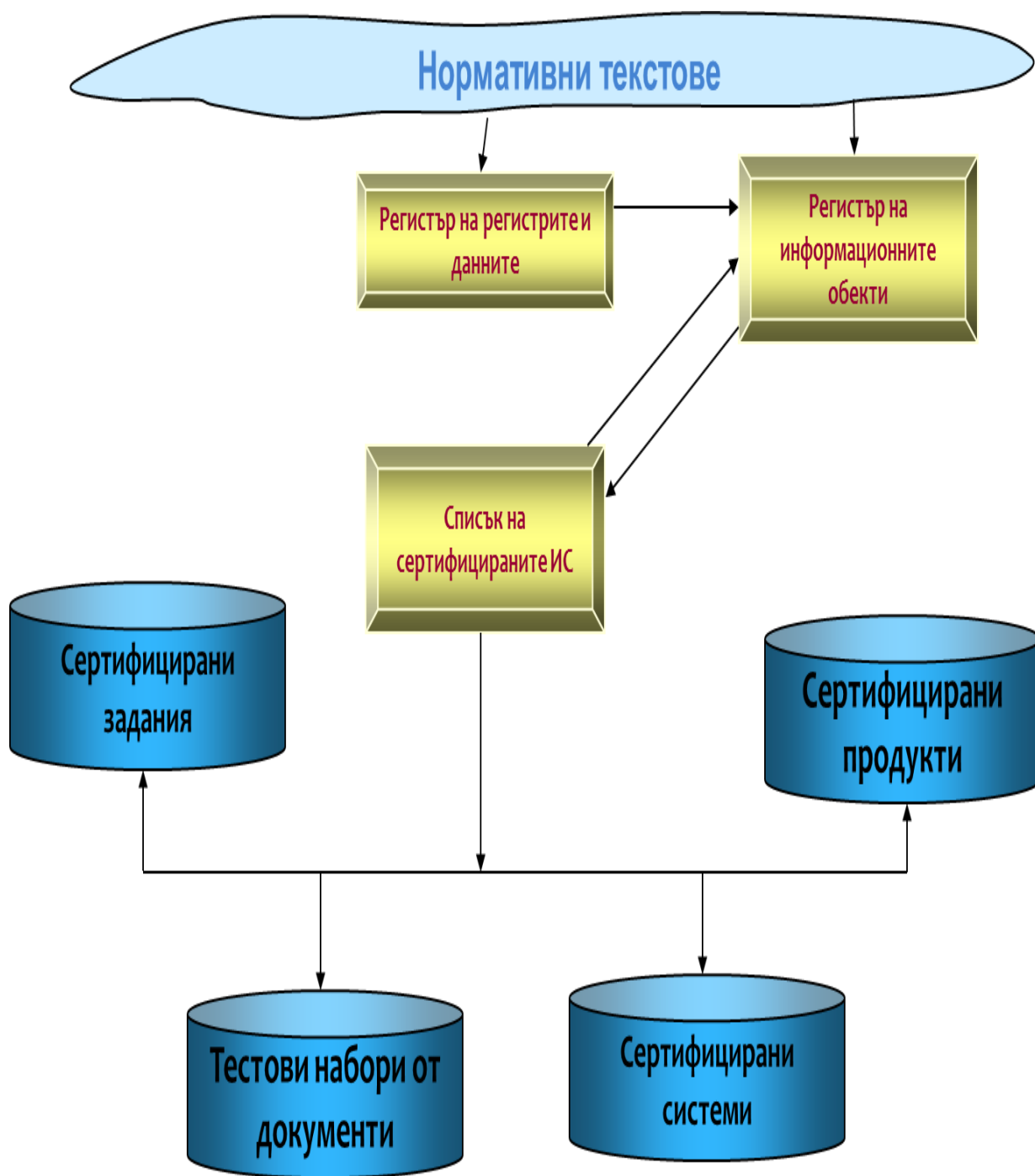
Национален модел на данните в администрацията



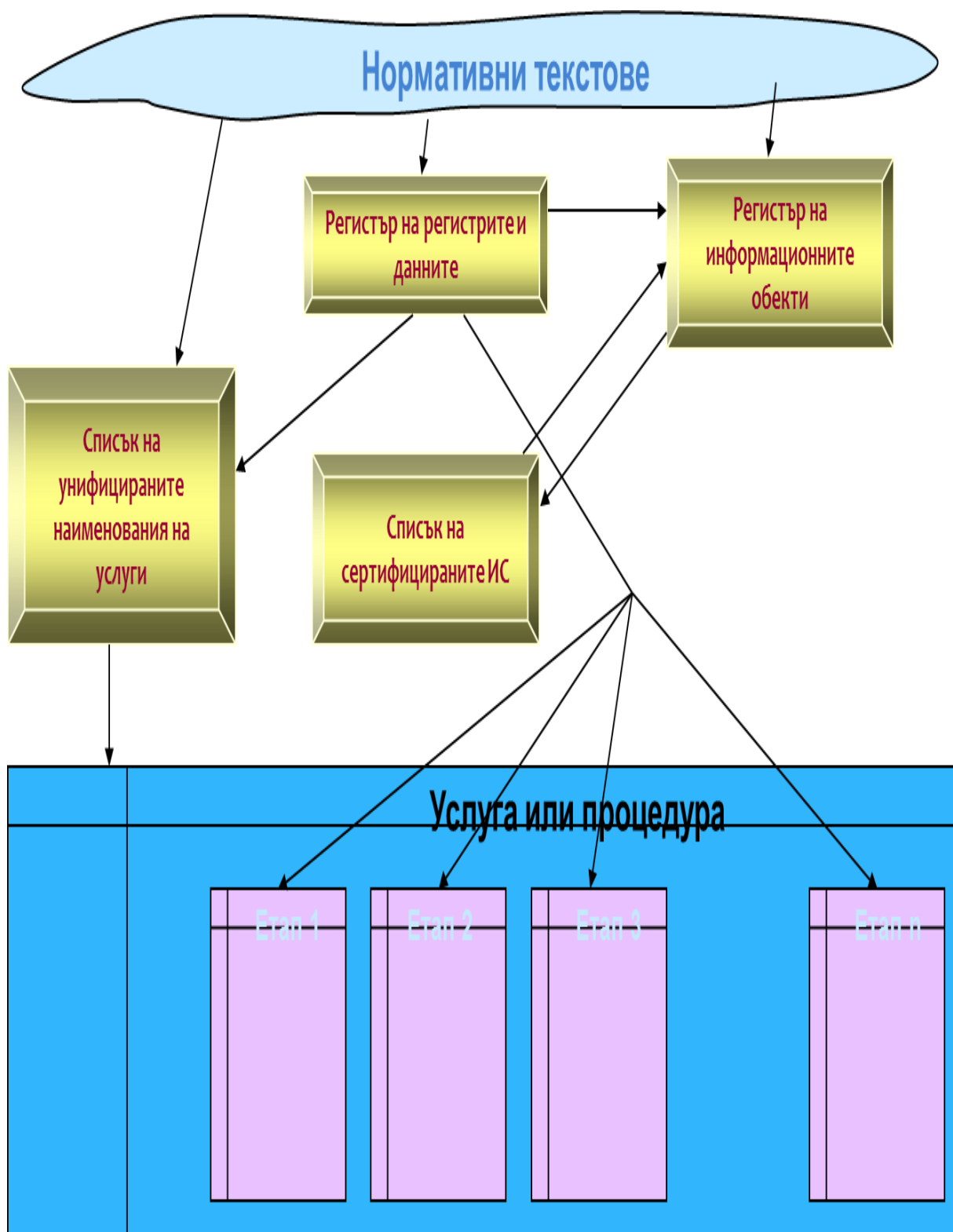
Фигура 4-13



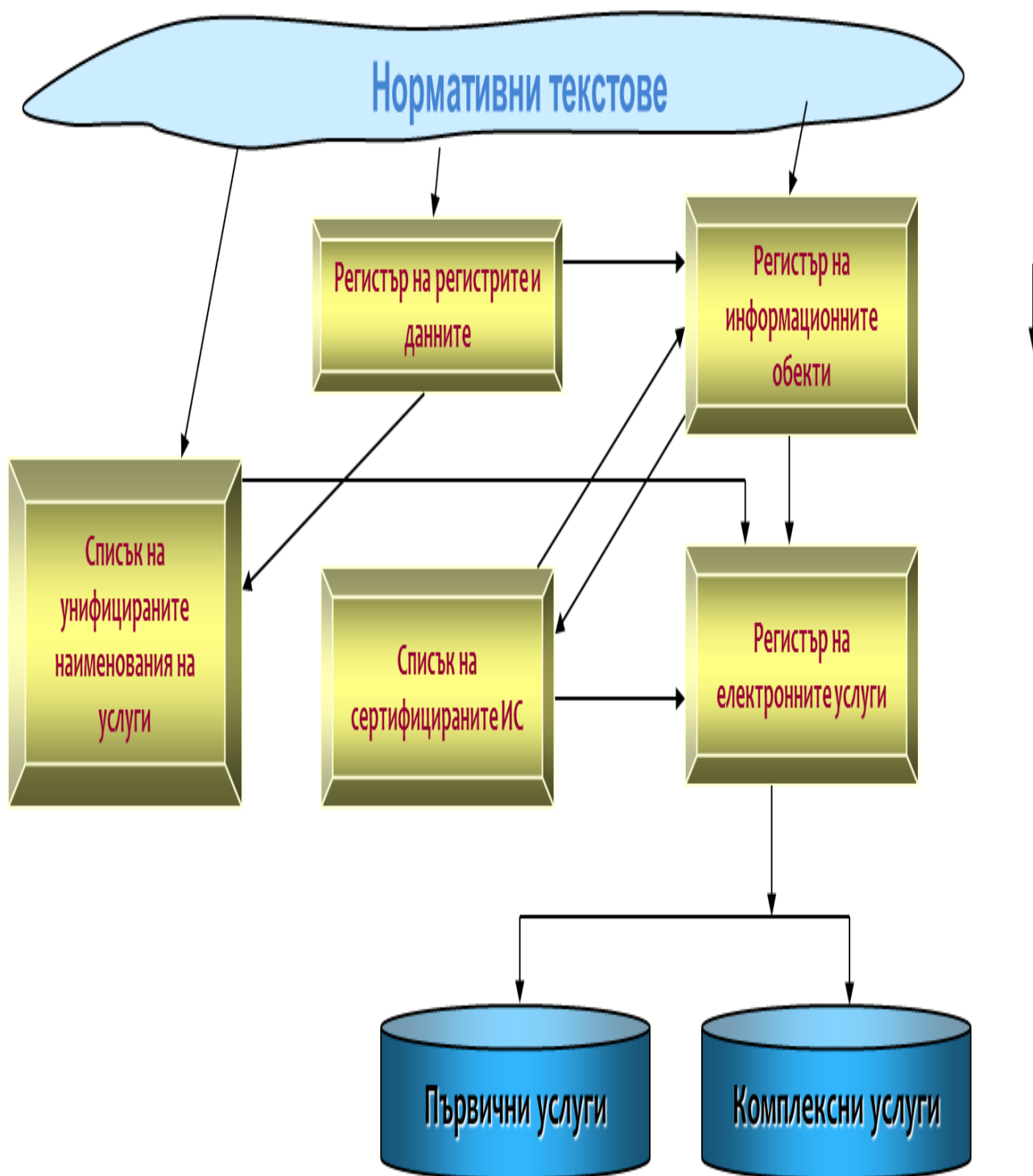
Фигура 4-14



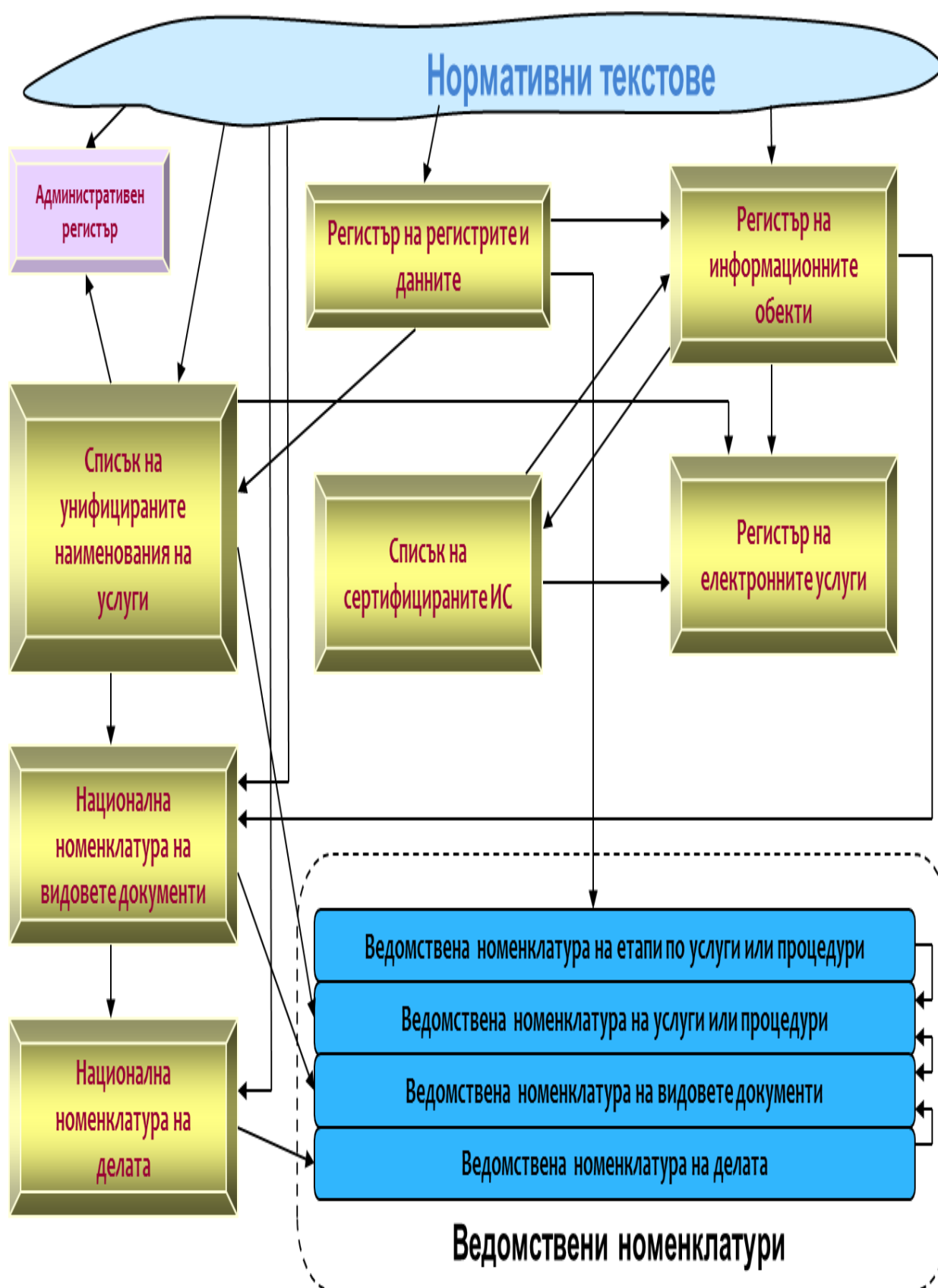
Фигура 4-15



Фигура 4-16



Фигура 4-17



Фигура 4-18

ГЛАВА 4.4

ЕДИННА СРЕДА ЗА ОБМЕН НА ЕЛЕКТРОННИ ДОКУМЕНТИ (ЕСОЕД)

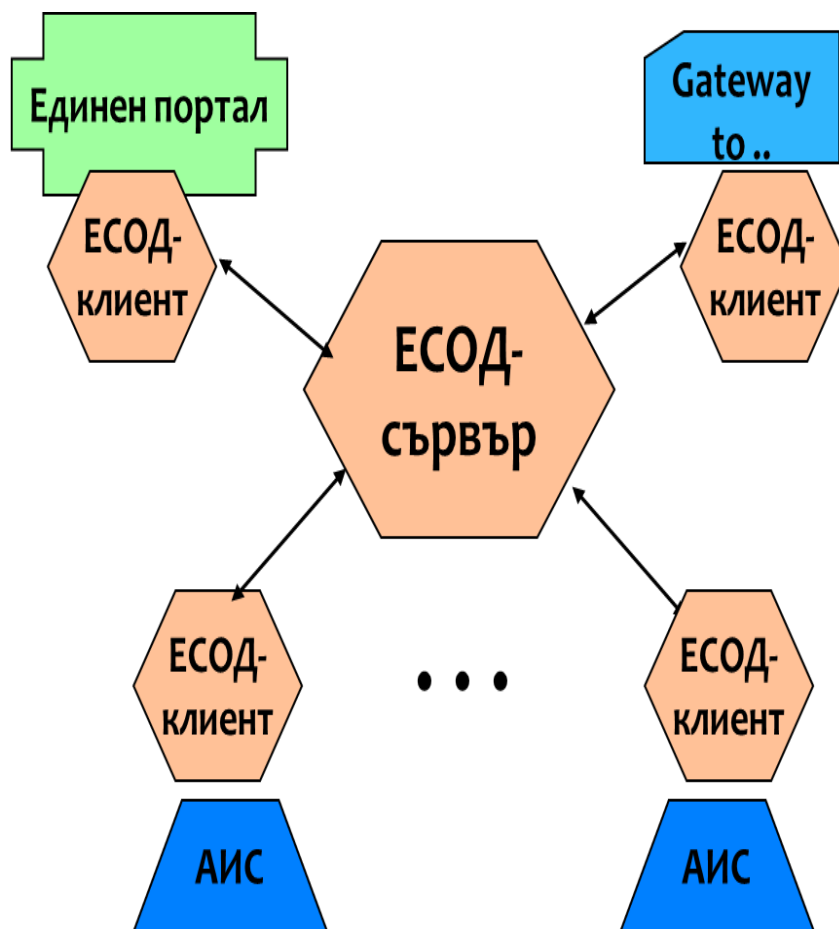
Нормативни основания

Законът за електронното управление предвижда всички вътрешни електронни административни услуги да се предоставят задължително чрез единната среда за обмен на електронни документи.

ЕСОЕД се изгражда и поддържа от министъра на транспорта, информационните технологии и съобщенията в съответствие с Наредба за изискванията към единната среда за обмен на електронни документи, приета от Министерския съвет с постановление № от и обнародвана в Държавен вестник брой.

Определение на ЕСОЕД

ЕСОЕД е управляема среда за сигурен стандартизиран обмен на документи, вписани в регистъра на информационните обекти, между лица, регистрирани за участие в обмена.



Фигура 4-19

Използване на ЕСОЕД

Посредством ЕСОЕД административните органи задължително предоставят вътрешни електронни административни услуги на:

- други административни органи,
- лица, осъществяващи публични функции;
- организации, предоставящи обществени услуги.

Чрез ЕСОЕД могат да се предоставят електронни административни услуги от административните органи, лицата, осъществяващи публични функции и организациите, предоставящи обществени услуги на граждани и организации.

Чрез ЕСОЕД единният портал за достъп до електронни административни услуги комуникира с информационните системи на администрациите за предоставяне на електронни административни услуги на гражданите и организациите.

Изисквания към ЕСОЕД

ЕСОЕД осигурява средства за сигурен обмен на електронни документи само между лица, регистрирани за участие в обмена.

Обменът в ЕСОЕД се осъществява въз основа на Интернет протоколи.

Ако посредством ЕСОЕД се налага да се обменят на неструктурирани документи, те се включват в съдържанието на структурирани електронни документи, регистрирани в регистъра на информационните обекти.

При обмен на електронни документи през ЕСОЕД всички участници са равнопоставени, т.е. при обработка на заявлението за вътрешна електронна административна услуга никой няма предимство или приоритет.

Архитектура на ЕСОЕД

Обменът на електронни документи между информационните системи на участниците в обмена чрез ЕСОЕД се извършва чрез комуникационен сървър. Връзката между информационните системи на участниците в обмена и комуникационния сървър се осъществява чрез специализирано програмно приложение за връзка – комуникационен клиент.

Комуникационният клиент се предоставя от Министъра на транспорта, информационните технологии и съобщенията безплатно за ползване от участниците в обмена.

Инсталационен пакет на комуникационния клиент ще може да бъде изтеглен от интернет-страниците на Министерството на транспорта, информационните технологии и съобщенията, заедно с подробно ръководство за инсталация и използване.

Протокол за обмен и спецификация на интерфейса

Протоколът за обмен на документи чрез ЕСОЕД се разработва от Министъра на транспорта, информационните технологии и съобщенията въз основа на спецификация на консорциума W3C - SOAP (Simple Object Access Protocol) версия 1.2 и следващите.

Протоколът за обмен на документи чрез ЕСОЕД ще бъде публикуван на Интернет-страницата на Министерството на транспорта, информационните технологии и съобщенията .

Спецификацията на интерфейса между информационните системи на участниците в обмена и комуникационния клиент ще бъде публикуван на интернет-страницата на Министерството на транспорта, информационните технологии и съобщенията за нуждите на разработчиците, които да го вградят в информационните системи на участниците в обмена.

ЕСОЕД и административните информационни системи

Преносът на електронен документ през ЕСОЕД се извършва между информационните системи на участниците в обмена.

Администрациите се включват към ЕСОЕД чрез своите административни информационни системи (АИС) по смисъла на Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите.

Една администрация може да се включи към ЕСОЕД с повече от една АИС, ако поддържа такива, или с повече от една регистрации на една АИС, ако това се налага за целите на обмена.

Пренос на електронен документ

Преносът на електронен документ между двама участници в обмена се извършва през комуникационния сървър в рамките на една процедура за обмен документ при следните условия:

- с една процедура за обмен се пренася само един електронен документ;
- документът, който се пренася, може да е и съставен и да съдържа в себе си неограничен брой други електронни документи, включително и неструктурирани.

Една и съща информационна система може да стартира няколко паралелни процедури за обмен.

Пренос на електронен документ

Преносът на електронен документ между двама участници в обмена се извършва през комуникационния сървър в рамките на една процедура за обмен документ при следните условия:

- с една процедура за обмен се пренася само един електронен документ;
- документът, който се пренася, може да е и съставен и да съдържа в себе си неограничен брой други електронни документи, включително и неструктурирани.

Една и съща информационна система може да стартира няколко паралелни процедури за обмен.

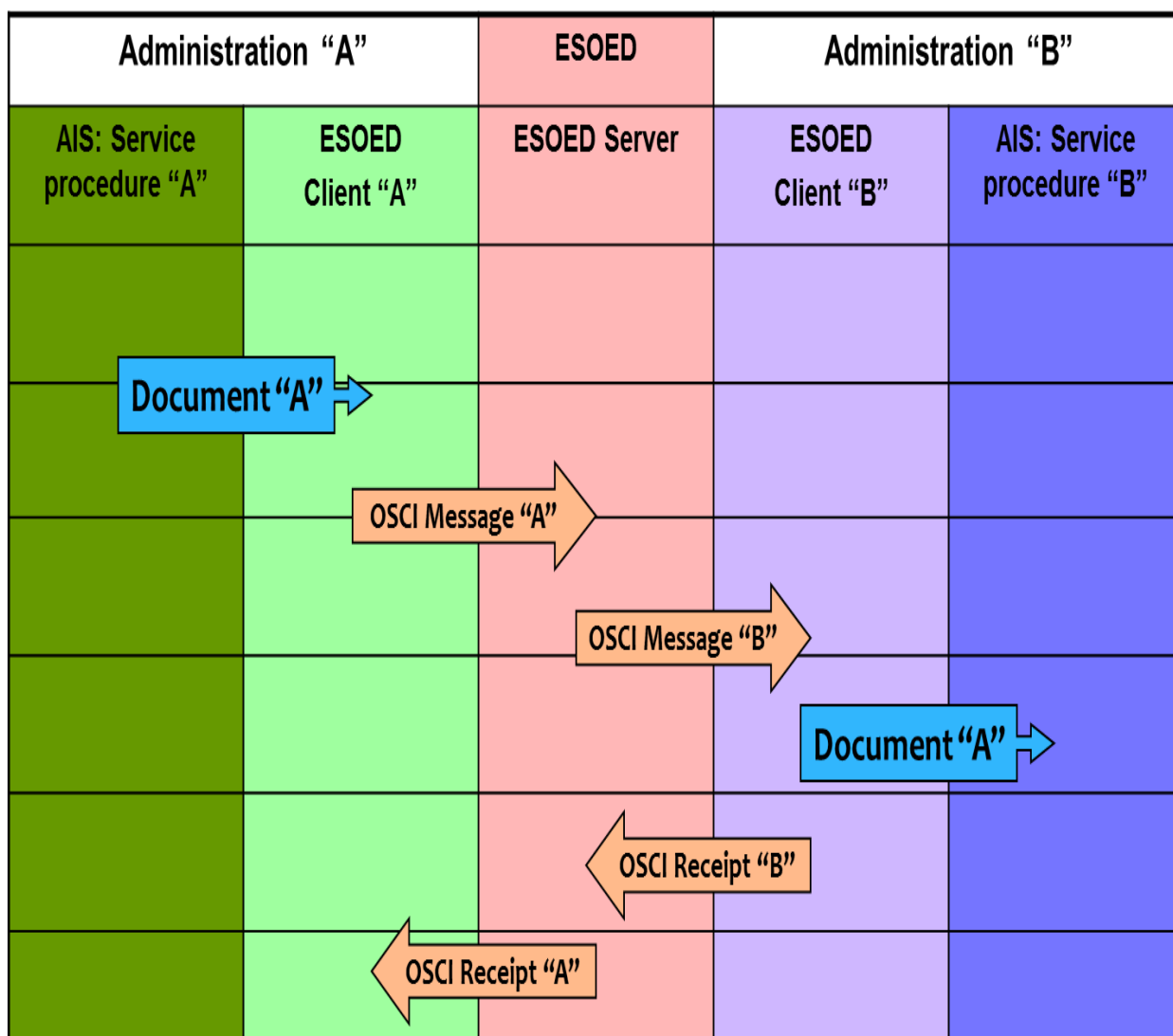
Процедура за обмен

Всяка процедура за обмен на документ се извършва на две сесии, както следва:

- сесия за обмен, при която комуникационният клиент на изпращащия участник изпраща съобщение до комуникационния сървър (ще я наричаме „първа” сесия);
- сесия за обмен, при която комуникационният сървър изпраща съобщение до комуникационния клиент на приемащия участник (ще я наричаме „втора” сесия).

Съобщенията съдържат пренасяния документ. Те се създават като видове електронни документи и се регистрират в регистъра на информационните обекти от Министъра на транспорта, информационните технологии и съобщенията .

Схема на изпълнение на двете сесии за обмен на документ



Фигура 4-20

Приключване на сесиите

Втората сесия приключва след връщане на съобщение за край на сесия от комуникационния клиент на получаващия участник до комуникационния сървър.

Първата сесията приключва след връщане на съобщение за край на сесия от комуникационния сървър до комуникационния клиент на изпращащия участник.

Съобщението по за край на първата сесия се генерира от комуникационния сървър след получаване на съобщението по за край на втората сесия.

Time out на втората сесия

Когато времето на реализация на втората сесията за обмен надхвърли максимално допустимото (time out), комуникационният сървър:

- прекратява изпълнението на сесията по обмен на съобщение;
- изпраща документа, съдържащ се в съобщението, на официалния електронен адрес на получаващата страна;
- връща на комуникационния клиент на изпращащия участник, съобщение за промяната в начина на пренос на документа от пренос през ЕСОЕД към пренос чрез електронна поща.

Невъзможност за изпращане

В случай, че комуникационният сървър не успее да изпрати документа на официалния електронен адрес на получаващата страна, той връща съобщение за това на комуникационния клиент инициирал сесията за обмен на документа се.

Комуникационният клиент уведомява информационната система на изпращащия участник за невъзможността за изпращането. Комуникационният сървър отхвърля всякакви по-нататъшни съобщения от комуникационния клиент на получаващата страна по прекратената съгласно сесия.

Time out на първата сесия

Когато времето на реализация на първата сесията за надхвърли максимално допустимото, комуникационният клиент на изпращащия участник:

- прекратява изпълнението на сесията за обмен на съобщение;
- съобщава на информационната система на изпращащия участник, че преносът е неуспешен.

Комуникационният клиент отхвърля всякакви съобщения от комуникационния сървър по прекратената сесия.

Идентификация на участниците в обмена

Участникът, изпращащ съобщение посредством сесия за обмен, се идентифицира със своя IP-адрес пред комуникационния сървър.

Участникът, който получава документ в процедура за обмен, се идентифицира от комуникационния сървър за целите на изпращането с уникален регистров идентификатор, създаден при регистрацията му в ЕСОЕД.

Пренос в криптирана форма

Съдържанието на съобщенията се пренася в криптирана форма за нуждите на обмена. Служебната информация в съобщенията не е криптирана и е със състав и организация на данните съгласно спецификацията на консорциума W3C - SOAP („Simple Object Access Protocol”) версия 1.2 и следващите.

Криптирането се осъществява чрез методи на асиметрична криптография посредством публичния ключ на участника - адресат на съобщението.

Всеки участник в обмена, чрез своя комуникационен клиент, включително и комуникационният сървър, подписва изпратените съобщения. Подписът се използва само за осигуряване на автентичност и интегритет на изпращаните съобщения за нуждите на обмена чрез комуникационния клиент, съответно комуникационния сървър.

Криптиране

Удостоверенията за публичен ключ, които използват участниците в обмена през ЕСОЕД за криптиране на съобщенията за нуждите на обмена, се издават от вътрешна инфраструктура на публичния ключ за всички администрации, изградена и поддържана от Министъра на транспорта, информационните технологии и съобщенията. Те се издават при регистрация на участник в обмена през ЕСОЕД списъка на участниците.

Удостоверение по предходната алинея се издава за комуникационния сървър при неговата служебна регистрация в списъка на участниците в ЕСОЕД от Министъра на транспорта, информационните технологии и съобщенията.

Проверки

Комуникационният сървър декриптира изпращаните до него съобщения и извършва проверка на пренесения документ в декриптираното съобщение за съответствие с регистрацията му като вид документ в регистъра на информационните обекти. Проверката се извършва само по отношение на съответствие на структурата на данните и за нежелан софтуер.

При неуспешна проверка комуникационният сървър връща съобщение на участника, изпратил документа, че получаването на документа не се потвърждава, съгласно Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите.

Участници в ЕСОЕД

Министърът на транспорта, информационните технологии и съобщенията води списък на участниците в ЕСОЕД.

Списъкът на участниците в ЕСОЕД е база от данни, изградена в АИС на ЕСОЕД, съдържаща формализирани описания на участниците в ЕСОЕД, във връзка с обмена на документи между тях.

Комуникационният сървър има директен достъп до данните в списъка.

Списък на участниците

В списъка се вписват следните данни:

- данни, идентифициращи администрацията, лицето, осъществяващо публични функции, организацията, предоставяща обществени услуги или получателя на електронни административни услуги;
- наименование на участника;
- IP-адрес - интернет-адреса, от който информационната система на участника изпраща или получава съобщения;
- предоставяне на услуги - отбелязва се, че участникът предоставя електронни услуги посредством ЕСОД;
- валидност на участие в обмена, със стойности „разрешен обмен” или „забранен обмен”.

За едно лице могат да се впишат повече от един участник в ЕСОД, за които се вписват различни наименования и IP-адреси.

Регистрация на процедурите по обмен на документи

Всяка процедура за обмен на документ през ЕСОЕД се регистрира автоматично. На регистрация не подлежи съдържанието на пренасяните документи през ЕСОЕД. Регистрираните данни не подлежат на изтриване и корекция и се съхраняват безсрочно.

За всеки осъществен достъп до данните по регистрацията автоматично се регистрират следните данни:

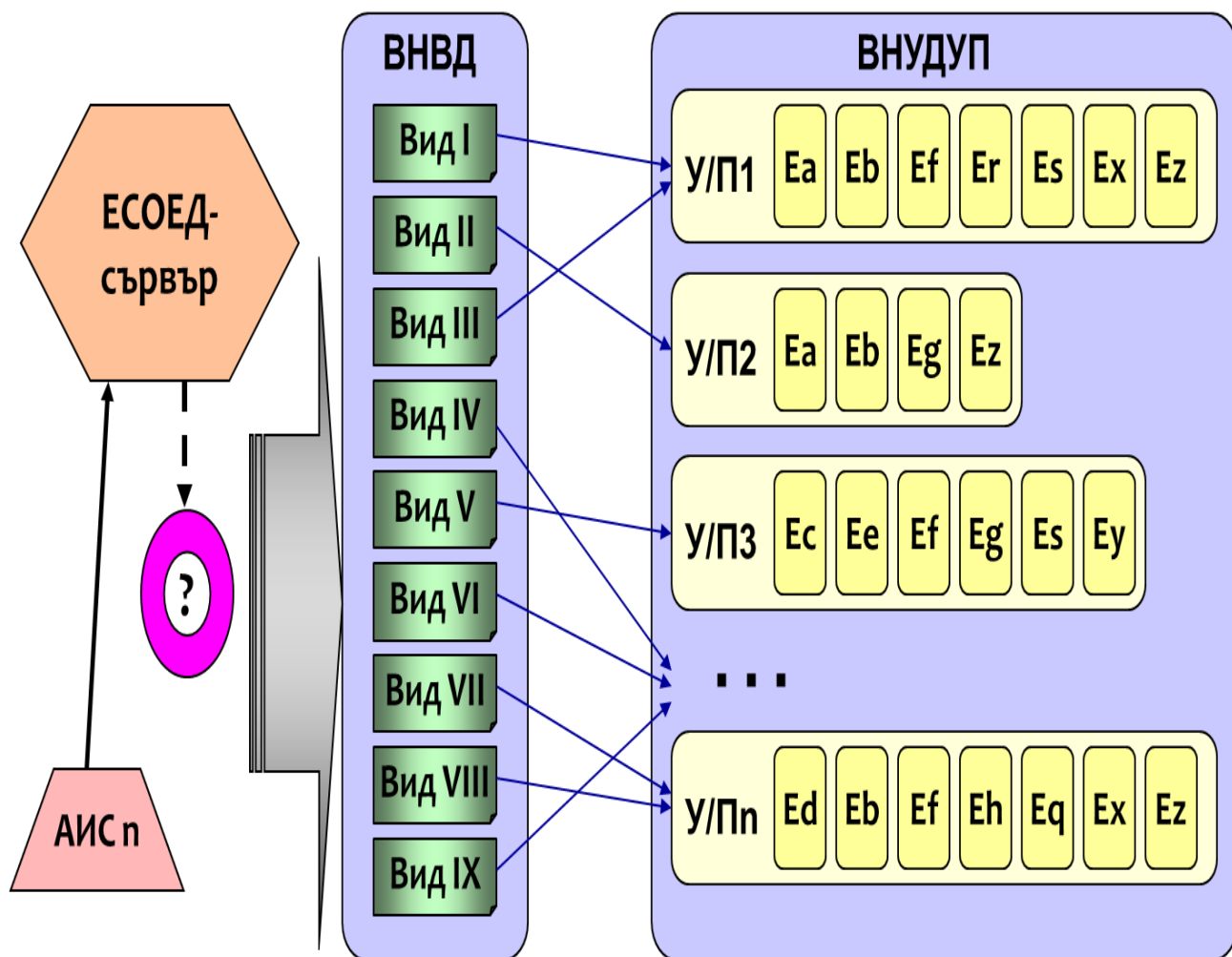
- - данни, идентифициращи чрез АИС лицето, осъществило достъпа;
- - време на влизане в режим на достъп;
- - време на излизане от режим на достъп;
- - вид на данните – до декриптираните и проверявани документи или до данните за процедурите за обмен на документ през ЕСОЕД.

Нива на адресация при обмен през ЕСОЕД

Адресация на ниво “съобщение”- чрез IP

Адресация на ниво “пренос на документ”- УРИ на регистрация на участник

Адресация на ниво услуга или процедура- УРИ на регистрация на документ-заявление

ЕСОЕД-обмена през погледа на потребителите

Фигура 4-21

Свързване на администрация към ЕСОЕД

1. Администрацията се договаря с доставчика на АИС да извърши включването в ЕСОЕД;
2. Администрацията се регистрира като участник в ЕСОЕД;
3. Администрацията сваля от сайта на МТИТС инсталационен комплект на Комуникационния клиент и го инсталира на свой компютър;
4. Администрацията извършва тест на свързаността с ЕСОЕД, като заявява услуга за получаване на извлечение от Списъка на участниците, като използва симулатор на АИС, който се доставя заедно с КК;
5. Доставчикът на АИС изучава документацията на интерфейса между КК и АИС, публикуван на сайта на МТИТС и доразвива своята АИС, за да се интегрира с КК;
6. Доставчикът интегрира своята АИС с ЕСОЕД, като съблюдава спецификацията на интерфейса за интеграция;
7. Доставчикът на АИС демонстрира свързаност с ЕСОЕД, като през АИС подава заявка за услугата за извлечение от Списъка на участниците и с АИС получава отговора по заявката;

8. Всякакви обструкции на доставчика за неработоспособност на АИС се проверяват с тест чрез симулатора на АИС

Необходимост от свързаност към ЕСОЕД

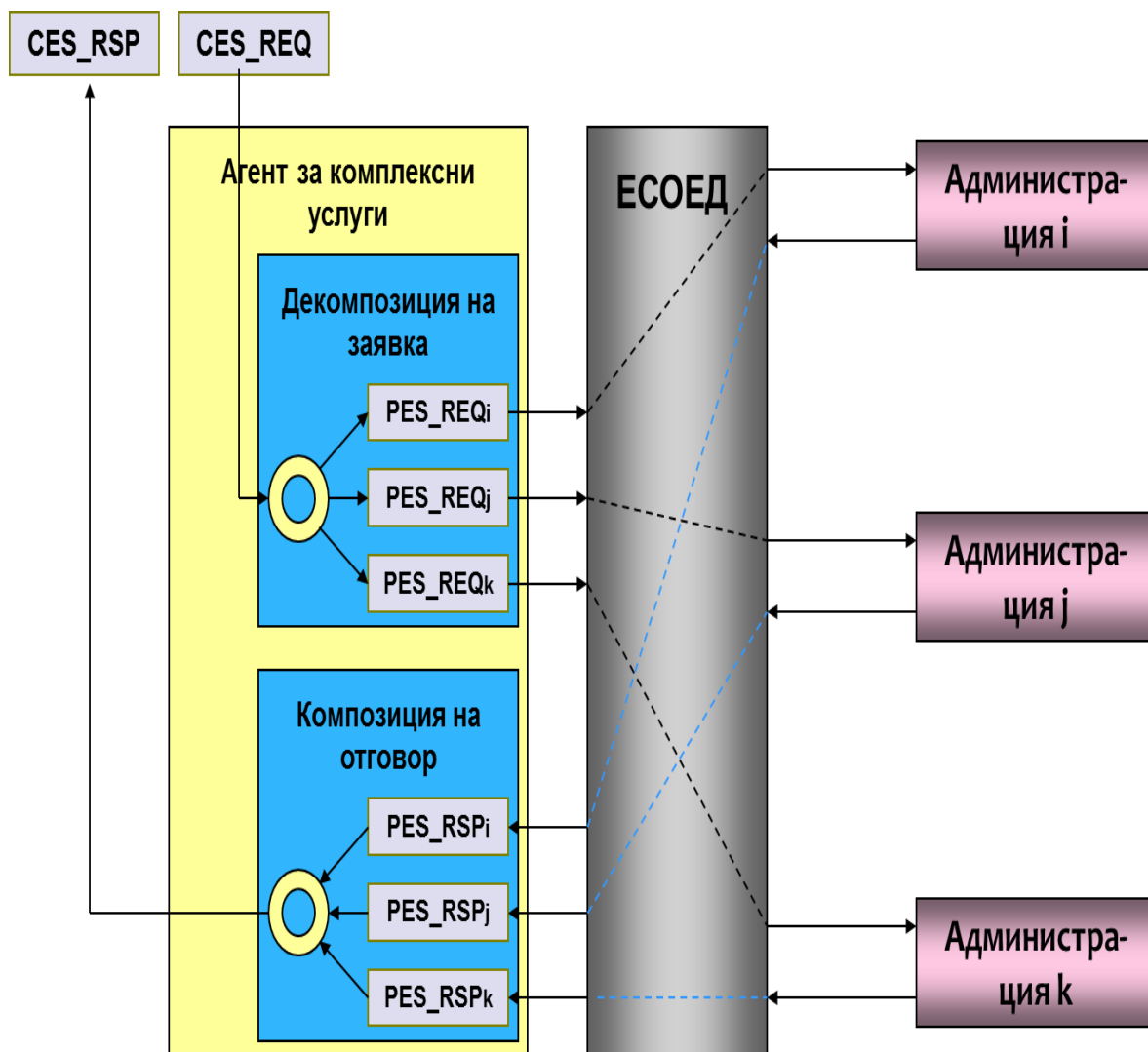
Без ЕСОЕД е невъзможно да се извършва идентификация на физически и на юридически лица

Без ЕСОЕД може да се предоставят само анонимни услуги

За да се извършва идентификация на физически и на юридически лица е необходимо администраторите на данни за тях също да са свързани към ЕСОЕД и да предоставят необходимите услуги

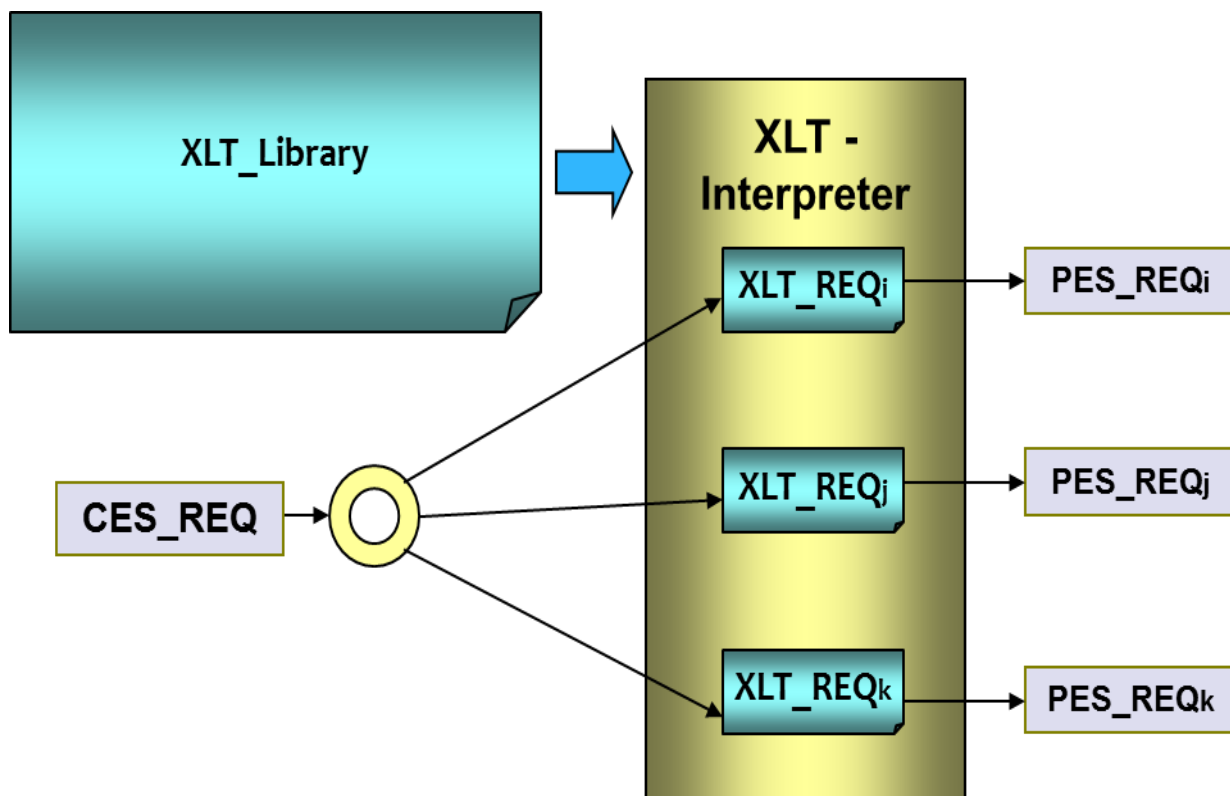
През ЕСОЕД ще се осъществява целият обмен на документи между администрациите

Изпълнение на комплексна услуга



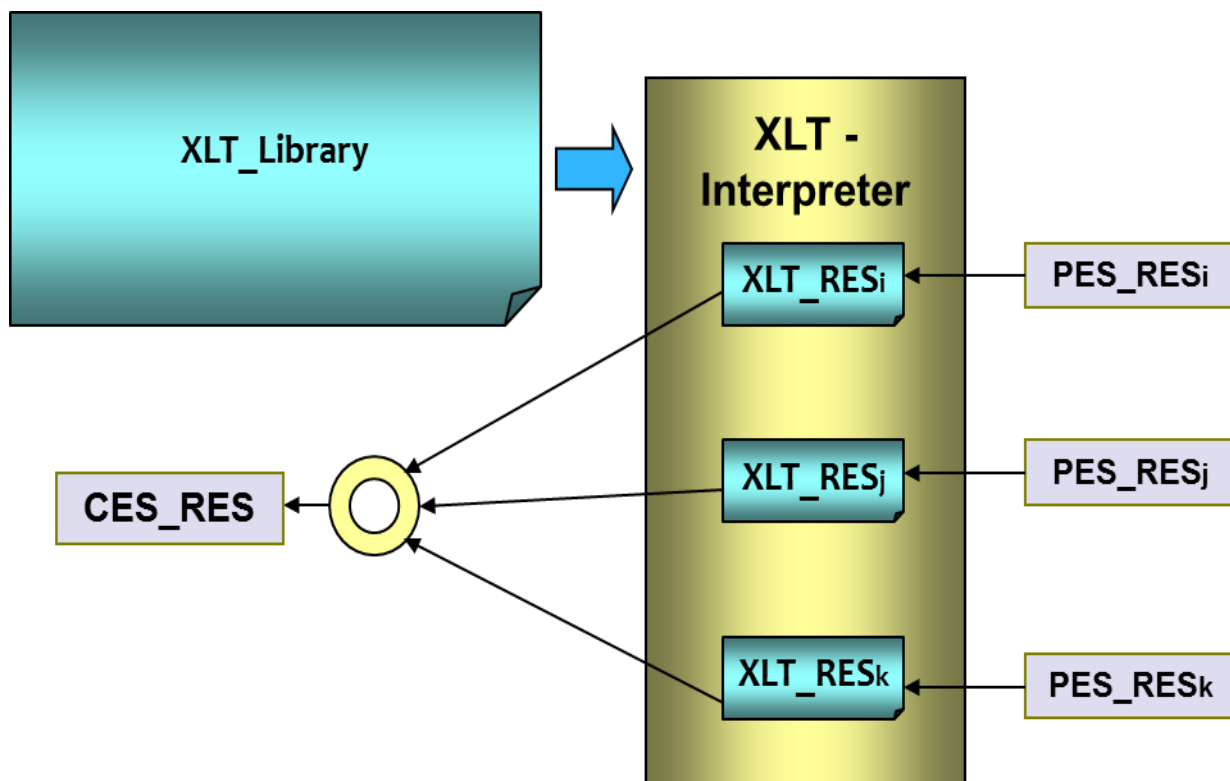
Фигура 4-22

Декомпозиция на заявки



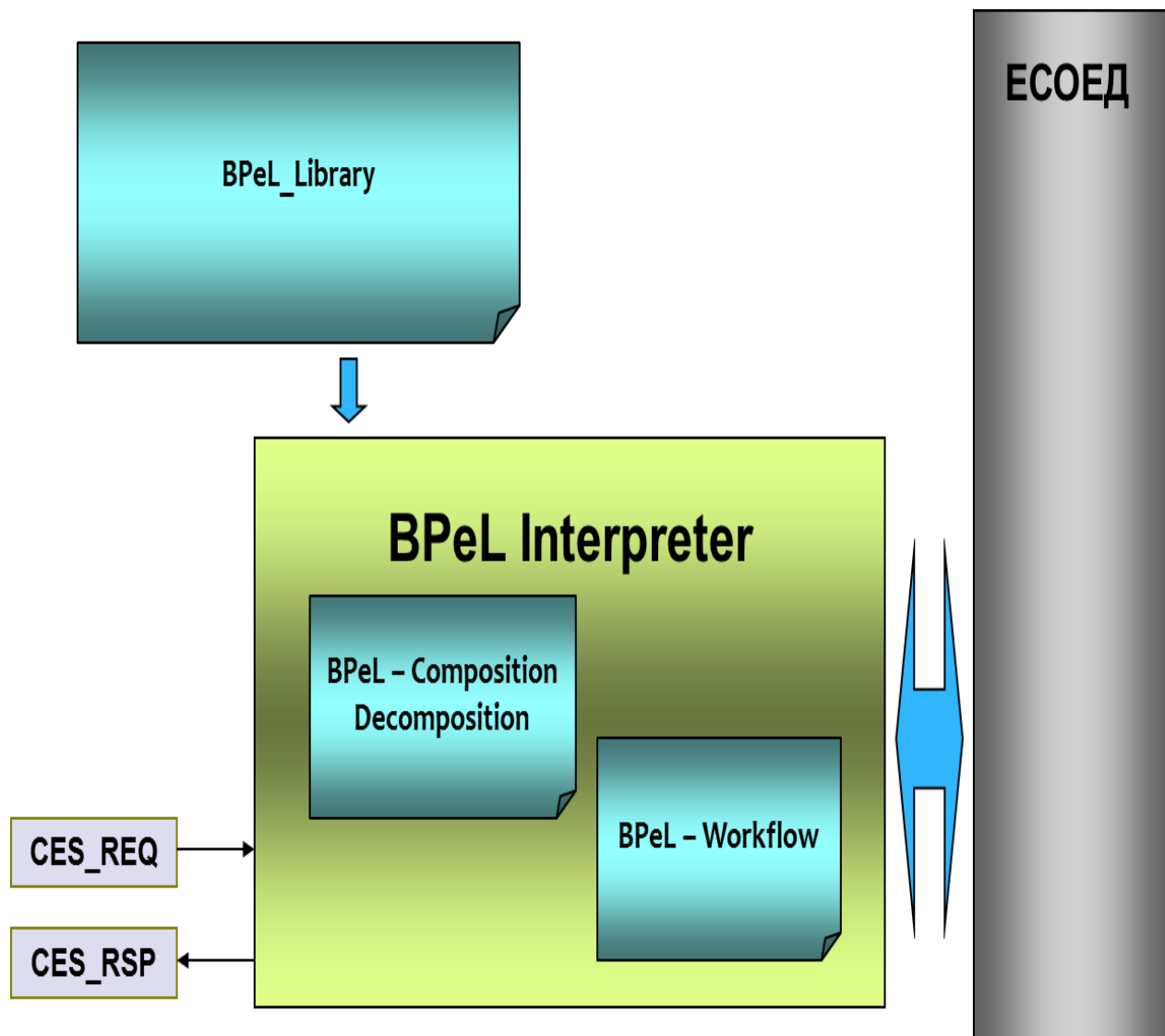
Фигура 4-23

Декомпозиция на отговори



Фигура 4-24

Управление изпълнението на комплексна услуга



Фигура 4-25

ГЛАВА 4.5

СПИСЪЦИ НА АКРЕДИТИРАНИТЕ ЛИЦА И СЕРТИФИЦИРАНИТЕ СИСТЕМИ

Законова регламентация

1. В списъците на акредитираните лица и на сертифицираните системи и продукти се вписва обстоятелства относно лицата, акредитирани за сертифициране на информационни системи, съответно относно сертифицираните информационни системи и продукти.

2. Списъците се водят от Министъра на транспорта, информационните технологии и съобщенията чрез овластени от него лица.

3. Списъците са бази от данни, управлявани от информационна система, съдържаща описанията на състава и организацията на данните.

4. В списъците се поддържа история на вписванията.

5. Списъкът на лицата, акредитирани за сертифициране на информационни системи се състои от един раздел – „Акредитирани лица”, в който се вписват обстоятелствата относно тези лица.

6. В списъка на лицата, акредитирани за сертифициране на информационни системи се вписват следните обстоятелства:

- уникален идентификатор, име, съответно наименование на заявителя;
- уникален идентификатор, име, телефон и адрес на електронна поща на представляващите лица;
- срок на валидност на акредитацията;
- дата на първоначална акредитация;
- основание за спиране или отнемане на акредитацията.

7. В списъка на сертифицираните информационни системи се вписват следните видове обекти:

- обекти от вид „сертифицирана система”;
- обекти от вид „сертифицирано приложение”;
- обекти от вид „сертифицирано задание”;
- обекти от вид „тестов набор от документи”.

Общ вид

Списък на акредитираните лица и списък на сертифицираните системи и продукти

1 Списък на акредитираните лица и списък на сертифицираните системи и продукти

Начална страница | Нормативна база | Списък на акредитираните лица | Списък на сертифицираните информационни системи ▼

Списък на акредитираните лица

Списък на сертифицираните информационни системи

- Списък на сертифицираните системи
- Списък на сертифицираните приложения
- Списък на сертифицираните задания
- Списък на тестовите набори от документи

Нормативна база

Други сайтове

- Оперативна съвместимост на приложения, свързани с електронното правителство
- Национален регистър на стандартите

Начало

Законът за електронното управление, влязъл в сила на 12.06.2008 г., урежда дейността на административните органи при работа с електронни документи, предоставянето на административни услуги по електронен път и обмена на електронни документи между административните органи.

В своята четвърта глава Законът регламентира изискванията за постигане на оперативна съвместимост в информационните системи на административните органи и посочва държавния орган, отговорен за разработването и провеждането на политиката в тези области, включително осъществяването на съответния контрол – Държавната агенция за информационни технологии и съобщения.

Съгласно Закона за електронното управление, Националната рамка за оперативна съвместимост и Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност, административните информационни системи взаимодействат в условията на т.н. „активна оперативна съвместимост“, която се осъществява чрез комплекс от мерки:

- а) спазване на определена съвкупност от международно приети стандарти;
- б) изграждане на спомагателни инструменти, като регистри, преносна среда и т.н.;
- в) сертифициране на административните информационни системи за съответствие с правилата и стандартите за оперативна съвместимост, регламентирани в Наредбата.

Настоящите Списъци на акредитираните лица и на сертифицираните системи и продукти са разработени в съответствие с чл. 58 ал. 1 и 2 на Закона за електронното управление, глава седма от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност и са предназначени за разработчиците на информационни системи и специалисти в областта на информационни технологии.

Фигура 4-26

ЧАСТ 5

СТРУКТУРА И ФУНКЦИОНАЛНОСТИ НА АДМИНИСТРАТИВНА ИНФОРМАЦИОННА СИСТЕМА (АИС)

ГЛАВА 5.1

АДМИНИСТРАЦИЯТА КАТО ОБЕКТ НА АВТОМАТИЗАЦИЯ. ОБЩА СХЕМА НА ВЪТРЕШНАТА АРХИТЕКТУРА НА АДМИНИСТРАТИВНАТА ИНФОРМАЦИОННА СИСТЕМА

Администрацията като обект на автоматизация

Административният орган извършва многобройни и разнообразни дейности. Главната особеност в това е, че:

- всички тези дейности са регламентирани от нормативни документи;
- всички тези дейности и процедурите по тяхната реализация трябва да са унифицирани и еднотипни, независимо от вида на административния орган, отрасъла, размера, географските, икономически и демографски особености.

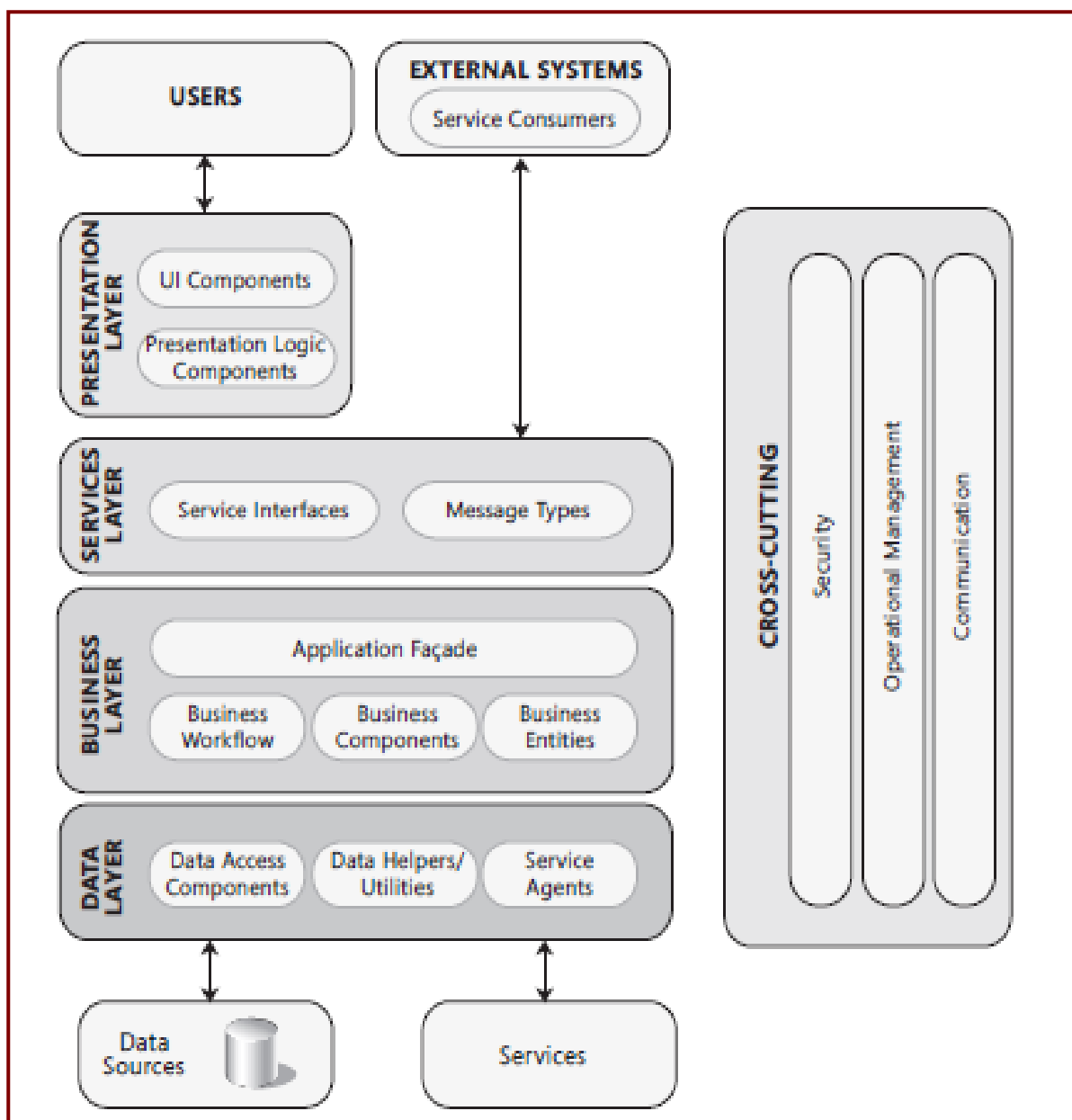
Така че, можем да говорим за „административен орган” (типизиран обект) като обект на автоматизация. При това, на преден план неминуемо са проблемите, свързани с интеграцията и оптимизацията на взаимодействието на различните модули на административната система, занимаващи се с разнообразните дейности: стопански, социални, инфраструктурни и пр.

Важен въпрос при това е унификацията и формализацията на данните, тъй като едни и същи данни се използват в различни системи, посочени по-горе. Това поставя въпроса за оптимизация на процесите по набиране, съхраняване, обработка и предаване на данните (всъщност, на едни и същи данни). При интеграция на системите би могло да се отиде към съхраняване на едни и същи данни на едно място, независимо от това, на какви системи ще се предоставят за обработка.

Обща схема на вътрешната архитектура на административната информационна система

Общата схема на вътрешната архитектура на административната информационна система (АИС) ще бъде получена вследствие на оценката на взаимодействието на три референтни схеми:

Референтния модел на приложната информационна архитектура.



Фигура 5-1

Този модел е представен от четири слоя:

а) презентационният слой осигурява „он-лайн” достъпа на потребителите до ресурсите и услугите на системата. Той съдържа потребителския интерфейс и управлява взаимодействието с потребителите. В допълнение към компонентите, които организират обмена, включва процедури за контрол на достъпа и представянето на данните;

б) сервизен слой (или слой на услугите) – тъй като приложните функционалности се предоставят като услуги, в модерните архитектури самите сервизни функционалности се отделят като слой. В слоя на услугите се дефинират и внедряват конвенциите за обмен на данни и сервизните интерфейси. Една от най-важните концепции е, че услугата никога не представя същността на вътрешните процеси или на работните компоненти, използвани от приложението. В частност, гарантира се, че данновите формати няма да преминат от съответния слой през бизнес слоя към услугите;

в) бизнес слоя включва обикновено следното:

- т.н. „приложна фасада”, т.е. компонент, който поддържа опростен интерфейс към компонентите на работните процеси, често чрез комбиниране на няколко бизнес-операции в една операция. Това прави бизнес-логиката на процесите по лесна за използване и намалява взаимозависимостите между процесите, тъй като за потребителите, извикващи услугата или процедурата, не е необходимо да са запознати с подробностите за компонентите на работните процеси и за връзките между тях;
- т.н. „компоненти на бизнес-логиката” – бизнес логиката се определя като логика на всяко припожение, която засяга извличането, обработката, трансформацията и управлението на данните в приложението; прилагането на бизнес-правила и политики; както и осигуряването на съгласуваността и валидността на тези данни. За да се максимизира възможността за повторна употреба на работните процеси, компонентите на бизнес-логиката не трябва да съдържат специфични елементи на бизнес-поведение.

От своя страна, компонентите на бизнес логиката могат да бъдат разделени на следните две категории:

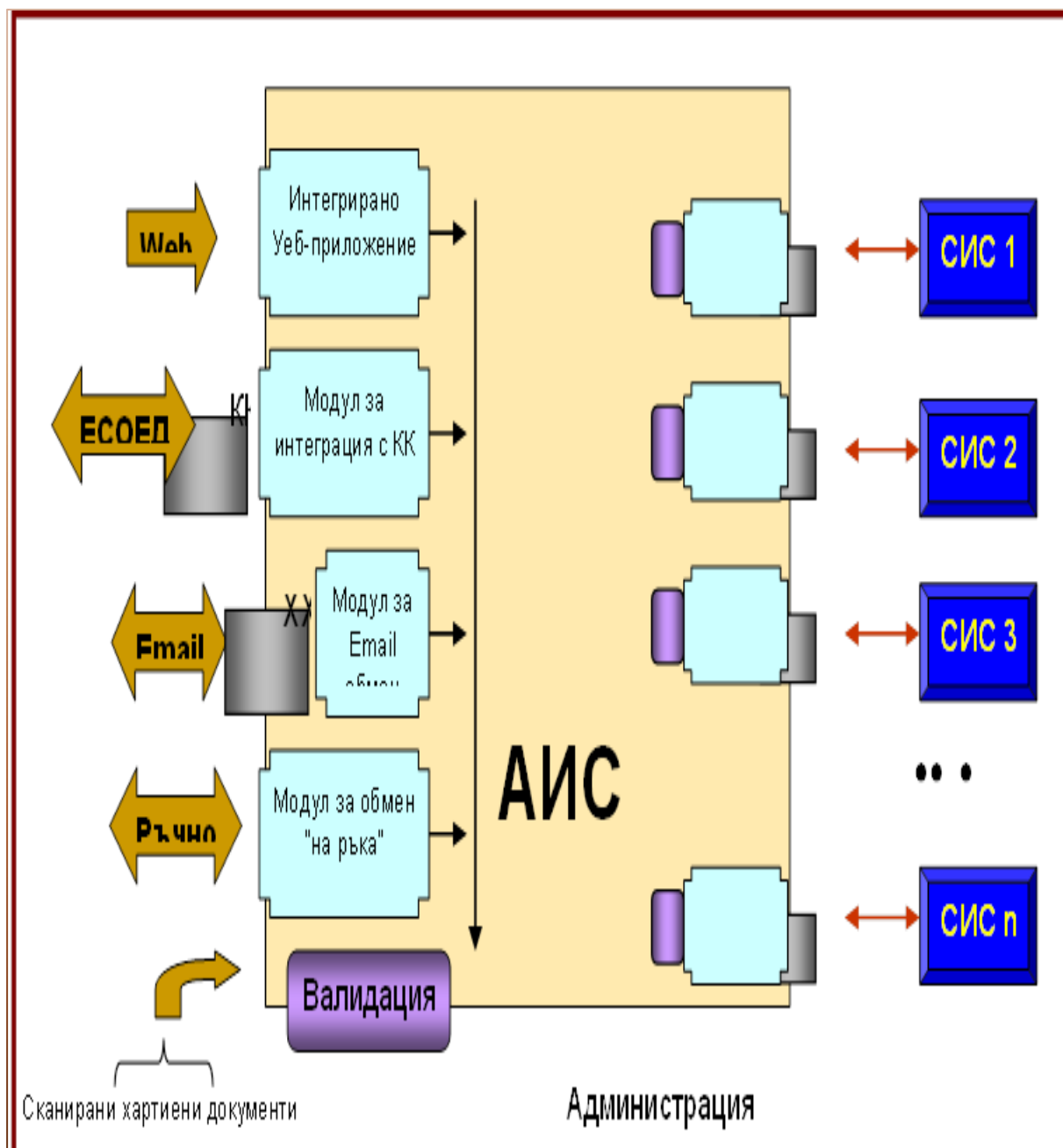
- компоненти на работните потоци – те получават от потребителския интерфейс данни за изискванията на потребителя и ги предават към управлението на работните процеси. Тези компоненти се изпозват при координиране на сложни многостъпкови работни процеси;
- компоненти на бизнес единиците – бизнес единиците (или по-общо, бизнес обектите) свързват бизнес логиката и необходимите данни, като представят реалните елементи на работните процеси (такива, като поръчка, клиент и т.н.) в рамките на приложението. Те съхраняват стойностите на данните и ги представят като определени свойства; предоставят програмируем достъп до бизнес данни и свързаната с тях функционалност. Бизнес елементите също така служат за валидиране на данните, като осигуряват последователност на бизнес логиката и изпълнение на съответните бизнес правила.

г) данновият слой в общия случай включва следните компоненти:

- т.н. „компоненти за достъп до данните” – съдържат абстрактно описание на логиката за достъп до подразбиращите се хранилища на данни. Те централизират общите функционалности на достъпа с цел да направят приложението по-лесно за конфигуриране и управление. Някои рамки за достъп могат да изискват от разработчика да дефинира и приложи обща логика за достъп до данните в отделна помощна програма или модул от компоненти. Други рамки, включително т.н. „Object/Relational Mapping (O/RM) frameworks” прилагат тези компоненти автоматизирано, силно намалявайки кода за достъп, който разработчикът трябва да напише;
- т.н. „сервизни агенти” – когато бизнес компонентът трябва да получи достъп до данни, предоставяни от външна услуга, има нужда да се приложи код за управление на семантиката на комуникацията с тази

конкретна услуга. Сервизните агенти прилагат компоненти за достъп до данните, които изолират други повиквания на услуги от конкретното приложение и предлагат допълнителни услуги, като кеширане, „оф-лайн“-поддържане и базово сравняване на форматите на данните, които услугата предлага, с форматите, които приложението изисква.

Функционалната схема на АИС



Фигура 5-2

Тази функционална схема показва обединяващото или средищно положение на административната информационна система (АИС) и нейните интерфейси с „външната среда“ и с другите информационни системи на административното звено. Тези интерфейси се реализират чрез специализирани приложения, интегрирани в АИС:

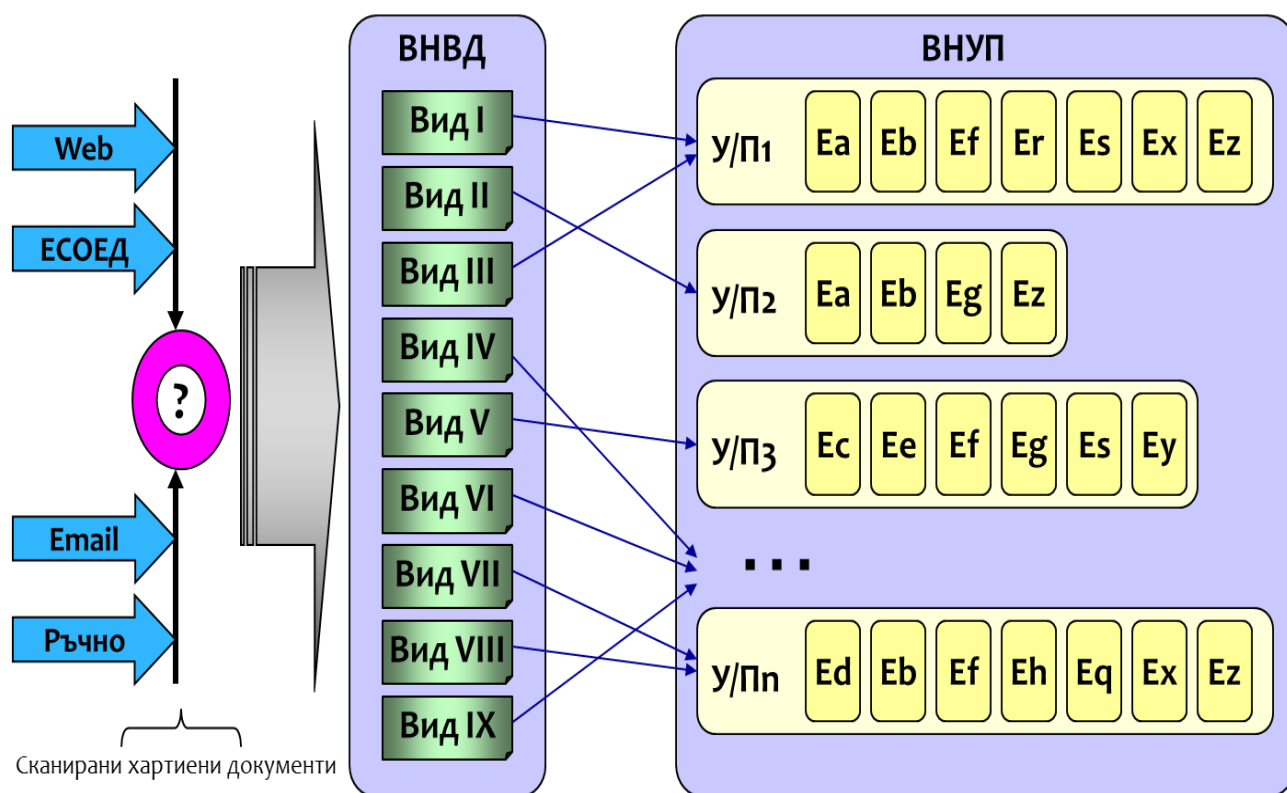
а) за връзка с външните източници на информация:

- интегрирано Уеб-приложение;
- модул за интеграция с Комуникационния клиент (КК) на Единната среда за обмен на електронни документи (ЕСОЕД);
- модул за електронна поща;
- модул за въвеждане на информация, съхранявана на магнитни и други външни носители.

Всички тези модули взаимодействат с интегрирано в АИС приложение за валидация.

б) интерфейсни модули за връзка с другите информационни системи на общинската администрация – за тях в наредбите към Закона за електронно управление не съществува специфична регламентация. За осигуряване на единообразие се препоръчва обменът да става чрез XML-съобщения без ограничения към тяхното съдържание.

Схема на задействане на процедурите в АИС



Фигура 5-3

Показани са четирите вида вход на електронни документи плюс входа на сканирани копия на хартиени документи. Документите са описани във Ведомствената номенклатура на видовете документи (ВНВД). Постъпването в системата на определен документ еднозначно задейства определена процедура от описаните във Ведомствената номенклатура на услугите и процедурите (ВНУП). Процедурите се състоят от унифицирани етапи. По този начин в АИС са дефинирани всички потоци работни процеси (workflows).

Вътрешна комуникационна инфраструктура

Един от ключовите фактори, които влияят върху проектирането на приложението (в частност, на разпределеното приложение), е начинът по който се проектира комуникационната инфраструктура на всяка една част от приложението. Компонентите могат да комуникират всеки един поотделно с всички останали, например, да се изпрати потребителско запитване към бизнес слоя и след това да се променят данните в данния слой.

Когато компонентите се намират на едно и също физическо ниво, често трябва да се разчита на директна връзка между тях. Когато, обаче, елементите са разположени на физически отделни сървъри и клиентски машини (което, всъщност, е по-честия сценарий), трябва да се осигури ефективна и надеждна комуникация между съставките на тези слоеве.

Като цяло, може да се избира между директна комуникация (т.н. метод за извикване на компонентите) и комуникация, базирана на съобщения. Предимствата на втората комуникация са многобройни – такива, като възможността за отделяне на компонентите един от друг.

Отделените компоненти не само повишават възможностите за поддръжка, но също така дават гъвкавост и възможност за лесна промяна на стратегията за разпространение в бъдеще.

От друга страна, комуникацията, базирана на съобщения, изисква да се решат редица въпроси, свързани с производителността, надеждността и информационната сигурност. Тази комуникация позволява да се предложи услуга чрез дефиниране на сервизен интерфейс. Потребителите могат да я извикват чрез подаване на XML-базирано съобщение през транспортен канал.

Извикването на услуга чрез предаване на съобщение е обикновено предназначено за отдалечени потребители, но този интерфейс може да ползва също така и локалните потребители.

При комуникацията, базирана на съобщения, ключов се явява въпроса за избор между синхронни и асинхронни стилове на общуване.

Синхронната комуникация е по-подходяща за сценарии, при които трябва да се гарантира реда, по който са получени повикванията, или когато трябва да се изчака връщане на потвърждение за повикването.

Асинхронната комуникация е по-подходяща за сценарии, при които възможността за отговор е много важна, но не може да се гарантира, че обектът ще бъде на разположение.

При избора на синхронна или асинхронна комуникация трябва да се има предвид следното:

- за постигане на максимална ефективност, слабо свързаните или минимизирани системи безусловно трябва да използват асинхронен модел на комуникация. Ако някои потребители могат да извършват само синхронни повиквания, трябва да се предвиди т.н. опаковане на асинхронните услуги в компоненти, които изпълняват синхронна комуникация с потребителя;
- в случаите, когато трябва да се гарантира последователността, в която се извършват операциите, или когато се използват операции, които зависят

от резултата на предшестващи операции, по-подходящ е синхронния модел;

- за извършване на асинхронни повиквания по време на процеса с използване на платформени функции, като „начало”, „край” или „обратно повикване” трябва да се използва асинхронния метод. За повиквания, които са извън процеса, такива като повиквания през физическите нива и граници, по-подходящи са асинхронните заявки за услуга.

ГЛАВА 5.2

СРЕДИЩНО ПОЛОЖЕНИЕ НА АДМИНИСТРАТИВНАТА ИНФОРМАЦИОННА СИСТЕМА.

Законът за електронното управление и наредбите към него

Законът за електронното управление и наредбите към него (преди всичко, Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите) дефинират административната информационна система (АИС) като основна система в административното звено – главен фактор за постигане на оперативна съвместимост и информационна сигурност на цялата информационна инфраструктура на съответната администрация. Останалите информационни системи биха могли да се групират в следните класове:

- информационни системи, обработващи стопански данни;
- информационни системи, осигуряващи поддръжка на регистри данни;
- специализирани информационни системи.

Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите дефинира АИС чрез:

- дефиниции на около 95 вида данни
- структури от тези данни
- функции по поддръжка на данните и структурите

Регламентът на Наредбата не ограничава АИС по отношение поддръжката на допълнителни данни, структури и функции по тяхната обработка. Ръководителите на администрациите осигуряват разработването и внедряването на административна информационна система (АИС) в ръководените от тях администрации.

АИС

АИС осигуряват поддържането и обработката на данните за оборота на електронни документи и документи на хартиен носител при предоставянето на административни услуги и изпълнение на административни процедури. Процедури са всички работни процеси в администрацията или между различните администрации, които включват вътрешен оборот на документи и които не представляват предоставяне на административни услуги и вътрешни електронни административни услуги, АИС поддържат и осигуряват съхранението на приетите и създаваните електронните документи за срок не по-малък от 20 години, по начин позволяващ възпроизвеждане на документите, без загуба на данни. Създаването на електронните документи в администрацията се осигурява със средствата на АИС или на външни програмни приложения.

Изградената АИС осигурява възможност за извеждане на всички данни, дефинирани в Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрацията, в документ, създаден от министъра на транспорта, информационните технологии и съобщенията и регистриран в регистъра на информационните обекти, съгласно чл. 43, ал. 2 от Закона за електронното управление.

АИС трябва да бъде сертифицирана за по реда на глава шеста от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

Всички данни за факти, процеси, както и всички служебни технически данни, необходими за осъществяването на административната дейност, се поддържат със средствата и в средата на АИС. Всяко създаване на данни в АИС се придружава с автоматичен запис за лицето, което е извършило създаването и времето на извършването му. Регистрираните данни не подлежат на корекция или унищожаване и се съхраняват за срок не по-малък от двадесет години.

АИС поддържа съвкупност от свързани данни – информационни обекти, върху които като неделими единици са приложими функции по създаване, унищожаване, управление на достъпа и други функции. Данните в състава на информационния обект се създават автоматично или на ръка в АИС.

За осигуряване на достъп и за управлението на достъпа до ресурсите на АИС, в нея се поддържат информационни обекти от вида „потребител”. За обслужване на съвместната поддръжка на електронни документи и документи на хартиен носител, в АИС се поддържат информационни обекти от вида „документ”. Минималният състав на данните в описанието на този вид информационен обект е определен в Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите. За изпълнение на процедурите за контрол на административната дейност, в АИС се поддържат информационни обекти от вида „задача”,

Регистрация на документи във всяка администрация се извършва в официален документен регистър, представляващ база от данни в състава на АИС. Официалният документен регистър се поддържа от упълномощени от ръководителя на администрацията лица. Ръководителят на администрацията извършва вписване на официалния документен регистър в регистъра на регистрите и данните.

В една АИС може да има повече от един официален документен регистър, като и в една администрация може да има повече от една АИС. В тези случаи всеки официален документен регистър се вписва в регистъра на регистрите и данните. Чрез АИС се осигурява воденето, съхранението и достъпа до официалния документен регистър по начин, който осигурява контрол върху пълнотата на извършените вписвания, включително поправяне на грешки на администрацията.

Общата класификационна схема за документи обхваща класификацията на всички видове документи определени в АИС, независимо дали документът е в електронна форма или на хартиен носител.

Преписката е набор от тематично свързани документи. В АИС се създава преписка по документ:

а) с който е заявена електронна административна услуга, включително когато самият документ е на хартиен носител, но изрично е заявено желание за предоставяне на услугата по електронен път;

б) с който се инициира процедура по обработка

Преписката се състои от три раздела – официален, вътрешен и контролен. Всеки от разделите се представя със списък от връзки към документи в АИС, класирани в съответния раздел.

Ведомствената номенклатура на видовете документи се поддържа със средствата на АИС. Услугите, включени в номенклатурата, са регистрирани в Списъка с унифицираните наименования на административните услуги.

За всяка услуга или процедура, чието изпълнение е започнало, се поддържа статус на изпълнение.

Ръководителят на администрацията осигурява интеграция на Уеб-базираното приложение за приемане на заявления за електронни административни услуги и документи, инициращи процедури, с внедрената в администрацията АИС. Електронни документи се получават от администрациите чрез електронна поща, когато това е допустимо от нормативен акт. Електронни документи се получават на физически носител, когато това е допустимо от нормативен акт.

Електронни документи могат да се получават и чрез Единната среда за обмен на електронни документи (ЕСОЕД), като за целта АИС поддържа модул за интеграция с комуникационния клиент (КК) на ЕСОЕД.

ГЛАВА 5.3

ИЗИСКВАНИЯ КЪМ УПРАВЛЕНИЕТО НА ЖИЗНЕНИЯ ЦИКЪЛ В АИС ПРИ СЪВМЕСТНО ИЗПОЛЗВАНЕ НА ЕЛЕКТРОННИ И ДОКУМЕНТИ НА ХАРТИЕН НОСИТЕЛ.

Предпоставка за пораждаване на нови изисквания:

Основна предпоставка е новият - електронният носител на съдържание, който започва да се използва в работата на администрацията, съгласно новия законов регламент на нейната дейност. Следствие от това е задължителното използване на Административна информационна система (АИС), като основно средство за съхранение и обработка на електронно съдържание. Тоест, появява се принципно нова инфраструктура за съхранение и обработка на съдържание, която е коренно различна от тази при хартиените документи.

Законът за електронното управление (ЗЕУ) и наредбите към него регламентират съвместното поддържане на двата типа инфраструктура и начините за извършване на административната дейност в тях.

АИС – основно средство за съхранение и обработка на информация

Член 7 на ЗЕУ задължава администрациите да поддържат всички данни, събирани, съхранявани и обработвани в процеса на извършване на административната дейност задължително в средата на АИС. Във връзка с това, администрациите се задължават да сканират всички получени хартиени документи и да осигуряват обработката на така снетото графично изображение само и изключително със средствата на АИС. След сканирането на получен хартиен документ, същият директно отива за съхранение в качеството му на физически носител - оригинал. Движение на този оригинален носител във връзка с обработка на съдържанието му не се предвижда. Движение на документи на хартиен носител се предвижда само за такива, чието сканиране технологично не е възможно.

Може да се каже, че от старите средства за управление на жизнения цикъл на документите, регламентирани в отменената Единна държавна система за деловодство (ЕДСД) остават само средствата за съпровождане на хартиения носител на съдържание, когато неговото използване е неминуемо.

Понятие за „документ”, поддържан с АИС

Дефиницията (описанието) на документ в АИС включва данни по създаване и обработка на съдържанието на документа, разглеждано като една от данните в него. При електронните документи съдържанието на документа са данни - файл в съответния формат, а при успешно сканираните хартиени документи - това е файл с неговото сканирано изображение.

Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите дефинира минимален състав на данните в описанието на документ в АИС. Това са данни за:

- получаването или създаването на документа;
- отразени становища по него;
- неговата регистрация;
- неговата класификация, включително и в схемата на организация на разположението на хартиените документи в хранилището;
- неговия престой в Номенклатурата на делата, която съгласно наредбата вече се нарича Номенклатура на схемите за съхранение на документите;
- други данни.

Регистрация на документи

Наредбата въвежда по-специален режим на регистрация на документи, който се извършва по схемата „един документ - един уникален регистров идентификатор (УРИ)”. Този режим е необходим за да се осигури уникална регистрация на документите не само за дадена администрация, а за всички администрации и комуникиращите с тях субекти. Във връзка с това е въведена нова конструкция на данните по регистрацията на документ - те общо се наричат „уникален регистров идентификатор” и той включва:

а) регистров индекс - всеки регистър, който се използва от администрациите с цел издаване на УРИ, подлежащ на използване от външни лица и организации трябва да бъде регистриран в Регистъра на регистрите и данните. Така дадена администрация получава за своя официален документен регистър уникален регистров индекс, с който нейният регистър е различим (по издавания УРИ) сред всички регистри, поддържани от администрациите;

б) пореден регистров номер - такъв пореден номер се издава от официален документен регистър при всяка регистрация на документ. За всяка календарна година, този номер започва да се генерира от „1”;

в) дата на получаване или подписване на документ - това е датата на получаване на входящ документ, или датата на подписване на изходящ документ.

Тоест, ако се регистрира получен документ в официален документен регистър, регистриран с регистров индекс „2178”, при генериран пореден номер „0341” на 21.02.2008, то издаденият УРИ ще бъде: 2178-0341-21.02.2008.

Самата регистрация на получавани документи се извършва също по нова схема. В зависимост от това, дали вече е издаден валиден УРИ за този документ от друг официален документен регистър, тази схема предвижда два варианта на регистрация, както следва:

- при наличие на валиден УРИ - за валиден УРИ се счита УРИ, издаден от регистриран в Регистъра на регистрите и данните документен регистър. Като УРИ на регистрация се вписва вече издадения валиден УРИ;
- при липса на валиден УРИ - генерира се УРИ от официалния документен регистър, в който се извършва регистрацията. Като дата на получаване или подписване се вписва датата на регистрация.

Регистрацията на електронни и документи на хартиен носител се извършва по абсолютно еднотипен начин. Уникалният регистров идентификатор се поддържа с АИС в състава на описанието на регистрирания документ. При регистрация на получени хартиени документи, локално генерираният УРИ се нанася собствено ръчно върху хартиеното изображение на получения документ.

Наредбата не ограничава поддържането с АИС само на един официален документен регистър.

Електронен вариант на преписка

АИС трябва да поддържа структурата „преписка” в качеството ѝ на набор от тематично свързани документи. Наредбата не регламентира точно как се поддържа структурата, като единствено налага изискването, за влизащите в преписка документи да се поддържа вътрешна номерация. Друга особеност на новия тип преписка е поддържането на три раздела в една и съща преписка. Това са:

а) официален раздел - в този раздел се поместват всички документи, които съгласно ЗЕУ трябва да се достъпни за потребител на електронна услуга през Интернет. Това са документите с които е заявена услуга и документи, които администрацията е издала или приела от други администрации във връзка с изпълнение на услугата;

б) вътрешен раздел - в този раздел се поместват всички документи, които администрацията е създавала за вътрешно ползване във връзка с изпълнение на услугата;

в) контролен раздел - в този раздел се поместват всички документи, които са отстранени от официалния раздел. Така се осигурява средство за контрол на състава на документите в официалния раздел.

С цел повишаване ефективността на административната дейност, Наредбата задължава АИС да предоставя функционалност, осигурява други функции като:

- един и същи документ да може да се класифицира в произволен брой раздели на различни преписки;
- една и съща преписка да може да се класифицира в произволен брой други преписки и/или произволни класификационни схеми.

Приемане на документи от страна на администрацията

Новият нормативен регламент урежда извършването на дейностите по приемане на документи, както следва:

а) през Уеб-приложение

Администрациите са длъжни да интегрират към своите АИС Уеб-приложения, които осигуряват online подаване на електронни документи към администрациите.

Във връзка с това може да се посочат следните особености:

- Приемат се заявки за електронни услуги само като формализирани документи в XML-формат;
- Работи се по схемата «един документ – една заявка за услуга;
- Заявлението за услуга, в качеството си на XML-документ служи и за контейнер, пренасящ и приложени документи, ако има такива;
- Приложените документи може да не бъдат в XML-формат, а във всеки един от форматите, посочени в Наредбата за електронните услуги;
- Всички документи в XML-формат трябва да бъдат регистрирани в Регистъра на информационните обекти;

- Преди етапа на разпознаване на вида на заявлението (тоест идентификация на заявената услуга) се извършват редица проверки, дефинирани в Наредбата за електронните услуги.

За успешно пренесен документ през Уеб-приложението може да се каже:

- направените проверки са успешни;
- крайт на преноса е завършил със създаване на документ в АИС и предстои да се извърши идентификация на процедурата по обработка на приетия документ.

б) по електронна поща

До голяма степен процесът е аналогичен, като по-важните разлики са както следва:

- преносът на документ, прикачен към електронно съобщение се извършва от приложение, интегрирано с АИС;
- извършват се аналогични проверки както при пренос през Уеб, но съобщения за открити нередности се изпращат само off line, като съобщения по електронната поща.

Критериите за успешно пренесен документ са същите.

в) електронни документи, доставени в администрациите на физически носител

До голяма степен процесът е аналогичен, като по-важните разлики са както следва:

- преносът на документ от физически носител се извършва от приложение, интегрирано с АИС;
- извършват се аналогични проверки както при пренос през Уеб, но за открити нередности се уведомява директно приносителя на документа.

Критериите за успешно пренесен документ са същите.

г) през ЕСОЕД

До голяма степен процесът е аналогичен, като по-важните разлики са както следва:

- Преносът изисква интеграция на АИС с ЕСОЕД-клиент;
- Извършват се част от проверките, защото самият пренос през ЕСОЕД предвижда или извършване на проверки, или поради наложени изисквания на обмена през ЕСОЕД прави част от проверките ненужни.

Критериите за успешно пренесен документ са същите.

Документи на хартиен носител

Процедурата по принцип съответства на прилаганата в момента, като по-важните разлики са, както следва:

- Необходимите проверки се извършват като се анализира съдържанието на заявлението върху оригиналния хартиен носител;
- Във всички случаи, за всяко прието заявление се създава документ в АИС;
- В документа в АИС се отразяват открити нередности при проверките, като самият хартиен документ се съхранява, като доказателство за това;

- Ако изходът от проверките е положителен, приетият документ се сканира.

Тоест, приемането практически завършва отново с готовност да се извърши идентификация на процедурата по обработка на приетия документ.

Разпределение на приети документи за обработка

Разпределението предвижда класификация на приетите документи в три категории:

- Документи, инициращи услуги или процедури.
- По принцип това са заявления за услуги или разпореждания във връзка с дейности, развивани между администрациите.
- Наредбите не изключват подаване дистанционно и на документи, стартиращи изпълнение на вътрешно административни процедури - например заявление за продължаване на отпуск;
- Документи, заявени в хода на изпълнение на услуги или процедури.
- Това са отговори на заявени вътрешни административни услуги, или документи, заявени към получатели на административни услуги, които вече са иницирали изпълнението на някаква услуга;
- Документи, отнасящи се общо за услуги или процедури, намиращи се в изпълнение.
- Тези документи не са заявени от администрацията, но са изпратени по инициатива на заявителите на услуги, които вече са иницирали изпълнение на такива.

Когато се открие документ от първата категория се извършва:

- а) определяне на вида на документа, съгласно дефинираните видове документи във Ведомствената номенклатура на видовете документи;
- б) идентификация на услугата или процедурата, която стартира този документ;
- в) стартиране на идентифицираната процедура.

С това практически е приключил процесът на разпределяне на документи от тази категория. За документите от другите категории се извършва обработката, посочена по-долу.

Стартиране на изпълнението на услуга или процедура

Стартирането включва извършване на следните дейности:

- а) създава се в АИС (начален) статус на изпълнение на съответната услуга или процедура;
- б) статусът се създава по идентифицираната чрез инициращия документ на предходния етап услуга или процедура;
- в) статусът се представя с набор от задачи в състава на списъка „Неизпълнени етапи”. Всеки етап е представен с обект в АИС от типа задача; това дава възможност изпълнението на етап да се отчита като персонално извършена дейност. Всеки етап има отговорен изпълнител, посочен в неговата дефиниция;
- г) инициращият документ се предава на отговорния изпълнител на първия етап от списъка „Неизпълнени етапи”;

д) ако даден етап подлежи на автоматично изпълнение се извършва следното:

- идентифицира се програмния модул, който автоматично изпълнява етапа. Този модул е представен в описанието на етапа по начин, който го адресира с възможност за неговото активиране;
- Предава се инициращия документ чрез съответния интерфейс на АИС към модула и се стартира работата на документа.

Заявяване на документ към външни лица и организации

Примери за това са:

- искане за нови документи по заявена услуга;
- уведомление за изчислен размер на плащане по услуга; в случая се очаква документ, потвърждаващ плащането с цел да се продължи изпълнението на услугата;
- заявка за данни по идентификация на физическо или юридическо лице, към съответния администратор на първични данни; това е типичен случай на вътрешна административна услуга, иницирана във връзка с услуга, заявена от физическо или юридическо лице;
- други.

Искането към външни лица и организации се изпраща по електронна поща, а искане във връзка с изпълнение на вътрешно административни услуги се изпраща през ЕСОЕД. Самото искане представлява електронен документ, регистриран в официалния документен регистър на администрацията. Този документ се създава в хода на изпълнение на услуга или процедура и от него има връзка към статуса на изпълнението и връзка към преписката по изпълнението. Искането се включва към набора от документи с обща характеристика „документи, иницирали услуги или процедури в процес на изпълнение”, поддържан в АИС.

Наредбата не ограничава поддържането с АИС само на един набор от документи с обща характеристика „документ, иницирали услуги или процедури в процес на изпълнение”.

Обработка на документ, заявен в хода на изпълнение на услуга или процедура

След идентификацията на принадлежността на получен документ към тази категория се извършва следното:

- а) извлича се от получения документ УРИ на документа, с който е заявен;
- б) по така извлечения УРИ се открива документа-заявление в набора от документи с обща характеристика „изпратен документ в изчакване на отговор”;
- в) по този документ-заявление се определя статуса и преписката на услугата или процедурата, при изпълнението на която е подадена заявката;
- г) полученият документ се включва в така откритата преписка и се стартира обработката му с така открития статус на изпълнение на съответната услуга или процедура, която го е заявила;
- д) за целите на обработката документът се предава на изпълнителя на първия етап в списъка „неизпълнени етапи” на статуса;

е) ако този етап се изпълнява машинно, предаването на документа за обработка активира съответния програмен модул, който се идентифицира чрез отговорния изпълнител на етапа, който контролира неговите функции.

Обработка на документ за текущо изпълнявана услуга или процедура, който не е заявен в хода на нейното изпълнение

След идентификацията на принадлежността на получен документ към тази категория се извършва следното:

а) извлича се от получения документ УРИ на документа, с който е иницирано изпълнение на услуга или процедура. Този УРИ задължително е посочен в получения документ;

б) по така извлечения УРИ се открива инициращия документ в набора от документи с обща характеристика „документи, иницирали услуги или процедури в процес на изпълнение”;

в) по този документ се определя статуса и преписката на услугата или процедурата, за която е предназначен документа;

г) полученият документ се включва в така откритата преписка и се стартира обработката му с така открития статус на изпълнение на съответната услуга или процедура, която го е заявила;

д) за целите на обработката документът се предава на отговорния изпълнител по услугата или процедурата. Отговорният изпълнител взема решение за обработката на документа; това решение може да промени хода на изпълнение на услугата или процедурата.

Резолиране на документи

Наредбата пряко не променя наличната традиция на извършване на този процес, но може да се посочат следните особености в регламента на извършването му в условията на АИС:

- наредбата не регламентира „резолюция”-та, като свободен текст, съдържащ указания за обработка на документ; във връзка с това в описанието на документ не е предвидена специална данна, която да съдържа този текст, но няма ограничения такава да бъде въведена;
- наредбата разглежда резолюцията по документ като поставяне на една или повече задачи, произтичащи от документа или свързани с неговата обработка;
- тоест, не се ограничава въвеждането на резолюция и като свободен текст, но се задължава на базата на този текст да се дефинира в АИС обект от типа „задача”, което да се включи под общия механизъм за контрол изпълнението на поставените задачи.

Създаване на документи

Наредбата въвежда само два общи регламента, във връзка със създаването на документи:

а) документи се създават само в средата на АИС, с което започва управление на жизнения им цикъл;

б) за всеки документ трябва да има създаден образец, по който се създава съдържанието на документа.

В случая понятието „образец” трябва да се разглежда в максимално широк смисъл. Тоест, образецът може да бъде както XML- конструкция, регистрирана в Регистъра на информационните обекти като електронен документ, но може да бъде и като неструктуриран текст, в някои от допустимите формати, съгласно Наредбата за електронните услуги.

Движение на документи между участниците в неговата обработка

Наредбата не предвижда създаване на екземпляри, които се предоставят на следващия в обработката служител. Тоест, наредбата не предвижда осъществяване на движение на документите чрез създаване на екземпляри за изпращане вътре в администрацията.

Целият модел на организация на административната дейност се базира на следните принципи:

- даден документ се поддържа само в един екземпляр в АИС;
- създаването на електронен документ в АИС винаги е свързано и със създаване на достъп до него;
- да се предаде електронен документ от един служител на друг означава предаваният да осигури на приемащия документа достъп до него с ресурсите на АИС;
- всяко движение на документ между служители в администрацията по описаната схема с предоставяне на достъп се регистрира по време и авторство в АИС.

Отразяване на становища по документи

Възможните становища, които могат да бъдат изказани във връзка с обработката на документ са унифицирани като текст и влияние върху процеса на обработка. Те са:

а) съгласен - не променя хода на изпълнение на процедура по обработка на документ; възможно е да се допълни текст, отразяващ детайли на становището;

б) несъгласен - не променя хода на изпълнение на процедура по обработка на документ; задължително се посочват мотиви на несъгласието;

в) за доработка - връща изпълнението на процедурата, в състава на която се обработва документа на по-ранен етап; задължително се дават указания за доработката-или към становището, или директно се въвеждат в текста на съдържанието на документа;

г) прекратявам процедурата - прекратява се изпълнението на процедурата

Освен това се отбелязват и следните факти:

- Създал документ;
- Кorigирал документ;
- Подписал документ.

Това са факти по създаване и обработка на документ, които пряко нямат смисъла на становища, просто защото касаят създаване, корекция или допълване (при подписване) на съдържание на документ. Наредбата дефинира становищата преди всичко като средство за отразяване на етапи по създаване и обработка на документ, ето защо смисълът на становищата се свързва основно с влиянието им на процедурата. Разгледано по-общо, становищата са унифицирани дефиниции на факти по обработка на документи. Наредбата ги третира именно като такива и ги приравнява по формат на представяне в АИС на посочените по-горе факти по създаване, коригирани и подписване на документ.

Преход от обработка на електронно в хартиено съдържание и обратно

Наредбата специално регламентира правия и обратния преход, за да се осигури работоспособност на нейното прилагане и при липса на достатъчно компютърни ресурси в АИС или умения за използването им от служителите в администрацията. Изхождайки от базовия характер на електронната форма на поддържане на съдържание в администрацията, т.н. „прав” преход е преходът от електронна в хартиена форма. Този преход е най-типичен при отразяване на становище по документ и включва следните действия:

а) служителят, обслужващ прехода, разпечатва съдържанието на обработвания документи и всички изказани до момента становища и регистрирани факти по неговата обработка;

б) подписва се собственоръчно и предава подписаната разпечатка на служителя, който ще отрази становището си върху нея. Подписът има традиционния смисъл на „Вярно с оригинала”, като под „оригинал” в случая се има в предвид информацията в АИС.

Служителят отразява на ръка върху разпечатката своето становище и го предава на служителя, който трябва да извърши „обратния” преход- от хартиен носител на съдържание в електронен. Последният въвежда изказаното становище от името на неговия автор, но АИС регистрира че самото въвеждане е направено от съответния служител. След извършване на въвеждането, служителят се подписва на хартиената разпечатка в уверения на това, че правилно е въвел в АИС отразеното на хартия становище.

Издаване на електронни документи от администрацията

а) от документа, подлежащ на издаване, се генерира в АИС „екземпляр за издаване” и между двата документа се изгражда връзка;

б) екземплярът за издаване се регистрира в официалния документен регистър, като на този етап се въвежда само регистровия номер, тоест регистровия индекс на официалния документен регистър и генерирания пореден номер;

в) регистровият номер се въвежда в съдържанието на документа;

г) подписва се документа и се изпраща в регистратурата; с полагане на подписа в документа се въвежда последния елемент на уникалния регистров идентификатор на документа- датата на неговото подписване; на този етап тя се намира само в съдържанието на документа;

д) служител в регистратурата въвежда в АИС датата от електронния подпис като съдържание на данната „дата на получаване или подписване на документ”.

Така подписания и регистриран електронен документ се изпраща на получателя му и това се в АИС отразява

Издаване на документи на хартиен носител от администрацията

- а) от документа, подлежащ на издаване, се генерира в АИС „екземпляр за издаване” и между двата документа се изгражда връзка;
- б) разпечатва се съдържанието на документа и се представя за подпис;
- в) подписаният хартиен документ се занася в регистратурата;
- г) служител в регистратурата извършва пълна регистрация на документа в АИС, като се генерира регистровия номер и се въвежда текущата дата като дата на подписване на документа;
- д) така генерирания УРИ се нанася ръчно върху хартиения документ;
- е) така подписания и регистриран хартиен документ се изпраща на получателя, или се предава лично при поискване.

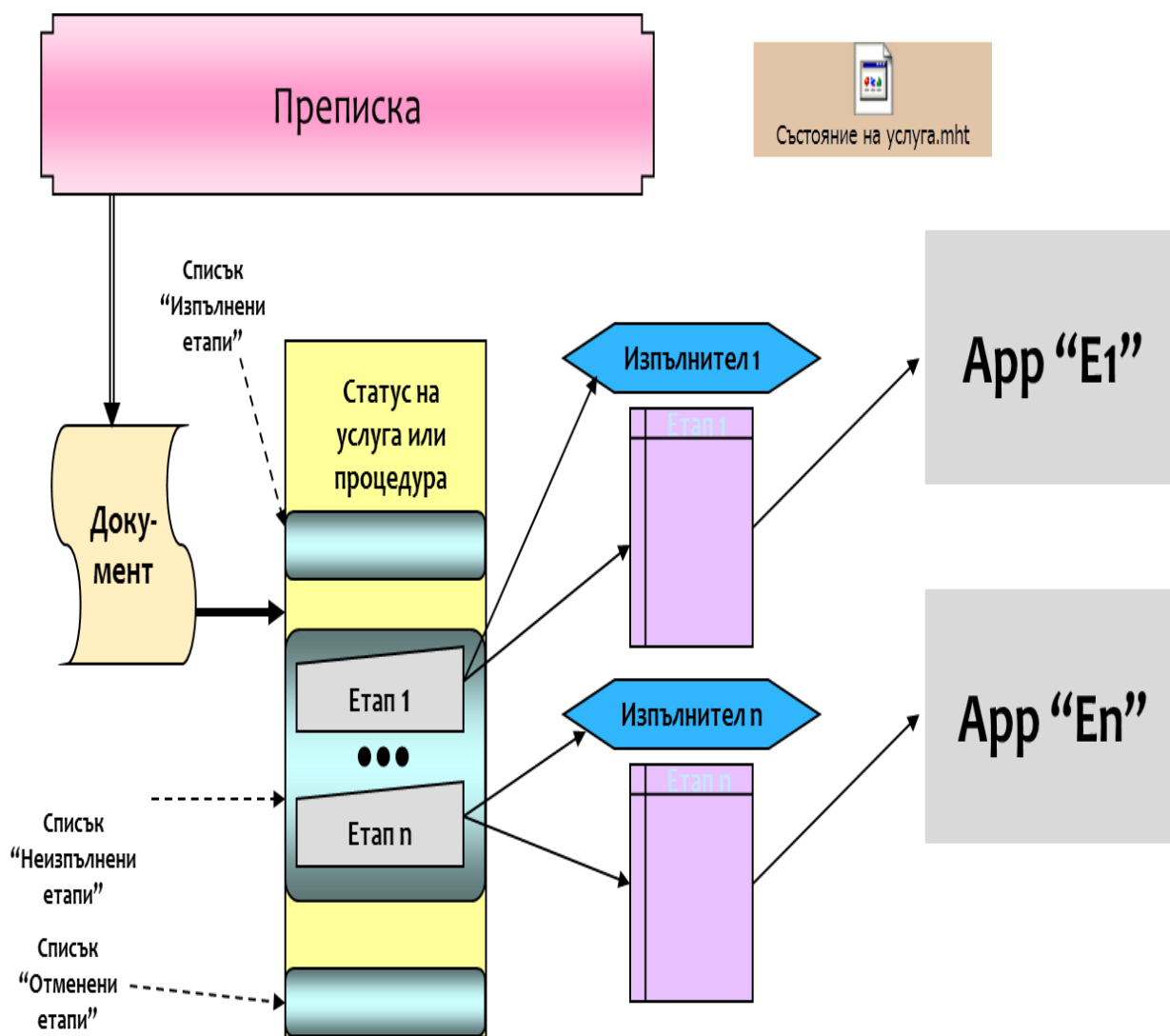
Класификационни структури за поддръжка на масиви от документи

Наредбата не налага никаква конкретна схема за класификация на документи и всички други обекти, които администрациите поддържат с АИС. Това дава пълна свобода на администрациите да развият и поддържат класификационни схеми, които съответстват на спецификата на администрациите и изпълняваните от тях услуги и процедури.

ГЛАВА 5.4

ВЪЗЛАГАНЕ И ОТЧИТАНЕ НА ЗАДАЧИ ЧРЕЗ ИЗПОЛЗВАНЕТО НА ЕЛЕКТРОННИ ДОКУМЕНТИ. КОНТРОЛ НА ДЕЙНОСТТА ЧРЕЗ АИС.

Статус на услуга или процедура, като елемент от контрола на административната дейност



Фигура 5-4

Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите дефинира статуса на изпълнение на услуга като набор от задачи, разпределени в три списъка, както следва:

- изпълнени етапи;
- неизпълнени етапи;
- отменени етапи.

Предпоставките за припокриването на информационния обект „етап” с обекта „задача” са:

- дефиницията на етап включва набор от действия, чието изпълнение дава крайните продукти по етапа, което почти изцяло съответства и на дефиницията на задача в АИС;
- стартирането на изпълнение на услуга или процедура практически предопределя изпълнението на изграждащите ги етапи, включително и задължението на съответните изпълнители по етапи да извършат необходимите действия по тях.

Тоест, стартирането на услуга или процедура може да се разглежда като автоматично генериране на краен брой задачи към съответните изпълнители по етапи. Тези задачи не са „спуснати” от висшестоящи ръководители, а произтичат от организацията на дейностите и длъжностните характеристики на тези, които трябва да ги изпълняват. Но това не ги прави по-маловажни от пряко възложените им задачи. Наредбата прехвърля голяма част от данните в дефиниция на етап в дефиницията на задача. Тоест, ако се визуализират задачи и етапи в рамките само на еднакви данни, те практически са неразличими. Точно това дава възможност, етапите да се визуализират чрез задачите, с които се възлага и отчита тяхното изпълнение.

Съгласно Закона за електронното управление (ЗЕУ), администрациите са длъжни да предоставят информация за състоянието на изпълнението на заявена услуга. Наредбата регламентира това, като дефинира посочените по-горе списъци от задачи, но имената на самите списъци ги отнасят към етапи. Именно съдържанието на тези списъци се визуализира през Интернет, във връзка с изпълнение на посоченото изискване на ЗЕУ. Тоест статусът се дефинира като изпълнени / неизпълнени / отменени задачи, но те визуализират текущото им изпълнение като изпълнение на етапи.

Заявителите на услуги получават пълната информация съгласно ЗЕУ, като от тяхна гледна точка те получават информация за изпълнени, предстоящи или отменени етапи, независимо че през Интернет за тях се визуализират данни от дефиниции на задачи. От друга страна, за самата администрация се осигурява еднородна среда за представяне на нейната дейност, което прави контрола лесен и разбираем. Тоест, контролът се извършва по еднотипна схема, независимо от това дали задачите върху които се разпростира са пряко възложени, или са косвено дефинирани при стартиране на изпълнение на услуга или процедура.

Контрол на сроковете за изпълнение на услуги

За всяка законово дефинирана услуга има максимално допустим срок за изпълнение. Дефинирането на сроковете за изпълнение на етапите се извършва в съответствие със средно необходимото време за изпълнение на дейностите по етапа. Самото ресурсно осигуряване на съответните администрации във връзка с гарантиране на необходимия капацитет за изпълнение в срок на изпълняваните услуги в повечето случаи също се оразмерява по усреднени критерии. За кампанийно предоставяни услуги се правят допълнителни схеми за ресурсно осигуряване за критични интервали от време, но отново по същите усреднени критерии.

В общия случай, администрацията работи с относително преоразмерен капацитет. Това означава, че ако една услуга по нормативен регламент трябва да се изпълни за 14 дни, представена чрез сума от времената на отделните етапи тя би трябвало да се изпълни за по-кратък (в някои случаи значително) срок.

В реалната практика, поради натовареност на някои от изпълнителите по етапи е възможно някой етап да се „разтегне” във времето, но като цяло услугата да се изпълни в законово регламентирания срок. Чрез общата схема за контрол на дейността ще се регистрира, че е на лице правилно изпълнение на услугата като цяло и в същото време неизпълнение в срок на един или повече етапи. Второто е отразено като неизпълнение на една или повече задачи „в актива” на съответните изпълнители.

Това е явно противоречие и схемата за контрол не предвижда пряка връзка между двете. Ето защо, тя предвижда обща процедура по контрол на срокове по изпълнение на услуги. Тази процедура не се интересува от изпълнението на етапите, изграждащи дадена услуга, а само от спазване на крайния срок. Тя разглежда самото предоставяне на услуги като процес със статистическа оценка на качеството на неговото изпълнение, поне що се отнася до спазване на законово допустимия срок. Във връзка с това се дефинират интервали на просрочване както следва:

- а) приключили в срок;
- б) просрочени с една седмица;
- в) просрочени с две седмици;
- г) просрочени с повече от две седмици.

Дефинирането на различни интервали има за задача да открие устойчиви тенденции за неизпълнение, включително и при наличие на коригиращи мерки.

Във връзка с това се въвеждат следните критерии, за регистрирано устойчиво неизпълнение:

- а) просрочени с една седмица - над 15 на сто;
- б) просрочени с две седмици - над 10 на сто;
- в) просрочени с повече от две седмици - над 5 на сто.

Процедурата за контрол предвижда прилагането на регламентиран набор от мерки, както следва:

- а) санкциониране на ръководители за лошо изпълнение на служебните им задължения;
- б) структурни промени;
- в) увеличаване на ресурсите на административните звена в рамките на съответното ведомство;
- г) усъвършенстване на организацията на административната дейност.

Самото прилагане на мерките също е регламентирано както следва:

- а) описание на проблемите, които трябва да се решат;
- б) описание на проект или набор от проекти, с които ще се извършат промените;
- в) обща спецификация на ресурсите - човешки и финансови, необходими за реализация на проектите;
- г) общо разписание на реализацията на проектите във времето.

Тоест, самата идеология на контрола може да се представи със следните тези:

- регистрацията на неизпълнение в срок на услуги е дефинирана като чисто техническа дейност, напълно развързана от обработката на регистрираните резултати;
- регистрираните резултати не само не може да не бъдат обработени, но самата обработка не може да бъде палиативна, тоест трябва да съответства на регламента в наредбата;
- да се обработят резултати от регистрирано некачествено изпълнение на услуги означава да се планират и проведат съответните организационни мероприятия, чиято дефиниция също не може да бъде палиативна, а в съответствие с наложения регламент;
- самото изпълнение на мероприятията се представя като набор от процедури, дефинирани в състава на вътрешните правила, с което тяхното изпълнение автоматично попада под контрол.

Така Наредбата осигурява качество и контрол на коригиращите мерки, чрез аналогични средства за контрол. С това, идеологията на този тип контрол напълно съответства на съвременното схващане за контрол, което въвежда затворен цикъл на вътрешен контрол, а външният контрол се упражнява, като „контрол върху контрола”. В така разгледаната схема за контрол трябва да се отбележи, че самата работа със задачи практически отива на заден план, защото са работи само със срокове по обработка на документи, в качеството им на заявления за услуги. Тоест, самият контрол на дейността се извършва само по параметри на обработка на документи. Що се касае до регистрацията на индивидуалното изпълнение на задачи, съответстващи на етапи, в тази схема то не присъства, но регистрацията му е на лице.

Контрол на изпълнението на пряко възложени задачи

Такива задачи възникват при:

- резолване на получен документ, който не стартира услуга, а е необходимо ръководен орган да организира неговата обработка;
- изпълнение на вътрешно административни дейности, инициирани от непредвидени външни или вътрешни причини;
- други, нерегламентирани като услуги и/ли процедури действия на администрацията.

Трябва да се посочи, че за да се възложи пряко задача от ръководен орган не е задължително за целта администрацията да е получила документ от вън, или сама тя да е изработила вътрешно такъв.

Контролът на пряко възложените задачи се осъществява по класическата схема, която накратко се свежда до:

- периодичен преглед на изпълнението на поставени задачи и възлагане на нови; извършва се в рамките на колективни обсъждания- оперативки, периодични анализи и т.н.;
- самият преглед се извършва с подготовка на текущо изпълняваните задачи, като се класифицират в три категории- изпълнени, неизпълнени и в изпълнение;

- освен нови задачи, в резултат на прегледа се променят срокове, изпълнители и т.н.

Като резултат от контрола е налице регистрацията на индивидуалното изпълнение на поставените задачи.

Обща организация на персоналния контрол на дейността

Контролът на изпълнението на услуги се извършва по схема, която основно се базира на регистрацията на факти по обработка на документи, във връзка с изпълнение на услуги.

Заедно с това, Наредбата задължава използване на АИС, която регистрира, като задача:

- работата на отговорен изпълнител по етап;
- отразяването на становище;
- отразяването на факт по обработка на документ.

Към този набор задачи се приобщават и задачите, които пряко са възложени от ръководен орган. Нещо повече, отговорен изпълнител по етап може да възложи задачи във връзка с изпълнение на етапа на своите подчинени, при това в неявна форма, като изиска от тях становище по обработван документ. Така, в рамките на дефинираната задача, съответстваща на работата по етап може да се появят още задачи, които са възложени от отговорния изпълнител по етапа.

От гледна точка на АИС, всички изредени до тук задачи са абсолютно еквивалентни и върху тях може да се приложи еднотипна обработка.

Наредбата регламентира обработка, която включва:

- поддръжка на наборите от задачи, изпълнени от даден служител за контролиран интервал от време;
- класификация на тези задачи, в зависимост от това колко пъти са променяни сроковете на изпълнение;
- използване на така регистрираните данни по персоналната активност на служителите при тяхната атестация.

Наредбата не регламентира точно как се използват тези данни при атестация, защото това е обект на друга законова уредба. Но Наредбата регламентира оценка на административния капацитет на звената, представен чрез резултатите от регистрираното персонално участие на служителите в административния процес. Освен оценката, съответната администрация е длъжна да приложи съответните коригиращи мерки, в случай на налични проблеми в дадено административно звено.

Предпоставка за пораждаване на нови изисквания

Основна предпоставка е новият - електронният носител на съдържание, който започва да се използва в работата на администрацията, съгласно новия законов регламент на нейната дейност. Следствие от това е задължителното използване на Административна информационна система (АИС), като основно средство за съхранение и обработка на електронно съдържание. Тоест, появява се принципно нова инфраструктура за съхранение и обработка на съдържание, която е коренно различна от тази при хартиените документи.

Законът за електронното управление (ЗЕУ) и наредбите към него регламентират съвместното поддържане на двата типа инфраструктура и начините за извършване на административната дейност в тях.

АИС – основно средство за съхранение и обработка на информация

Член 7 на ЗЕУ задължава администрациите да поддържат всички данни, събирани, съхранявани и обработвани в процеса на извършване на административната дейност задължително в средата на АИС. Във връзка с това, администрациите се задължават да сканират всички получени хартиени документи и да осигуряват обработката на така снетото графично изображение само и изключително със средствата на АИС. След сканирането на получен хартиен документ, същият директно отива за съхранение в качеството му на физически носител - оригинал. Движение на този оригинален носител във връзка с обработка на съдържанието му не се предвижда. Движение на документи на хартиен носител се предвижда само за такива, чието сканиране технологично не е възможно.

Може да се каже, че от старите средства за управление на жизнения цикъл на документите, регламентирани в отменената Единна държавна система за деловодство (ЕДСД) остават само средствата за съпровождане на хартиения носител на съдържание, когато неговото използване е неминуемо.

Понятие за „документ”, поддържан с АИС

Дефиницията (описанието) на документ в АИС включва данни по създаване и обработка на съдържанието на документа, разглеждано като една от данните в него. При електронните документи съдържанието на документа са данни - файл в съответния формат, а при успешно сканираните хартиени документи - това е файл с неговото сканирано изображение.

Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите дефинира минимален състав на данните в описанието на документ в АИС. Това са данни за:

- получаването или създаването на документа;
- отразени становища по него;
- неговата регистрация;
- неговата класификация, включително и в схемата на организация на разположението на хартиените документи в хранилището;
- неговия престой в Номенклатурата на делата, която съгласно наредбата вече се нарича Номенклатура на схемите за съхранение на документите;
- други данни.

Регистрация на документи

Наредбата въвежда по-специален режим на регистрация на документи, който се извършва по схемата „един документ - един уникален регистров идентификатор (УРИ)”. Този режим е необходим за да се осигури уникална регистрация на документите не само за дадена администрация, а за всички администрации и комуникиращите с тях субекти. Във връзка с това е въведена нова конструкция на данните по регистрацията на документ - те общо се наричат „уникален регистров идентификатор” и той включва:

а) **регистров индекс** - всеки регистър, който се използва от администрациите с цел издаване на УРИ, подлежащ на използване от външни лица и организации трябва да бъде регистриран в Регистъра на регистрите и данните. Така дадена администрация получава за своя официален документен регистър уникален регистров индекс, с който нейният регистър е различим (по издавания УРИ) сред всички регистри, поддържани от администрациите;

б) **пореден регистров номер** - такъв пореден номер се издава от официален документен регистър при всяка регистрация на документ. За всяка календарна година, този номер започва да се генерира от „1”.

В) **дата на получаване или подписване на документ** - това е датата на получаване на входящ документ, или датата на подписване на изходящ документ.

Тоест, ако се регистрира получен документ в официален документен регистър, регистриран с регистров индекс „2178”, при генериран пореден номер „0341” на 21.02.2008, то издаденият УРИ ще бъде: 2178-0341-21.02.2008.

Самата регистрация на получавани документи се извършва също по нова схема. В зависимост от това, дали вече е издаден валиден УРИ за този документ от друг официален документен регистър, тази схема предвижда два варианта на регистрация, както следва:

- при наличие на валиден УРИ - за валиден УРИ се счита УРИ, издаден от регистриран в Регистъра на регистрите и данните документен регистър. Като УРИ на регистрация се вписва вече издадения валиден УРИ;
- при липса на валиден УРИ - генерира се УРИ от официалния документен регистър, в който се извършва регистрацията. Като дата на получаване или подписване се вписва датата на регистрацията.

Регистрацията на електронни и документи на хартиен носител се извършва по абсолютно еднотипен начин. Уникалният регистров идентификатор се поддържа с АИС в състава на описанието на регистрирания документ. При регистрация на получени хартиени документи, локално генерираният УРИ се нанася собствено ръчно върху хартиеното изображение на получения документ.

Наредбата не ограничава поддържането с АИС само на един официален документен регистър.

Електронен вариант на преписка

АИС трябва да поддържа структурата „преписка” в качеството ѝ на набор от тематично свързани документи. Наредбата не регламентира точно как се поддържа структурата, като единствено налага изискването, за влизащите в преписка документи да се поддържа вътрешна номерация. Друга особеност на новия тип преписка е поддържането на три раздела в една и съща преписка. Това са:

а) **официален раздел** - в този раздел се поместват всички документи, които съгласно ЗЕУ трябва да се достъпни за потребител на електронна услуга през Интернет. Това са документите с които е заявена услуга и документи, които администрацията е издала или приела от други администрации във връзка с изпълнение на услугата;

б) **вътрешен раздел** - в този раздел се поместват всички документи, които администрацията е създала за вътрешно ползване във връзка с изпълнение на услугата;

в) контролен раздел - в този раздел се поместват всички документи, които са отстранени от официалния раздел. Така се осигурява средство за контрол на състава на документите в официалния раздел.

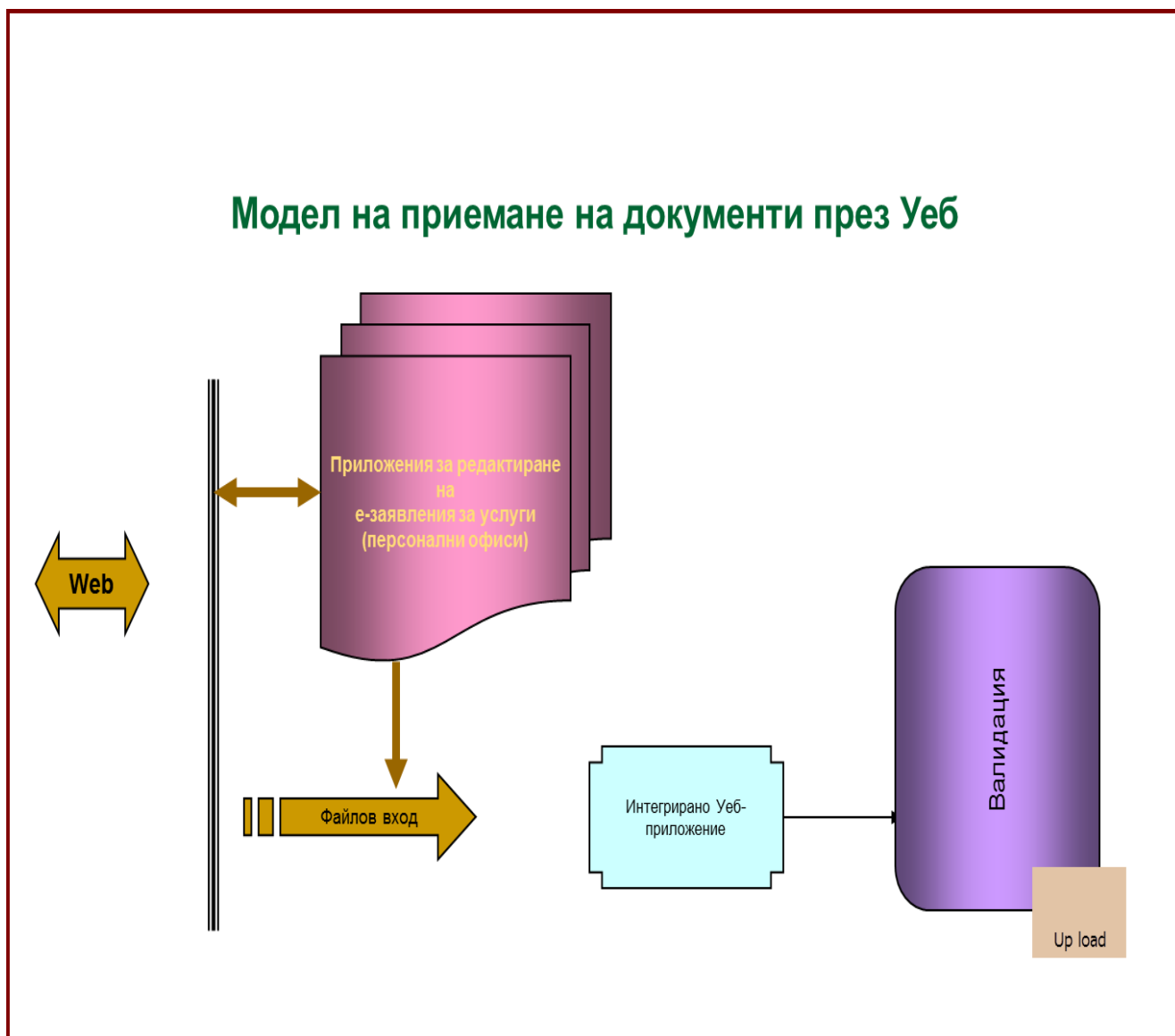
С цел повишаване ефективността на административната дейност, Наредбата задължава АИС да предоставя функционалност, осигурява други функции като:

- един и същи документ да може да се класифицира в произволен брой раздели на различни преписки;
- една и съща преписка да може да се класифицира в произволен брой други преписки и/или произволни класификационни схеми.

Приемане на документи от страна на администрацията

Новият нормативен регламент урежда извършването на дейностите по приемане на документи, както следва:

- а) през Уеб-приложение;



Фигура 5-5

Администрациите са длъжни да интегрират към своите АИС Уеб-приложения, които осигуряват online подаване на електронни документи към администрациите.

Във връзка с това може да се посочат следните особености:

- Приемат се заявки за електронни услуги само като формализирани документи в XML-формат;
- Работи се по схемата «един документ – една заявка за услуга»;
- Заявлението за услуга, в качеството си на XML-документ служи и за контейнер, пренасящ и приложени документи, ако има такива;
- Приложените документи може да не бъдат в XML-формат, а във всеки един от форматите, посочени в Наредбата за електронните услуги;
- Всички документи в XML-формат трябва да бъдат регистрирани в Регистъра на информационните обекти;
- Преди етапа на разпознаване на вида на заявлението (тоест идентификация на заявената услуга) се извършват редица проверки, дефинирани в Наредбата за електронните услуги.

За успешно пренесен документ през Уеб-приложението може да се каже:

- направените проверки са успешни;
- край на преноса е завършил със създаване на документ в АИС и предстои да се извърши идентификация на процедурата по обработка на приетия документ.

б) по електронна поща;

До голяма степен процесът е аналогичен, като по-важните разлики са както следва:

- преносът на документ, прикачен към електронно съобщение се извършва от приложение, интегрирано с АИС;
- извършват се аналогични проверки както при пренос през Уеб, но съобщения за открити нередности се изпращат само off line, като съобщения по електронната поща.

Критериите за успешно пренесен документ са същите.

в) електронни документи, доставени в администрациите на физически носител

До голяма степен процесът е аналогичен, като по-важните разлики са както следва:

- преносът на документ от физически носител се извършва от приложение, интегрирано с АИС;
- извършват се аналогични проверки както при пренос през Уеб, но за открити нередности се уведомява директно приносителя на документа.

Критериите за успешно пренесен документ са същите.

г) през ЕСОЕД

До голяма степен процесът е аналогичен, като по-важните разлики са както следва:

- Преносът изисква интеграция на АИС с ЕСОЕД-клиент;

- Извършват се част от проверките, защото самият пренос през ЕСОЕД предвижда или извършване на проверки, или поради наложени изисквания на обмена през ЕСОЕД прави част от проверките ненужни.

Критериите за успешно пренесен документ са същите.

Документи на хартиен носител

Процедурата по принцип съответства на прилаганата в момента, като по-важните разлики са, както следва:

- Необходимите проверки се извършват като се анализира съдържанието на заявлението върху оригиналния хартиен носител;
- Във всички случаи, за всяко прието заявление се създава документ в АИС;
- В документа в АИС се отразяват открити нередности при проверките, като самият хартиен документ се съхранява, като доказателство за това;
- Ако изходът от проверките е положителен, приетият документ се сканира.

Тоест, приемането практически завършва отново с готовност да се извърши идентификация на процедурата по обработка на приетия документ.

Разпределение на приети документи за обработка

Разпределението предвижда класификация на приетите документи в три категории:

- Документи, инициращи услуги или процедури;
- По принцип това са заявления за услуги или разпореждания във връзка с дейности, развивани между администрациите;
- Наредбите не изключват подаване дистанционно и на документи, стартиращи изпълнение на вътрешно административни процедури - например заявление за продължаване на отпуск;
- Документи, заявени в хода на изпълнение на услуги или процедури;
- Това са отговори на заявени вътрешни административни услуги, или документи, заявени към получатели на административни услуги, които вече са иницирали изпълнението на някаква услуга;
- Документи, отнасящи се общо за услуги или процедури, намиращи се в изпълнение.

Тези документи не са заявени от администрацията, но са изпратени по инициатива на заявителите на услуги, които вече са иницирали изпълнение на такива.

Когато се открие документ от първата категория се извършва:

- а) определяне на вида на документа, съгласно дефинираните видове документи във ведомствената номенклатура на видовете документи;
- б) идентификация на услугата или процедурата, която стартира този документ;
- в) стартиране на идентифицираната процедура.

С това практически е приключил процесът на разпределяне на документи от тази категория. За документите от другите категории се извършва обработката, посочена по-долу.

Стартиране на изпълнението на услуга или процедура

Стартирането включва извършване на следните дейности:

а) създава се в АИС (начален) статус на изпълнение на съответната услуга или процедура;

б) статусът се създава по идентифицираната чрез инициращия документ на предходния етап услуга или процедура;

в) статусът се представя с набор от задачи в състава на списъка „Неизпълнени етапи”. Всеки етап е представен с обект в АИС от типа задача; това дава възможност изпълнението на етап да се отчита като персонално извършена дейност. Всеки етап има отговорен изпълнител, посочен в неговата дефиниция;

г) инициращият документ се предава на отговорния изпълнител на първия етап от списъка „Неизпълнени етапи”;

д) ако даден етап подлежи на автоматично изпълнение се извършва следното:

- идентифицира се програмния модул, който автоматично изпълнява етапа. Този модул е представен в описанието на етапа по начин, който го адресира с възможност за неговото активиране;
- Предава се инициращия документ чрез съответния интерфейс на АИС към модула и се стартира работата на документа.

Заявяване на документ към външни лица и организации

Примери за това са:

- искане за нови документи по заявена услуга;
- уведомление за изчислен размер на плащане по услуга; в случая се очаква документ, потвърждаващ плащането с цел да се продължи изпълнението на услугата;
- заявка за данни по идентификация на физическо или юридическо лице, към съответния администратор на първични данни; това е типичен случай на вътрешна административна услуга, иницирана във връзка с услуга, заявена от физическо или юридическо лице;
- други.

Искането към външни лица и организации се изпраща по електронна поща, а искане във връзка с изпълнение на вътрешно административни услуги се изпраща през ЕСОЕД. Самото искане представлява електронен документ, регистриран в официалния документен регистър на администрацията. Този документ се създава в хода на изпълнение на услуга или процедура и от него има връзка към статуса на изпълнението и връзка към преписката по изпълнението. Искането се включва към набора от документи с обща характеристика „документи, иницирали услуги или процедури в процес на изпълнение”, поддържан в АИС.

Наредбата не ограничава поддържането с АИС само на един набор от документи с обща характеристика „документ, иницирали услуги или процедури в процес на изпълнение”.

Обработка на документ, заявен в хода на изпълнение на услуга или процедура

След идентификацията на принадлежността на получен документ към тази категория се извършва следното:

- а) извлича се от получения документ УРИ на документа, с който е заявен;
- б) по така извлечения УРИ се открива документа-заявление в набора от документи с обща характеристика „изпратен документ в изчакване на отговор”;
- в) по този документ-заявление се определя статуса и преписката на услугата или процедурата, при изпълнението на която е подадена заявката;
- г) полученият документ се включва в така откритата преписка и се стартира обработката му с така открития статус на изпълнение на съответната услуга или процедура, която го е заявила;
- д) за целите на обработката документът се предава на изпълнителя на първия етап в списъка „неизпълнени етапи” на статуса;
- е) ако този етап се изпълнява машинно, предаването на документа за обработка активира съответния програмен модул, който се идентифицира чрез отговорния изпълнител на етапа, който контролира неговите функции.

Обработка на документ за текущо изпълнявана услуга или процедура, който не е заявен в хода на нейното изпълнение

След идентификацията на принадлежността на получен документ към тази категория се извършва следното:

- а) извлича се от получения документ УРИ на документа, с който е иницирано изпълнение на услуга или процедура. Този УРИ задължително е посочен в получения документ;
- б) по така извлечения УРИ се открива инициращия документ в набора от документи с обща характеристика „документи, иницирали услуги или процедури в процес на изпълнение”;
- в) по този документ се определя статуса и преписката на услугата или процедурата, за която е предназначен документа;
- г) полученият документ се включва в така откритата преписка и се стартира обработката му с така открития статус на изпълнение на съответната услуга или процедура, която го е заявила;
- д) за целите на обработката документът се предава на отговорния изпълнител по услугата или процедурата. Отговорният изпълнител взема решение за обработката на документа; това решение може да промени хода на изпълнение на услугата или процедурата.

Резолиране на документи

Наредбата пряко не променя наличната традиция на извършване на този процес, но може да се посочат следните особености в регламента на извършването му в условията на АИС:

- наредбата не регламентира „резолюция”-та, като свободен текст, съдържащ указания за обработка на документ; във връзка с това в описанието на документ не е предвидена специална данна, която да съдържа този текст, но няма ограничения такава да бъде въведена;
- наредбата разглежда резолюцията по документ като поставяне на една или повече задачи, произтичащи от документа или свързани с неговата обработка;
- тоест, не се ограничава въвеждането на резолюция и като свободен текст, но се задължава на базата на този текст да се дефинира в АИС обект от типа „задача”, което да се включи под общия механизъм за контрол изпълнението на поставените задачи.

Създаване на документи

Наредбата въвежда само два общи регламента, във връзка със създаването на документи:

- а) документи се създават само в средата на АИС, с което започва управление на жизнения им цикъл;
- б) за всеки документ трябва да има създаден образец, по който се създава съдържанието на документа.

В случая понятието „образец” трябва да се разглежда в максимално широк смисъл. Тоест, образецът може да бъде както XML- конструкция, регистрирана в Регистъра на информационните обекти като електронен документ, но може да бъде и като неструктуриран текст, в някои от допустимите формати, съгласно Наредбата за електронните услуги.

Движение на документи между участниците в неговата обработка

Наредбата не предвижда създаване на екземпляри, които се предоставят на следващия в обработката служител. Тоест, наредбата не предвижда осъществяване на движение на документите чрез създаване на екземпляри за изпращане вътре в администрацията.

Целият модел на организация на административната дейност се базира на следните принципи:

- даден документ се поддържа само в един екземпляр в АИС;
- създаването на електронен документ в АИС винаги е свързано и със създаване на достъп до него;
- да се предаде електронен документ от един служител на друг означава предаваният да осигури на приемащия документа достъп до него с ресурсите на АИС;

- всяко движение на документ между служители в администрацията по описаната схема с предоставяне на достъп се регистрира по време и авторство в АИС.

Отразяване на становища по документи

Възможните становища, които могат да бъдат изказани във връзка с обработката на документ са унифицирани като текст и влияние върху процеса на обработка. Те са:

- а) съгласен - не променя хода на изпълнение на процедура по обработка на документ; възможно е да се допълни текст, отразяващ детайли на становището;
- б) несъгласен - не променя хода на изпълнение на процедура по обработка на документ; задължително се посочват мотиви на несъгласието;
- в) за доработка - връща изпълнението на процедурата, в състава на която се обработва документа на по-ранен етап; задължително се дават указания за доработката-или към становището, или директно се въвеждат в текста на съдържанието на документа;
- г) прекратявам процедурата - прекратява се изпълнението на процедурата

Освен това се отбелязват и следните факти:

- Създал документ;
- Коригирал документ;
- Подписал документ.

Това са факти по създаване и обработка на документ, които пряко нямат смисъла на становища, просто защото касаят създаване, корекция или допълване (при подписване) на съдържание на документ. Наредбата дефинира становищата преди всичко като средство за отразяване на етапи по създаване и обработка на документ, ето защо смисълът на становищата се свързва основно с влиянието им на процедурата. Разгледано по-общо, становищата са унифицирани дефиниции на факти по обработка на документи. Наредбата ги третира именно като такива и ги приравнява по формат на представяне в АИС на посочените по-горе факти по създаване, коригирани и подписване на документ.

Преход от обработка на електронно в хартиено съдържание и обратно

Наредбата специално регламентира правия и обратния преход, за да се осигури работоспособност на нейното прилагане и при липса на достатъчно компютърни ресурси в АИС или умения за използването им от служителите в администрацията. Изхождайки от базовия характер на електронната форма на поддържане на съдържание в администрацията, т.н. „прав” преход е преходът от електронна в хартиена форма. Този преход е най-типичен при отразяване на становище по документ и включва следните действия:

- а) служителят, обслужващ прехода, разпечатва съдържанието на обработвания документи и всички изказани до момента становища и регистрирани факти по неговата обработка;
- б) подписва се собственоръчно и предава подписаната разпечатка на служителя, който ще отрази становището си върху нея. Подписът има традиционния смисъл на „Вярно с оригинала”, като под „оригинал” в случая се има в предвид информацията в АИС.

Служителят отразява на ръка върху разпечатката своето становище и го предава на служителя, който трябва да извърши „обратния“ преход- от хартиен носител на съдържание в електронен. Последният въвежда изказаното становище от името на неговия автор, но АИС регистрира че самото въвеждане е направено от съответния служител. След извършване на въвеждането, служителят се подписва на хартиената разпечатка в уверения на това, че правилно е въвел в АИС отразеното на хартия становище.

Издаване на електронни документи от администрацията

а) от документа, подлежащ на издаване, се генерира в АИС „екземпляр за издаване“ и между двата документа се изгражда връзка;

б) екземплярът за издаване се регистрира в официалния документен регистър, като на този етап се въвежда само регистровия номер, тоест регистровия индекс на официалния документен регистър и генерирания пореден номер;

в) регистровият номер се въвежда в съдържанието на документа;

г) подписва се документа и се изпраща в регистратурата; с полагане на подписа в документа се въвежда последния елемент на уникалния регистров идентификатор на документа- датата на неговото подписване; на този етап тя се намира само в съдържанието на документа;

д) служител в регистратурата въвежда в АИС датата от електронния подпис като съдържание на данната „дата на получаване или подписване на документ“.

Така подписания и регистриран електронен документ се изпраща на получателя му и това се отразява в АИС

Издаване на документи на хартиен носител от администрацията

а) от документа, подлежащ на издаване, се генерира в АИС „екземпляр за издаване“ и между двата документа се изгражда връзка;

б) разпечатва се съдържанието на документа и се представя за подпис;

в) подписаният хартиен документ се занася в регистратурата;

г) служител в регистратурата извършва пълна регистрация на документа в АИС, като се генерира регистровия номер и се въвежда текущата дата като дата на подписване на документа;

д) така генерирания УРИ се нанася ръчно върху хартиения документ;

е) така подписания и регистриран хартиен документ се изпраща на получателя, или се предава лично при поискване.

Класификационни структури за поддръжка на масиви от документи

Наредбата не налага никаква конкретна схема за класификация на документи и всички други обекти, които администрациите поддържат с АИС. Това дава пълна свобода на администрациите да развият и поддържат класификационни схеми, които съответстват на спецификата на администрациите и изпълняваните от тях услуги и процедури.

ЧАСТ 6

СТАНДАРТИ ЗА ЕЛЕКТРОНЕН ОБМЕН НА ДАННИ

Електронен обмен на данни

Проведената от структурите на ООН работа по унификация на търговските процедури и стандартизация на обменяните документи се явява основа за по-нататъшното усъвършенстване на електронната търговия чрез въвеждане на електронния обмен на данни. Същността на електронния обмен е в следното: служебната кореспонденция, финансовите, административните, застрахователните, транспортните и пр. документи да се заменят с предаване на съобщения, структурирани по строги международни правила, директно по комуникационните линии между компютрите на участниците в сделката или свързаните с нея дейности.

В практиката всяка фирма има собствена вътрешна информационна система със специфичен формат на данните, което затруднява директния обмен на документите между различните предприятия. Ако някой от участниците в документооборота наложи своя вътрешен стандарт на другите си партньори, на по-малките фирми ще се наложи да осигурят на своите информационни системи възможности те да “разбират” много различни формати на документи. От друга страна, по определянето на формата, по който ще се обменят документите, биха възникнали дълги и безплодни дискусии между отделните бизнес партньори. За да се избегне тази ситуация, са въведени EDI стандартите.

Електронният обмен на данни (EDI - Electronic Data Interchange) е мрежова услуга, предлагаща обмен на данни, която е стандартизирана и независима от конкретните платформи. Американският Национален институт за стандарти и технологии (NIST) определя EDI като: ”обмен между компютри на стриктно форматираните съобщения, които представят документи, различни от монетарните инструменти. EDI съдържа в себе си последователност от съобщения между две страни, всяка от които може да бъде и изпращач, и получател. Форматираните данни, представляващи документите, могат да бъдат пренесени от изпращача до получателя както чрез телекомуникация, така и чрез физически транспортирани средства за електронно съхранение на данни”.

Характерни особености на EDI:

- определя данните като поле във файл, форматът на който е стандартизиран и зависи от конкретната област на дейност (например набор 810 се използва за предаване на фактури);
- по мрежата се предават само специфичните за документа данни. В пълен вид той се появява само на екрана и при разпечатване;
- разполага се на приложното ниво на OSI модела;
- не зависи от средата за предаване на съобщения;
- работи не само с текстове, но и с неподвижни изображение, фрагменти, звук и т.н.;
- структурата му се определя от набор транзакции, които позволяват да се структурират и идентифицират данните, необходими за изпълнение на конкретна делова операция;

- управлява номерирането на транзакциите и потвърждение за получаване им.

В развитите страни електронният обмен на данни се разглежда като един от най-съществените елементи от широко развиващия се процес на усъвършенстване на управлението на икономиката (т.н. Business Process Reengineering).

За да може да се използва реално в електронната търговия, електронният обмен на данни трябва да бъде легализиран, т.е. трябва да се основава на международно приети правила, които да узаконяват всички негови елементи. Включително, електронните съобщения би трябвало да имат доказателствена стойност пред съдебните или арбитражни органи в случай на разглеждане на спорове между участващите в електронната търговска дейност страни.

За да бъде осигурена тази легализация на електронния обмен на данни, международните организации са приели редица нормативни документи. Такива документи съществуват и в националните законодателства.

UN/EDIFACT – стандарт за електронен обмен на данни

Съкращението UN/EDIFACT се разшифрира като "Правила на ООН за електронен обмен на документи за администрацията, търговията и транспорта" (United Nations rules for Electronic Data Interchange For Administration, Commerce and Transport).

Първоначално всяка развита държава е имала собствени EDI стандарти (DAKOM в Швеция, GENCOD във Франция, TRADACOMS в Англия, SEDAS в Германия и др.), което значително е затруднявало търговията между тези страни. Поради това, посочената в предишните части Работна група 4 към Икономическата комисия за Европа на ООН (от 1994 г. UN/CEFACT) разработва международен стандарт за обмен на електронни документи UN/EDIFACT.

На база на тази разработка Международната организация по стандартизация (ISO) приема през 1996 г. UN/EDIFACT като международен стандарт ISO 9735. През 2002 г. беше приета актуализирана версия на този стандарт, която е в сила понастоящем.

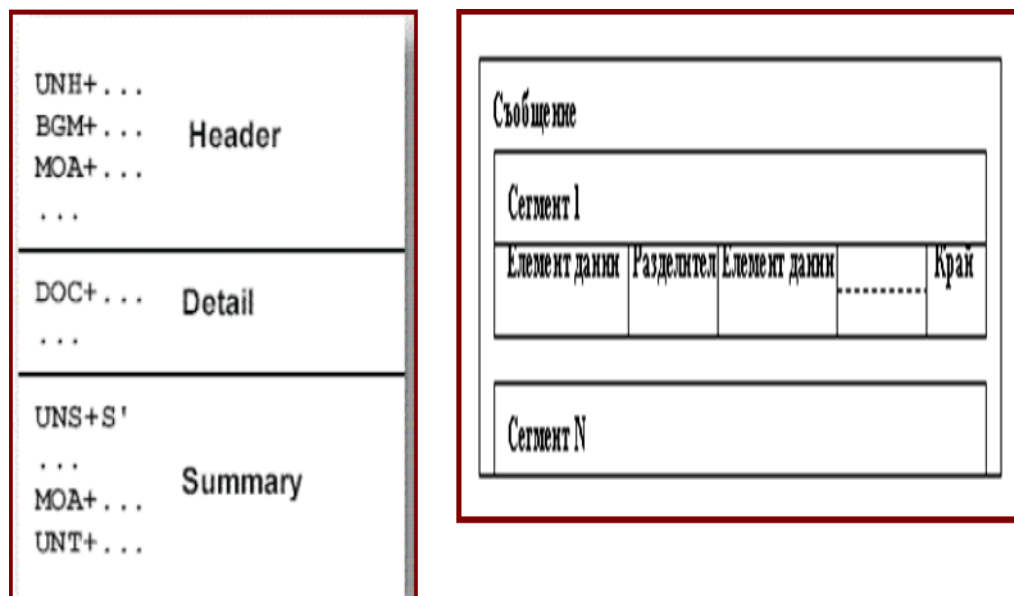
Главните особености на този стандарт са, както следва:

- обменът се осъществява чрез съобщения;
- стандартизацията на ниво съобщение е по типа на използвания документ;
- съобщенията имат йерархическа структура и се състоят от сегменти.
- стандартизацията на данните се осъществява на ниво сегменти и елементи на данните;
- сегментите могат да се групират по определен признак;
- незапълнените сегменти могат да се изпускат;
- типовите полета се записват във вид на код;
- съставът и запълването на справочниците се стандартизира на три нива – международно, национално и корпоративно;
- стандартът е независим от езика, използван за общуване.

Стандартът предвижда всяко съобщение да има уникален 6-значен код от заглавни букви. За различни приложения са разработени стандартни съобщения, които отговарят на конкретен документ, унифициран и стандартизиран от същата работна група. Тези

документи са представени в поддържаната от UN/CEFACT директория на електронните съобщения, която се актуализира ежегодно. Понастоящем тези съобщения са над 180.

Например: INVOIC е електронно съобщение, което отговаря на документа „фактура“, PAYORD – на документа „платежно нареждане“, IFTMCS – железопътна товарителница и т.н.

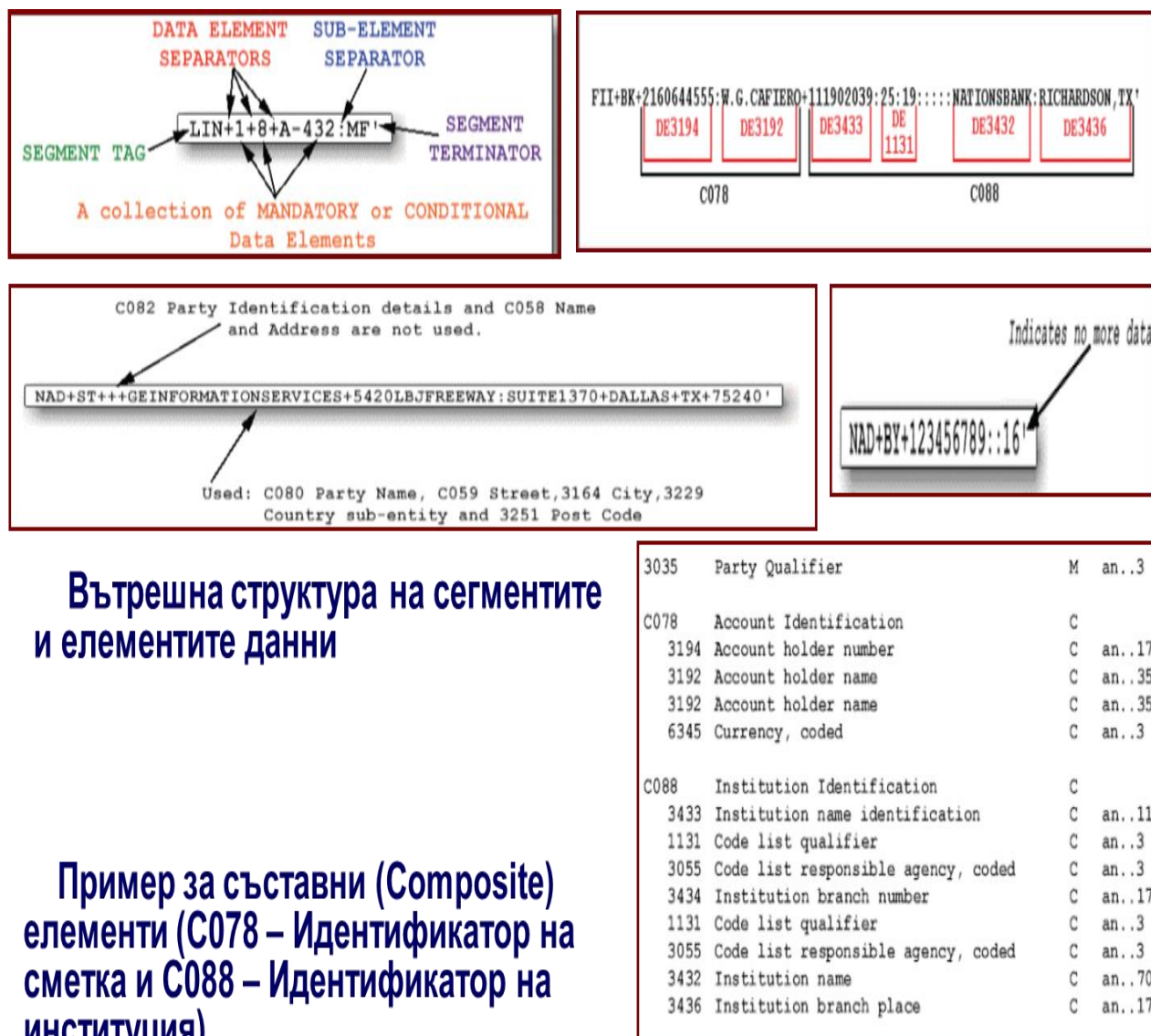


Фигура 6-1

Position	Tag	Name	Req	Rept
0010	UNH	Message Header	M	1
0020	BGM	Beginning of Message	M	1
0030	BUS	Business Function	C	1
0040	DTM	Date/Time/Period	M	4
0050	Segment Group 1		C	2
0060	RFF	Reference	M	1
0070	DTM	Date/Time/Period	C	1
0080	FTX	Free Text	C	5
0090	PAI	Payment Instructions	C	1
0100	FCA	Financial Charges Allocation	C	1
0110	Segment Group 2		M	1
0120	MOA	Monetary Amount	M	1
0130	CUX	Currencies	C	1
0140	DTM	Date/Time/Period	C	2
0150	RFF	Reference	C	1
	etc.			
	etc.			

Сегментът е съставна част на съобщението. Всеки сегмент има 3-значен код от заглавни букви. Сегментите завършват със конкретен символ. Стандартът предвижда около 200 различни типа сегменти.

Сегментите се състоят от елементи данни, които могат да бъдат прости (аналог се явява полето данни) и съставни (2-3 полета данни). Елементите данни нямат имена. Те са разделени със разделител (символ "плюс"). Всеки елемент заема определеното си място в сегмента. Ако някой от елементите не е необходим, то той се замества с разделител. Предназначението на всеки елемент се определя в справочник на сегментите EDSD, който влиза в набора стандарти UN/EDIFACT.



Фигура 6-2

Всички елементи данни (съставни и прости), които се използват в международната търговия, както и правилата за тяхното използване, са описани в международния стандарт ISO 7372.

Анализът на търговската транзакция и образуващите я цикли е позволил да бъдат разработени съставните части на електронния обмен, или казано иначе – на неговата морфология. Това включва следните документи, които се поддържат и публикуват от UN/CEFACT и всяка година се актуализират:

а) Справочник на стандартните електронни съобщения на ООН (досега са разработени и са в различни фази на утвърждаване над 180 съобщения – регламентирани структури от данни, изпълняващи конкретна делова или административна функция). В повечето случаи съобщението е еквивалент на точно определен документ: фактура, платежно нареждане, митническа декларация, нареждане за превоз, застрахователна полица и т.н.;

б) Справочник на стандартните сегменти на ООН – сегментите са групи от данни, формиращи съобщението и свързани с някаква точно определена функция в него. Например, сегментът LOC (Place/Location Identification) изпълнява функциите да идентифицира мястото на определено действие, отразено в съответния документ (производство, натоварване, плащане и т.н), както и местата на свързаните с това действие релации.

в) Справочник на стандартните прости елементи от данни на ООН – т.е. единици от данни, формиращи сегмента, за който са определени методите на идентификация, описание и предоставяне на значението. Например, в споменатия сегмент LOC един от простите елементи е 3227 – „Квалификатор на мястото”.

Простите елементи са обединени в 9 групи, както следва:

I група – служебни елементи;

II група – елементи, свързани с дати и периоди от време;

III група – елементи, свързани с адреси, места, страни, субекти;

IV група – елементи, свързани с клаузи, условия, инструкции и др.;

V група – елементи, свързани с плащания, финанси, статистика и др.;

VI група – елементи, свързани с мерни единици;

VII група - елементи, свързани с продукцията и стоки;

VIII група – елементи, свързани с транспортния процес;

IX група – други елементи.

г) Справочник на стандартните съставни елементи на ООН – това са групи от няколко концептуално свързани прости елементи, образуващи общо понятие. Например, в сегмента LOC, споменат по-горе, съставният елемент C517 „Идентификация на мястото” се състои от четири прости елемента, както следва:

3225 „Идентификатор на мястото”;

1131 „Квалификатор на кодовия списък”;

3035 „Институция, отговорна за кодовия списък” и

3224 „Код на мястото”

д) Списък на кодовете на ООН – под код се разбира поредица от символи, използвани да идентифицират елементите от данни в символична форма, така че да бъдат разпознати от компютъра. Например:

- кодовете на България и българската валута (лев) в буквена и цифрова форма са съответно: BG, BGN и 100;
- в простия елемент от данни 3139 „функции в контакта” кодовете са: AG – агент, BK – банка, CA – превозвач (Carrier), C – получател (Consignee), IN – застраховател (Insurer), SU – доставчик (Supplier) и т.н.;
- в простия елемент от данни 4431 „Гаранции при плащането” кодът 10 означава „Банкова гаранция”, 11 – „Държавна гаранция”, 12 – „Гаранция от трета страна и т.н.

Необходимо е да се подчертае, че методите за създаване на UN/EDIFACT са го направили независим от хардуерната и софтуерна платформа, от приложните задачи, от

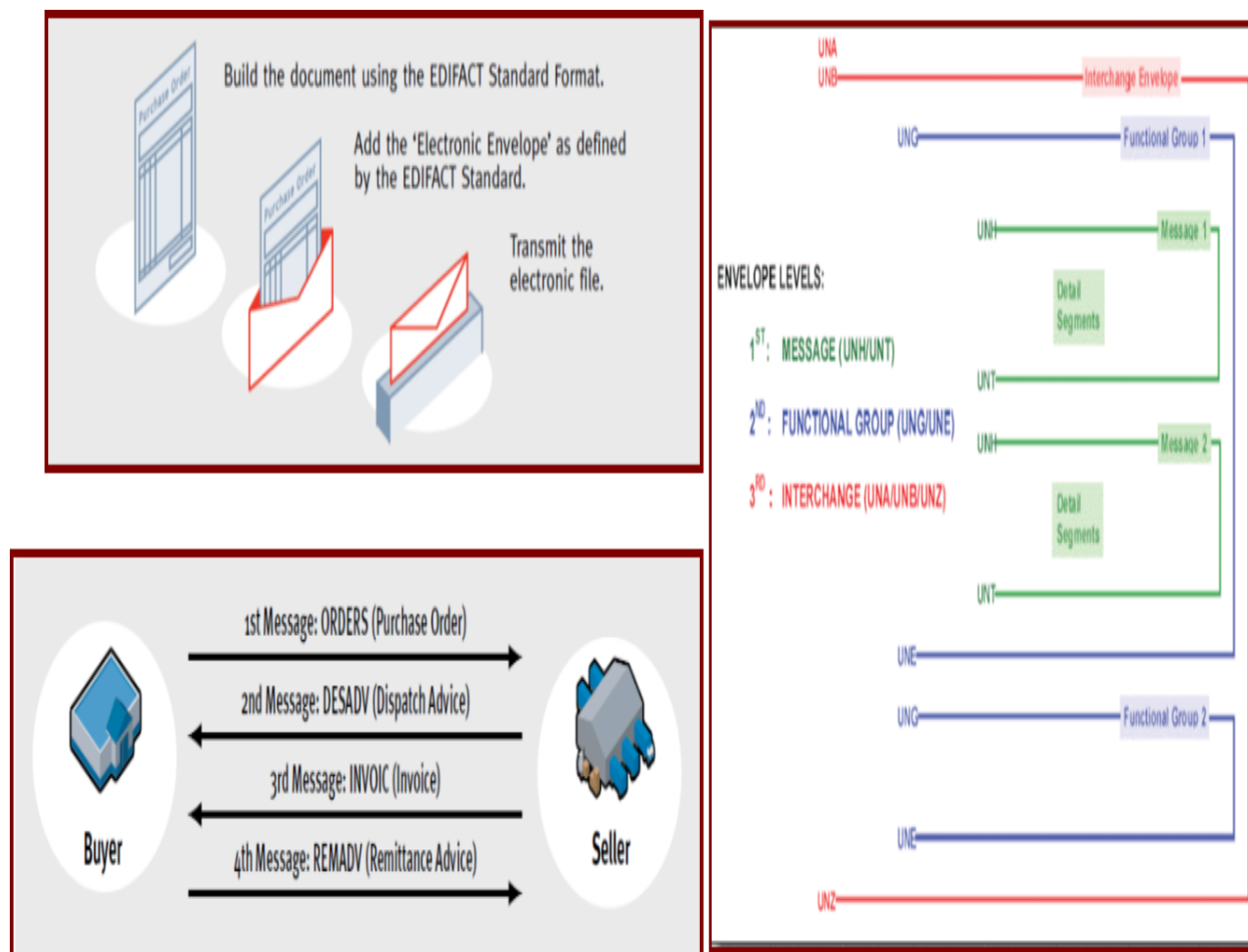
протоколите за телекомуникационен обмен. Вzeti са мерки за ограничаване до минимум на влиянието на вътрешните информационни системи, между които се осъществява електронния обмен. Всичко това е създадо предпоставки за утвърждаването на UN/EDIFACT като универсално средство за междусистемни комуникации.

Поради сложността и спецификата на обменяните документи в отделните бизнес отрасли, EDIFACT се състои от няколко подмножества типови документи, специфични за конкретната област. По известните от тях са:

- SWIFT – за финансовите институции;
- EANCOM – за производство за стоки за масова употреба;
- ODETTE – за автомобилната промишленост;
- EDIFICE – за електронна промишленост;
- EDITEX – за текстилната промишленост;
- EDILIBE – за търговията с книги;
- CEFIC – за химичната промишленост;
- RINET – за застраховането;
- EDIFURN – за мебелната промишленост и др.

При класическия EDI процес предприятието А изпраща електронен документ до предприятието В. Източникът на документа е In-house (ERP, CRM или др.) приложението на А. Адаптерът на EDI приложението поема документа и го вкарва в EDI системата. Първоначално документът е в т.н. In-house1 формат (специфичен за информационната система на А). Той бива конвертиран от конвертора в някой от EDI стандартите (в зависимост от договорката между бизнес партньорите).

За успешното конвертиране се грижи т.н. mapping - скриптово описание, което дефинира как да се преобразуват данните от единия формат в другия. Така създаденият EDI документ се изпраща до комуникационен порт, който се грижи за транспортирането до бизнес партньора В. Пристигнал в В, EDI документът преминава през обратната обработка: комуникационен порт, който се грижи за получаването или изпращането на EDI документите. Накрая адаптерът се грижи за доставяне на вече четимото съобщение към вътрешната информационна система на В.



Фигура 6-3

Класическото EDI приложение трябва да има задължително следните елементи:

а) Адаптери за връзка с In-house - информационната система на клиента (ERP, CRM, ...). Адаптерите са специфични и могат да бъдат различни както по отношение на ERP системата, така и по отношение на нейната версия. При наличие на непопулярна и слабо разпространена In-house (ERP) система, може да се наложи доработка или разработка на адаптер специално за конкретната ERP система.

б) Конвертирането между различните формати документи е основна функция на всяка EDI система, затова конверторът играе основна роля. Той би трябвало да може да извършва както синтактични конверсии (разделители, сегментни тагове, използвани символни множества, възможности за повторения и др.), така и семантични конверсии (извършват аритметични и стрингови операции над полета, като може да ги обединяват или разделят, сменят кодовете в съответствие със специфичните за клиента кодове и др.). Също така от конвертора се очаква да може да групира и разделя съобщенията. Групирането се отнася за изходните съобщения към един получател, така че да бъдат изпратени в една сесия. Разделянето е необходимо за пристигналите в една сесия съобщения на отделни изпращачи, които да се обработват едно по едно от ERP системата.

в) Комуникационният модул е друг важен съставен елемент на EDI софтуера. Той трябва да е достатъчно гъвкав, за да предложи възможност за изпращане на EDI документите по различни комуникационни канали.

Класическите протоколи, по които се ползват още от зората на EDI, са:

- X.400 - e-Mail стандарт на ITU;
- OFTP Odette File Transfer Protocol, може да работи в/у ISDN;;
- TCP/IP, X.25 или X.31;
- FTAM (File Transfer Access and Management).

Освен тях съществува голям набор от национално, продуктово, или браншово-специфични протоколи в рамките на определени VAN (Value Added Network) мрежи. Освен тях с появата на Интернет за комуникация се използват Интернет протоколите SMTP, HTTP, FTP, на тяхна база се изграждат Web-базирани специфични EDI протоколи като AS1 и AS2.

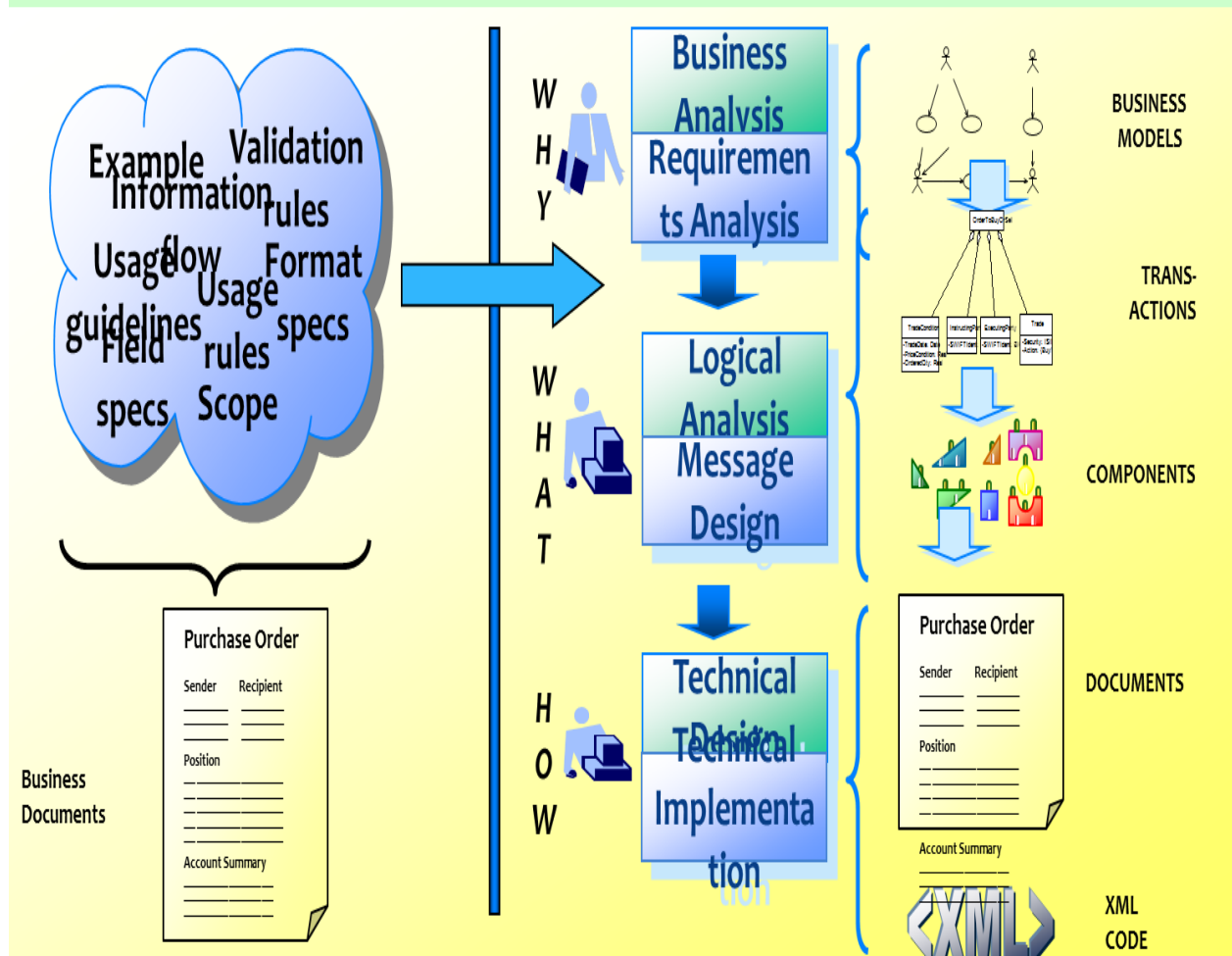
г) Мениджмънт на пристигащите и изпращаните документи - тъй като EDI включва бизнес транзакции и целта е този процес да бъде автоматизиран и да протича без надзор, важно е този тип софтуер да бъде в състояние да контролира потока от съобщения.

Това включва следните функционалности:

- лог на получените и изпратените съобщения (Logging of messages);
- одит на съобщенията, т.е. да може във всеки един момент да се проследява пътя на всяко едно съобщение (Audit trails);
- възстановимост на съобщенията (Recovery files), т.е. да се запазва съдържанието на съобщението, така че при възникването на грешка на някой от следващите етапи информацията да не се губи и да може да се рестартира обработката на съобщението;
- система за докладване на грешки (Error reports); възможност за даване на статус на всяко едно съобщение (Status reports);
- архивиране и почистване на системата (Purging and Archiving) от напълно обработените съобщения;
- сигурност - системата трябва да може да поддържа определено ниво на сигурност както при прехвърлянето на данните, така и в цялата система. Нивото на сигурност зависи от естеството на бизнес-процесите. То може да варира от елементарна защита с парола за вход до автентификация на партньорите с цифрови подписи и криптиране на данните.

Инициатива “Electronic Business XML”

Съвместната инициатива на UN/CEFACT и OASIS, наречена ebXML, имаше за цел да съчетае повече от 20-годишния опит на EDI с възможностите на XML, така че да се избегнат ограниченията на UN/EDIFACT.



Фигура 6-4

ebXML - усъвършенстван стандарт за обмен на данни

Системите ebXML (Electronic Business using eXtensible Markup Language) представляват семейство от XML-базирани електронни стандарти, чиято основна цел е да предоставят XML-инфраструктура за глобален обмен на електронна бизнес информация по интероперативен, безопасен и консистентен начин между всички бизнес партньори по света. Основават се на XML (eXtensible Markup Language) – специализиран метаезик за създаване, съхранение и обмен на структурирани данни.

ebXML може да бъде определен и като модулен пакет от спецификации, които осъществяват финансово - правната кореспонденция между различни по размер, разположение и ориентация бизнес институции. Посредством технологията ebXML и преди всичко, нейната компютързация се заражда и един изцяло нов стандартен електронен метод за обмен и обновяване на съобщения и база данни, реален контрол на бизнес-взаимоотношения, както и регулация на бизнес-процесите между редица съвместно

коопериращи бизнес-единици. В това число влизат финансови агенти като банки, индустриални предприятия, държавни институции, техните подразделения, вътрешен и външен транспортен сектор, както и много фирми с различен по рода си предмет на дейност.

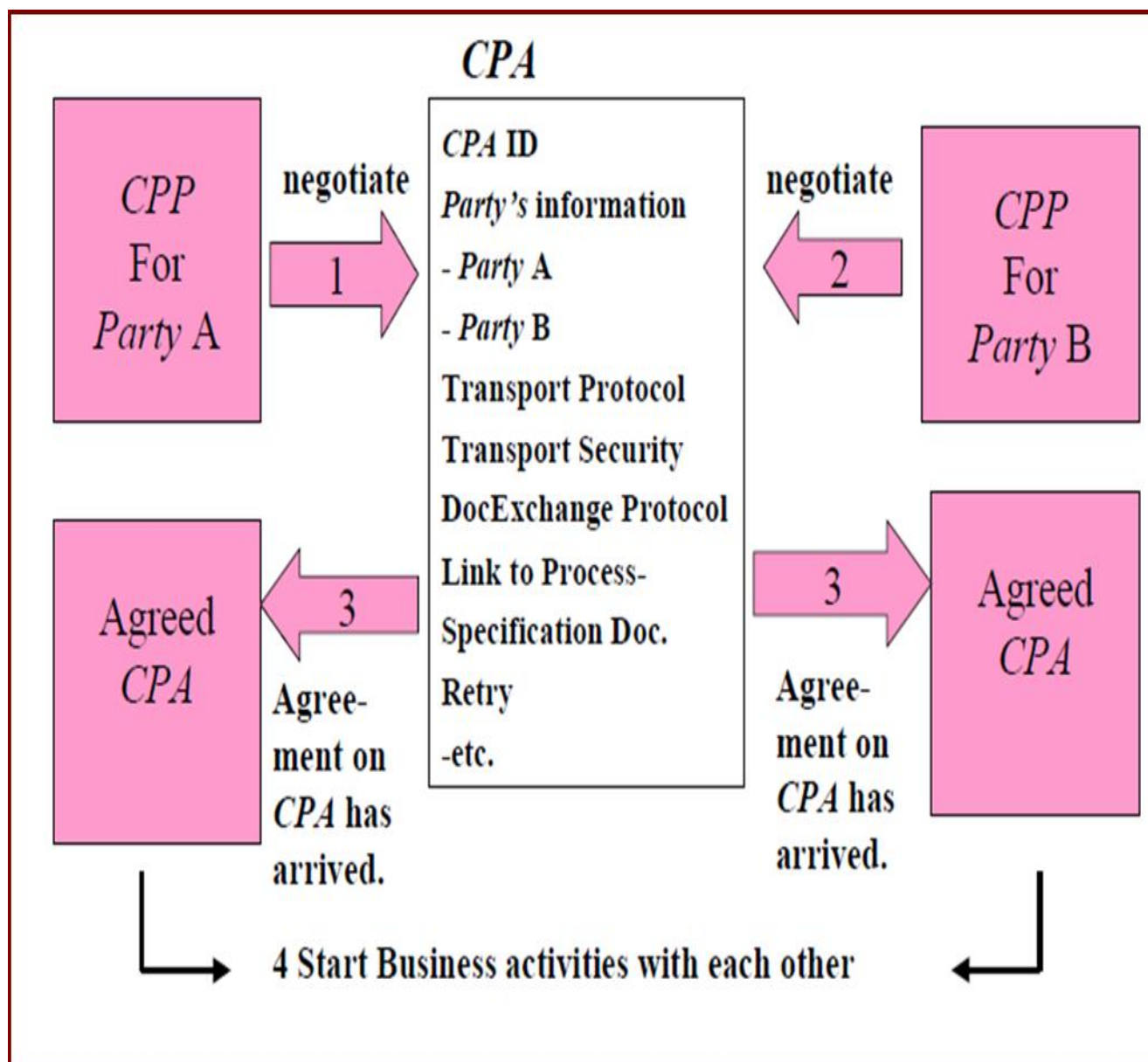
Исторически ebXML стандартите са основоположени и развити от самото им начало през 1999 от интернационалния консорциум ОАЗИС (OASIS - Organization for the Advancement of Structured Information Standards), както и от вече споменатия UN/CEFACT. Професионалното направление на тези две организации е предимно свързано с развитието, въвеждането и интегрирането на стандарти за бизнес - електронно и мрежово обслужване на клиенти във фундаменталните сектори на всяка една икономика.

OASIS и UN/CEFACT следват общите днешни пазарни тенденции и визират възможности за глобална информационна електронизация на повечето световни пазари, с цел подпомагане на държавни политики, намаляване на транс-акцизни такси, улеснен обмен на данни и намаляване на бюрокрацията. С това и основната идея за въвеждане и ратифициране на един всеобщо приет унифициран е-стандарт става и директно определящ фактор за редица държави, чиито основни насочености са да поощряват, защитават, улесняват и подобряват наличните условия на своите бизнес, търговски и административни организации и фирми във вътрешен и световно - икономически план.

В допълнение на това, ebXML цели и сходимост в информационен план – възможност за всички компании от всички среди и размери да допринесът и оптимизират вече съществуващи EDI решения, прераствайки в един конвергиращ XML базиран стандарт, носител на дълбок глобален опит в електронния бизнес. Именно това са и основните идеи, заложили в ebXML, намерили силен отзвук в повечето модерни и надеждни електронни информационни системи на 21 век.

Първоначалната идея на създателите на ebXML обхваща пет нива спецификации на данни, включвайки XML стандарти за всяко едно от тях : първо - процеси, обусловени в рамките на бизнеса ; второ - ключови за дейността данни и информационни компоненти; трето - споразумения по колаборационни протоколи ; четвърто - съобщения и пето - регистри и репозитории. Тези пет основни компонента стават предмет на дейност на създателите в периода 1999 – 2002 г. Те се изпълняват на базата на нормативен документ с изисквания и като допълнително условие се създава ebXML техническа архитектурна спецификация. Впоследствие специализираното подразделение на Международната организация по стандартизация ISO TC 154 ратифицира предложените пет ebXML спецификации като международни стандарти ISO 15000, части 1-5. Формалното разпределение на имената има следния ред : част 1 – колаборативно – партньорско споразумение, част 2 – сервизна спецификация по съобщенията, част 3 – регистрационно-информационен модел, част 4 - регистрационно- сервизна спецификация и част 5 – техническа спецификация на ключови за дейността данни и информационни компоненти. Поддръжката и обновлението на ebXML остава под контрола на концептуалните му създатели, като компанията „freeebXML” поема инициативата около изграждането и внедряването на ebXML - базиран софтуер с отворен код, чиято техническа редакция може да бъде свободно проведена от сектора или организацията, участващи в обмена на данни в електронен вид.

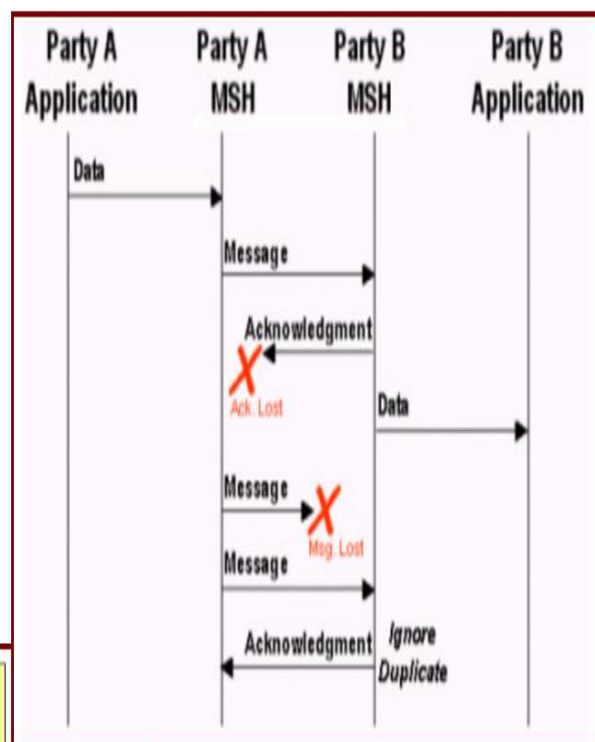
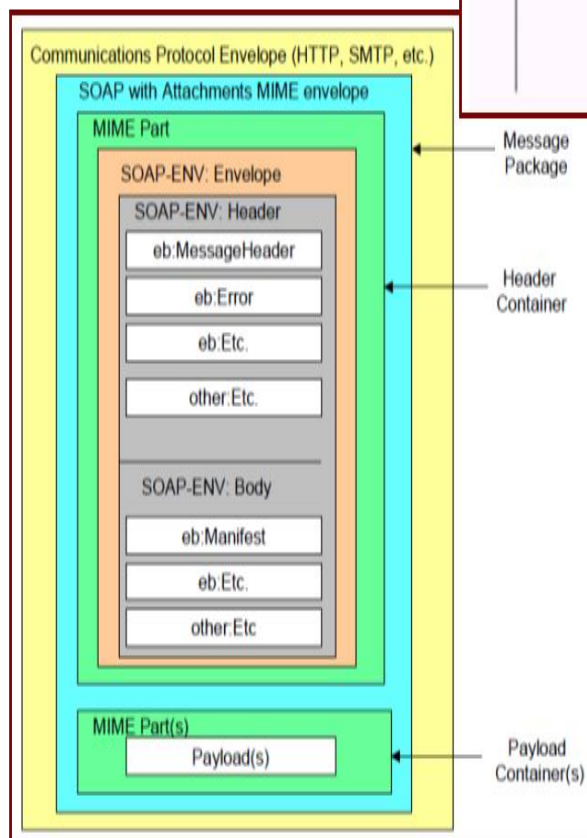
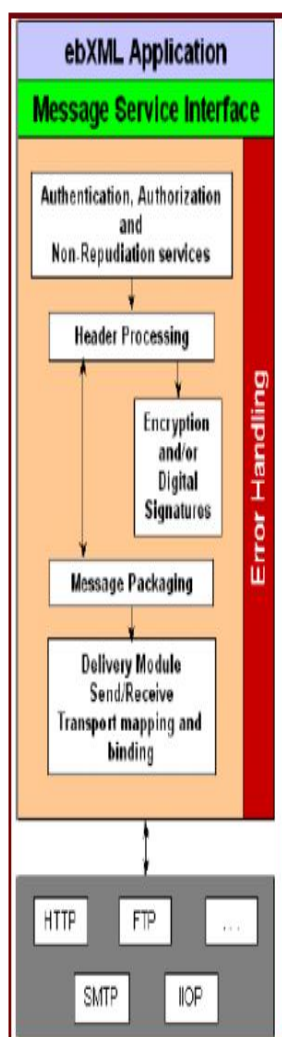
Спецификация “Colaboration Protocol Agreement”



Фигура 6-5

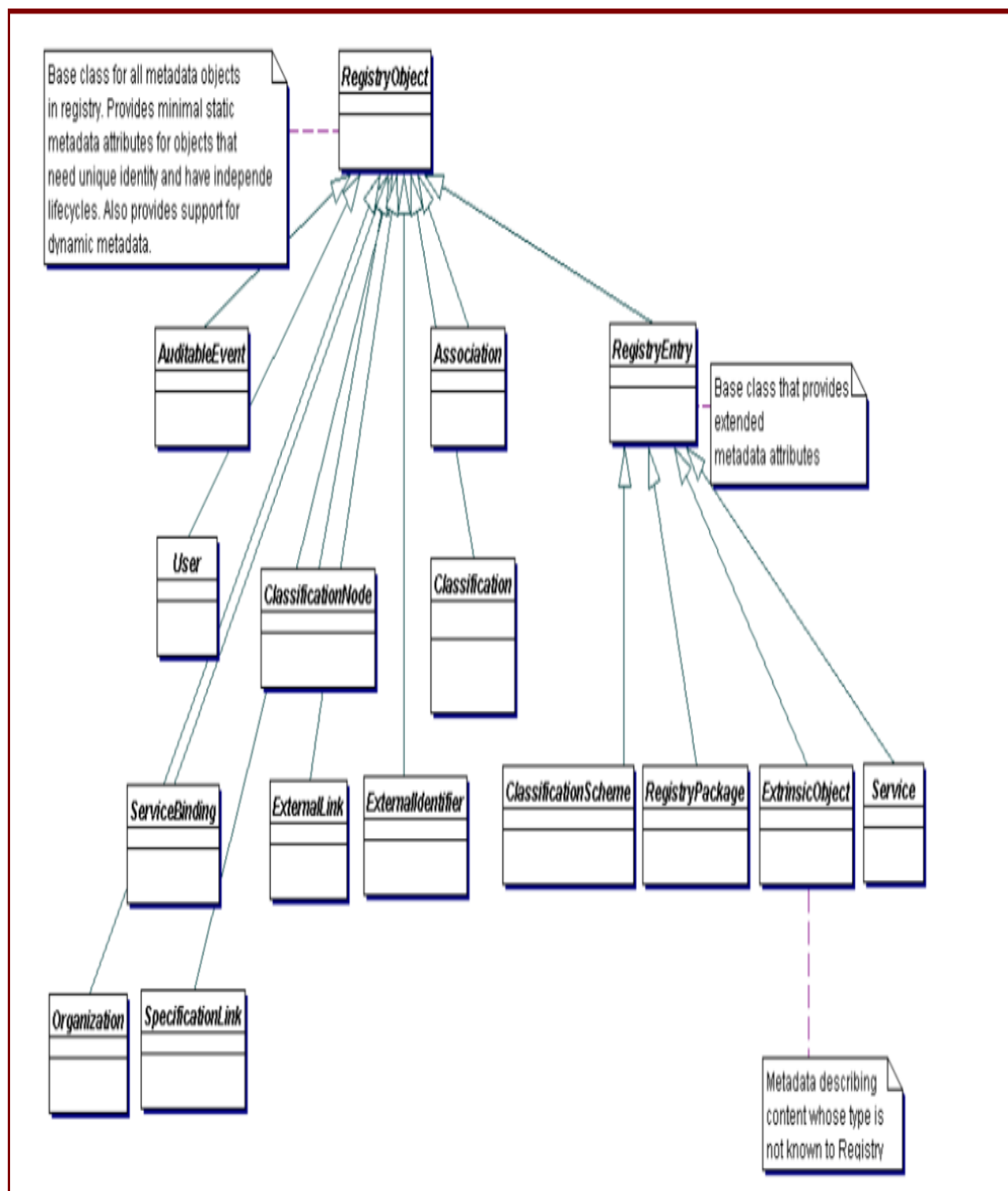
Спецификация “Messaging Service”

Спецификацията се базира _____
на протоколната спецификация
SOAP на W3C _____



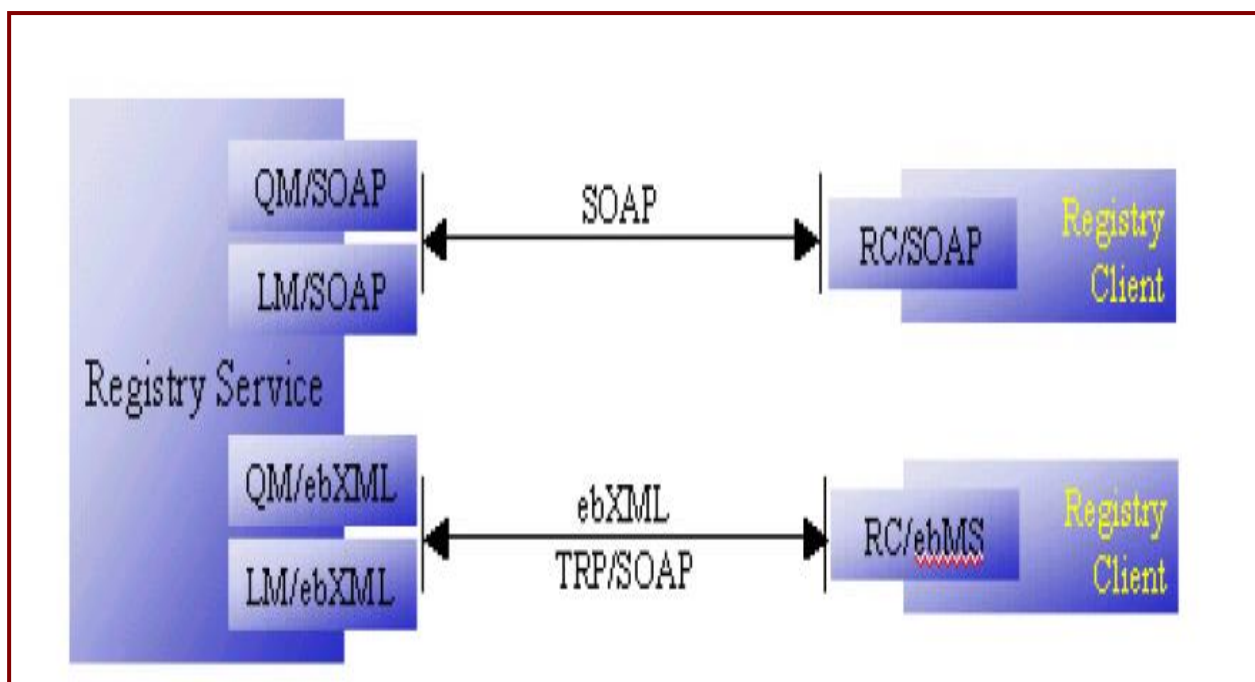
Фигура 6-6

Спецификация “Registry Information Model”



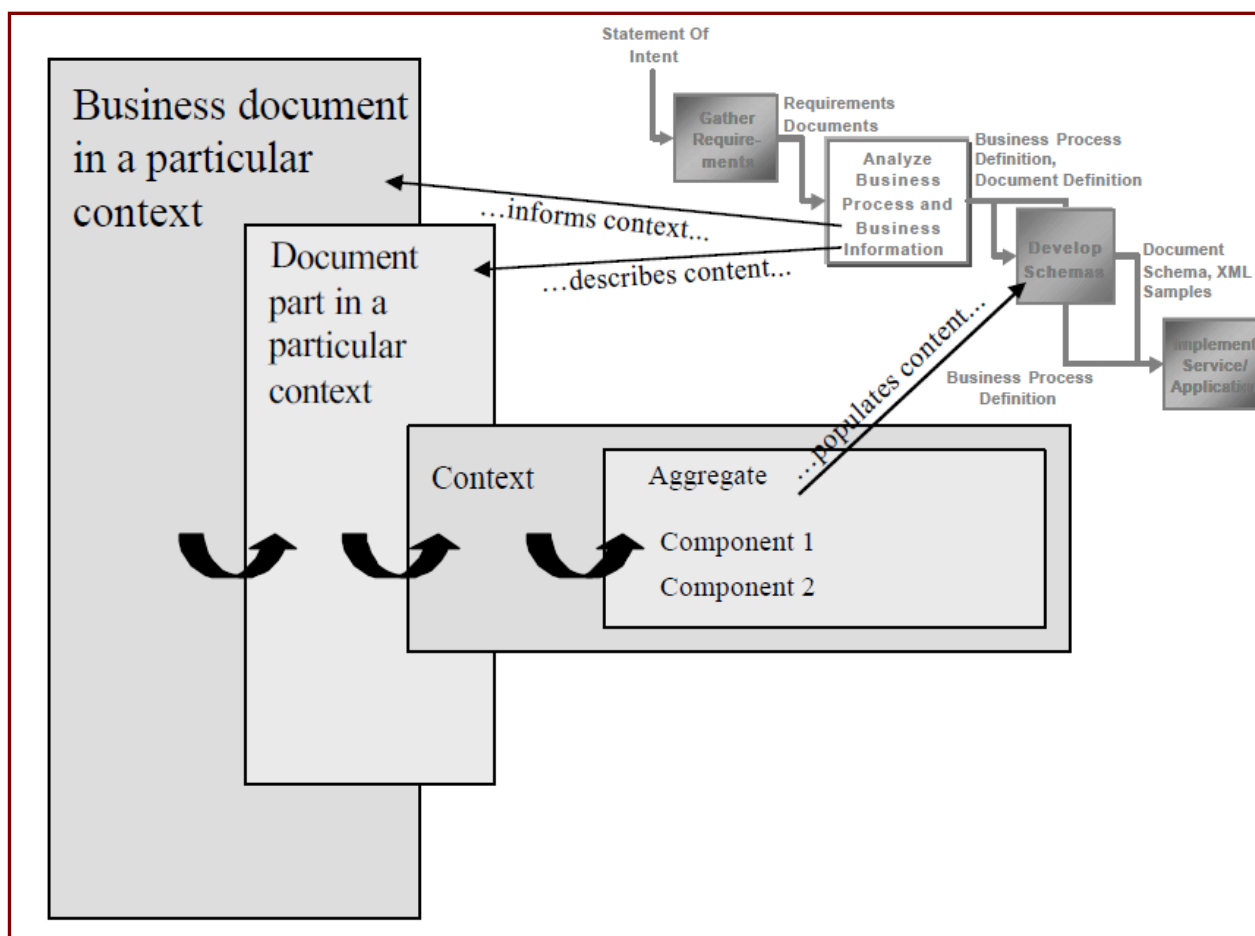
Фигура 6-7

Спецификация “Registry Services”



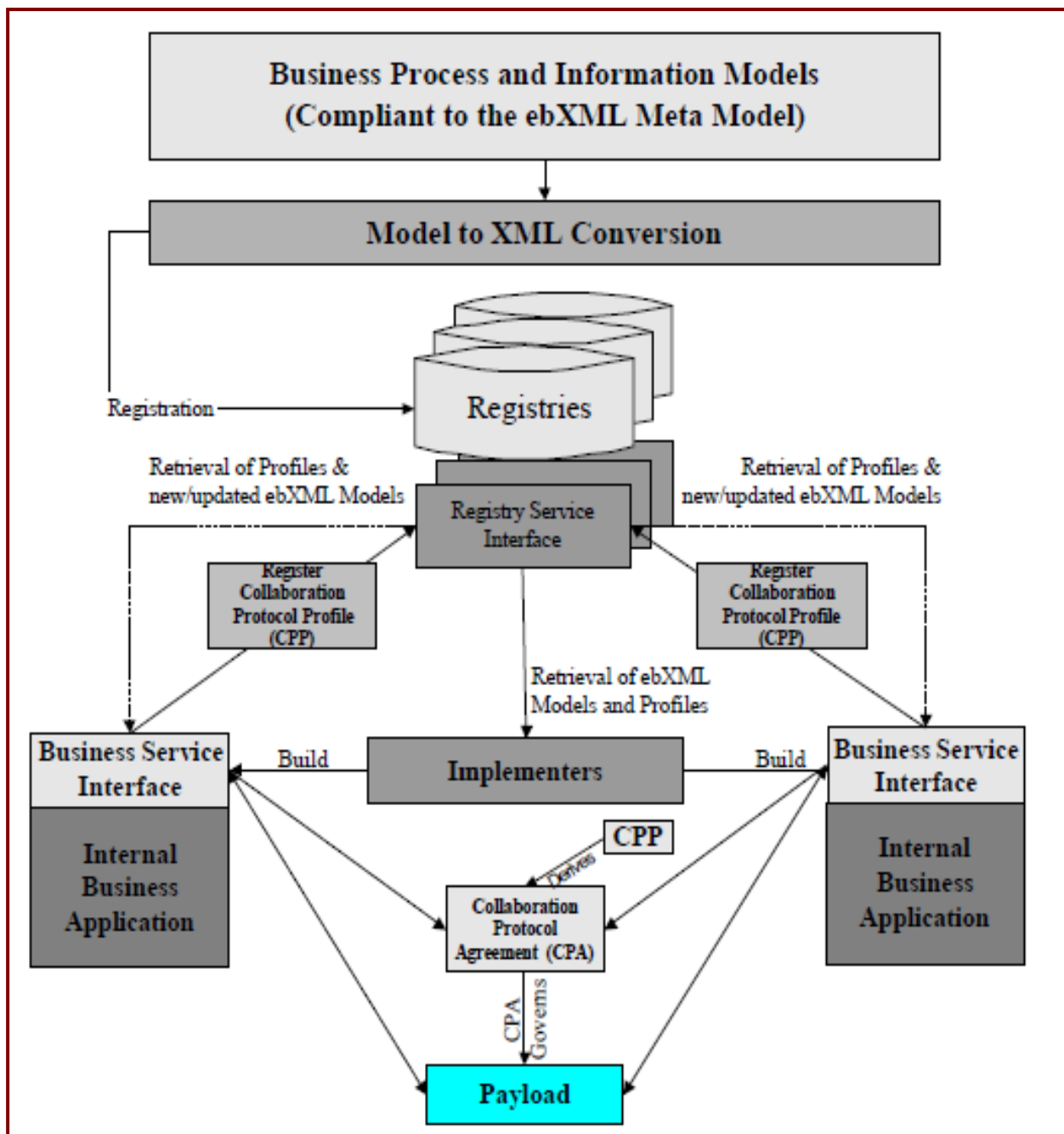
Фигура 6-8

Спецификация “Core Components”



Фигура 6-9

Спецификация “Technical Architecture”



Фигура 6-10

ebXML - усъвършенстван стандарт за обмен на данни

Архитектурата на ebXML представлява уникална по рода си система от концепции, чиито основи са силно теоретични и кодифицирани в документален вид, но в последствие компетентно разработени и реализирани в ebXML-стандартни компютърни програмни среди с широко приложение в бизнес секторите. От техническа гледна точка, ebXML възниква въз основа на по-ранните разработки на обектно - ориентирания ooEDI (object oriented EDI –Electronic Data Interchange), моделиращите методологии UML / UMM, и така наречените XML markup технологии във връзка със създадените X12 EDI "Future Vision" разработки, спонсирани от фамилията електронни стандарти ANSI X12 EDI, които са и първите основополагащите в световен план американски стандарти за обмен на електронни данни (ANSI).

Сливането на тези всички компоненти – теоретични концепции, методологии, стандарти и информационни методи на базата на компютърни езици и иновативни електронни технологии, дава развитието на едно етапно във времето и силно финансово поощрено развитие на ebXML покрай двамата си спонсора. От теоретична гледна точка, ebXML търпи и до днешен ден оптимизации и промени в повечето си аспекти. Докато стандартите ebXML, приети от ISO и OASIS, се опитват да предоставят готови ефективни XML механизми, които да могат да бъдат приложени директно в практически ситуации, самата архитектура на ebXML е предимно фокусирана върху концепциите и методологиите, които могат да бъдат създадени и предоставени на голямо количество потребители с цел те да приспособят e-Business решения в професионалната сфера. Типичен пример за използването на една конкретна ebXML базирана спецификация е CCTS (Core Components Technical Specification), която е интегрирана в компютърната бизнес среда на OASIS. Именно CCTS, посредством нейните основни XML фундаменти, позволява извършването на бизнес транзакции, съставяне на разписки, платежни и поръчкови ордери, уведомления за доставки и пр.

От основно значение в структурата на ebXML са съобщенията и мерките за сигурност, които биват създавани и упражнявани при обмена на информацията, както и тези, задавани с цел предпазване на съдържанието им. В контекста на понятието съобщения (messaging), е целесъобразно да се разгледат тези ebXML спецификации, при които обмена на данни и предприетите за това мерки за сигурност са ясно дефинирани. Към това се отнасят колаборативно – партньорските споразумения (ISO 15000, част 1). Колаборативно – партньорските споразумения са XML базирани документи, които специфицират търговски споразумения между бизнес-партньори.

По правило всеки един партньор има свой собствен документ, наречен Collaboration Protocol Profile (CPP), в който са описани правомощията и задълженията на съответната страна във формат XML. В тази връзка, в един CPP документ са задължително упоменати протоколите за съобщенията, които ще се поддържат и спектъра на мерките за сигурност, които са създадени с цел тяхна защита. На по-високо ниво са така наречените формални CPA документи, които са възникнали от сливането на два CPP документа и съдържат правна информация за отношенията между двете страни.

В един стандартен CPP-документ се съдържат следните данни:

- информация относно разпознаването на документа: автентични знаци за разпознаване на всяка една от участващите страни и тяхната роля в рамките на едно търговско споразумение;
- информация за сигурността - например, използвани ли са цифрови подписи и какви алгоритми се използват от тях;
- информация относно комуникацията - протоколите, които ще бъдат използвани при обмена на документи;
- е-Адрес на крайните получатели - URL адресът, предимно необходим за сервизни и съобщения от висока важност;
- правила, които трябва да се следват, когато потвърждения за изпратени съобщения не са получени, както и такива, които включват детайли като приблизително време за чакане преди преизпращане и до колко пъти може да се преизпраща дадено съобщение;
- дали трябва да бъдат игнорирани дублирани съобщения;

- дали са необходими потвърждения за всички получени/изпратени съобщения.

Тези изисквания на СРР заставят участващите страни да уточнят електронно-правните условия и могат да бъдат тълкувани като условия, посредством които се установяват допустими рамки на съдържание и начини за обмена на съобщенията. В тази връзка е нужно са се отбележи, че еднакви формални правомощия относно обмена на съобщенията се делегират и на двете страни в едно споразумение.

Страните са задължени да представят пълна информация за техните налични електронни ресурси, електронни подписи, протоколи, адреси, както и правила за приемане, изпращане и преизпращане на съобщения. Тази чисто формална дейност се съгласува и от двете страни и взема с консенсусно решение.

Като ефективна защитна мярка за сигурност на обмена е въведен и така нареченият ebMS (e-Message Service Specification). Той представлява комуникационно-неутрален механизъм, който трябва да бъде следван от системите, изпращащи съобщения (така наречените Message Service Handlers (MSH)), за да могат те да обменят по електронен начин техните бизнес- документи, договори, както и финансови средства.

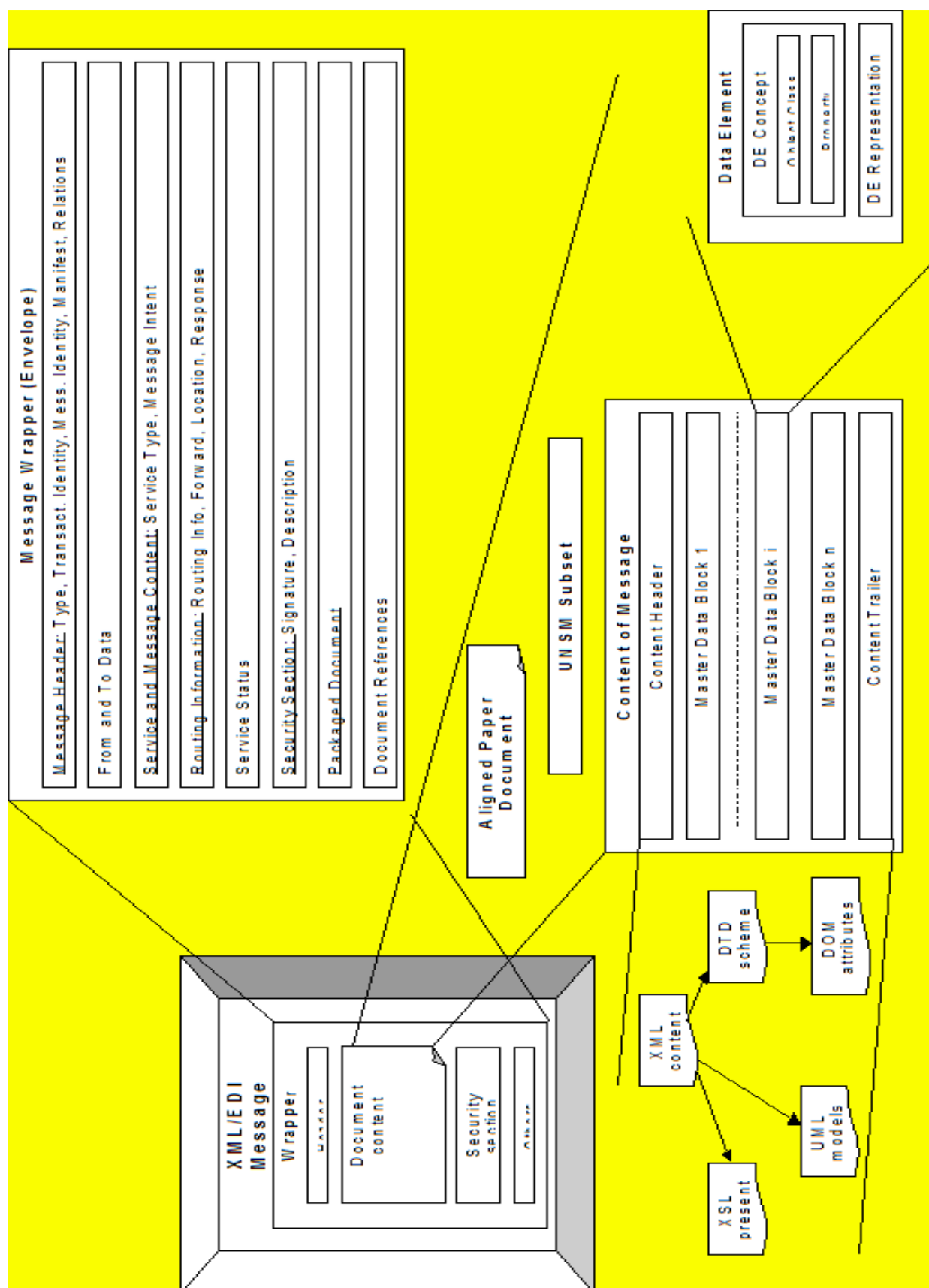
Последната версия на тази спецификация - ebMS 2.0, е изградена на база на препоръката на W3C SOAP (Simple Object Application Protocol). Съобщението съдържа мета-данните (много от които са СРР изисквания), необходими за размяна на бизнес-документи по сигурен и неоспорим начин, така както и данни за обмен на движими или недвижими активи / имущество, акции, пари в кеш, чекове и пр.

Редица подобни съобщения могат да бъдат прикрепени към определена SOAP-структура. В много случаи, форматът на всички съобщения е извън рамките на ebXML спецификациите, поради което се налага вземането на допълнителни мерки за сигурност на обмена. При това за всяко ebMS съобщение се изисква наличието на:

- автентичен идентификатор (ID) на съобщението;
- получател на съобщението;
- изпращач на съобщението;
- идентификатор на обмени, към които могат да се свържат сходни съобщения;
- цифров подпис, който се базира на “XML Signature”-спецификации;
- индикация за това, дали трябва да бъдат игнорирани дублирани съобщения;
- индикация за това, дали са необходими потвърждения.

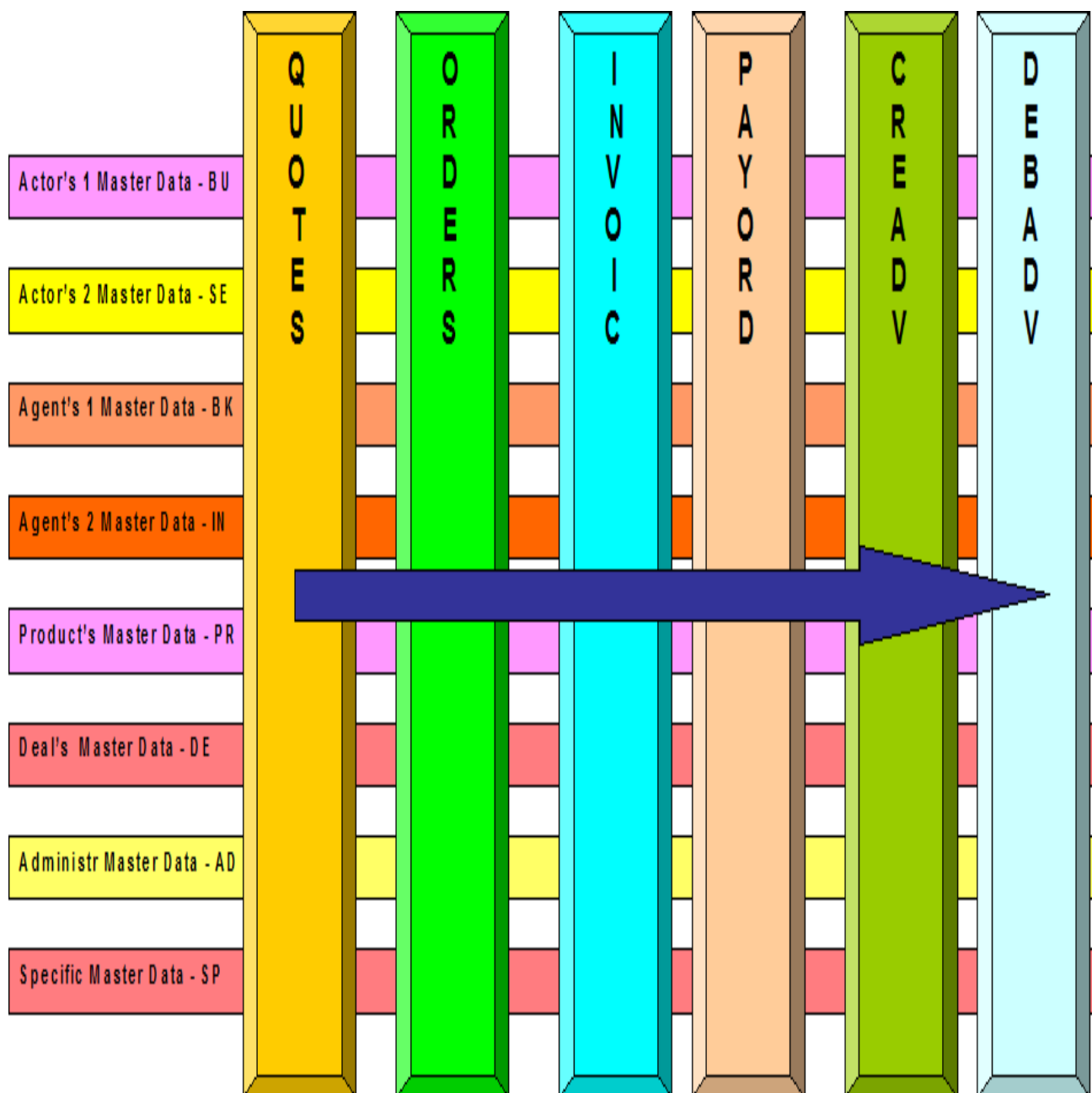
Именно тези изисквания обхващат обема на необходимата и от двете страни допълнителна информация, която трябва да е налична, за да удостоверят автентичността на документа. Самият механизъм ebMS е сам по себе си двуслойна мярка за сигурност – от едната страна той е директен и не позволява намесата на трети лица. За това са единствено необходими вече описаните MSH лица, които осъществяват трансфера на информацията. От друга страна, ebMS въвежда и няколко допълнителни поднива на сигурност на съдържанието като дигиталния подпис, ID на съобщението, както и потвърждение при получаването му. Мерки за сигурност на ниво съдържание на информацията са и често налагани чрез дубликатни форми с автентично съдържание и кодиране. Въпреки, че най-често срещаните протоколи за обмен са HTTP и SMTP, ebMS остава най-практичния и сигурен комуникационен неутрален протокол с широко приложение в бизнес средите.

Структура на ebXML съобщението



Фигура 6-11

Верига електронни съобщения



Фигура 6-12

Верига от свързани с бизнеса документи



Фигура 6-13

Добри практики в България – електронно фактуриране

През последните две-три години в България бяха внедрени решения за електронно фактуриране. Освен пионера „Банксервиз” АД тази услуга се предлага и от други фирми, например, Транскарт.

Електронната фактура е базирана на следните основни елементи: създаване на цифрово копие на фактурата; подписване на цифровата фактура чрез електронен подпис; изпращане към получателя (клиента) и съхранение и архивиране на електронната фактура.

Предимства на електронните фактури, е че тя позволява намаляване на оперативните разходи с 50-80%. Освен неоспоримите предимства за издателя, електронната фактура облекчава и получателите, тъй като те получават фактурите в момента на издаването им, с използването ѝ отпада и необходимостта от съхранение и архивиране, на лице е възможност за автоматизирана обработка на входящите фактури.

Формата и съдържанието на електронната фактура е необходимо да бъдат съобразени със законовите рамки. Изискванията относно електронната фактура са заложили в: Закона за електронния документ и електронния подпис (ЗЕДЕП), Закона за счетоводството, Закона за ДДС и Директивата 2006/112/ЕС на Съвета на Европейския съюз. Електронната фактура е електронен данъчен и счетоводен документ.

Необходимо е използване на квалифициран електронен подпис, издаден от Доставчик на удостоверителни услуги. Съгласно ЗЕДЕП квалифицираният електронен

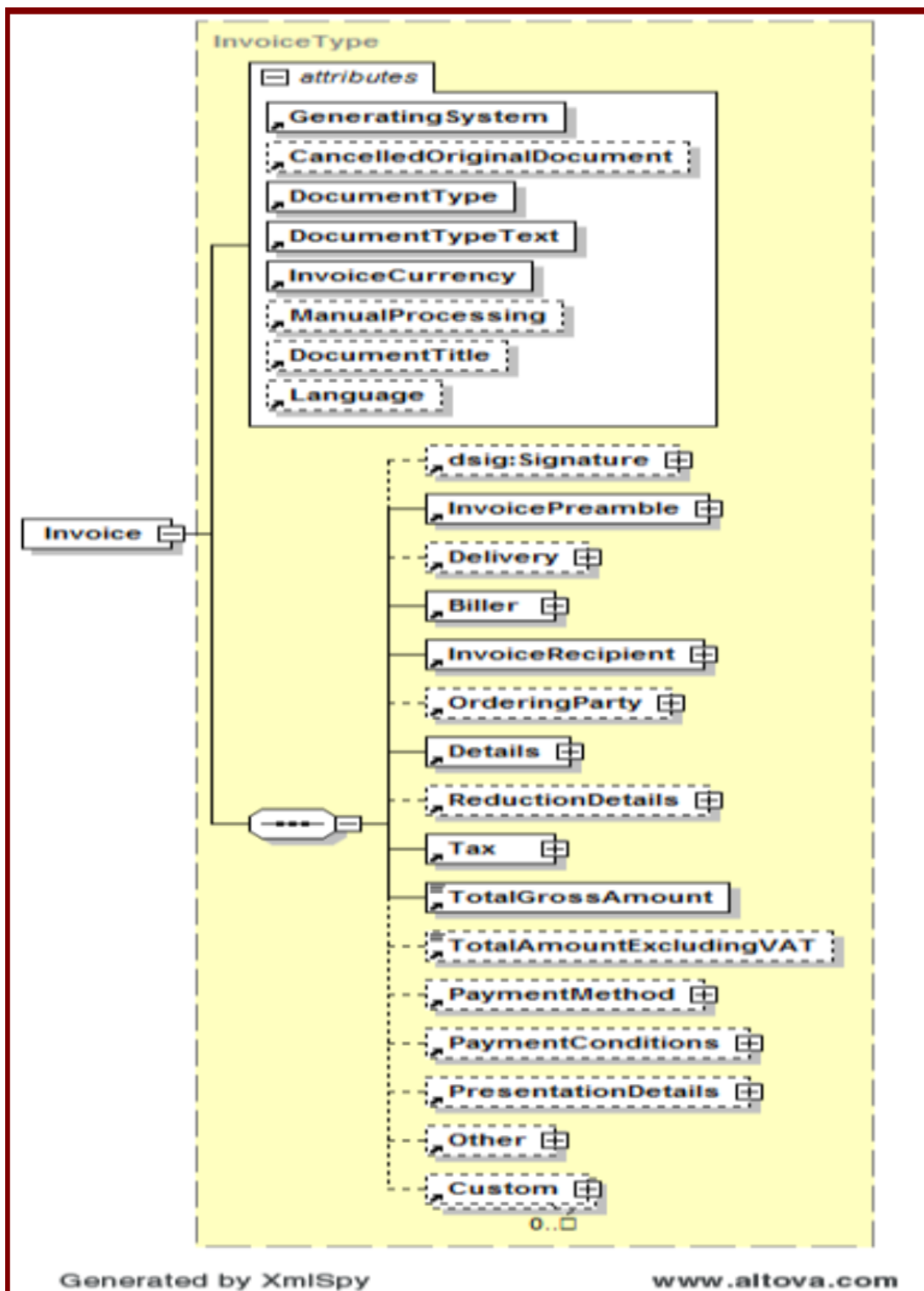
подпис има значение на саморъчен подпис по отношение на всички лица и институции. Електронен подпис се издава от Доставчик на удостоверителни услуги (ДУУ), регистриран от Комисията за регулиране на съобщенията. Издаването става лично на автора на електронния подпис след представяне на документ за самоличност в офиса на ДУУ.

Електронните фактури трябва да са във формат, който се експортира от някоя от поддържащите ERP системи (Enterprise Resource Planning – единна система, ползваща обща база данни на организацията, която обхваща всички бизнес процеси във фирмата - планиране, бюджетиране и контрол в областта на производството, доставките, продажбите, складовото стопанство, ресурсите, проектите и счетоводната отчетност).

Данните за изготвяне на фактури, които се поддържат в информационната система на издателя, може да не са пълни или коректни, затова е необходимо тяхното допълване и коригиране на грешки. Извършва се проверка и актуализация на всички реквизити които се включват в Електронната фактура:

- Име и адресни данни на получател;
- Име и адресни данни на издател;
- Идентификационен номер и ДДС номер на издател;
- Идентификационен номер и ДДС номер на получател;
- Номера и дати на фактури;
- Реквизити свързани с ДДС(облагаема сума, данъчна ставка, изчислен размер);
- Реквизити свързани с фактурираните стоки или услуги.

Описаните чрез унифицирания XML формат фактури трябва да бъдат визуализирани за преглед или отпечатване при получателите. Всеки издател има различен вид показвани реквизити и дизайн на фактурите си. Затова е необходимо разработване на XSL трансформация за визуализиране на електронната фактура, според изискванията на издателя за вид, дизайн, лого и т.н



Фигура 6-14

SOAP (Simple Object Access Protocol)

SOAP (Simple Object Access Protocol) е протокол за обмен на структурирана информация при имплементацията на уеб услуги при компютърните мрежи. SOAP осигурява лесна, разширяема и богата XML рамка за съобщения. Протоколът увеличава оперативната съвместимост в различни, хетерогенни среди.

Спецификацията SOAP в момента се поддържа от XML работната група на World Wide Web Consortium.

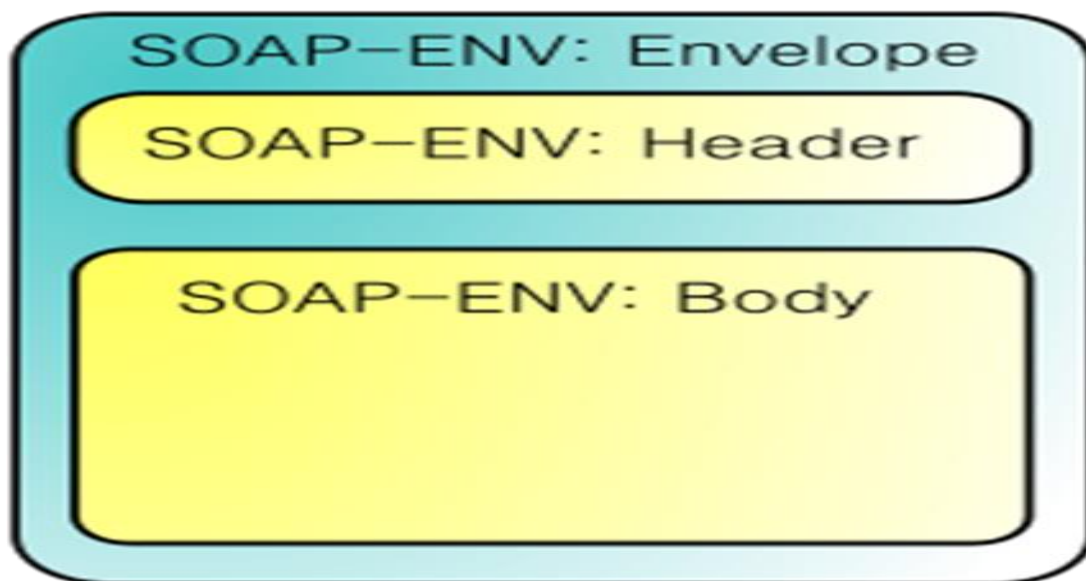
Примерно SOAP съобщение:

```
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <OrderItem>
      <PartNumber>WIDGET204</PartNumber>
      <Quantity>7</Quantity>
      <CustomerID>C00215</CustomerID>
    </OrderItem>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

SOAP – Важни характеристики

Лек (lightweight) – изисква единствено възможност за получаване и изпращане на HTTP пакети и за обработка на XML

- Построен върху отворени технологии, не зависи от конкретен доставчик, няма доминиращ доставчик на SOAP;
- Разширяем спрямо транспортния протокол и представянето на данните;
- Насърчава създаването на слабо-обвързани разпределени среди приложения.



Фигура 6-15

ЧАСТ 7

ОЦЕНКА НА СЪОТВЕТСТВИЕТО

ГЛАВА 7.1

ИЗПЪЛНЕНИЕ НА ДЕЙНОСТИТЕ ПО ОСИГУРЯВАНЕ НА ОПЕРАТИВНА СЪВМЕСТИМОСТ И ИНФОРМАЦИОННА СИГУРНОСТ СЪГЛАСНО ИЗИСКВАНИЯТА НА ЗЕУ

1. Подготовка на Информационната система за оценка на съответствие с изискванията за оперативна съвместимост и информационна сигурност.

1.1. Основания за оценка на съответствието

1.1.1. Нормативни изисквания

Съгласно Закона за изменение на Закона за електронното управление (ДВ, бр. 20 от 28.02.2013 г.) сертификацията на информационни системи на административните органи за оперативна съвместимост и информационна сигурност, извършвана от акредитирани лица, се заменя с оценка за съответствие с изискванията за оперативна съвместимост и информационна сигурност, извършвана от Министъра на транспорта, информационните технологии и съобщенията.

Кръгът от информационни системи в администрацията, подлежащи на сертификация, се определя от чл. 20 ал. 1 и 2, както и чл. 103 ал. 1 от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

Изискванията по отношение на информационната сигурност се определят в чл. 39 от горепосочената Наредба.

Методиката и правилата за оценка на съответствието на информационната система с изискванията за оперативна съвместимост и информационна сигурност се определят в Глава Шеста на горепосочената Наредба – раздели I, II и VII.

1.1.2. Установяване на ситуацията

Функционалният анализ на Информационната система трябва да покаже дали тази система може да бъде отнесена към чл. 20 ал. 1 от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност, т.е. това е административна информационна система, която създава електронни документи, регламентирани в Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите или към чл. 20 ал. 2, т.е. специализирана информационна система, осигуряваща изцяло или частично функциите на административна информационна система, доколкото създават електронни документи, регламентирани в Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите. Това могат да бъдат следните функции:

реализация на функции, свързани с поддържане на данни и процедури по тяхната обработка, специфицирани в чл. 4 и следващите от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите

Такива данни например са:

- данни по регистрация на документи, обменяни между администрациите или администрациите и гражданите;
- данни касаещи контрол и управление на работните процеси в администрациите;
- други данни, специфицирани в посочената наредба.
- реализация на функции по свързване на информационната система с Единната среда за обмен на електронни документи;
- реализация на функции по приемане на данни в електронна форма през Уеб или електронна поща, като приетите данни стартират административни процедури, изпълнявани ръчно, или машинно, но с поемане на отговорност от страна на администрацията за тяхното изпълнение в съответствие с нормативната уредба или специфични вътрешни правила;
- Реализация на функции по изпълнение на електронни услуги със средствата на информационната система;
- Реализация на функции по управление и контрол на административната дейност.

Тези проверки трябва да покажат дали системата подлежи на оценка за съответствие с изискванията за оперативна съвместимост и информационна сигурност по смисъла на Глава Шеста на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

1.2. Проверка на обстоятелствата, свързани с оценката за съответствие

За да може на Информационната система да премине успешно оценката за съответствие с изискванията за оперативна съвместимост и информационна сигурност, Изпълнителят трябва да вложи в нейната разработка тези изисквания, както и ще извърши вътрешна проверка на обстоятелствата, свързани със оценката за съответствие. При проверката трябва да бъдат използвани като основа методиките за извършване на проверка на съответствието с изискванията за оперативна съвместимост и информационна сигурност на някои от бившите акредитирани лица.

1.2.1. Проверка на обстоятелствата, свързани с чл. 125 от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност

Изискванията, съдържащи се в посочения член от Наредбата са, както следва: за всеки документ, създаден от административната информационна система, посочен в приложение № 1 към Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите, се проверява:

- а) възможността за въвеждане в ръчен или автоматичен режим на стойностите на данните в състава на проверяван документ;
- б) възможността за генериране в ръчен или автоматичен режим на валиден документ от проверявания тип, съдържащ данните, въведени по т. А.

Приложение № 1 към чл. 6 от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите включва следните документи, които трябва да се създават от административните информационни системи:

- “Потвърждаване за получаване”;
- «Съобщение, че получаването не се потвърждава» и
- “Контейнер за пренос”.

1.2.1.1. Проверка на създаването на електронен документ „Потвърждение за получаване“

За целите на проверката трябва да бъде извършено следното:

- а) въвеждане в ръчен режим в ИС съдържанието на данните, включени в документа;
- б) автоматично стартиране на създаването на документа "Потвърждаване за получаване".

Обект на проверката е файлът със създадения документ, относно изпълнението на следните изисквания:

- а) документът е създаден в съответствие с регистрацията му в Регистъра на информационните обекти;
- б) съставът на данните в него е съгласно въведените в процеса на създаване на документа данни.

Електронният документ „Потвърждение за получаване“ е вписан в Регистъра на информационните обекти с уникален регистров идентификатор (УРИ) 0010-00002. На него съответства сегмент "ReceiptAcknowledgedMessage" с УРИ 0009-000019 и следната XSD-структура

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="http://ereg.egov.bg/segment/0009-000019"
  xmlns="http://ereg.egov.bg/segment/0009-000019"
  xmlns:espbdb="http://ereg.egov.bg/segment/0009-000002"
  xmlns:dett="http://ereg.egov.bg/value/0008-000005"
  xmlns:duri="http://ereg.egov.bg/segment/0009-000001"
  xmlns:aisun="http://ereg.egov.bg/segment/0009-000018"
  xmlns:ausui="http://ereg.egov.bg/value/0008-000038"
  xmlns:aisuri="http://ereg.egov.bg/value/0008-000039"
  xmlns:aiscai="http://ereg.egov.bg/value/0008-000037"
  xmlns:esa="http://ereg.egov.bg/segment/0009-000016"
  xmlns:dturi="http://ereg.egov.bg/segment/0009-000003"
  xmlns:dtn="http://ereg.egov.bg/value/0008-000007"
  xmlns:xdsig="http://ereg.egov.bg/segment/0009-000004"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified">
  <xsd:import namespace="http://ereg.egov.bg/segment/0009-000002"/>
  <xsd:import namespace="http://ereg.egov.bg/value/0008-000005"/>
  <xsd:import namespace="http://ereg.egov.bg/segment/0009-000001"/>
  <xsd:import namespace="http://ereg.egov.bg/segment/0009-000018"/>
  <xsd:import namespace="http://ereg.egov.bg/value/0008-000038"/>
  <xsd:import namespace="http://ereg.egov.bg/value/0008-000039"/>
```

```

<xsd:import namespace="http://ereg.egov.bg/value/0008-000037"/>
<xsd:import namespace="http://ereg.egov.bg/segment/0009-000016"/>
<xsd:import namespace="http://ereg.egov.bg/segment/0009-000003"/>
<xsd:import namespace="http://ereg.egov.bg/value/0008-000007"/>
<xsd:import namespace="http://ereg.egov.bg/segment/0009-000004"/>
<xsd:element name="ReceiptAcknowledgedMessage"
type="ReceiptAcknowledgedMessage"/>
  <xsd:complexType name="ReceiptAcknowledgedMessage">
    <xsd:annotation>
      <xsd:documentation xml:lang="bg">Потвърждаване за
получаване</xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
      <xsd:element name="ElectronicServiceProvider"
type="espbd:ElectronicServiceProviderBasicData" minOccurs="0"/>
      <xsd:element name="TransportType"
type="dett:DocumentElectronicTransportType" minOccurs="0"/>
      <xsd:element name="DocumentURI" type="duri:DocumentURI"
minOccurs="0"/>
      <xsd:element name="ReceiptTime" type="xsd:dateTime" minOccurs="0"/>
      <xsd:element name="RegisteredBy" minOccurs="0">
        <xsd:complexType>
          <xsd:choice>
            <xsd:element name="Officer">
              <xsd:complexType>
                <xsd:sequence>
                  <xsd:element name="PersonNames"
type="aisun:AISUserNames" minOccurs="0"/>
                  <xsd:element name="AISUserIdentifier"
type="ausui:AISUserIdentifier" minOccurs="0"/>
                </xsd:sequence>
              </xsd:complexType>
            </xsd:element>
            <xsd:element name="AISURI" type="aisuri:AISURI"/>
          </xsd:choice>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="CaseAccessIdentifier"
type="aiscai:AISCaseAccessIdentifier" minOccurs="0"/>
      <xsd:element name="Applicant" type="esa:ElectronicServiceApplicant"
minOccurs="0"/>
      <xsd:element name="DocumentTypeURI" type="dturi:DocumentTypeURI"
minOccurs="0"/>
      <xsd:element name="DocumentTypeName"
type="dtn:DocumentTypeName" minOccurs="0"/>
      <xsd:element name="Signature" type="xdsig:XMLDigitalSignature"
minOccurs="0"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

```

След ръчното въвеждане на данните системата трябва да генерира следния документ (данните са примерни):

```
<?xml version="1.0" encoding="UTF-8"?>
<ReceiptAcknowledgedMessage>
  <ElectronicServiceProviderBasicData>
    <EntityBasicData>
      <EntityName>Министерство на транспорта</EntityName>
      <EntityIdentifier>130403691</EntityIdentifier>
    </EntityBasicData>
    <ElectronicServiceProviderType>Административен
орган</ElectronicServiceProviderType>
  </ElectronicServiceProviderBasicData>
  <DocumentElectronicTransportType>Получаване на електронен документ
чрез Уеб-приложение</DocumentElectronicTransportType>
  <DocumentURI>
    <RegisterIndex>25</RegisterIndex>
    <DocumentSequenceNumber>220</DocumentSequenceNumber>
    <ReceiptOrSigningDate>04.01.2013</ReceiptOrSigningDate>
  </DocumentURI>
  <ReceiptTime>16:52:59</ReceiptTime>
    <RegisteredBy>
      <Officer>
        <AISUserNames>
          <PersonNames>
            <PersonFirstName>Петър</PersonFirstName>
            <PersonMiddleName>Иванов</PersonMiddleName>
            <PersonLastName>Петров</PersonLastName>
            <PersonPseudonim></PersonPseudonim>
          </PersonNames>
        </AISUserNames>
        <AISUserIdentifier>началник</AISUserIdentifier>
      </Officer>
    </RegisteredBy>
    <AISCaseAccessIdentifier>abcd</AISCaseAccessIdentifier>
  <ElectronicServiceApplicant>
    <RecipientGroup>
      <ElectronicStatementAuthor>
        <PersonBasicData>
          <PersonNames>
            <PersonFirstName>Иван</PersonFirstName>
            <PersonMiddleName>Петров</PersonMiddleName>
            <PersonLastName>Иванов</PersonLastName>
            <PersonPseudonim></PersonPseudonim>
          </PersonNames>
          <PersonIdentifier>
            <EGN>7009076653</EGN>
          </PersonIdentifier>
        </PersonBasicData>
```

```

</ElectronicStatementAuthor>

<ElectronicServiceAuthorQuality>представител</ElectronicServiceAuthorQuality>
  <ElectronicServiceRecipient>
    <EntityBasicData>
      <EntityName>АБВ ЕООД</EntityName>
      <EntityIdentifier>030272497</EntityIdentifier>
    </EntityBasicData>
  </ElectronicServiceRecipient>
</RecipientGroup>
<EmailAddress>ivan@gmail.com</EmailAddress>
</ElectronicServiceApplicant>
<DocumentTypeURI>
  <RegisterObjectURI>
    <BatchNumber>14</BatchNumber>
    <BatchNumber>25</BatchNumber>
  </RegisterObjectURI>

  </DocumentTypeURI>
  <DocumentTypeName>писмо</DocumentTypeName>
  <XMLDigitalSignature>
    <DigestValue>bLk5t/uOvICEKB/WwkzAY7kDRYE=</DigestValue>

    <SignatureValue>kP3n3YzeUwC+IYtPm4nzI7d6OtOiEGHtgflq5+pOW35ypyJbz8Uf5
    Gh624P5ftAY2HWQfNDq/xk0iIypbjWPuGXx1KHfX5YjfSkmhKIm219/07IDKzvQTUHT
    IdfFWZbWZRgUzMIZLgpidiWaSzP+Zo6HnIP3um0DR4He8V9I3mE=</SignatureValu
    e>

    <KeyInfo>
      <X509Data>
        <X509IssuerSerial>

        <X509IssuerName>System.Security.Cryptography.X509Certificates.X500Distinguish
        edName</X509IssuerName>

        <X509SerialNumber>142243333473566811131755752049628590115</X509SerialN
        umber>

        </X509IssuerSerial>

        <X509Certificate>MIICRTCCAbKgAwIBAgIQawMRzOPJIKRHbx1A826wlzAJBgUrDg
        MCHQUAMDExLzAtBgNVBAMeJgBDAEUUAUgBUAF8AUwBJAEcATgBfAFQARQBT
        AFQAXwBDAEUUAUgBUMB4XDTA5MTIzMTIyMDAwMFOXDTEyMTIyMDAwMF
        owMTEvMC0GA1UEAx4mAEEMARQBSAFQAXwBTAEkARwBOAF8AVABFAFMVA
        BfAEEMARQBSAFQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ3PDKXIG
        GL2w9fvWQn6kxgtg2h5NwUYfBlwWRMIs5mAhSKSto4CAdg4voHgWTcXZvN9BEQ
        CxzjwaHE5n3NyBv401okX6BxKd6rVYDGBnEeluy98xftBBmCwRY05CwiYv3u6P+q
        PGBkLv4tSSK3s6F69tO2tXbnK1sYXCBntAzZAgMBAAGjZjBkMGIGA1UdAQRbMFm
        AEAwKeENekD5eofDfY8gE7bGhMzAxMS8wLQYDVQQDHiYAQwBFAFIAVABfAFM
        ASQBHAE4AXwBUAEUAUwBUAF8AQwBFAFIAVIIQawMRzOPJIKRHbx1A826wlzA
        JBgUrDgMCHQUAA4GBACUX6OTjyeQigxbRrSokbCZcd2VOuoM4dSByQDof3Stkthr
        FpX6LySswdvX6VSYuRd1ZTLXFn7R7e7xVssfl9evHnFoXTxeDapA+3opY3JF317d7

```



```

yQggOLDeOp07wyzHIKLiwLZ+Qf7BzyKKaKzREuVUD4Zla3mkpu+bdvGIIF2C</X50
9Certificate>
      </X509Data>
    </KeyInfo>
  </XMLDigitalSignature>
</ReceiptAcknowledgedMessage>

```

При ръчното въвеждане на данни, съдържащи грешки, системата трябва да генерира съобщения за грешки, съдържащи следните термини:

- 0006-000069 (Невалидна структура на обекта съгласно XML дефиницията му, вписана в регистъра на информационните обекти);
- 0006-000015 (Полето <Field> от секцията <Section> трябва да е попълнено.) и
- 0006-000023 Попълването на секцията <Section> е задължително

С това проверката се определя за успешна.

1.2.1.2. Проверка на създаването на електронен документ „Съобщение, че получаването не се потвърждава“

За целите на проверката трябва да бъде извършено следното:

а) въвеждане в ръчен режим в ИС съдържанието на данните, включени в документа;

б) автоматично стартиране на създаването на документа "Съобщение, че получаването не се потвърждава".

Обект на проверката е файлът със създадения документ, относно изпълнението на следните изисквания:

а) документът е създаден в съответствие с регистрацията му в Регистъра на информационните обекти;

б) съставът на данните в него е съгласно въведените в процеса на създаване на документа данни.

Електронният документ „Съобщение, че получаването не се потвърждава“ е вписан в Регистъра на информационните обекти с уникален регистров идентификатор (УРИ) 0010-00001. На него съответства сегмент "ReceiptNotAcknowledgedMessage" с УРИ 0009-000017 и следната XSD-структура

```

<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="http://ereg.egov.bg/segment/0009-000017"
  xmlns="http://ereg.egov.bg/segment/0009-000017"
  xmlns:duri="http://ereg.egov.bg/segment/0009-000001"
  xmlns:espbd="http://ereg.egov.bg/segment/0009-000002"
  xmlns:dett="http://ereg.egov.bg/value/0008-000005"
  xmlns:eddt="http://ereg.egov.bg/value/0008-000006"

```

```

xmlns:esa="http://ereg.egov.bg/segment/0009-000016"
xmlns:dturi="http://ereg.egov.bg/segment/0009-000003"
xmlns:dtm="http://ereg.egov.bg/value/0008-000007"
xmlns:xdsig="http://ereg.egov.bg/segment/0009-000004"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
<xsd:import namespace="http://ereg.egov.bg/segment/0009-000001"/>
<xsd:import namespace="http://ereg.egov.bg/segment/0009-000002"/>
<xsd:import namespace="http://ereg.egov.bg/value/0008-000005"/>
<xsd:import namespace="http://ereg.egov.bg/value/0008-000006"/>
<xsd:import namespace="http://ereg.egov.bg/segment/0009-000016"/>
<xsd:import namespace="http://ereg.egov.bg/segment/0009-000003"/>
<xsd:import namespace="http://ereg.egov.bg/value/0008-000007"/>
<xsd:import namespace="http://ereg.egov.bg/segment/0009-000004"/>
<xsd:element name="ReceiptNotAcknowledgedMessage"
type="ReceiptNotAcknowledgedMessage"/>
<xsd:complexType name="ReceiptNotAcknowledgedMessage">
<xsd:annotation>
<xsd:documentation xml:lang="bg">Съобщение, че получаването не се
потвърждава</xsd:documentation>
</xsd:annotation>
<xsd:sequence>
<xsd:element name="MessageURI" type="dturi:DocumentURI"
minOccurs="0"/>
<xsd:element name="ElectronicServiceProvider"
type="espb:ElectronicServiceProviderBasicData" minOccurs="0"/>
<xsd:element name="TransportType"
type="dett:DocumentElectronicTransportType" minOccurs="0"/>
<xsd:element name="Discrepancies" minOccurs="0">
<xsd:complexType>
<xsd:sequence>
<xsd:element name="Discrepancy"
type="eddt:ElectronicDocumentDiscrepancyType" maxOccurs="unbounded"/>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
<xsd:element name="Applicant" type="esa:ElectronicServiceApplicant"
minOccurs="0"/>

```

```

        <xsd:element name="DocumentTypeURI" type="dturi:DocumentTypeURI"
minOccurs="0" />
        <xsd:element name="DocumentTypeName"
type="dtn:DocumentTypeName" minOccurs="0" />
        <xsd:element name="MessageCreationTime" type="xsd:dateTime"
minOccurs="0"/>
        <xsd:element name="Signature" type="xdsig:XMLDigitalSignature"
minOccurs="0"/>
    </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

След ръчното въвеждане на данните системата трябва да генерира следния документ (данните са примерни):

```

<?xml version="1.0" encoding="UTF-8"?>
<ReceiptNotAcknowledgedMessage>
  <ElectronicServiceProviderBasicData>
    <EntityBasicData>
      <EntityName>Министерство на транспортаИПА</EntityName>
      <EntityIdentifier>130403691</EntityIdentifier>
    </EntityBasicData>
    <ElectronicServiceProviderType>Административен
орган</ElectronicServiceProviderType>
  </ElectronicServiceProviderBasicData>
  <DocumentElectronicTransportType>Получаване на електронен документ
чрез Уеб-приложение</DocumentElectronicTransportType>
  <ElectronicDocumentDiscrepancyType>Подаваното заявление не е в
нормативно установения формат </ElectronicDocumentDiscrepancyType>
  <DocumentURI>
    <RegisterIndex>25</RegisterIndex>
    <DocumentSequenceNumber>220</DocumentSequenceNumber>
    <ReceiptOrSigningDate>04.01.2013</ReceiptOrSigningDate>
  </DocumentURI>
  <ElectronicServiceApplicant>
    <RecipientGroup>
      <ElectronicStatementAuthor>
        <PersonBasicData>
          <PersonNames>
            <PersonFirstName>Иван</PersonFirstName>
            <PersonMiddleName>Петров</PersonMiddleName>
            <PersonLastName>Иванов</PersonLastName>
            <PersonPseudonim></PersonPseudonim>
          </PersonNames>
          <PersonIdentifier>
            <EGN>7009076653</EGN>
          </PersonIdentifier>

```

```

        </PersonBasicData>
    </ElectronicStatementAuthor>

    <ElectronicServiceAuthorQuality>представител</ElectronicServiceAuthorQuality>
    <ElectronicServiceRecipient>
        <EntityBasicData>
            <EntityName>АБВ ЕООД</EntityName>
            <EntityIdentifier>030272497</EntityIdentifier>
        </EntityBasicData>
    </ElectronicServiceRecipient>
    </RecipientGroup>
    <EmailAddress>ivan@gmail.com</EmailAddress>
    </ElectronicServiceApplicant>
    <DocumentTypeURI>
        <RegisterObjectURI>
            <BatchNumber>14</BatchNumber>
            <BatchNumber>25</BatchNumber>
        </RegisterObjectURI>

    </DocumentTypeURI>
    <DocumentTypeName>писмо</DocumentTypeName>
    <XMLDigitalSignature>
        <DigestValue>bLk5t/uOvICEKB/WwkzAY7kDRYE=</DigestValue>

    <SignatureValue>kP3n3YzeUwC+IYtPm4nzi7d6OtOiEGHtgflq5+pOW35ypyJbz8Uf5Gh6
    24P5ftAY2HWQfNDq/xk0iIypbjWPuGXx1KHfX5YjfSkmhKIm219/07IDKzvQTUHTldfFWZ
    bWZRgUzMIZLgpidiWaSzP+Zo6HnIP3um0DR4He8V9I3mE=</SignatureValue>
        <KeyInfo>
            <X509Data>
                <X509IssuerSerial>

    <X509IssuerName>System.Security.Cryptography.X509Certificates.X500DistinguishedN
    ame</X509IssuerName>

    <X509SerialNumber>142243333473566811131755752049628590115</X509SerialNum
    ber>

                </X509IssuerSerial>

    <X509Certificate>MIICRTCCAbKgAwIBAgIQawMRzOPJIKRHbx1A826wIzAJBgUrDgMC
    HQUAMDExLzAtBgNVBAMEJgBDAEUUAUgBUAF8AUwBJAEcATgBfAFQARQBTAFAQX
    wBDAEUUAUgBUMB4XDTA5MTIzMTIyMDAwMFoXDTEyMTIzMTIyMDAwMFowMTEvM
    C0GA1UEAx4mAEEMARQBSAFQAXwBTAEkARwBOAF8AVABFAFMAVABfAEEMARQB
    SAFQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ3PDKXIGGL2w9fvWQn6kx
    gtg2h5NwUYfBlwWRMIs5mAHSKSto4CAAdg4voHgWTcXZvN9BEQCxjzwaHE5n3NyBv4
    01okX6BxKd6rVYDGBnEeluy98xfyBBmCwRY05CwiYv3u6P+qPGBkV4tSSK3s6F69tO
    2tXbnK1sYXCBntAzZAqMBAAGjZjBkMGIGA1UdAQRbMFmAEAWKeENekD5eofDfY8g
    E7bGhMzAxMS8wLQYDVQQDHiYAAQwBFAFIAVABfAFMASQBHAE4AXwBUAEUAUwB
    UAF8AQwBFAFIAVILQawMRzOPJIKRHbx1A826wIzAJBgUrDgMCHQUAA4GBACUX6O
    TjyeQigxbRrSokbCZcd2VOuoM4dSBYQDof3StkthrFpX6LySswdvX6VSYuRd1ZTLXFn7
    R7e7xVssfl9evHnFoXTxeDapA+3opY3JF317d7yQggOLDeOp07wyzHIKLiW LZ+Qf7BzyK
    KaKzREuVUD4Zla3mkpu+bdvGIIF2C</X509Certificate>

```

```

        </X509Data>
    </KeyInfo>
</XMLDigitalSignature>
</ReceiptNotAcknowledgedMessage>

```

При ръчното въвеждане на данни, съдържащи грешки, системата трябва да генерира съобщения за грешки, съдържащи следните термини:

- 0006-000028 (Документът "Грешки в съдържание на документ" трябва да съдържа поне една регистрирана грешка в съдържанието на проверявания документ);
- 0006-000069 (Невалидна структура на обекта съгласно XML дефиницията му, вписана в регистъра на информационните обекти);
- 0006-000015 (Полето <Field> от секцията <Section> трябва да е попълнено) и
- 0006-000023 (Попълването на секцията <Section> е задължително).

С това проверката се определя за успешна.

1.2.1.3. Проверка на създаването на електронен документ „Контейнер за пренос“

За целите на проверката трябва да бъде извършено следното:

- въвеждане в ръчен режим в ИС съдържанието на данните, включени в документа;
- автоматично стартиране на създаването на документа "Контейнер за пренос".

Обект на проверката е файлът със създадения документ, относно изпълнението на следните изисквания:

- документът е създаден в съответствие с регистрацията му в Регистъра на информационните обекти;
- съставът на данните в него е съгласно въведените в процеса на създаване на документа данни.

Електронният документ „Контейнер за пренос“ е вписан в Регистъра на информационните обекти с уникален регистров идентификатор (УРИ) 0010-00003. На него съответства сегмент "TransferContainer" с УРИ 0009-000021 и следната XSD-структура

```

<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="http://ereg.egov.bg/segment/0009-000021"
  xmlns="http://ereg.egov.bg/segment/0009-000021"
  xmlns:duri="http://ereg.egov.bg/segment/0009-000001"
  xmlns:std="http://ereg.egov.bg/value/0008-000042"
  xmlns:etd="http://ereg.egov.bg/value/0008-000043"
  xmlns:td="http://ereg.egov.bg/segment/0009-000020"
  xmlns:xdsig="http://ereg.egov.bg/segment/0009-000004"

```

```

xmlns:xsd="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
<xsd:import namespace="http://ereg.egov.bg/segment/0009-000001"/>
<xsd:import namespace="http://ereg.egov.bg/value/0008-000042"/>
<xsd:import namespace="http://ereg.egov.bg/value/0008-000043"/>
<xsd:import namespace="http://ereg.egov.bg/segment/0009-000020"/>
<xsd:import namespace="http://ereg.egov.bg/segment/0009-000004"/>
<xsd:element name="TransferContainer" type="TransferContainer"/>
<xsd:complexType name="TransferContainer">
  <xsd:annotation>
    <xsd:documentation xml:lang="bg">Контейнер за
пренос</xsd:documentation>
  </xsd:annotation>
  <xsd:sequence>
    <xsd:element name="DocumentURI" type="duri:DocumentURI"
minOccurs="0"/>
    <xsd:element name="ShortTransferDescription"
type="std:ShortTransferDescription" minOccurs="0"/>
    <xsd:element name="ExpandedTransferDescription"
type="etd:ExpandedTransferDescription" minOccurs="0"/>
    <xsd:element name="TransferredDocuments" minOccurs="0">
      <xsd:complexType>
        <xsd:sequence>
          <xsd:element name="Document" type="td:TransferredDocument"
maxOccurs="unbounded"/>
        </xsd:sequence>
      </xsd:complexType>
    </xsd:element>
    <xsd:element name="Signature" type="xdsig:XMLDigitalSignature"
minOccurs="0"/>
  </xsd:sequence>
</xsd:complexType>
</xsd:schema>

```

След ръчното въвеждане на данните системата трябва да генерира следния документ (данните са примерни):

```

<?xml version="1.0" encoding="UTF-8"?>
<TransferContainer>

```

```

    <DocumentURI>
    <RegisterIndex>25</RegisterIndex>
    <DocumentSequenceNumber>220</DocumentSequenceNumber>
    <ReceiptOrSigningDate>04.01.2013</ReceiptOrSigningDate>
  </DocumentURI>
  <ShortTransferDescription>От А до Б</ShortTransferDescription>
  <ExpandedTransferDescription>Да                                се                                достави
незабавно</ExpandedTransferDescription>
  <TransferredDocument>
    <FileContent>WWWamrwkdldmjkjdjdijx</FileContent>
    <ShortTransferDescription>Важно писмо</ShortTransferDescription>
    <ExpandedTransferDescription>Много                                важно
писмо</ExpandedTransferDescription>
    <FileType>text/plain</FileType>
    <DocumentURI>
      <RegisterIndex>87</RegisterIndex>
      <DocumentSequenceNumber>111</DocumentSequenceNumber>
      <ReceiptOrSigningDate>04.01.2013</ReceiptOrSigningDate>
    </DocumentURI>
  </TransferredDocument>
  <XMLDigitalSignature>
    <DigestValue>bLk5t/uOvICEKB/WwkzAY7kDRYE=</DigestValue>

<SignatureValue>kP3n3YzeUwC+IYtPm4nzi7d6OtOiEGHtgflq5+pOW35ypyJbz8Uf5Gh6
24P5ftAY2HWQfNDq/xk0iIypbjWPuGXx1KHfX5YjfSkmhKIm219/07IDKzvQTUHTIdfFWZ
bWZRgUzMiZLgpidiWaSzP+Zo6HnIP3um0DR4He8V9I3mE=</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509IssuerSerial>

<X509IssuerName>System.Security.Cryptography.X509Certificates.X500DistinguishedN
ame</X509IssuerName>

<X509SerialNumber>142243333473566811131755752049628590115</X509SerialNum
ber>

        </X509IssuerSerial>

<X509Certificate>MIICRTCCAbKgAwIBAgIQawMRzOPJIKRHbx1A826wIzAJBgUrDgMC
HQUAMDExLzAtBgNVBAMeJgBDAEUUAUgBUAF8AUwBJAEcATgBfAFQARQBTAFAQAX
wBDAEUUAUgBUMB4XDTA5MTIzMTIyMDAwMFOXDTEzMTIyMDAwMFowMTEvM
C0GA1UEAx4mAEMARQBFAFQAXwBTAEkARwBOAF8AVABFAFMAVABfAEMARQB
SAFQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ3PDKXIGGL2w9fvWQn6kx
gtg2h5NwUYfBlwWRMIs5mAHSKSto4CAAdg4voHgWTcXZvN9BEQCxjwaHE5n3NyBv4
01okX6BxKd6rVYDGBnEeluy98xfyBBmCwRY05CwiYv3u6P+qPGBKjv4tSSK3s6F69tO
2tXbnK1sYXCBntAzZAqMBAAGjZjBkMGIGA1UdAQRbMFmAEAWKeENekD5eofDfY8g
E7bGhMzAxMS8wLQYDVQQDHiYAAQwBFAFIAVABfAFMASQBHAE4AXwBUAEUUAUwB
UAF8AQwBFAFIAVABfAFMAVABfAFMAVABfAFMAVABfAFMAVABfAFMAVABfAFMAVABf
TjyeQigxbRrSokbCZcd2VOuoM4dSBYQDof3StkthrFpX6LySswdvX6VSYuRd1ZTLXFn7
R7e7xVssfl9evHnFoXTxeDapA+3opY3JF317d7yQggOLDeOp07wyzHIKLiWZ+Qf7BzyK
KaKzREuVUD4Zla3mkpu+bdvGIIF2C</X509Certificate>
      </X509Data>

```

```

        </KeyInfo>
    </XMLDigitalSignature>
</TransferContainer>

```

При ръчното въвеждане на данни, съдържащи грешки, системата трябва да генерира съобщения за грешки, съдържащи следните термини:

- 0006-000027 (В "Контейнер за пренос" трябва да се включи поне един пренасян документ);
- 0006-000069 (Невалидна структура на обекта съгласно XML дефиницията му, вписана в регистъра на информационните обекти);
- 0006-000015 (Полето <Field> от секцията <Section> трябва да е попълнено).

С това проверката се определя за успешна.

1.2.2. Проверка на обстоятелствата, свързани с чл. 128 от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност

Изискванията, съдържащи се в посочения член от Наредбата, касаят информационната сигурност на системата и са реферирани към чл. 39 от същата Наредба.

1.2.2.1. Проверка за съхранение на данните в системата единствено в СУБД

Проверката ще бъде успешна, ако след деактивиране на СУБД, достъпът до ресурсите на ИС е невъзможен и самата тя не може да се стартира.

1.2.2.2. Проверка за наличие на сертификация на използваната СУБД

Проверката ще бъде успешна, ако като използваната СУБД притежава сертификат за информационна сигурност по международния стандарт ISO/IEC 15408:2005 (Common Criteria for Information Technology Security Evaluation).

1.2.2.3. Проверка на достъпа до ресурсите на информационната система

Проверката ще бъде успешна, ако достъпът до ресурсите на системата се разрешава само след въвеждане на парола като средство за персонална идентификация.

1.2.2.4. Проверка на поддръжката на многопотребителски режим

Проверката ще бъде успешна, ако се установи, че:

- автоматично се регистрират данни за лицето, което е извършило създаването или промяната на обектите, и времето на извършването;
- за всички видове данни в състава на обектите, включително и за автоматично генерираните, е осигурена визуализация на съдържанието, наименованието и определението им.

1.2.2.5. Проверка на съвместната работа с файлово съдържание на документи

Проверката ще бъде успешна, ако се установи, че:

- достъпът до файловото съдържание на документите може да се осъществи само със средствата на ИС и с никакви други средства извън нея;
- достъпът на потребител до файлово съдържание, отворено вече за редактиране, може да се осъществи от друг потребител само в режим за четене;

- след промяна на файловото съдържание, отворено в режим на редактиране и последващо съхраняване на същото в ИС, то може да бъде четено отново;
- достъп до редактирано файлово съдържание имат всички потребители.

1.2.2.6. Проверка относно защитата на съдържанието на документ срещу унищожаване или подмяна

Проверката ще бъде успешна, ако се установи, че:

- потребителят, активирал защитата на документа, не може да унищожи или подмени файловото му съдържание;
- потребителят, получил защитения документ, не може да унищожи или подмени файловото му съдържание.

1.2.2.7. Проверка на защитеността на доверителната изчислителна система

Проверката ще бъде успешна, ако се установи, че:

- идентифициращата информация е защитена от нерегламентиран достъп;
- доверителната изчислителна система поддържа област за собственото изпълнение, защитена от външни въздействия и от опити да се следи хода на нейната работа;
- информационната система разполага с технически и програмни средства, позволяващи периодично да се проверява коректността на компонентите на доверителната изчислителна система;
- защитните механизми са преминали тест, който е потвърдил, че неоторизиран ползвател няма очевидна възможност да получи достъп до доверителната изчислителна система.

1.3. Общ извод относно оценката за съответствие

Положителният резултат на всички горепосочени проверки недвусмислено ще покаже, че информационната система е подготвена за оценка на съответствието.

2. Подготовка на приложенията за редактиране и визуализация на електронни документи и за проверка на електронни документи за оценка на съответствието

С промените в Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност сертификацията на приложения не е задължителна, а опционална. Чл. 98 ал. 2 от посочената наредба гласи: «Заинтересувано лице по чл. 104, ал. 2 може да поиска допълнителна сертификация за оперативна съвместимост и информационна сигурност на програмни приложения за визуализация и редактиране на електронни документи и приложения за проверка на електронни документи за съответствие с регистрацията им в регистъра на информационните обекти.»

Основите на нормативния регламент за сертификация на програмни продукти, свързани с електронни документи, са заложи в раздел четвърти на глава четвърта на Закона за електронното управление. По-подробно процедурите по сертификация са описани в наредбите към закона.

Съответствието на внедряваните от административните органи продукти, свързани с електронни документи, с установените нормативни изисквания за оперативна

съвместимост и информационна сигурност се удостоверява от министъра на транспорта, информационните технологии и съобщенията.

Методиката, правилата за извършване на оценката за съответствие се определят с Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност. Министерството на транспорта, информационните технологии и съобщенията води списък (по същество, регистър) на оценените информационни системи и програмни продукти. Министърът на транспорта, информационните технологии и съобщенията осигурява свободен и безплатен достъп до посочените списъци.

На оценка за съответствие с изискванията за оперативна съвместимост и информационна сигурност подлежат програмни приложения, които:

- а) изпълняват функции по визуализация и/или редактиране на електронни документи;
- б) в състава на други приложения или системи изпълняват функции по проверка на електронни документи за съответствие с регистрацията им в регистъра на информационните обекти.

Оценката се извършва по искане на заинтересовано лице - доставящо или разработващо програмното приложение. За всеки вид електронен документ, регистриран в регистъра на информационните обекти, заинтересованото лице представя набор от документи от същия вид, съдържащи тестови данни за провеждане на тестове за съответствие с регистрацията в регистъра на информационните обекти. Само един документ от набора от документи не трябва да съдържа отклонения от регистрацията на съответния вид документ.

Тестовите се създават по начин, позволяващ заложените в тях грешни стойности и нарушенията в организацията на данните да представят всички възможни отклонения от регистрацията на съответния вид документ в регистъра на информационните обекти. За всеки документ, съдържащ тестови данни, заинтересованото лице представя документ от типа „Регистрирани грешки в съдържание на документ”, който съдържа описание на грешките в тестовия документ, съгласно вписаната в регистъра на информационните обекти номенклатура на грешките за съдържащите се в документите информационни обекти. Отговорността за пълнотата на набора от документи, съдържащи тестови данни, е на акредитираното лице, извършващо сертификацията. Министърът на транспорта, информационните технологии и съобщенията вписва наборите в списъка на сертифицираните информационни системи.

За всеки документ, регистриран в регистъра на информационните обекти се изготвя списък на данните, съдържащи се в документа. Този списък за тествания документ се изготвя като справка по чл. 14, т. 7 от Наредбата за водене, съхраняване и достъп до регистъра на информационните обекти и регистъра на електронните услуги.

Промени във вписани набори от документи се извършват при:

- а) установяване на грешки в документите с тестове;
- б) установяване на функционална непълнота в тестовите в набор от документи.

Промени в набора документи могат да се извършват и от министъра на транспорта, информационните технологии и съобщенията.

Заинтересовано лице може да поиска от оценка за оперативна съвместимост и информационна сигурност на приложение за визуализация или редактиране на електронни документи. За целта се извършват следните проверки за установяване на техническата функционалност на приложението за:

а) четене и визуализиране на съдържание на електронен документ от файл, записан в информационната система, намираща се под контрол на потребителя, или записан върху външен носител;

б) създаване на електронен документ от вида „Регистрирани грешки в съдържание на документ“, съдържащ резултатите от проверка на съхранения електронния документ, за съответствие с регистрацията му в регистъра на информационните обекти;

в) наличие на функционалност за вярна и точна визуализация на всички грешки, резултат от извършване на тестове с набора от документи, съдържащи тестови данни при изпълнение на проверката по т. б;

г) наличие на функционалност за вярна и точна визуализация на съобщенията, съдържащи наименованията и описанията на всички грешки, предизвикани при извършване на тестове с набора от документи;

д) наличие на функционалност за вярна и точна визуализация на съдържанието, наименованието и описанието на всички данни, съгласно регистрацията на визуализирания електронен документ в регистъра на информационните обекти.

При оценка за оперативна съвместимост и информационна сигурност на приложение за редактиране на електронни документи, освен горепосочените проверки, се извършват и проверки за установяване на наличието на функционалност за:

а) запис на електронен документ като файл в информационната система, намираща се под контрол на потребителя, включително и върху външен носител;

б) създаване, изтриване и корекция на съдържанието на всички данни, съгласно регистрацията на електронния документ в регистъра на информационните обекти.

Резултатите от извършените проверки се отразяват в документ от вида „Резултати от тестове за оперативна съвместимост по документ“.

Тестовите за приложение за визуализация или редактиране, което работи с няколко документа, се извършват за всеки от тях.

При разширяване обхвата на електронните документи, които могат да се визуализират или редактират със сертифицираното приложение, се извършват проверки за оценка само за новите документи.

Заинтересовано лице може да поиска оценка на съответствие за оперативна съвместимост и информационна сигурност на приложение за проверка на електронни документи за съответствие с регистрацията им в регистъра на информационните обекти. За целта се извършват следните проверки за установяване на техническата функционалност на приложението за:

а) четене на съдържание на електронен документ от файл, записан в информационната система, намираща се под контрол на потребителя, или записан върху външен носител;

б) създаване на електронен документ от вида „Регистрирани грешки в съдържание на документ“, съдържащ резултатите от проверка на съхранения електронния документ, за съответствие с регистрацията му в регистъра на информационните обекти.

За оценка на електронни документи за съответствие с регистрацията им в регистъра на информационните обекти се прилагат съответна правилата, посочени за приложенията за визуализация и редактиране. Регистрацията на резултатите от проверките се извършва чрез въвеждане на данни в документа „Резултати от тестове за оперативна съвместимост по документ“. При открити нередности, предписанията за отстраняването им се дефинират

на базата на тяхната регистрация, извършена в документа за регистрация на резултатите от извършените проверки. След отстраняване на нередностите, всички проверки по сертификацията се извършват отново и се създава нов документ „Резултати от тестове за оперативна съвместимост по документ”.

3. Методика за проверка на пълнота на тестови набори

Условията и дейностите по проверка за пълнота на набори от тестови документи и регистрацията на резултатите от извършените дейности са, както следва:

3.1. Условия и особености при проверка на набор от тестови документи

3.1.1. Изходни данни за извършване на проверката

Набор от тестови документи за сертификация на приложения се изготвят за всеки вид електронен документ. За всеки тестови документ (документ с тестово съдържание) се предоставя и съответстващия му документ от типа "Регистрирани грешки в съдържание на документ". Този документ съдържа формализирано описание на грешките в тестовия документ, съгласно вписана в регистъра на информационните обекти номенклатура на възможните грешки за всяка данна във вид документ, за който ще се сертифицира дадено приложение.

Изходните данни за проверка на набора се съдържат в справка за съдържащите се данни и грешките, касаещи тяхната валидност. Справката се получава със заявяване на съответната услуга към Регистъра на информационните обекти (РИО). Задължението за предоставяне на тази справка е съгласно чл.15, т.7 от Наредбата за регистрите на информационните обекти и на електронните услуги.

3.2. Проверка на изисквания, гарантиращи пълнота на набора

Изискванията са както следва:

- Сертификацията на приложения касае тяхната способност да извършват проверки за валидност на XML-документи. Това означава, че в набора от тестови документи задължително трябва да присъстват такива, даващи възможност да се извършат базовите проверки за «валиден XML-документ».
- Наличие в набора на тестови документ с „правилна” конструкция и съдържание, съответстващи на регистрацията на вида документ в РИО. Възможно е конструкцията на документа да допуска алтернативни варианти на конструкцията на негови компоненти. От гледна точка на тестването, това създава нови видове документи, които може да се смятат за „вариант на основния вид”, „под-вид на основния вид” и т.н. Това разширява основното изискване за наличие на един тестови документ, който „не трябва да съдържа отклонения от регистрацията на съответния вид документ” (чл.108, ал.2 от Наредбата) и върху вариантите (под-видовете и т.н.) на основния вид документ. Тоест, за тестовия набор трябва да се създадат толкова тестови документи с „правилно съдържание”, колкото са вариантите на вида документ, за който се изготвя наборът.
- Осигуряване на тестово съдържание с набора от тестови документи, гарантиращо пълно симулиране на всички грешки, дефинирани за всички данни за конкретен вид документ. Ако дефиницията на дадена грешка

съдържа варианти на възможните отклонения, за всеки вариант на това отклонение, тоест за всеки вариант на грешката трябва да се осигури тестови документ.

- Осигуряване на тестово съдържание с набора от тестови документи, гарантиращо пълно симулиране на всички грешки и за алтернативни варианти на конструкцията на негови компоненти. И за тези компоненти, ако дефиницията на дадена грешка съдържа варианти на възможните отклонения, за всеки вариант на това отклонение, тоест за всеки вариант на грешката
- трябва да се осигури отделен тестови документ.

3.3. Проверка за валидност на имената на тестовите документи, съдържащи грешки

Имената на тестовите документи съдържащи грешки се създават по схема, която позволява:

- Да се идентифицира вида документ, за който се отнася тестовия документ. Идентификацията на вида документ се извършва с неговия уникален регистров идентификатор (УРИ) на регистрацията в РИО;
- Да се идентифицира проверката, за която е предназначен тестовия документ. Всяка проверка касае конкретна данна, тоест и самата проверка може да се отъждестви с УРИ на регистрацията на тази данна в РИО. Но ако данната се среща няколко пъти в конструкцията на даден вид документ, това означава, че за всяко нейно участие в конструкцията трябва да се дефинира отделна проверка, тоест отделен тестови документ. Във връзка с това, идентификацията на данна трябва да се извършва с нейния вътрешен (за вида документ) адрес. Този адрес се формира с последователността от идентификатори на сегментите, през които минава пътя на достъп до данната. Сегментите се идентифицират с техните УРИ на регистрацията в РИО.

При това положение представянето на пътя за достъп до данна чрез УРИ на сегменти ще съдържа много излишна информация, включваща:

- УРИ на основния сегмент на дадения вид документ - той винаги ще присъства във всеки път за достъп и може да се изпуска, защото се подразбира;
- Регистровия индекс на УРИ на сегмент, през който минава пътя; този индекс за всички сегменти е един и същи и може да се изпуска; ето защо от УРИ на сегмент остава само поредния номер на регистрацията му в РИО

Тоест, името на тестови документ, който се отнася за:

- Тестване на вид документ с УРИ: уууу-nnnn;
- За проверка на данна с УРИ: xxxx-nnnn;
- С път до данната, представен чрез УРИ на сегменти както следва: zzzz-000a, zzzz-000b и zzzz-000c.

би трябвало да се формира по следния начин:

уууу-nnnn_000a_000b_000c_ xxxx-nnnn.xml

3.4. Проверка за валидност на имената на тестови документи, несъдържащи грешки

Имената на тестовите документи несъдържащи грешки се създават по схема, която позволява:

- Да се идентифицира вида документ, за който се отнася тестовия документ. Идентификацията на вида документ се извършва с неговия УРИ на регистрацията в РИО;
- Да се посочи факта, че документът не съдържа грешки. За тази цел в името на документа се включва текстовия низ „ОК”;
- Да се идентифицира вариант на документа, в случай че негови компоненти съдържат допустими алтернативни варианти.

Вариант на документ ще се представя с посочване на избрана от няколко алтернативни варианта конструкция на данна. Самата данна се идентифицира с нейния УРИ и очевидно с пътя до нея.

Тоест, имената на тестови документи с вярно съдържание, които се отнасят за:

- Тестване на вид документ с УРИ: yyyu-nnnn;
- За алтернативни варианти, представени с данни с УРИ: gggg-000e и gggg-000d;
- С път до алтернативните данни, представен чрез УРИ на сегменти както следва: zzzz-000f, zzzz-000g и zzzz-000h

би трябвало да се формира по следния начин:

yyyu-nnnn_ok_000f_000g_000h_gggg-000e.xml
yyyu-nnnn_ok_000f_000g_000h_gggg-000d.xml

Ако документът с УРИ: yyyu-nnnn няма варианти, за него се създава само един тестови документ с вярно съдържание, който ще има име:

yyyu-nnnn_ok.xml

3.5. Проверка за валидност на имената на документи от вида "Регистрирани грешки в съдържание на документ"

Имената на съответните документи от вида "Регистрирани грешки в съдържание на документ" се създават по схемата:

<име на тестови документ>_Error

Тест, документ от вида "Регистрирани грешки в съдържание на документ", създаден за тестови документ с име «yyyu-nnnn_000a_000b_000c_xxxx-nnnn.xml» ще бъде:

yyyu-nnnn_000a_000b_000c_xxxx-nnnn_Error.xml

3.6. Регистрация на резултатите от създаването на тестовия набор

Регистрацията на резултатите от създаването на тестовия набор се извършва чрез въвеждане на данни в документа „Резултати от тестове за оперативна съвместимост по документ”.

Практически след приключване на работата по тестовия набор от документи, самият документ „Резултати от тестове за оперативна съвместимост по документ” би трябвало да бъде напълно готов за извършване на проверка на дадено приложение за работата му със съответния вид документ.

3.7. Проверка на тестовите документи в набора

3.7.1. Проверка на тестови документи с вярно съдържание

Анализира се конструкцията на вида документ, за който се създава набора и се определя необходимостта от създаване на варианти на тестови документи с валидно съдържание.

Дефинират се имената, вариантите на конструкциите и се проверява:

- има ли в предоставения набор, тестови документи със съответното име
- откритите тестови документи имат ли съдържание, отговарящо на изискванията, резултат
- от направения анализ се създава валидно съдържание за тях.

3.7.2. Проверка на тестови документи от вида „невалиден xml-документ”

Проверява се в предоставения набор за наличие на следните тестови документи:

- Тестови документ, който е с формат различен от текстови. Името на такъв документ с .doc-формат би трябвало да е със следната конструкция:
 - **yyyy-nnnn_no_doc.xml**
- Тестови документ, който е с текстови формат, но не отговаря на xml-спецификацията. Името на този документ би трябвало да е от вида:
 - **yyyy-nnnn_no.xml**
- Проверява се дали този тестови документ има съдържание в разрез с xml-спецификацията. Тестови документ, който отговаря на xml-спецификацията, но не е регистриран в РИО като вид уууу-nnnn

Името на този документ би трябвало да е от вида:

- **yyyy-nnnn_no_registration.xml**
- Проверява се дали този xml- документ има валидно xml-съдържание, но не е регистриран в РИО като вид уууу-nnnn

3.7.3. Проверка на тестови документи с невалидно съдържание

За всяка данна и за всяка грешка, дефинирана за нея в справката от РИО се извършва следното:

- а. Проверява се наличието в набора на тестови документ, с име, формирано по дефинирания по-горе начин

- б. Проверява се в съдържанието на тестовия документ дали има информация, съответстваща на грешката, която се симулира с този документ

Ако видът документ предвижда варианти с алтернативни конструкции, за всеки вариант се проверяват и тестовите документи, които симулират грешките към данните в алтернативната конструкция, която формира варианта на тествания документ.

4. Изпълнение на изискванията за оперативна съвместимост при разработката и внедряването на електронните административни услуги

Разработката и внедряването на електронни административни услуги се базира на Закона за електронното управление (ЗЕУ) и наредбите към него – преди всичко, с изискванията за изпълнение на услуги, заявявани по електронен път, посочени в Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите (НВОЕДДХНА) и в съответствие с изискванията за приемане на електронни документи от Наредбата за електронните административни услуги (НЕАУ).

Това се реализира главно чрез:

- внедряване на Ведомствена номенклатура на услуги и процедури (ВНУП), Ведомствена номенклатура на етапи по услуги или процедури (ВНЕУП) и Ведомствена номенклатура на видовете документи (ВНВД);
- внедряване на унифицирани етапи от услугите (такива като «Приемане на документи на електронен носител», «Идентификация на заявителя на електронна административна услуга» и пр).

В изпълнение на изискванията е необходимо:

- да се проектира оптимизиране на работните процеси по предоставяне на административните услуги с оглед тяхното реализиране по електронен път;
- да се опишат оптимизирания работни процеси в детайлни работни карти на бъдещите процеси по предоставяне на административни услуги.

Анализът на съществуващите практики за предоставяне на електронни административни услуги от администрациите показва следното:

а) общите нормативни изисквания към описание на текущите процеси по предоставяне на административни услуги в централни и други администрации в България са дефинирани в Наредбата за административното обслужване, приета на основание Закона за администрацията и във връзка с Административно-процесуалния кодекс;

б) съгласно Наредбата за административното обслужване, всяка администрация е задължена да осигури информация с описание на предоставяните от нея административни услуги, включваща:

- наименование на административната услуга, съответстващо на Списъка на унифицираните наименования на административните услуги (СУНАУ);
- нормативна уредба по предоставянето на административната услуга;
- процедура по предоставяне на административната услуга, изискванията и необходимите документи;
- образци на документи, които се попълват за предоставяне на административната услуга;

- срока на действие на индивидуалния административен акт, издаван в изпълнение на съответната административна услуга;
- таксите или цените на съответните административни услуги.

В изпълнение на горните изисквания, трябва да се разработят съответни правила и процедури по предоставяне на конкретните административни услуги, като:

- установяване съответствие със СУНАУ, а при необходимост – съответни предложения за промени в СУНАУ, отразяващи съвременното състояние на услугите;
- изготвяне на съответни заявления като електронни документи;
- осигуряване обявяването на сроковете за изпълнение и таксите в съответствие с Наредбата за административното обслужване;
- в изпълнение на Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите услугата трябва да се комплектува от унифицирани етапи на услуги / процедури, които ще бъдат вписани в Регистъра на регистрите и данните и ще бъдат включени във Ведомствената номенклатура на етапи от услуги или процедури (ВНЕУП) на съответната административна информационна система (АИС).

Стриктното придържане към нормативните изисквания позволява и рязко да се повиши ефективността на контрола върху процеса на разработката на услуги и силно да се облекчи извършването му. Във връзка с това, трябва да се изготвят подробни дефиниции на:

а) състава и последователността на етапите, с които се представят дейностите по разработка на услуги;

б) съдържанието на дейностите в състава на самите етапи;

в) особеностите на извършване на тези дейности;

г) описание на крайните продукти от извършването на тези дейности

Като изходни данни се идентифицира услуга, представена с:

а) унифицирано наименование;

б) състав на документите, с които се заявява услугата;

в) състав на документите, които се изработват в отговор на изпълнение на услугата;

с) състав на документите, с които се изправят нередности при заявяване на услугата;

г) общо представяне на процеса на обработка на данни при изпълнение на услугата

Услугата се реализира в средата на реална АИС, съответстваща на изискванията за оперативна съвместимост и информационна сигурност по смисъла на раздел седми от глава шеста на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност (НОИОСИС).

Във връзка с това трябва да бъдат дефинирани действия по създаване на обекти и въвеждане на съдържание на данни в тях, без да се обясняват средствата за извършване на тези действия. Всички цитирани обекти и данни в тях ще съответстват на техните

дефиниции в Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите (НВОЕДДХНА).

По този начин, създаването на услуги в средата на, и със средствата на реалната АИС ще осигури:

- а) директна използваемост на крайните резултати от създаване на услугата;
- б) контрол на междинните и крайните резултати във вида им, в който те ще се използват при реалното изпълнение на услугата, без възможни грешки от преноса им от средата на създаване в средата за тяхното изпълнение;
- в) възможност за автоматично генериране на заявления за вписване на услуги, етапи по услуги и данни в съответните регистри.

Изпълнението включва следните етапи:

а) анализ на етапите на изходната дефиниция на услугата - обхваща всички етапи на изходната дефиниция на услугата. Целта на анализа е да определи за всеки етап:

- наличие на законова допустимост за изпълнение на етапа в автоматичен режим, без човешко участие;
- наличие на технологична възможност за изпълнение на етапа в автоматичен режим, без човешко участие.
- б) създаване на описание на услугата, като елемент от Ведомствената номенклатура на услуги и процедури (ВНУП). Етапът включва следните стъпки:
 - създава се нов елемент във ВНУП в АИС;
 - съдържанието на описанието на услуга се въвежда в новосъздадения елемент съгласно „Инструкция за създаване на елемент от ВНУП”.

За така създадения елемент от ВНУП се въвеждат съответните данни:

- въвежда се съответното съдържание за всички данни, специфицирани в ал.2 на чл.58 от НВОЕДДХНА, с изключение на данната „уникален регистров идентификатор на административна услуга или административна процедура”;
- за всеки документ, приеман от заявителя, или издаван към него се допълват нови данни в списъка с данните, които се съдържат в документа, необходими за изпълнение на услугата в автоматичен режим.

Крайните продукти от изпълнение на етапа са:

- създаден нов елемент във ВНУП, с попълнено съдържание на данните в него;
 - въведено съдържание на всички данни, представящи създаваната услуга, като елемент на ВНУП;
 - коригирани списъци с унифицирани данни, съдържащи се в документите приемани, или издавани във връзка с изпълнение на услугата.
- в) създаване на списък с етапите по услугата. Етапът включва следните стъпки:
- въвеждат се елементите на списъка в състава на новия елемент на ВНУП, с който се представя ново създаваната услуга;

- за всеки елемент се посочва съответствието му на подходяща унифицирана дефиниция на етап по услуга или процедура, налична във Ведомствената номенклатура на етапи по услуги или процедури (ВНЕУП);
- при липса на подходяща дефиниция във ВНЕУП във ВНЕУП, се проверява за наличие на такава в раздел „Унифицирани етапи” на Регистъра на регистрите и данните; ако има такава тя се зарежда във ВНЕУП;
- при неуспешно търсене на налична унифицирана дефиниция на етап по предходната точка, се създава нов елемент на ВНЕУП.

За всеки елемент от списъка на създаваната услуга, съгласно чл.58 от НВОЕДДХНА се въвеждат данни за:

- изпълнител на етапа;
- време за изпълнение на етапа;
- крайни продукти по изпълнение на етапа;
- специфични условия за изпълнение на етапа в администрацията, която ще изпълнява услугата.

Крайните продукти от изпълнение на етапа са:

- създаден списък с етапи по услуга;
- евентуално създадени нови елементи от ВНЕУП;
- евентуално създадени нови елементи от номенклатурата на крайни продукти по етапи от изпълнение на услуги или процедури.

г) създаване на унифицирани дефиниции на етапите от списъка, създаден по Етап в). По принцип създаването на такива унифицирани дефиниции се инициира при изпълнение на предишния етап, като се създават „празни дефиниции на етапи”. Възможно е да се създаде нов елемент на ВНЕУП и по общи съображения, когато се създават пакет от тематично близки услуги. В този случай, създаването на „празни дефиниции на етапи” може да се извърши при извършване на един общ анализ на пакета. Етапът включва следните стъпки:

- последователно се обработват унифицираните дефиниции на всички налични „празни дефиниции на етапи”;
- въвежда се съответното съдържание в данните в тези елементи.
- за всяка „празна дефиниция на етап” се въвеждат съдържание за данните, специфицирани в ал.2 на чл.55 на НВОЕДДХНА.

Крайните продукти от изпълнение на етапа са попълнени данни за всички налични „празни дефиниции на етапи”.

д) преглед за технологично съответствие на създадената услуга. Етапът включва следните стъпки:

- със средствата на АИС се извлича от ВНУП текста на описанието на унифицираната дефиниция на така създадената услуга - това е описанието на услугата, което съдържа данните подлежащи на регистрация в Списъка на унифицираните наименования на административните услуги;

- проверяват се всички текстове, представящи унифицираната дефиниция на услугата, без оглед на начина на тяхното съхранение в АИС;
- проверява се текстовото описание за пълно технологично съответствие;
- при откриване на грешка се прави съответната корекция в съответния елемент на ВНУП или ВНЕУП;
- след всяка корекция се извършва ново генериране на пълното описание на унифицираната дефиниция на услугата и се подновява прегледа от първата процедура;
- при необходимост от въвеждане на нов етап в състава на услугата се изпълняват частично или пълно действия от предишните етапи и след това се преминава към изпълнението;
- ако при изпълнението се окаже, че новосъздаден етап се отхвърли, тоест той не участва вече в дефиницията на нито една услуга, този етап се премахва от ВНЕУП и за него не се стартира процедура по регистрацията му в раздел „Унифицирани етапи” на Регистъра на регистрите и данните.

Крайните продукти от изпълнение на етапа са:

- утвърдена за технологично съответствие унифицирана дефиниция на услугата;
- утвърдена за регистрацията услуга;
- актуализирана ВНЕУП;
- създаден списък от етапи, подлежащи на регистрацията;
- създаден списък на услуги, в които влизат коригирани етапи на услуга в хода на изпълнение на този етап от Методологията.

е) преглед за законосъобразност на създадена услуга. Действията по изпълнение на етапа са аналогични на тези по предишния етап. Единствената разлика е, че правният експерт има водеща роля по извършване на прегледа за съответствие.

Възможно е при въвеждане на корекции във връзка с открити правни проблеми да се стигне и до технологични корекции. Тези корекции се извършват заедно с корекциите, касаещи открит правен проблеми и отново се извършва преглед, но в случая той комбинира и анализ за технологично и анализ за правно съответствие. Прегледът за законосъобразност обхваща и списъците с унифицирани данни, представящи документите, приемани или издавани във връзка с изпълнение на услугата.

Крайните продукти от изпълнение на етапа от Методологията са същите както по предходния етап. В случая, обаче, те имат гарантирано съответствие и с нормативния регламент на процесите, които представя унифицираната дефиниция на услугата.

ж) преглед за съответствие със заданието за създаване на услугата - този преглед се прави с участието на специалистите, работили до момента върху създаването на услугата, и на специалисти от администрацията, която ще заяви вписването на услугата и евентуално етапи към нея. Действията са аналогични на действията по предишния етап. Възможно е, при въвеждане на корекции във връзка със забележки на приемащата администрация да се стигне и до корекции; след тези корекции се извършват и анализ за технологично и анализ за правно съответствие. Прегледът за съответствие със заданието обхваща и списъците с унифицирани данни, представящи документите, приемани или издавани във връзка с изпълнение на услугата.

Крайните продукти от изпълнение на етапа от Методологията са:

- утвърдена унифицирана дефиниция на услуга, подлежаща на вписване в СУНАУ;
- утвърдени за вписване етапи по услуги, ако такива са създадени;
- утвърдени списъците с унифицирани данни, представящи документите, приемани или издавани във връзка с изпълнение на услугата.

Подаването на заявления за електронните административни услуги обикновено се извършва чрез уеб-базирано приложение, свързано с Интернет сайта на административната единица. При това, потребителският интерфейс трябва да отговаря на изискванията на Глава трета на Наредбата за електронните административни услуги. В съответствие с изискванията на чл. 43 от същата наредба като резервни канали може да бъде осигурено получаването на електронните заявления чрез електронна поща и на физически носител.

Внедряване на услугите се извършва в съответствие с въведения от Закона за електронното управление и наредбите нов административен модел със следните основни особености, като:

а) за всеки документ ще има регламент за неговата обработка, представен с процедурно описание;

б) се децентрализира отговорността по контрол на изпълнението на процедурите:

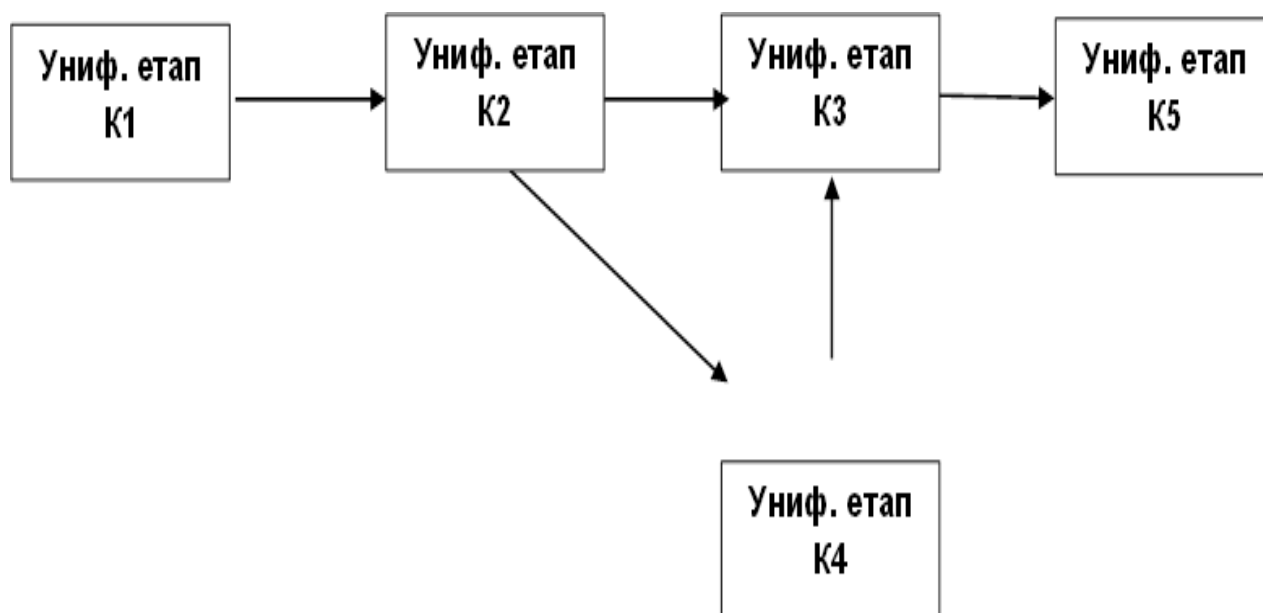
- отговорност на ниво “етап от услуга”
- отговорност на ниво “услуга”
- отговорност на ниво “администрация”

в) се въвеждат се унифицирани дефиниции на услуги и процедури, базирани на унифицирани дефиниции на етапи по услуги и процедури. Те се поддържат от АИС в съответствие с Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите (НВОЕДДХНА);

г) се поддържа Ведомствена номенклатура на услуги и процедури (ВНУП), Ведомствена номенклатура на етапи по услуги или процедури (ВНЕУП) и Ведомствена номенклатура на видовете документи (ВНВД). Взаимодействието между тези номенклатури е показано в фигурата по-долу:

Работната карта на процесите по изпълнението на услугата се състои от обща част, отразяваща описанията на услугата / процедурата, и съвкупност работни карти на унифицираните етапи, участващи в услугата / процедурата.

Схематичен вид на услугата / процедурата



Фигура 7-1

Формат на работната карта

Обща част – глава на работната карта
Уникален регистров идентификатор на административната услуга или административната процедура съгласно чл. 58 ал. 2 т. 1 от НВОЕДДХНА
Наименование на услуга или процедура съгласно чл. 58 ал. 2 т. 2 от НВОЕДДХНА
Описание на услуга или процедура съгласно чл. 58 ал. 2 т. 3 от НВОЕДДХНА
Отговорен за услуга или процедура съгласно чл. 58 ал. 2 т. 4 от НВОЕДДХНА
Срок за изпълнение на услуга или процедура съгласно чл. 58 ал. 2 т. 5 от НВОЕДДХНА
Списък на етапи от услуга или процедура съгласно чл. 58 ал. 2 т. 6 от НВОЕДДХНА
Указания за услуга или процедура съгласно чл. 58 ал. 2 т. 7 от НВОЕДДХНА
Етап № 1 от услуга или процедура
Уникален регистров идентификатор на етап съгласно чл. 55 ал. 2 т. 1 от НВОЕДДХНА
Наименование на етап съгласно чл. 55 ал. 2 т. 2 от НВОЕДДХНА
Определение на етап съгласно чл. 55 ал. 2 т. 3 от НВОЕДДХНА
Изпълнител на етап съгласно чл. 55 ал. 2 т. 4 от НВОЕДДХНА
Срок за изпълнение на етап съгласно чл. 55 ал. 2 т. 5 от НВОЕДДХНА
Набор от видове създавани документи съгласно чл. 55 ал. 2 т. 6 от НВОЕДДХНА
Указания относно етап съгласно чл. 55 ал. 2 т. 7 от НВОЕДДХНА
Набор от крайни резултати от етап съгласно чл. 55 ал. 2 т. 8 от НВОЕДДХНА
Етап № 2 от услуга или процедура
.....
Етап № k от услуга или процедура
.....
Етап № n от услуга или процедура
.....

Основните унифицирани етапи съгласно чл. 55 ал. 2 т. 7 от НВОЕДДХНА се реализират както следва:

А. Унифициран етап «Приемане на документи на електронен носител» - при приемане на електронни документи чрез Уеб, електронна поща или от приносител на физически носител се извършват автоматично стандартни проверки, както следва:

а) проверка по Чл. 48, ал. 1, т. 1 от Наредбата за електронните административни услуги (НЕАУ): дали подаваното заявление е във формата по чл. 63 и размерът на заявлението заедно с приложенията не надвишава определения от административния орган размер за електронните административни услуги, предоставяни от съответната администрация - проверката за форматните изисквания по чл. 63 включва не само проверка за наличност на синтактично правилно оформен XML-документ, но и дали документът е регистриран в Регистъра на информационните обекти, дали е валиден съгласно регистрацията си и дали администрацията е обявила на своята Интернет страница, че поддържа приемането на такъв вид документ, респективно дали изпълнява заявената с него услуга или процедура. Проверката за допустим размер на подадения електронен документ се извършва по отношение на ограничението на този размер, публикувано на Интернет страницата на приемащата администрация.

При неуспешен изход от описаните по-горе проверки се създава документ от вида "Съобщение, че получаването не се потвърждава", с който се оповестява подателят за неуспешния изход.

Като причина за непотвърждаването при недопустим размер на подаден документ се посочва: „Размерът на заявлението заедно с приложенията надвишава определения от административния орган размер за електронните административни услуги, предоставяни от съответната администрация.” Документи с недопустим размер се съхраняват в АИС на приемащата администрация.

Като причина за непотвърждаването при форматно несъответствие на подаден документ се посочва: „Подаваното заявление не е в нормативно установения формат”. Документът с форматно несъответствие се съхранява в АИС на приемащата администрация.

б) проверка по Чл. 48, ал. 1, т. 2 от НЕАУ: дали приложените към заявлението документи са във форматите по чл. 65 от НЕАУ - проверката се извършва за всички приложени документи в състава на приемания документ, ако има такива.

При неуспешен изход от проверката се създава документ от вида "Съобщение, че получаването не се потвърждава", с който се оповестява подателят за неуспешния изход.

Като причина за непотвърждаването се посочва: „Приложените към заявлението документи не са в нормативно установения формат”. Документът с посоченото несъответствие се съхранява в АИС на приемащата администрация.

г) проверка по Чл. 48, ал. 1, т. 3 от НЕАУ: дали подаваното заявление и приложенията към него не съдържат вируси и друг нежелан софтуер съгласно изискванията на наредбата по чл. 43, ал. 2 от Закона за електронното управление - проверката се извършва за всички приложени документи, в състава на приемания документ, ако има такива.

При неуспешен изход от проверката се създава документ от вида "Съобщение, че получаването не се потвърждава", с който се оповестява подателят за неуспешния изход.

Като причина за непотвърждаването се посочва: „Подаденото заявление и приложенията към него съдържат вируси или друг нежелан софтуер”. Документът с посоченото несъответствие се съхранява в АИС на приемащата администрация.

д) проверка по Чл. 48, ал. 1, т. 4 от НЕАУ: дали подаваното заявление съдържа уникален идентификатор на заявителя и на получателя на електронната административна услуга, когато законът изисква идентификация за предоставяне на съответната услуга - проверката се извършва за всички приложени документи в състава на приемания документ, ако има такива.

При неуспешен изход от проверката се създава документ от вида "Съобщение, че получаването не се потвърждава", с който се оповестява подателят за неуспешния изход.

Като причина за непотвърждаването се посочва: „Подаденото заявление не съдържа уникален идентификатор на заявителя и на получателя на електронната административна услуга”. Документът с посоченото несъответствие се съхранява в АИС на приемащата администрация.

Особености при приемане чрез Уеб:

- стартиране на приемането се извършва само при подаден адрес на електронна поща, съгласно Чл. 48 ал.1 т.5 от НЕАУ;
- съдържанието на документа "Съобщение, че получаването не се потвърждава" се изпраща online към подателя на документа в рамките на Интернет сесията по подаване;
- документът "Съобщение, че получаването не се потвърждава" се изпраща прикачен към електронно съобщение и на посочения от подателя адрес на електронна поща.

Особености при приемане чрез електронна поща:

- всеки прикачен документ към електронно съобщение се обработва самостоятелно, без да се търси връзка с други евентуално прикачени документи;
- като адрес за изпращане на документа "Съобщение, че получаването не се потвърждава" се използва адресът, от който е изпратено съобщението с подавания документ(и);
- съдържанието на полето subject на обратното съобщение, към което е прикачен документа "Съобщение, че получаването не се потвърждава", се формира от съдържанието на полето на съобщението, с което е изпратен документът, като в началото се добавя символния низ „Re:”.

Особености при приемане на физически носител:

- приемането се отказва, ако приемащата администрация няма техническата възможност да прочете съдържанието на съответния тип носител, ако носителът е повреден или ако при достъп до него се открие нежелан софтуер;
- приемането се извършва само ако приносителят на физическия носител подаде синтактично валиден адрес на електронна поща;
- при изявено желание съдържанието на документа "Съобщение, че получаването не се потвърждава" се предоставя в разпечатан и подписан вид;

- след издаване на документа "Съобщение, че получаването не се потвърждава" или след приемането му, физическият носител се съхранява от приемащата администрация.

Особености при изпращане на документа "Съобщение, че получаването не се потвърждава":

- ако документът е подаден чрез Уеб, електронна поща или на физически носител, в документа "Съобщение, че получаването не се потвърждава" се посочва името на файла, с който е подадено неговото съдържание;
- ако документът "Съобщение, че получаването не се потвърждава" се изпраща прикачен към електронно съобщение, съдържанието на полето Subject на съобщението се формира по схемата: „Отхвърлен документ „<име на подадения файл>” от <име на приемащата администрация>.

При успешно извършване на проверките, приемащата администрация регистрира приетия документ, създава по него преписка и стартира обработката му. Заедно с това създава, класира в официалния раздел на преписката и изпраща на подателя документ „Потвърждаване за получаване”. Приетият документ, заедно с преписката по него, се предава за обработка на следващия етап от изпълнение на услугата или процедурата.

Ако документът „Потвърждаване за получаване” се изпраща прикачен към електронно съобщение, съдържанието на полето Subject на съобщението се формира по схемата: „Приет документ „<име на подадения файл>” от <име на приемащата администрация>.

Б. Унифициран етап «Идентификация на заявителя на електронна административна услуга» - след приемането на входящо електронно подписано заявление за услуга се извършва автоматично:

а) идентификация на заявителя (по чл. 55 ал. 1 т. 2 на Наредбата за електронните административни услуги). Това трябва да стане чрез вътрешна електронна административна услуга (изпращане на съответно заявление през ЕСОЕД в ЕСГРАОН или Регистър ЛНЧ на МВР).

б) опционално – при е-Услуга за юридическо лице - проверка за идентичност на юридическо лице и за представителната власт на автора на заявлението (по чл. 52 ал. 1 т. 3 и чл. 55 ал. 2 на Наредбата за електронните административни услуги). Това също трябва да стане чрез вътрешна електронна административна услуга (изпращане на съответно заявление през ЕСОЕД в Търговския регистър или Регистър БУЛСТАТ).

Тук трябва да се добави следното: новият Закон за електронният документ и електронния подпис (ЗЕДЕП) (чл. 24) не предвижда реквизит “титуляр” в удостоверението за електронен подпис. Включването му в политиките на някои доставчици на удостоверителни услуги не променя този факт.

Освен това, аналогично на идентификацията на физически лица, удостоверението за е-Подпис не може да бъде източник на информация за представителната власт на автора.

в) валидация на квалифициран електронен подпис (КЕП). Този процес трябва да се раздели на три под-процеса:

в1) проверка на електронния подпис, т.е. алгоритмична проверка за интегритет на документа (чл. 52 ал. 1 т. 1 от Наредбата), в т.ч.:

- изчисляване на контролната сума и сравняване с електронно подписната такава;
- проверка в рамките на подписаните/пре-подписаните данни.

Тази проверка трябва да се осъществи в АИС на административния орган, предоставящ е-Услуга.

в2) проверка на авторството, т.е. установяване на съответствието между името на заявителя, посочено в заявлението (и идентифицирано по т. 1) и името на автора, съдържащо се в удостоверението (чл. 55 ал. 1 т. 1 от Наредбата). Тази проверка също се осъществява в АИС на административния орган, предоставящ е-Услуга с помощта на вътрешна електронна административна услуга – запитване на МВР (служба „Документи за самоличност на български граждани“) дали трите имена (string) на латиница, записани в удостоверението, отговарят на името (на кирилица) и ЕГН на автора на заявлението. Това може да се осъществи само при строго спазване от всички издатели на удостоверения на условието: имената на автора да бъдат записани в удостоверението точно, както са в личната карта и да не се допуска вписването на псевдоним, което е обявено в политиките на някои издатели;

в3) валидиране на удостоверението за електронен подпис. Това трябва да включва:

в3.1) изграждане на веригата през оперативните органи до базовия оперативен орган;

в3.2) проверка на периода на валидност, вписан в удостоверението спрямо времето на подписване (чл. 52 ал. 1 т. 2а от Наредбата) – в случай на липса на удостоверенията за време (Time Stamping), за такова време ще се приема времето на постъпване на заявлението в АИС;

в3.3) проверка на атрибутите на удостоверението (чл. 52 ал. 1 т. 2б от Наредбата), в т.ч.:

- наличие на атрибут за квалифициран електронен подпис;
- проверка за вписаната политика.

в3.4) проверка на т.н. “Revocation Status” на удостоверението (чл. 52 ал. 1 т. 2г от Наредбата). Това се извършва или чрез листване на Списъка с отменените удостоверения (CRL - Certification Revocation List) на издателя, или чрез електронен обмен с него по протокола OCSP (Online Certificate Status Protocol).

в3.5) проверка на електронния подпис на сертификата (изискване на XAdES) чрез изчисляване на контролната сума и сравняване с електронно подписната такава.

При неуспешно провеждане на поне една от горните проверки, по данните от заявлението автоматично се генерира „Отказ от изпълнение на услуга“, класифицира се в преписката по заявлението и се подава за по-нататъшна обработка на изпълнителя по етапа. Той довършва текста на съдържанието на отказа, като посочва правното и фактическото основание за отказ и редът за неговото обжалване.

В заявлението за услуга се отразява становище „Несъгласен“, класифицира се документа-отказ в преписката и се предава за обработка на следващия етап.

Документът „Отказ от изпълнение на услуга“ се регистрира и се подписва с КЕП. За дата на издадения документ „Отказ от изпълнение на услуга“ се счита датата в електронния подпис в документа.

Ако данните за търговското дружество са валидни се проверява за съответствие на данните за представляващия го, със съответните данни, посочени за заявител в заявлението. Ако липсва съответствие се изготвя документ „Отказ от изпълнение на услуга”. Отразява се по заявлението за услуга становище „Несъгласен”, класифицира се документа-отказ в преписката и се предава за обработка на следващия етап.

При констатиране на съответствие се проверява идентичността на данните за представляващ търговското дружество. Ако не може да се установи идентичността на представляващия се изготвя документ „Отказ от изпълнение на услуга” и в него се посочват причините за постановяване на отказа.

При установена идентичност, за заявителя на услугата се изготвя документ „Данни за идентификация на физическо лице” и се класифицира в преписката.

Извършено плащане се регистрира от финансовото звено на административния орган. Съответният служител създава документа „Уведомление за наредено плащане” и го изпраща на изпълнителя на етапа, заедно с преписката, по която се очаква плащането.

И в заключение, в съответствие с Раздел седми на Глава четвърта на НВОЕДДХНА трябва да се осигури поддържане на „статус на изпълнение“ на електронните административни услуги. Този статус ще бъде достъпен „он-лайн“ на заявителя на съответната услуга.

Вписване на електронните административни услуги

То трябва да се извършва в строго съответствие със Закона за електронното управление, наредбите към него и Инструкцията за правилата и критериите за използването им при вписвания в регистрите на информационните обекти и електронните услуги, утвърдена от министъра на транспорта, информационните технологии и съобщенията на 21.01.2010 г. Подготвителните действия по попълване на основния документ - Заявлението за вписване – се извършват в следния ред: от данните и техните дефиниции към документите, свързани с услугата, и накрая – самата услуга.

Националният модел на данните в администрациите е разработен по проект PHARE PROJECT :“Strengthening the capacity of the Bulgarian public administration for implementing the e Government Strategy” BG2004/016-711.10.01 (Lot 1) EuropeAid/122540/D/SV/BG:. Въз основа на този модел се дефинират следните етапи на създаване на електронен документ:

- регистрация на неунифицирано описание на данна - раздел „Обстоятелства” на Регистъра на регистрите и данните;
- регистрация на унифицирано описание на данна - раздел „Унифицирани данни” на Регистъра на регистрите и данните;
- регистрация на формализирано описание на данна - раздели „Стойности”, „Номенклатури” и „Сегменти” на Регистъра на информационните обекти;
- административна регистрация на електронен документ - раздел „Документи” на Регистъра на информационните обекти;

Първият етап е елемент от осигуряване на прехода от неунифицирани към унифицирани данни. Вторият етап практически дава началото на постигане на семантична оперативна съвместимост на ниво „данни” в българското електронно правителство. Важен елемент от регистрацията по първия етап е посочването на съответната унифицирана дефиниция на данна за една или повече неунифицирани данни. Така се маркира прехода от неунифициран в унифициран вид за данните. Третият етап регистрира формализирания вид на вече унифицирани данни, като използва опростен модел, съдържащ три вида данни:

стойност, номенклатура и сегмент. Като сегмент се дефинира и конструкцията на бъдещ електронен документ. Четвъртият етап регистрира електронен документ, като регистрацията има чисто административен характер. Тя гарантира, че за даден вид електронен документ има легално дефинирана XML конструкция и за нея е осигурено сертифицирано приложение за неговата визуализация или редактиране.

Ето защо се формулира задължителното изискване всички данни в състава на електронен документ, които са регламентирани в някакъв нормативен документ да бъдат обработени последователно по всички етапи, посочени по-горе.

Във връзка с изпълнение на електронни услуги очевидно ще се наложи да бъдат използвани данни, които нямат текущ нормативен регламент. Поддръжката на оперативна съвместимост осигурява такава възможност, като се „прескача“ първия етап. Изпълнението на останалите етапи, включително и когато изкуствено създадената данна се използва в състава на електронен документ остава задължително. Фактът на регистрация на данната още на втория етап я прави легална на ниво „семантика“, тоест данната може да се използва в нормативни текстове. След нейната регистрация на третия етап е налице легална XML-дефиниция на данната, която може да се използва при конструиране на електронни документи. Независимо от прескачането на първия етап, останалите етапи остават задължителни. С това финално регистрираните версии на формализирани данни в Регистъра на информационните обекти са абсолютно равностойни и в правен и в технологичен аспект.

Биха могли да бъдат дефинирани следните принципи при унификация на данни:

- унификацията на единични данни не винаги е ефективна. Добре е да се работи с набори от семантично близки данни, дори и когато този набор се формира от данни, които са извън обхвата на конкретно решавана задача;
- проверка на качеството на създадена унифицирана данна се прави, като тя се замести в нормативните текстове, където се цитира нейния неунифициран изходен вид.

При изпълнение на горните препоръки трябва да се изработи оптимална дефиниция на унифицираната данна, която най-добре отразява нейната семантика и може да замести максимален брой неунифицирани данни.

В болшинството от случаите, създаваните електронни услуги са еквивалентни на налични и изпълнявани в административната практика услуги, заявявани и изпълнявани с хартиени документи. Новосъздадената електронна услуга се изпълнява по същата технология, както и нейния „хартиен“ аналог. Разликите се свеждат основно до следното:

- заявяването се извършва с електронен документ, който задължително трябва да е регистриран в Регистъра на информационните обекти;
- в повечето случаи и отговорът по услугата е електронен документ, за който важи същото изискване за регистрация в Регистъра на информационните обекти;
- променена е реализацията на етапа на приемане на заявления по услугата, като се извършва съгласно предписанията на Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите;
- ако отговорът по услугата е също електронен документ съответно се променя и етапа от нейното изпълнение, който регламентира именно издаването на този отговор;

- останалата част от технологията (процеса) на изпълнение на услугата остава по същество непроменена, независимо от начина по който се реализира информационната обработка на документите по услугата.

Ето защо, по отношение на състава на данните в електронни документи, които имат хартиен, при това нормативно дефиниран аналог може да се формулират следния принцип: „Всички данни, които представят по същество съдържанието на заявената услуга трябва да присъстват в електронната версия на документа в същия състав, в който присъстват и в хартиената версия”.

Легализацията на междинните и крайните резултати от цялостния процес по разработката на електронни документи включва три етапа:

а) дейности по легализация на конструкцията на електронен документ - легализацията е свързана основно с регистрация на данни. Тоест, подготовката на документите за регистрацията на данни е задължителната част от дейностите. Освен тези задължителни дейности, разработчикът на електронни документи е желателно да извърши и други дейности, с които би гарантирал бързо и успешно извършване на легализацията, тоест на вписването на данни по, и самата конструкция (като сегмент) в Регистъра на информационните обекти. Така дефинираните „пожелателни” дейности се вписват по един естествен начин в общия набор от дейности и той може да се представи както следва:

- идентификацията трябва да бъде придружена с прецизно търсене в раздел „Обстоятелства” на Регистъра на регистрите и данните за вече налично извършено вписване. Ако се открие такава наличност, отпада необходимостта от вписване. Предвид спецификата на вписване на неунифицирана данна като свободен текст, това търсене трябва да вземе в предвид тази специфика;
- подготовка на документи за вписване на неунифицирана данна в раздел „Обстоятелства” на Регистъра на регистрите и данните;
- внасяне на корекции в документите по вписване, ако има забележки от МТИТС;
- дефиниране на данните по вписване на унифицирана данна;
- проверка за наличие на вече регистрирана аналогична данна, или данна с дублиращо се име. Ако има аналогична данна, която по смисъл съответства на конструираната се възприема вече регистрираната. Ако е налице дублиране на името, то името на конструираната унифицирана данна се променя, за да се избегне това несъответствие с изискванията за успешно вписване;
- подготовка на документи за вписване на унифицирана данна;
- внасяне на корекции в документите по вписване, ако има забележки от МТИТС
- Дейностите по легализация на конструкцията на електронен документ приключват успешно при наличие на вписан документ в раздел „документи” на Регистъра на регистрите и данните със статус "приложение за визуализация в процедура по сертификация".

б) дейности по легализация на приложение за поддръжка на електронен документ – тези дейности се разглеждат като част от дейностите по изработване на приложение за визуализация и редактиране на електронния документ. При подготовката на легализация

проверката за съответствие се изпълнява от самия разработчик, за да се открият изпреварващо нередности, както следва:

- изработване на самото приложение;
- създаване на тестовия набор, съгласно „Методика за проверка на пълнота на тестови набори“;
- подготовка на документи за вписване на тестовия набор;
- внасяне на корекции в документите по вписване на тестовия набор и евентуално в самия тестови набор, до успешното му вписване в Списъка на сертифицираните системи- раздел "Тестови набори от документи";
- подготовка на инсталационен комплект на приложението съгласно изискванията за извършване на проверка на съответствие;
- тестово извършване на проверките за съответствие и внасяне на съответните корекции в приложението и/или документите за сертификация.

в) дейности по заключителна легализация на електронен документ:

- подготовка на документите за окончателно вписване на електронния документ. Съществена, макар и малка част от тази подготовка е вземане на УРИ на вписване на приложението в Списъка на сертифицираните системи - раздел "Сертифицирани приложения";
- отразяване на открити несъответствия в документите по вписване, до успешното извършване на същото.

Вписване на услуга, етапи по нея и унифицирани данни в състава на документите, приемани и издавани при изпълнение на услугата може да добие чисто техническа реализация, ако Съветът по вписванията няма забележки по предложението за вписване.

Със средствата на АИС се генерира автоматично по-голяма част от съдържанието на заявлението за вписване на услуга, евентуално на заявленията за вписване на етапи и заявления за вписване на унифицирани данни в раздел „Унифицирани данни“ на Регистъра на регистрите и данните. Останалите необходими данни се въвеждат на ръка. Документите се подписват от ръководителя на администрацията, заявител на вписванията, и се предават в МТИТС.

При наличие на чисто технически забележки по документите в заявката за вписване, те се отстраняват в оперативен порядък до извършване на заявените вписвания. При наличие на забележки, които водят до промени по същество в създадената услуга, съответните корекции се извършват чрез повторно изпълнение на предишни етапи, като до известна степен може да се допусне комбинирано изпълнение на етапи

Временно изпълнение на услуга, до вписването ѝ в СУНАУ изисква наличие на УРИ на регистрация в този списък. Във връзка с това се генерира пълния текст на унифицираната дефиниция на услугата, по него се създава документ в АИС и този документ се регистрира в официалния документен регистър на администрацията. Така генериранят УРИ се вписва като УРИ на услугата във ВНУП в АИС. За всички приемани и издавани документи по изпълнение на услугата се изготвят шаблони. Всички приемани и издавани документи по изпълнение на услугата се въвеждат във Ведомствената номенклатура на видовете документи (ВНВД)

5. Одит на административна информационна система

Основна задача на одита на административна информационна система (АИС) е да се даде оценка на степента ѝ на готовност за сертификация за оперативна съвместимост и информационна сигурност по смисъла на Глава шеста от Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

Законът за електронното управление регламентира това изискване, както следва:

„Чл. 56. (1) Административните органи използват информационни системи, които са сертифицирани за съответствие с изискванията на този закон за оперативна съвместимост и информационна сигурност.

(2) При провеждане на обществени поръчки за внедряване на информационни системи административните органи задължително включват като изискване тези системи да са сертифицирани за оперативна съвместимост и информационна сигурност.

Чл. 57. (1) Съответствието на внедряваните от административните органи информационни системи с установените нормативни изисквания за оперативна съвместимост и информационна сигурност се удостоверява от акредитирани от министъра на транспорта, информационните технологии и съобщенията лица.

(2) Методиката, правилата за извършване на оценката за съответствие, начинът на акредитация на лицата по ал. 1 и изискванията към тяхната дейност се определят с наредба.

§ 6 от Преходните и заключителни разпоредби: Административните органи привеждат информационните си системи в съответствие с изискванията на този закон и препоръките на министъра на транспорта, информационни технологии и съобщенията по § 5 в срок една година от обнародването на закона.”

Провеждането на одита на административна информационна система (АИС) се базира на Методиката на бившата Държавна агенция по информационни технологии и съобщения (ДАИТС) за провеждане на преглед в изпълнение на § 5 от Преходните и Заключителните разпоредби към Закона за електронното управление (ЗЕУ).

Методиката е съобразена с текущото ресурсно осигуряване на административната дейност с инструкции за това как да се извършват промените в средата на административните информационни системи. Във връзка с това са дефинирани липсващи инструкции, които трябва да се създадат и които излизат извън обхвата на самия преглед.

На пръв поглед, задачата за преглед на информационните системи е поставена доста общо, защото не се визира техния тип. Това може да постави в обхвата на прегледа и такива системи, като системите за счетоводна поддръжка, системите за управление на човешките ресурси и други типове системи, които най-общо влизат в класа на системи за управление на структурирани данни. Тези системи по принцип са дефинирани пряко или косвено от вече съществуващи законови регламенти – например, Закона за счетоводството и очевидно не влизат в обхвата на прегледа. Тези типове системи са обект на контрол от самите потребители в процеса на изпълнение на служебните им задължения и практически не се използват системи от тип, който не отговаря на съответната нормативна регулация.

Така обект на прегледа остават системите, които касаят работата с документи, или както в момента се наричат деловодни, документооборотни или просто документни системи. Действащият регламент преди приемането на ЗЕУ (или по-точно, преди Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите), който е използван като задание за създаване на почти всички налични системи от този тип, е Единната държавна система за деловодство, създадена през 1975г., с

последна редакция от 1986г. Очевидно тя е напълно негодна да регламентира не само работата с електронни документи, но и поддръжката на работата с хартиени документи с компютърни средства.

Ето защо, задачата, която се решава от прегледа, е доста тежка и по същество има характера на дефиниране на политика и нейното практическо прилагане. Всъщност, като част от ресорната политика в областта на информационните технологии, тази задача предшества задачата за сертификация на информационните системи за информационна сигурност и оперативна съвместимост. Двете задачи по тематика са много близки, но съвсем не са идентични.

Задачата за преглед на информационни системи има за цел да даде препоръки към наличните информационни системи във връзка с готовността им за сертификация. Но тя няма да регистрира изпълнението на задълженията на администрациите във връзка с изпълнението на отговорностите им по прилагане на ЗЕУ. Тоест, прегледът на информационните системи по-скоро е предписание за това какво трябва да направят администрациите, за да изпълнят изискванията на ЗЕУ във връзка с осигуряване на технически и организационни ресурси за съвместна работа с електронни и хартиени документи в условията на оперативна съвместимост.

За разлика от това, резултатите от проведена процедура по сертификация на информационни системи обективно ще оценяват доколко дадена администрация е изпълнила изискванията на ЗЕУ. Нещо повече, неуспешна сертификация на дадена информационна система практически ще блокира нейното прилагане в администрацията, което е много важно за нейните доставчици. Тоест, и администрациите и доставчиците на информационни системи ще бъдат много чувствителни към резултатите от сертификация, което ще бъде един от критичните моменти в изпълнение на изискванията на ЗЕУ.

В този смисъл, може да се каже, че задачата за текущ преглед на информационните системи подава важни сигнали към администрациите и доставчиците на информационни системи, за да извършат необходимата подготовка, осигуряваща успешна сертификация на по-късен етап. Тази особеност е отчетена при разработване на Методиката за нейното изпълнение.

Най-критичният елемент от методическите пособия за извършване на обективен преглед на информационните системи е наборът критерии за оценка годността на информационните системи за обслужване на административната дейност със съвместно използване на хартиени и електронни документи.

Стандартното дефиниране на набор от такива критерии се развива по схемата "Данни->Структури за поддръжка на данните->Функции, осигуряващи поддръжката на данни и структурите от данни". Няма предпоставки да не се спазва тази схема, ето защо тя е използвана при дефиниране на набора от критерии. Освен това, наборът е направен при стриктно придържане към основните три изисквания, на които такива критерии трябва да отговарят:

а) необходимост - за всеки от дефинираните критерии може да се посочи поне едно изискване, дефинирано пряко в нормативен регламент, или да се посочи неоспорима причинно следствена връзка между изискване в нормативен регламент и критерий за оценка на информационните системи. Преки връзки с нормативен регламент има най-много при дефиниране на критерии, касаещи типовете данни и специфика на тяхната поддръжка, които трябва да осигуряват информационните системи. Повечето от самите текстови дефиниции на данни са взети от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите, към ЗЕУ.

б) достатъчност - изискването за достатъчност засяга покриване не само на всички критерии, дефинирани пряко или косвено от нормативните регламенти, но и допълнителни критерии, които засягат ефективността на поддръжката на данни и структури, системната поддръжка, настройки и т.н. За целите на методиката изискването за достатъчност може да се сведе само до набор от критерии, които дават отговор на въпроса дали дадена информационните системи въобще може да поддържа електронно съдържание, а не в кои аспекти може да прави това, колко ефективно, лесно и т.н.

Между другото наборът от критерии може да се сведе само до един, а именно дали информационните системи поддържа файловото съдържание на електронни документи в база данни, като достъпът до него е само през ресурсите на АИС. Информационната система, която изпълнява такъв критерий, принципно може да поддържа работа с електронни документи, като за неизпълнението на останалите критерии може да се даде препоръка за доработка. Но ако обемът на доработките е толкова голям, че практически се преработва цялата система, ясно е, че оценяваната система не е пригодна за работа с електронни документи, защото препоръката в действителност посочва необходимостта от нова информационна система, независимо, че това се дефинира като „пълна преработка на оценяваната”.

Ето защо, изпълнението на изискването за „достатъчност” на набора от критерии е съобразено с възможността при дефиниране на препоръки към информационните системи да може да се направи преценка, дали обемът на препоръките всъщност не дефинира нова информационна система, тоест препоръките за промени с цел сертификация да се заменят с препоръка за подмяна на (оценената като негодна) информационна система.

в) инвариантност - това изискване осигурява независимост на критериите по отношение платформи на реализация на информационните системи, конкретни конструктивни решения и т.н.

Казано по друг начин, критериите в Методиката са дефинирани така, че да не се създават предпоставки за фаворизиране на налични информационни системи чрез залагане в критериите на конкретни технически реализации, характерни за тези системи. Това води до текстови изказ с доста висока степен на абстракция и общност на приложимостта. Такива текстове са трудни за възприемане и за практическо прилагане. Това автоматически се отразява на подбора на специалистите, които реално ще ги прилагат при прегледа на информационните системи.

Препоръките по принцип се отнасят за информационните системи. Но по същество, те се адресират към администрациите, особено когато касаят замяна на налична информационна система. Ето защо, за една и съща система, различни администрации ще получат едни и същи препоръки. В действителност, различните администрации може би имат нужда от по-пространни и по задълбочени препоръки във връзка с изпълнение на изискванията на ЗЕУ, но това не е обхванато от Методиката.

Ето защо, в нейния състав се предвижда дефиниране само на няколко типа (стандартни) препоръки. Препоръките трябва да се базират на унифицирана оценка, която в общ вид дефинира три нива на годност:

а) негодна за влизане в процедура по сертификация

Някои от изискванията са ключови. Тоест, неизпълнението на което и да е от тях директно прави дадена информационна система негодна. Ключови изисквания се дефинират върху:

- Данни;

- обекти, тоест набори от данни;
- структури за поддръжка на обекти.

Характеристиката „негодна” дефинира необходимостта от подмяна на информационната система с друга, или (почти) пълната ѝ модернизация.

б) необходима е подготовка за влизане в процедура по сертификация

По принцип информационната система се дефинира като годна, но трябва да се осигури липсваща функционалност, чрез доставка на нова, или модифициране на съществуващата информационна система.

Функционалността се дефинира върху:

- данни;
- обекти, тоест набори от данни;
- структури за поддръжка на обекти.

В случая обемът на липсващата функционалност е от значение и може да предефинира оценката на дадена информационна система, както следва:

- натрупването на липсваща функционалност в рамките на обект, до ниво на пълна липса на поддръжка дефинира допълнително ключово изискване, което не е изпълнено, тоест тогава информационна система се дефинира също като „негодна”;
- натрупването на липсваща функционалност в рамките на структури, до ниво на пълна липса на поддръжка също дефинира допълнително ключово изискване, което не е изпълнено, тоест тогава информационната системи се дефинира също като „негодна”;
- натрупването на липсваща функционалност общо за оценявана информационна система над дадено ниво също води до оценка „негодна”.

в) годна за влизане в процедура по сертификация

Годност се констатира и при наличие на неизпълнение на изисквания за функционалност, когато техният дял е под дадено ниво.

Оценката се базира на:

а) наличие на „ключови” изисквания

Неизпълнението дори и на едно „ключово” изискване дефинира „негодност” на информационната система. Оценката ще има за цел да открие и посочи всички неизпълнени ключови изисквания, за да бъдат включени в препоръките. В дефинираните критерии са обособени 14 ключови изисквания.

б) натрупване на препоръки за модификации

Необходимо е да се определи обема необходими модификации. Възможно е, този обем също да дефинира информационната система като негодна. Презумпцията е, че при голям обем на необходимите модификации, отстраняването им практически ще води до нова информационна система, независимо от това, че доставчикът и името ѝ може да останат същите.

Във връзка с това се дефинират три интервала за оценка по ниво на необходими модификации:

- До 25% - годни са за влизане в процедура по сертификация;
- 25-75% - допустим обем модификации;
- Над 75% - практически негодни за влизане в процедура по сертификация, тоест модификациите дефинират практически нова информационна система.

Процентът на модификациите се оценява, като за неизпълнение на дадено изискване се начисляват точки, приблизително съответстващи на обема модификации, необходими за неговото удовлетворяване.

За набори от тематично свързани изисквания се дефинира възможността, при неизпълнение на всички изисквания в набора да се регистрира общо неизпълнение, имащо ключова роля, тоест дефинира обща оценка за непригодност на информационната система.



РЕПУБЛИКА БЪЛГАРИЯ

Министерство на транспорта,
информационните технологии и съобщенията

Образец СЕГ

Приложение за вписване на сегмент

Пореден номер на
приложение в
заявлението *

B-16

Уникален
регистров
идентификатор

Y-0009-000016

(Уникалният регистров идентификатор се попълва, ако сегментът е вече вписан и се заявява промяна в обстоятелствата)

Наименование на
информационен
обект *

Търговец на зърно

(Наименование на информационния обект от вид "сегмент", с който обектът се индивидуализира еднозначно. Наименованието е уникално". То трябва да бъде същото, като вписаното в регистъра на регистрите и данните в раздел "Унифицирани данни")

Предназначение
на
информационен
обект *

Описание на търговец на зърно

(Кратко текстово пояснение на информационния обект от вид "сегмент". То трябва да бъде същото, като вписаното в регистъра на регистрите и данните в раздел "Унифицирани данни")

УРИ на данни *

Y-0003-000072

(Уникален регистров идентификатор на вписаното в раздел "Унифицирани данни" на регистъра на регистрите и данните унифицирано определение на данни, съответстващо на информационния обект от вид "сегмент")

Указания за
обработка на
информационен
обект *

**Обработката се извършва в съответствие с
приложената в полето "XML дефиниция" XSD схема.**

**При липса на попълнени данни в кой да е от
елементите се извежда съобщение за грешка с УРИ на
термин 0006-000015.**

(Описание в свободен текст или компютърно изпълними описания, които унифицират създаването на процедури по редактиране, визуализация и други видове обработка, свързани с информационния обект. Попълва се „няма“, ако няма специфични указания за обработката на информационния обект)

XML дефиниция
на
Сегмента *

```
<?xml version="1.0" encoding="utf-8"?>
<xsd:schema
targetNamespace="http://ereg.egov.bg/segment/Y0009-
000016"
xmlns="http://ereg.egov.bg/segment/Y0009-
000016"
```

```

xmlns:ebi=http://ereg.egov.bg/value/Y0008-000017
xmlns:ebn=http://ereg.egov.bg/value/Y0008-000018
xmlns:eut="http://ereg.egov.bg/value/Y0008-000019"

```

```

xmlns:xsd="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">

```

```

<xsd:import namespace="http://ereg.egov.bg/value/Y0008-000017"/>

```

```

<xsd:import namespace="http://ereg.egov.bg/value/Y0008-000018"/>

```

```

<xsd:import namespace="http://ereg.egov.bg/value/Y0008-000019"/>

```

```

<xsd:complexType name="GrainMerchant">

```

```

  <xsd:annotation>

```

```

    <xsd:documentation xml:lang="bg">Търговец на зърно</xsd:documentation>

```

```

  </xsd:annotation>

```

```

  <xsd:sequence>

```

```

    <xsd:element name=" GrainMerchantIdentifier"
type="gmi: GrainMerchantIdentifier " maxOccur="1"
minOccurs="0"/>

```

```

    <xsd:element name=" GrainMerchantName"
type="gmh: GrainMerchantName " maxOccur="1"
minOccurs="0"/>

```

```

    <xsd:element name=" GrainMerchantType"
type="gmt: GrainMerchantType" maxOccur="1"
minOccurs="0"/>

```

```

  </xsd:sequence>

```

```

</xsd:complexType>

```

```

</xsd:schema>

```

(Описание на структурата на обекта съгласно технически стандарт посредством дефиниция в XML формат с наименование, уникално за регистъра на информационните обекти, съдържаща други информационни обекти от вид "термин", "номенклатура", "стойност" или "сегмент", които вече са вписани в регистъра на информационните обекти)

Указания за проверка на валидност на сегмента *

Валидацията се извършва в съответствие с приложената в полето "XML дефиниция" XSD схема. При несъответствие се извежда съобщение за грешка с УРИ на термин 0006-000069.

(Правила за проверка на валидността на съдържанието на сегмента във формализиран вид съгласно стандарт, вписан в регистъра на стандартите, или по изключение в свободен текст. Правилата за проверка на валидност на сегмент във формализиран трябва да бъдат придружени от разбираемо по смисъл словесно описание на проверките. Попълва се „няма“, ако няма специфични указания за проверката на валидността на съдържанието)

Номенклатура на грешките *

0006-000069 (Невалидна структура на обекта съгласно XML дефиницията му, вписана в регистъра на информационните обекти)

0006-000015 (Полето <Field> от секцията <Section>

трябва да е попълнено.)

(Набор от грешки, определени в указанията за проверка валидността на сегмента съгласно тяхното вписване като термини в раздел "Термини". Попълва се „няма“, ако няма специфични указания за проверката на валидността на съдържанието)

Пояснение

Източник

Процедури в Националната служба по зърното

(Наименованието на стандарта, нормативния акт или друг документ, с който е въведено определението на обекта)



РЕПУБЛИКА БЪЛГАРИЯ

Министерство на транспорта,
информационните технологии и съобщенията

Образец СТ

Приложение за вписване на стойност

Пореден номер на
приложение в
заявлението *

Г-17

Уникален регистров
идентификатор

У-0008-000017

(Уникалният регистров идентификатор се попълва, ако стойността е вече
вписана и се заявява промяна в обстоятелствата)

Наименование на
информационен
обект*

Идентификатор на търговец на зърно

(Наименование на информационния обект от вид "стойност", с който обектът
се индивидуализира еднозначно. Наименованието е уникално. То трябва да
бъде същото, като вписаното в регистъра на регистрите и данните в раздел
"Унифицирани данни")

Предназначение на
информационен
обект*

Идентификатор на търговец на зърно

(Кратко текстово пояснение на информационния обект от вид "стойност". То
трябва да бъде същото, като вписаното в регистъра на регистрите и данните в
раздел "Унифицирани данни")

УРИ на данни *

У-0003-000073

(Уникален регистров идентификатор на вписаното в раздел "Унифицирани
данни" на регистъра на регистрите и данните, унифицирано определение на
данни, съответстващо на информационния обект от вид "стойност")

Указания за
обработка на
информационен
обект *

**Описва се в съответствие с приложената в полето
"XML дефиниция" XSD схема.**

(Описание в свободен текст или компютърно изпълними описания, които
унифицират създаването на процедури по редактиране, визуализация и други
видове обработка, свързани с информационния обект. Попълва се „няма“, ако
няма специфични указания за обработката на информационния обект)

XML дефиниция на
Стойността *

<?xml version="1.0" encoding="utf-8"?>

<xsd:schema
targetNamespace="http://ereg.egov.bg/value/Y-
0008-000017"

xmlns="http://ereg.egov.bg/value/Y-0008-000017"

xmlns:xsd="http://www.w3.org/2001/XMLSchema"

elementFormDefault="qualified">

```

<xsd:element name="GrainMerchantIdentifier"
type="xsd:long" maxOccurs="1" minOccurs="0">
<xsd:annotation>
<xsd:documentation xml:lang="bg">
Идентификатор на търговец на
зърно</xsd:documentation>
</xsd:annotation>
</xsd:element>
</xsd:schema>

```

(Описание на структурата на обекта съгласно технически стандарт посредством дефиниция в XML формат, съдържаща уникално за регистъра на информационните обекти наименование, както и описание на поддръжка на данни, различни от текстови, ако стойността съдържа такива)

Указания за проверка на валидност на стойността *

Валидацията се извършва в съответствие с приложената в полето "XML дефиниция" XSD схема. При несъответствие се извежда съобщение за грешка с УРИ на термин 0006-000069.

(Правила за проверка на валидността на съдържанието на стойността във формализиран вид съгласно стандарт, вписан в регистъра на стандартите, или по изключение в свободен текст. Правилата за проверка на валидност на стойността във формализиран вид трябва да бъдат придружени от разбираемо по смисъл словесно описание на проверките. Попълва се „няма“, ако няма специфични указания за проверката на валидността на съдържанието)

Номенклатура на грешките *

0006-000069 (Невалидна структура на обекта съгласно XML дефиницията му, вписана в регистъра на информационните обекти)

(Набор от грешки, определени в указанията за проверка валидността на стойността съгласно тяхното вписване като термини в раздел "Термини" Попълва се „няма“, ако няма специфични указания за проверката на валидността на съдържанието)

Пояснение

Източник

Процедури в Националната служба по зърното

(Наименованието на стандарта, нормативния акт или друг документ, с който е въведено определението на обекта)



РЕПУБЛИКА БЪЛГАРИЯ

Министерство на транспорта,
информационните технологии и съобщенията

Образец УД

Приложение за вписване на унифицирани данни

Пореден номер на
приложение в
заявлението ***Ж-72**Уникален регистров
идентификатор**У-0003-000072**

(Уникалният регистров идентификатор се попълва, ако унифицираните данни са вече вписани и се заявява промяна в обстоятелствата)

Наименование на
унифицираните данни ***Търговец на зърно**

(Наименование на унифицираните данни, което трябва да е уникално по отношение на наименованията на останалите вписани унифицирани данни, които са със статус "използваем")

Определение на
унифицираните данни ***Данни за търговец на зърно**

(Разширено текстово описание на унифицираните данни, позволяващо еднозначното им отграничение от останалите вписани унифицирани данни)

Вид или състав на
данните ***У0003-000073 Идентификатор на търговец на зърно****У0003-000074 Название на търговец на зърно****У0003-000075 Вид на търговец на зърно**

(Ако данните са единични се вписва "единични", а ако са съставни се вписва наборът от изграждащите данни)

Лица с право на достъп
до данните

(Списък с административните органи, лицата, осъществяващи публични функции и организациите, предоставящи обществени услуги, които въз основа на закон обработват тези данни. В списъка не се правят вписвания, когато данните са публични или до тях имат право на достъп неограничен кръг лица, съгласно закон)

Пояснение

Източник

Процедури в Националната служба по зърното

(Наименованието на стандарта, нормативния акт или друг документ, с който е въведено определението на обекта)



РЕПУБЛИКА БЪЛГАРИЯ

Министерство на транспорта,
информационните технологии и съобщенията

Образец УД

Приложение за вписване на унифицирани данни

Пореден номер на
приложение в
заявлението *

Ж-73

Уникален регистров
идентификатор

У-0003-000073

(Уникалният регистров идентификатор се попълва, ако унифицираните данни са вече вписани и се заявява промяна в обстоятелствата)

Наименование на
унифицираните данни *

Идентификатор на търговец на зърно

(Наименование на унифицираните данни, което трябва да е уникално по отношение на наименованията на останалите вписани унифицирани данни, които са със статус "използваем")

Определение на
унифицираните данни *

Идентификатор на търговец на зърно

(Разширено текстово описание на унифицираните данни, позволяващо еднозначното им отграничение от останалите вписани унифицирани данни)

Вид или състав на
данните *

Единични

(Ако данните са единични се вписва "единични", а ако са съставни се вписва наборът от изграждащите данни)

Лица с право на достъп
до данните

(Списък с административните органи, лицата, осъществяващи публични функции и организациите, предоставящи обществени услуги, които въз основа на закон обработват тези данни. В списъка не се правят вписвания, когато данните са публични или до тях имат право на достъп неограничен кръг лица, съгласно закон)

Пояснение

Източник

Процедури в Националната служба по зърното

(Наименованието на стандарта, нормативния акт или друг документ, с който е въведено определението на обекта)

ГЛАВА 7.2

КОНТРОЛ НА ОПЕРАТИВНАТА СЪВМЕСТИМОСТ

Нормативни основания

Контролът на оперативната съвместимост се осъществява според специална методика, разработена в съответствие с чл. 60 от Закона за електронното управление, според който Министерът на транспорта, информационните технологии и съобщенията „осъществява проверки на оперативната съвместимост на определена информационна система или на предприятиите от административния орган мерки чрез определени от него лица и да дава предписания за подобряването им”.

Методиката предполага не само еднократен акт на проверка на системите, систематизиране на резултатите и разработка на предложения, но и създаване на информационен ресурс за систематичен последващ контрол на проверената вече информационна системи. Т.е. резултатът от проверката трябва да бъде отразен в информационната система на Министерството на транспорта, информационните технологии и съобщенията. Това трябва да бъде информационен ресурс относно състоянието на информационните системи в администрацията от гледна точка на оперативната съвместимост, добре систематизиран и удобен за поддържане, актуализиране и ползване.

Дейности по контрола

Във връзка с контрола Министерството на транспорта, информационните технологии и съобщенията извършва набор от дейности, които може да се обобщят по тематика както следва:

- а) създаване на методически пособия за извършване на контрол на информационните системи;
- б) осигуряване на необходимия експертен потенциал, имащ капацитета да извършва контрола на информационните системи;
- в) осигуряване на необходимия административен потенциал за планиране, ръководство и провеждане на контрола;
- г) определяне на периодичността на контрола и начините за избор на информационните системи, които ще бъдат обект на контрола;
- д) действия по самия контрол.

Процедури по контрола

Методиката дефинира следните видове процедури по контрол на оперативната съвместимост:

1. По обект на контрола:
 - а) информационни системи;
 - б) електронни административни услуги;
 - в) вътрешни електронни административни услуги.
2. По инициализация на процедурата за контрол:

- а) в състава на планов мониторинг на административно звено;
- б) по сигнал на заинтересовано лице;
- в) в състава на непрекъснатия текущ мониторинг на сайтовете на администрацията, който осъществява контролното звено на МТИТС.

ГЛАВА 7.3

СЕРТИФИКАЦИЯ

Сертификации за оперативна съвместимост и мрежова и информационна сигурност

По същество, Наредбата за оперативна съвместимост и информационна сигурност предвижда две сертификации:

1. Оценка на съответствието на информационни системи и продукти, формулирана в Наредбата и осъществявана от Министъра на ТИТС. Това е задължително за новите системи и продукти, а за съществуващите ще се направи график в съответствие с резултатите от прегледа по § 5 от ПЗР на Закона.

Тази сертификация обхваща точно определени административните информационни системи;

2. Сертификация на вътрешните правила на административния орган като „Система за управление на информационната сигурност” по смисъла на ISO 27001:2005 от оправомощена за това организация. Наредбата предвижда това да стане в срок от 18 месеца.

Тази сертификация обхваща всички информационни системи на административния орган.

Обекти на оценката на съответствието

На оценка за съответствие с изискванията за оперативна съвместимост и информационна сигурност подлежат:

А. Задания за:

- разработване или придобиване на административна информационна система;
- изграждане на директна свързаност между информационни системи;
- разработване или придобиване на специализирани информационни системи.

Б. Информационни системи, които:

- имат функционалност съгласно изискванията на чл. 20 от Наредбата;
- са нова версия на информационни системи, които са вече сертифицирани.
- Оценката се извършва по искане на заинтересовано лице – доставящо или разработващо информационната система.

В. Програмни приложения, които:

- изпълняват функции по визуализация и/или редактиране на електронни документи;
- в състава на други приложения или системи изпълняват функции по проверка на електронни документи за съответствие с регистрацията им в регистъра на информационните обекти.

Оценката не включва извършване на проверки за наличие на авторски, сродни или други права на интелектуална или индустриална собственост върху проверяваните информационни системи и продукти.

Протокол за сертификация на задание

Протокол от извършени проверки по сертификация на Задание

Настоящият протокол съдържа данните от извършените проверки по сертификация на задание, както следва:

Задание:		
Въвеждат се всички данни, идентифициращи пълно и еднозначно предоставеното задание. Например данни за обхващана ОП, по която се изготвя заданието, проект в състава на който се извършват дейностите по заданието и т.н.		
Заинтересовано лице:		
Въвеждат се всички данни, идентифициращи пълно и еднозначно Заинтересованото лице, предоставило заданието.		
Проверки за АИС:		
Въвеждат се всички данни, идентифициращи пълно и еднозначно АИС, специфицирана в състава на едно задание. Ако в заданието се специфицират изисквания само към една АИС, настоящите данни не се попълват.		
Проверка: 1. Наличие на изискване за сертификация на придобивана или изграждана ИС, която по същество е Административна информационна система (АИС)		
Предпоставки, за оценка на дадена ИС, като АИС:		
а.	Реализация/наличие на функции на ИС, свързани с поддържане на данни и процедури по тяхната обработка, специфицирани в чл. 4 и следващите от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите	Налице /Липсва
б.	Реализация/наличие на функции по свързване на ИС с Единната среда за обмен на електронни документи	Налице /Липсва
в.	Реализация/наличие на функции по приемане на данни в електронна форма през Уеб или електронна поща, като приетите данни стартират административни процедури, изпълнявани ръчно, или машинно, но с поемане на отговорност от страна на администрацията за тяхното изпълнение в съответствие с нормативната уредба или специфични вътрешни правила	Налице /Липсва
г.	Реализация/наличие на функции по изпълнение на електронни услуги със средствата на ИС	Налице /Липсва
д.	Реализация/наличие на функции по управление и контрол на административната дейност	Налице /Липсва
В Заданието са посочени:		
1)	Изисквания за наличие на актуална сертификация на предлагана за придобиване АИС	ДА НЕ
2)	Указания за извършване на дейности за успешна сертификация на разработвана АИС, които са неразделна част от дейностите по заданието и ще бъдат извършени без допълнително доверяване, или разширение на сертифицираното Задание	ДА НЕ
Проверката се счита за успешна, когато:		
✓ Липсват предпоставки за оценка на дадена ИС, като АИС		
✓ Налице са предпоставки за оценка на дадена ИС, като АИС, но в Заданието изрично е посочено изискване за налична сертификация, или за извършване на такава		
Проверка: 2. Наличие на изискване за непълна сертификация на придобивана или изграждана специализирана ИС, която има елементи на Административна информационна система (АИС)		
Предпоставки, за оценка на компоненти на специализирана ИС, като компоненти на АИС:		
а.	Реализация/наличие на функции на специализираната ИС, свързани с поддържане на данни и процедури по тяхната обработка, специфицирани в чл. 4 и следващите от Наредбата за вътрешния оборот на електронни документи и документи на хартиен носител в администрациите	Налице /Липсва

Успешна
Неуспешна

Успешна
Неуспешна

Сертифицирани задания, вписани в Списъка на сертифицираните системи

Списък на акредитираните лица и списък на сертифицираните системи и продукти

Начална страница | Нормативна база | Списък на акредитираните лица | Списък на сертифицираните информационни системи

Търсене

Списък на сертифицирани задания

„Надграждане/реинженеринг на програмни продукти за оптимизиране на електронните процеси, свързани с административното обслужване в общините, Бобов дол, Сапарева баня, Бобошево и достъп до административните услуги на граждани и бизнес в кметствата на общини“

Данни, идентифициращи заинтересованото лице: Община Бобов дол
Данни за акредитираното лице, извършило сертификацията: ПМБА ЕООД, вписано в списъка на лицата, акредитирани за сертифициране на информационни системи под № 2.
Номер и дата на издадения сертификат: BG 02001/24 9.2009 г.

„Проучване, анализ и реинженеринг на процесите в Община Габрово, проектиране и разработка на електронни административни услуги, електронен регистър и ГИС, внедряване на системата интегриране на услугите. Доставка на базов ГИС сървър и настолен софтуер.“

Данни, идентифициращи заинтересованото лице: Община Габрово
Данни за акредитираното лице, извършило сертификацията: ПМБА ЕООД, вписано в списъка на лицата, акредитирани за сертифициране на информационни системи под № 2
Номер и дата на издадения сертификат: BG 02002/24 9.2009 г.

„Улесен достъп до по-бързи и по-качествени административни услуги чрез подобрена електронна система в общините Брусарци и Якимово“

Данни, идентифициращи заинтересованото лице: община Брусарци
Данни за акредитираното лице, извършило сертификацията: Демско ООД, вписано в списъка на лицата, акредитирани за сертифициране на информационни системи под №5
Номер и дата на издадения сертификат: BG 05001/29 9.2009 г.

„Развитие и усъвършенстване на информационна система „Лицензиране и регистри“ на Комисия за регулиране на съобщенията, във връзка с разработката на приложно програмно осигуряване.“

Данни, идентифициращи заинтересованото лице: Комисия за регулиране на съобщенията
Данни за акредитираното лице, извършило сертификацията: Джи Си Ес България ООД, вписано в списъка на лицата, акредитирани за сертифициране на информационни системи под № 3.
Номер и дата на издадения сертификат: BG 03001/30 9.2009 г.

„Оптимизиране на процесите и интегриране на административните услуги в община Полски Тръмбеш“

Данни, идентифициращи заинтересованото лице: Община Полски Тръмбеш
Данни за акредитираното лице, извършило сертификацията: Абеаус ЕООД, вписано в списъка на лицата, акредитирани за сертифициране на информационни системи под № 6.
Номер и дата на издадения сертификат: 6001/05.11.2009 г. 00:00:00

„Изграждане на електронна област съгласно изискванията на Закона за електронно управление“

Списък на акредитираните лица

Списък на сертифицираните информационни системи

Списък на сертифицираните системи

Списък на сертифицираните приложения

Списък на сертифицираните задания

Списък на тестовите набори от документи

Нормативна база

Други сайтове

Оперативна съвместимост на приложения, свързани с електронното правителство

Национален регистър на стандартите

Фигура 7-1

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions “Towards interoperability for European public services”, COM(2010) 744 final, 16.12.2010, Brussels, Belgium Annex 1 “European Interoperability Strategy for European public services”
2. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions “Towards interoperability for European public services”, COM(2010) 744 final, 16.12.2010, Brussels, Belgium Annex 2 “European Interoperability Framework for European Public Services”
3. Directive 2003/98/EC on the re-use of public sector information, 17.11.2003
4. “The Role of e-Government for Europe's Future”, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, COM(2003) 567
5. ISO/IEC 2382-01, Information Technology, Vocabulary, Fundamental Terms
6. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY, 1990
7. Report on "Key Principles of an Interoperability Architecture", 24.06.2004, Irish Presidency of the European Public Administration Network e-Government Working Group
8. Decision 2004/387/EC on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), 21.04.2004
9. The European e-Government Action Plan 2011-2015 "Harnessing ICT to promote smart, sustainable & innovative Government", COM(2010) 743, 15.12.2010, Brussels, Belgium
10. MODINIS Programme: follow-up of e-Europe 2005 action plan”, available at http://ec.europa.eu/information_society/eeurope/i2010/archive/modinis/index_en.htm “D2.7 Study on Interoperability at Local and Regional Level. Final Version”, 20.04.2007
11. “European Interoperability Framework for Pan-European eGovernment Services”, IDA working document, Version 4.2, 01.2004
12. “Proposal for a Decision of the European Parliament and of the Council on interoperability solutions for European public administrations (ISA)”, COM(2008) 583, 29.09.2008, Brussels, Belgium
13. “Final evaluation of the implementation of the IDABC programme”, Communication from the Commission to the European Parliament and the Council, COM(2009) 247, 29.05.2009, Brussels, Belgium
14. „ISA: Community Programme on interoperability solutions for European public administrations”, available at <http://ec.europa.eu/idabc/servlets/Doc6ffa.pdf?id=31770>

15. "ISA Work Programme - First revision", 2011
16. "eTEN: Trans-European e-Services", available at http://ec.europa.eu/information_society/activities/egovernment/implementation/eten/index_en.htm
17. "ICT Policy Support Programme", available at http://ec.europa.eu/information_society/activities/egovernment/implementation/ict_psp/index_en.htm
18. e-CODEX project, available at www.e-codex.eu
19. epSOS project, available at www.epsos.eu
20. PEPPOL project, available at www.peppol.eu
21. SPOCS project, available at www.eu-spocs.eu
22. STORK project, available at <https://www.eid-stork.eu/>
23. Ralf Klischewski Contextual Strategies towards Interoperability in e-Government Journal of Theoretical and Applied Electronic Commerce Research, ISSN 0718–1876 Electronic Version, VOL 6 / ISSUE 1 / APRIL 2011 / 26-42 © 2011 Universidad de Talca - Chile
24. W.E. Moen, Interim Report for the Z-Interop Project The Z39.50 Interoperability Testbed, School of Library and Information Sciences Texas Center for Digital Knowledge University of North Texas Denton, TX 76203
25. "European Interoperability Framework (EIF) – Towards Interoperability for European Public Services", Brochure accompanying the European Interoperability Framework communication, 2011
26. "European Interoperability Architecture: Phase 2 – Final Report: Common Vision for an EIA", v.2.0, 11.2011
27. "Architecture Guidelines for Trans-European Telematics Networks for Administrations", Version 7.1, IDA programme, 09.2004
28. Report "European Interoperable Infrastructure Services: Study on potential reuse of system components", v.1.1, 2009
29. Bollinger T., A Guide to Understanding Emerging Interoperability Technologies, MITRE, Washington 2000
30. Kantor, M.; Burrows J. H., "Electronic Data Interchange (EDI)". National Institute of Standards and Technology. Retrieved 2012-08-13
31. EICTA white paper on Interoperability, <http://www.eicta.org/files/WhitePaper-103753A.pdf>. Recommendations to governments and industry on ensuring interoperability by EICTA, the voice of the ICT and consumer electronics industry in Europe, 2004.

32. Teixeira de Sousa P., Stuckmann P., telecommunication network interoperability, TELECOMMUNICATION SYSTEMS AND TECHNOLOGIES - Vol. II
33. Dzida, W. International User-Interface Standardization. In J. Allen B. Tucker (Ed.), The Computer Science Engineering Handbook (pp. 1474 - 1493), Boca Raton, Florida: CRC Press, 1996
34. ATHENA Contribution to Interoperability Policy Action Plan Version 2 February, 2006
35. INTEROP Interoperability Research for Networked Enterprises Applications and Software Network of Excellence - Contract no.: IST-508 011 www.interop-noe.org
36. Blagoev L., Manolov S. Model Requirements for the Interoperable Content Management in e-Government, Proceedings of the International Conference on Information Technologies (InfoTech-2010)
37. Choy D., Brown A., Gur-Esh E., McVeigh R., Müller F., Content Management Interoperability Services (CMIS) Version 1.0, OASIS 2009
38. Manolov S., Trifonov R., Electronic Data Interchange Between ЧАCTies Involved In Incident Handling Process, Proceedings of the International Conference on Information Technologies (InfoTech-2012)
39. T. Vitvar, V. Peristeras, K. Tarabanis Semantic Technologies for E-Government Springer-Verlag Berlin Heidelberg 2010
40. S. Manolov Fully controled environment for interoperability between administrative information systems Proceedings of the International Conference on Information Technologies (InfoTech-2008)
41. Breaking Barriers to e-Government, Overcoming obstacles to improving European public services MODINIS study, Contract no. 29172, A Legal and Institutional Analysis of Barriers to e-Government Draft Deliverable 1b, 16/08/2006
42. "EUROPE 2020 - A strategy for smart, sustainable and inclusive growth", Communication form the Commission, COM(2010) 2020, 03.03.2010, Brussels, Belgium
43. "A Digital Agenda for Europe", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, COM(2010) 245, 26.08.2010, Brussels, Belgium
44. "European Interoperability Architecture: Phase 2 – Final Report: Common Vision for an EIA", v.2.0, 11.2011
45. "Supporting the European Interoperability Strategy Elaboration", Final Report Phase 1, 02.07.2009, Deloitte
46. "Achieving Technical Interoperability – the ETSI Approach", European Telecommunications Standards Institute, White Paper No. 3., October 2006

47. Sylvia Archmann, Just Castillo Iglesias, Interoperability and community building for transformational e-Government, www.epracticejournal.eu
48. Jylhänkangas R. “European Interoperability Strategy, Framework and the Levels of Interoperability”, Presentation at the Digital Agenda for Europe Going Local, 2011
49. European countries aligning their interoperability policies, <http://joinup.ec.europa.eu/news/european-countries-aligning-their-interoperability-policies>, March 13, 2012
50. Law on e-Governance In force as of 13 June 2008 Promulgated in SG no 46 of 12 June 2007
51. Ordinance on the electronic administrative services In force as of 13 June 2008 Adopted by Council of Ministers decree no. 107 of 19 May 2008 Published in State Gazette no. 48 of 23 May 2008
52. Ordinance on the requirements to the uniform environment for exchange of electronic documents Adopted by Decree of the Council of Ministers no 158 of 2 July 2008 Promulgated in SG no 62 of 11 July 2008
53. Ordinance on the general requirements for interoperability and information security In force as of 25 November 2008 Adopted by CoM Decree nr.279 of 17 November 2008 Promulgated in State Gazette, no. 101 of 25 November 2008
54. Ordinance on the registers of the information objects and the electronic services Effective as of 13 June 2008 Adopted by Decree of the Council of Ministers no.98 of 16 May 2008 Promulgated in SG, no 48 of 23 May 2008
55. Ordinance on the electronic signature certificates in the administrations Effective as of 13 June 2008 Adopted by Decree of the Council of Ministers no 97 of 16 May 2008 Promulgated in SG, no. 48 of 23 May 2008
56. Ordinance on the internal circulation of electronic documents and documents in hard-copy form in the administrations In force as of 13 June 2008 Adopted by CoM Decree no. 101 of 17 May 2008 Promulgated in State Gazette no. 48 of 23 May 2008
57. S. Manolov The right way to the real achievement of interoperability between the governmental information systems International workshop: “e-Government and data protection” (Varna, September 2006)
58. S. Manolov The interoperability requirements for pan-European electronic services Proceedings of the international conference on information technologies (InfoTech-2007), vol. 1
59. L. Blagoev, K. Spasov NMDPA – a ЧАСТ of the semantic network of the administration Proceedings of the international conference on information technologies (InfoTech-2013)