



РЕПУБЛИКА БЪЛГАРИЯ
ДЪРЖАВНА АГЕНЦИЯ „ЕЛЕКТРОННО УПРАВЛЕНИЕ“

СИСТЕМА ЗА ЕЛЕКТРОНЕН ОБМЕН НА СЪОБЩЕНИЯ (СЕОС)

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

ВЕРСИЯ 1.1, МАРТ-МАЙ 2017

СЪДЪРЖАНИЕ:

I. ВЪВЕДЕНИЕ	2
II. ОБЩИ ПОЛОЖЕНИЯ	2
III. РЕГИСТЪР НА УЧАСТНИЦИТЕ (РУ).....	3
IV. ОБМЕН НА СЪОБЩЕНИЯ МЕЖДУ УЧАСТНИЦИТЕ.....	7
V. СИГУРНОСТ НА ОБМЕНА НА СЪОБЩЕНИЯ	20
VI. ПРИЛОЖЕНИЯ	21

I. ВЪВЕДЕНИЕ

Настоящият документ представлява техническа спецификация на протокола използван в Системата за обмен на електронни съобщения (СЕОС).

Целта на документа е да опише реализираното и внедрено в държавната администрация решение за електронен обмен на съобщения. Той е от критична важност за ефективността на държавната администрация като цяло и гръбнак на електронното управление. Затова всяко едно решение в тази насока трябва да се характеризира с висока степен на ефективност, надеждност, сигурност, гъвкавост и скалируемост. Това са и целите, които си поставят настоящият протокол и всяка негова следваща версия.

Участие в обмена могат да взимат органите на централната и местната администрация, държавни предприятия и други субекти *различими по ЕИК/БУЛСТАТ*. Регистрацията на участник се осъществява чрез подаване от негова страна на Заявление за вписване или промяна на обстоятелства в регистъра на участниците в електронен обмен на документи, в което се декларира спазването на Общите условия.

Настоящата версия на протокола дава възможност за изпращане на документи и справка за тяхното състояние.

II. ОБЩИ ПОЛОЖЕНИЯ

Използвани термини

- **Участник** – всеки субект включен¹ в обмена на електронни съобщения по настоящия протокол;
- **Регистър на участниците** – централно хранилище на участниците в обмена на електронни съобщения;
- **Крайна точка** – софтуерен компонент участващ в обмена на съобщения, който може изпраща и получава съобщения;
- **Цифров сертификат** – електронен документ издаден от доставчик на удостоверителни услуги, който удостоверява принадлежността на X.509 публичен ключ (вж.RFC 2459) на субект в обмена на съобщения;
- **Списък с отменени сертификати** – списък от отменени сертификати (*certificate revocation list*) поддържан от издателя на съответния сертификат (вж.RFC 5280);
- **GUID** (или още **UUID**) – глобален уникален идентификатор (вж.RFC 4122);
- **УРИ** – уникален регистров индекс.

Транспортна среда

Описаният в настоящото описание електронен обмен се осъществява в обща мрежова среда. Комуникацията се осъществява по TCP/IP протокол.

Обменът на съобщения е peer-to-peer и това налага *директна двупосочна свързаност между крайните точки на участниците*.

Достъпът до Регистъра на участниците (РУ) е директен и това налага *директна едностранна свързаност между крайните точки на участниците от една страна и крайните точки на Регистъра на участниците от друга*.

¹ Процедурата по включване на участник в обмена не е обект на настоящия документ.

Проверката за валидност на сертификатите налага също така *директна еднопосочна свързаност между крайните точки на участниците от една страна и списъците с отменени сертификати от друга.*

Допустимо е мрежовата среда да бъде и Интернет при достатъчно висока защитеност на използваните транспортни сертификати.

Препоръчително е адресирането на участниците по *hostname*, вместо по IP адрес, което:

- спестява нуждата от обновяване на информацията в Регистъра, при смяна на IP адрес;
- позволява скалируемост чрез разпределяне на заявките към няколко IP адреса.

Крайните точки на участниците **могат** да се публикуват на избран от тях порт.²

Регистърът предоставя потребителски интерфейс, с който всеки участник да може да актуализира на информацията за себе си, и това налага *директна еднопосочна свързаност между участниците от една страна и крайните точки на Регистъра на участниците от друга.*

Когато два участника имат крайни точки в рамките на повече от една преносна среда, при възможност участниците **трябва** да използват тази с по-високо ниво на защита (напр. използване на частна мрежа Единната електронна съобщителна мрежа (ЕЕСМ) вместо Интернет).

Транспортни сертификати

Транспортните сертификати са цифрови сертификати използвани ексклузивно за достъп до Регистъра на участниците (РУ) и за обмена на съобщения по настоящия протокол. Транспортните сертификати се издават в съответствие с Процедура за генериране и издаване на транспортен сертификат.

Проверката на транспортните сертификати от страните участващи в обмена включва:

- **Задължителна** е проверка на датата на изтичане на сертификата;
- **Задължителна** е проверка на сертификата за наличие в списъците с отменени сертификати на издателя;
- **Препоръчително** е сверяване на полето "*Common Name*" на сървърния сертификат с наименованието на сървъра обслужващ крайната точка на участника.

III. РЕГИСТЪР НА УЧАСТНИЦИТЕ (РУ)

Регистърът на участниците цели да поддържа актуални данни за участниците в обмена на съобщения, т.ч. основна информация за участниците (ЕИК, наименование,

² **Препоръчително** е използваният порт за комуникация да бъде 443 или в диапазона от 1024 до 49151 и да не съвпада с някой от регистрираните в списъка на IANA, с цел избягване на конфликти с други стандартни услуги, които може да работят на същите портове на сървъра.

информация за технически контакт) и техните крайните точки (протоколите, адреси и състояние).

Регистърът предоставя на участниците програмен интерфейс за извличане на информация за останалите участници вписани в него.

Регистърът предоставя на всеки участник потребителски интерфейс за актуализиране на информацията съхранявана за него.

Структура на Регистъра на участниците (РУ)

За всеки участник регистъра предоставя следната информация:

1. Уникален идентификатор (GUID) на участника;
2. Уникален идентификатор (GUID) на родителски участник, ако има такъв (ако настоящият участник е клон на друг участник)³;
3. Идентификатор на участника (ЕИК/БУЛСТАТ);
4. Наименование на участника;
5. Данни за технически контакт:
 - Телефонен номер;
 - Факс номер;
 - Адрес на електронна поща.
6. Статус ("активен" или "неактивен");
7. Дата/час на последна промяна;
8. Сериен номер на транспортния сертификат;
9. Списък с предоставяни услуги, всяка от които съдържа следната информация:⁴
 - Уникален идентификатор (GUID) на вида на услугата;
 - Наименование на услугата;
 - Тип на услугата (вж. Услуги);
 - Версия на услугата (вж. Услуги);
 - Идентификатор за достъп до услугата;
 - Статус ("активен", "временно неактивен" или "неактивен").

Услуги

Услугите (крайните точки за достъп) се различават по вид и тип.

Видове услуги

Всеки вид услуга има своето наименование и уникален идентификатор (GUID).
Към момента са определени следните видове услуги:

³ Поддръжката на клонова структура на участниците на този етап е нефункционираща.

⁴ В бъдещи версии ще бъде добавен уникален идентификатор на крайната точка за целите на синхронизацията.

Наименование	Идентификатор
Документооборот	7060efa8-f1fa-4938-8b2b-12a78c86988f
...	...

Типове услуги и идентификатори на услуги

Типът услуга определя протокола за достъп до нея, а идентификаторът (URI) за достъп – адресът на крайната точка.

Към момента са дефинирани следните типове услуги и видове идентификатори:

Наименование	Код	Идентификатор	Примерен идентификатор
Електронен обмен на съобщения	service	Адрес на уеб услугата	https://agency.obmen.bg:8443/EGovExchange
Електронна поща	email	Електронен адрес	mailto:agency@egov.bg

Актуализиране на Регистъра на участниците (РУ)

Потребителският достъп до информацията в Регистъра се осъществява с използването на стандартен уеб браузер по защитен с помощта на транспортни сертификати HTTPS (HTTP-върху-TLS) (с използване на TLS 1.2 или по-висока) канал. Потребителят **трябва** да обърне внимание на проверката на сертификата на Регистъра, която браузерът извършва, а Регистърът **трябва** да осъществи проверка на сертификата на отсрещната страна (вж. Транспортни сертификати) и да го използва за автентикация и авторизация на извикването.

Транспортен слой за извличане на данни от Регистъра

Програмният достъп до информацията в Регистъра се осъществява с използването на SOAP 1.1 уеб услуги по защитен с помощта на транспортни сертификати HTTPS (HTTP-върху-TLS) (с използване на TLS 1.2 или по-висока) канал.

При осъществяване на достъп до уеб услугите на Регистъра, всяка от двете страни **трябва** да осъществи проверка на сертификата на отсрещната страна (вж. Транспортни сертификати) и да го използва за автентикация и авторизация на извикването.

Описание на протокола за извличане на данни от Регистъра на участниците

Протоколът за комуникация с Регистъра на участниците е описан в:

- **Приложение 1. Описание на услугата на Регистъра** – WSDL описание на операциите предлагани от уеб услугата на Регистъра;
- **Приложение 2. Описание на съобщенията на Регистъра** – XSD схема описваща данните предоставяни от уеб услугата на Регистъра.

Всеки участник в обмена се представя с XML обект със следната структура:

1. EntityIdentifier (xsd:string) – ЕИК/БУЛСТАТ на участника;
2. Guid (guid) – GUID;
3. ParentGuid (guid) – GUID на участника от горно ниво (в случай на клон);
4. AdministrativeBodyName (xsd:string) – наименование;
5. Contact – технически контакт. Обект със следните свойства:
 - Phone (xsd:string) – телефонен номер;
 - Fax (xsd:string) – факс номер;
 - EmailAddress (xsd:string) – имейл адрес.
6. CertificateSN – Сериен номер на транспортния сертификат на участника (в HEX формат) издаден от доставчика на удостоверителни услуги;
7. Services/Service – Списък от услуги, предоставяни от участника. Списък от обекти със следните свойства:
 - Guid (guid) – GUID;
 - Name (xsd:string) – наименование;
 - URI (xsd:anyURI) – идентификатор за достъп;
 - Status (xsd:string) – статус. Изброим списък със следните възможни стойности:
 - Active – активен;
 - TemporarilyInactive – временно неактивен;
 - PermanentlyInactive – неактивен.
 - Type (xsd:string) – тип (напр. "service", "email" и др.);
 - Version (xsd:integer) – версия (понастоящем 1).
8. LastChange (xsd:dateTime) – дата на последна промяна;
9. Status (xsd:string) – статус. Изброим списък със следните възможни стойности:
 - Active – активен;
 - Inactive – неактивен.

Извличане на данни от Регистъра

За осъществяване на обмен на съобщения, всеки участник използва информацията за останалите участници от Регистъра. Тези данни **могат** да се използват в **онлайн** и **офлайн** режим.

В **онлайн режим** обръщението към Регистъра става при изпращане и/или получаване на съобщение.

В **офлайн режим** приложението поддържа локално копие на съдържанието на Регистъра, като данните се синхронизират периодично. За целта се използват LastChange свойствата на отделните участници и на целия регистър.⁵

⁵ В бъдещи версии ще бъде добавен уникален идентификатор на крайната точка за целите на синхронизацията.

IV. ОБМЕН НА СЪОБЩЕНИЯ МЕЖДУ УЧАСТНИЦИТЕ

Обменът на информация между участниците се осъществява под формата на съобщения, като за целта подателят използва крайната точка на получателя описана в Регистъра на участниците. След осъществяване на връзка с крайната точка на получателя, подателят следва да изпрати подготвеното съобщение във формата описан в настоящия документ.

В резултат подателят може синхронно (в рамките на същата връзка) да получи един от следните резултати:

- **възниква изключение/грешка (*fault*)** – когато е възникнала системна грешка;
- **празен резултат** (резултатът е празен) – когато съобщението е прието и очаква обработка на приложно ниво;
- **съобщение-отговор** (резултатът съдържа съобщение) – когато обработката на съобщението на приложно ниво вече е започнала.⁶

Съобщението-отговор е отново съобщение в същия формат описан в настоящия документ.

Транспортен слой за обмен на съобщения

Обменът на съобщения между участниците се осъществява с използването на SOAP 1.1 веб услуги по защитен с помощта на транспортни сертификати HTTPS (HTTP-върху-TLS) (с използване на TLS 1.2 или по-висока) канал.

Подателят **трябва** да използва своя транспортен сертификат като клиентски сертификат, а получателят **трябва** да използва своя транспортен сертификат като сървърен.

Всяка от двете страни **трябва** да провери сертификата използван от отсрещната страна (вж.Транспортни сертификати).

Описание на протокола за обмен на съобщения

Протоколът за обмен на съобщения между участниците е описан в:

- **Приложение 3. Описание на услугата на участниците** – WSDL описание на операциите предлагани от веб услугата на на всеки участник;
- **Приложение 4. Описание на съобщенията между участниците** – XSD схема описваща данните обменяни от веб услугата на всеки участник и клиентските приложения.

Всяко съобщение обменяно по протокола се представя с XML документ със следната структура:

1. Header – заглавна част. Съдържа следните данни:

- Version (xsd:string) – версия на протокола (понастоящем "1");

⁶ В бъдещи версии отговорът ще бъде премахнат като възможност (като ще остане единствено възможността за изключение/грешка (*fault*) от самата веб услуга) или заменен със съобщение от тип "Потвърждаване на получаването".

- MessageType (MessageType) – тип на съобщението;
 - MessageDate (xsd:dateTime) – дата/час на създаване;
 - Sender (EntityType) – подател. Обект със следните свойства:
 - Identifier (xsd:string) – ЕИК/БУЛСТАТ;
 - AdministrativeBodyName (xsd:string) – наименование;
 - GUID (GUIDType) – GUID.
 - Recipient (EntityType) – получател. Обект със следните свойства:
 - Identifier (xsd:string) – ЕИК/БУЛСТАТ;
 - AdministrativeBodyName (xsd:string) – наименование;
 - GUID (GUIDType) – GUID.
 - MessageGUID (GUIDType) – GUID на съобщението;
2. Body – съдържание на съобщението. Може да съдържа един от следните елементи:
- DocumentRegistrationRequest (DocumentRegistrationRequestType) – заявление за регистриране на документ;
 - DocumentStatusRequest (DocumentStatusRequestType) – заявление за проверка на състоянието на документ;
 - DocumentStatusResponse (DocumentStatusResponseType) – известие за състояние на документ;
 - Error (ErrorMessageType) – известие за грешка.
3. Signature (ds:Signature) – електронен подпис на съобщението по стандарта XML Signature Syntax and Processing (2nd Edition). Подписването **трябва** да е извършено с транспортния сертификат на участника, а елементът **трябва** да съдържа информация за използвания при подписването сертификат.⁷

Обмен на съобщения

Обработка на грешки

Резултатът от обмена (изпращането и получаването) на съобщение може да бъде:

1. **Успешен** – когато целият процес на обмен е преминал без проблеми;
2. **Неуспешен** – когато на някой от етапите на обмен се е получила грешка или изключение. Неуспешният обмен може да се дължи на:
 - **Изключение/грешка (*fault*)** – грешката се дължи на изключителна ситуация възникнала при обработка (напр. проблем с връзката с БД). Възможен е повторен опит за изпращане на същото съобщение. **Препоръчително** е подателят да направи повторен опит след период от време (съгласно стратегията за повторен опит);
 - **Грешка при подателя** – грешката се дължи на несъответствие при подателя. Опитите за изпращане на същото съобщение следва да бъдат прекратени;

⁷ **Препоръчително** е при подписването да бъде използван [разширението XAdES](#), който дефинира старндартен начин за включване на удостоверение за време в подписаните XML документи.

- **Грешка при получателя** – грешката се дължи на несъответствие при получателя. Опитите за изпращане на същото съобщение следва да бъдат прекратени.

Стратегия за повторен опит

Исключение/грешка (*fault*) може да възникне по ред причини, сред които:

- липса на мрежова свързаност;
- уеб услугата на отсрещната страна не функционира;
- конфигурационен проблем;
- др.

В зависимост от причината и времето за реакция, времето необходимо за отстраняване на проблема може да варира.

По тази причина подателят на съобщението **трябва** да използва следната стратегия за повторен опит за осъществяване на обмена:

- Времето до първия повторен опит **трябва** да бъде 15 минути;
- Времето до всеки следващ опит **трябва** да бъде удвоявано;
- Общият брой на повторните опити **не трябва** да надхвърля 10 (или общо 11 опита).

Тази стратегия определя интервалите, през които се осъществява повторен опит:

Опит	Интервал	Време след първия опит
1.	–	–
2.	15 мин.	15 мин.
3.	30 мин.	45 мин.
4.	1 ч.	1 ч. и 45 мин.
5.	2 ч.	3 ч. и 45 мин.
6.	4 ч.	7 ч. и 45 мин.
7.	8 ч.	15 ч. и 45 мин.
8.	16 ч.	1 ден, 7 ч. и 45 мин.
9.	32 ч.	2 дни, 15 ч. и 45 мин.
10.	64 ч.	5 дни, 7 ч. и 45 мин.
11.	128 ч.	10 дни, 15 ч. и 45 мин.

Изпращане на съобщение

При изпращане на съобщение до избран получател, подателят **трябва** да следва следната процедура:

1. Проверява изходящото съобщение:

- (И.1)⁸ Проверява дали изходящото съобщение е валиден XML документ. Ако не, обменът се счита за **"Неуспешен – Грешка при подателя"**;
 - (И.2) Проверява дали изходящото съобщение съответства на XSD схемите за обмен на съобщения (вж.Приложение 4). Ако не, обменът се счита за **"Неуспешен – Грешка при подателя"**;
 - (И.3) Проверява дали подателят на съобщението съществува в списъка с участниците от Регистъра. Ако не, обменът се счита за **Неуспешен – Грешка при подателя"**;
 - (И.4) Проверява дали получателят на съобщението съществува в списъка с участниците от Регистъра. Ако не, обменът се счита за **"Неуспешен – Грешка при подателя"**;
 - (И.5) Проверява дали съобщението е електронно подписано. Ако не, обменът се счита за **"Неуспешен – Грешка при подателя"**;
 - (И.6) Проверява дали съобщението е електронно подписано с транспортния сертификат асоцииран с подателя в Регистъра. Ако не е, обменът се счита за **"Неуспешен – Грешка при подателя"**;
2. Установява връзка до избраната крайната точка на участника;
 3. (И.7) Проверява дали сървърният сертификат съвпада с транспортния сертификат асоцииран с получателя в Регистъра. Ако не – изпращането се прекратява, а обменът се счита за **"Неуспешен – Изключение"**;
 4. (И.8) Изпраща съобщението. В случай на изключение/грешка (*fault*), обменът се счита за **"Неуспешен – Изключение"**;
 5. Ако извикването е върнало отговор (резултат различен от null):⁹
 - (И.9) Проверява дали резултатът е валиден XML документ. Ако не, обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - (И.10) Проверява дали резултатът е валиден спрямо XSD схемите за съобщение (вж.Приложение 4). Ако не, обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - (И.11) Проверява дали подателят на отговора съвпада с получателя на входящото съобщение¹⁰. Ако не, обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - (И.12) Проверява дали получателят на отговора съвпада с подателя на входящото съобщение¹¹. Ако не, обменът се счита за **"Неуспешен – Грешка при получателя"**;

8 Кодът изписан в скоби преди всеки един сценарий в комбинация с версията на протокола се използва, за да бъде идентифициран в технически задания, при провеждане на тестове и изготвяне на протоколи от проверка за съвместимост.

9 В бъдещи версии отговорът ще бъде премахнат като възможност (като ще остане единствено възможността за изключение/грешка (*fault*) от самата веб услуга) или заменен със съобщение от тип "Потвърждаване на получаването".

10 При проверка на съответствието на участници се проверяват за съвпадение, както уникалният идентификатор (GUID) на участника, така и неговия идентификатор (ЕИК/БУЛСТАТ).

11 При проверка на съответствието на участници се проверяват за съвпадение, както уникалният идентификатор (GUID) на участника, така и неговия идентификатор (ЕИК/БУЛСТАТ).

- (И.13) Проверява дали съобщението-отговор е електронно подписано. Ако не е, обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - (И.14) Проверява дали съобщението-отговор е електронно подписано с транспортния сертификат асоцииран с получателя в Регистъра. Ако не е, обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - (И.15) Проверява се дали уникалният идентификатор на съобщението-отговор (MessageGUID) съвпада с този на вече получено/изпратено съобщение. Ако съвпада, обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - Според вида на съобщението-отговор се изпълняват се проверките на приложно ниво при и се взима предвид техният резултат.
6. Обменът се счита за **"Успешен"**.

Получаване на съобщение

След като подател осъществи връзка до крайната точка на получателя, получателят **трябва** да следва следната процедура:

1. (П.1)¹² Проверява дали е наличен клиентски сертификат. Ако не, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при подателя"**;
2. (П.2) Проверява дали входящото съобщение е валиден XML документ. Ако не, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при подателя"**;
3. (П.3) Проверява дали входящото съобщение съответства на XSD схемите за обмен на съобщение (вж.Приложение 4). Ако не, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при подателя"**;
4. (П.4) Проверява дали получателят на съобщението съвпада с участник¹³, за който настоящата крайна точка отговаря. Ако не, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при подателя"**;
5. (П.5) Проверява дали подателят на съобщението съвпада с активен участник от Регистъра¹⁴. Ако не, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при подателя"**;
6. (П.6) Проверява дали клиентският сертификат съвпада с транспортния сертификат асоцииран с подателя в Регистъра. Ако не, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при подателя"**;
7. (П.7) Проверява дали съобщението е електронно подписано. Ако не е, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при подателя"**;

12 Кодът изписан в скоби преди всеки един сценарий в комбинация с версията на протокола се използва, за да бъде идентифициран в технически задания, при провеждане на тестове и изготвяне на протоколи от проверка за съвместимост.

13 **Препоръчително** е при подписването да бъде използван разширението XAdES, който дефинира старндартен начин за включване на удостоверение за време в подписаните XML документи.

14 В бъдещи версии отговорът ще бъде премахнат като възможност (като ще остане единствено възможността за изключение/грешка (*fault*) от самата уеб услуга) или заменен със съобщение от тип "Потвърждаване на получаването".

8. (П.8) Проверява дали съобщението е електронно подписано с транспортния сертификат асоцииран с подателя в Регистъра. Ако не, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при подателя"**;
9. (П.9) Проверява дали уникалният идентификатор на съобщението (MessageGUID) съвпада с този на вече получено/изпратено съобщение. Ако съвпада, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при подателя"**;
10. Ако на този етап не се извършва обработка на съобщението на *приложно ниво*, получателят връща празен резултат (null).
11. Ако на този етап се извършва обработка на съобщението на *приложно ниво* и тя е неуспеша, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при получателя"**;
12. Ако на този етап се извършва обработка на съобщението на *приложно ниво* и тя е успешна:
 - (П.10) Проверява се дали резултатът е валиден XML документ. Ако не е, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - (П.11) Проверява дали резултатът е валиден спрямо XSD схемите за съобщение (вж.Приложение 4). Ако не, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - (П.12) Проверява се дали подателят на съобщението-отговор съвпада с получателя на входящото съобщение. Ако не, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - (П.13) Проверява се дали получателят на съобщението-отговор съвпада с подателя на входящото съобщение. Ако не, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - (П.14) Проверява се дали съобщението-отговор е електронно подписано. Ако не е, извикването генерира изключение, а обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - (П.15) Проверява се дали съобщението-отговор е електронно подписано с транспортния сертификат асоцииран с подателя в Регистъра. Ако не е, обменът се счита за **"Неуспешен – Грешка при получателя"**;
 - Връща се резултатът от обработката.
13. Обменът се счита за **"Успешен"**.

Видове съобщения

В момента се поддържат следните видове съобщения:

- Заявление за регистриране на документ;
- Заявление за проверка на състоянието на документ;
- Известие за състояние на документ;
- Известие за грешка.

Структурата на съобщенията в включена в Приложение 4.

При получаване на съобщение, след проверките на самите съобщение (на *транспортно ниво*), участниците **трябва** да извършват проверки и на тяхното съдържание (на *приложно ниво*) според вида на изпращаното/получаваното съобщение. При установяване на грешка в съдържанието на получено съобщение, получателят **трябва** да отговори със съобщение от тип "Известие за грешка".

Заявление за регистриране на документ

Заявлението за регистриране на документ се използва за изпращане на документ от един участник до друг участник с цел неговото регистриране и последващата работа.

Заявлението за регистриране на документ се описва от XML обект от тип DocumentRegistrationRequestType, свойствата на който са:

1. Document (DocumentType) – документ. Това е обект със следната структура:
 - DocID (DocumentIdentificationType) – идентификатор на документа. Състои се от:
 - DocumentNumber (DocumentNumberType) – номер или DocumentURI (DocumentURI) – УРИ на документа при подателя;
 - DocumentGUID (GUIDType) – GUID на документа, споделен между подателя и получателя на документа.
 - DocParentID (DocumentIdentificationType) – идентификатор на инициращия/родителския документ в преписката. Състои се от:
 - DocumentNumber (DocumentNumberType) – номер или DocumentURI (DocumentURI) – УРИ на инициращия/родителския документ в преписката при подателя;
 - DocumentGUID (GUIDType) – GUID на инициращия/родителския документ в преписката, споделен между подателя и получателя на документа.
 - DocKind (xsd:string) – вид (напр. Молба, Жалба и др.)
 - DocCorrespondentList/Correspondent (CorrespondentType) – списък на кореспондентите. Всеки от тях се описва с име, адрес, ЕГН или ЕИК/БУЛСТАТ и други допълнителни полета;
 - DocAttachmentList/Attachment (AttachmentFileType) – списък на прикачените файлове. Всеки от тях се описва с наименование, съдържание (xsd:base64Binary), коментар и MIME тип;
 - DocAbout (xsd:string) – относно (кратко описание на документа);
 - DocService (ServiceItemType) – услуга. Има значение, когато изпращаният документ е заявление за извършване на административна услуга. Състои се от:
 - ServiceName – наименование;
 - ServiceType – тип (напр. "Нормална", "Бърза" или "Експресна");
 - ServiceCode – код (идентификатор/УРИ).
 - DocComment (xsd:string) – допълнителен коментар
 - DocAddData (AdditionalDataType) – допълнителни данни. Използва се за пренос на допълнителни метаданни незадължителни за обработка.
 - DocReqDateClose (xsd:date) – краен срок за приключване на работата;

- DocAttentionTo (xsd:string) – служител, на вниманието на който трябва да се насочи;
 - Signature (ds:Signature) – електронен подпис на документа по стандарта XML Signature Syntax and Processing (2nd Edition). Подписването **трябва** да е извършено с транспортния сертификат на участника или електронния подпис на служителя изпращащ документа, а елементът **трябва** да съдържа информация за използвания при подписването сертификат.¹⁵
2. Comment (xsd:string) – коментар, свързан с изпращането. Използва се за пояснения от подателя.

Обработката на съобщение от този вид на *приложно ниво*, получателят **трябва** да следва следната процедура:

1. Подготвя съобщение-отговор от вид "Известие за състояние на документ" (DocumentStatusResponseType), в него установява:
 - GUID на документа (DocumentGUID) – GUID на документа (DocumentGUID) от заявлението за регистриране.
2. Търси документ с посочения GUID (DocumentGUID) и според резултата:
 - (ЗР.1)¹⁶ Ако документът е открит:
 - установява статус (DocRegStatus) "Документът вече е получен" (DS_ALREADY_RECEIVED).
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на получения и регистриран вече документ;
3. Ако документът не е открит, в зависимост от момента на регистриране на документа:
 - а) (ЗР.2) Ако регистрирането на документа е отложено, в съобщението-отговор установява:
 - установява статус (DocRegStatus) "Документът очаква регистриране" (DS_WAIT_REGISTRATION).
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на документа със съответната стойност от заявлението.
 - б) (ЗР.3) Ако регистрирането на документа е отказано, в съобщението-отговор установява:
 - установява статус (DocRegStatus) "Регистрирането на документа е отказано" (DS_REJECTED);
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на документа със съответната стойност от заявлението;
 - установява причина за отказ от регистриране (RejectionReason) с въведената причина за отказ от регистриране.
 - в) Ако се извършва регистриране на документа:

¹⁵ **Препоръчително** е при подписването да бъде използван разширението XAdES, който дефинира старндартен начин за включване на удостоверение за време в подписаните XML документи.

¹⁶ Кодът изписан в скоби преди всеки един сценарий в комбинация с версията на протокола се използва, за да бъде идентифициран в технически задания, при провеждане на тестове и изготвяне на протоколи от проверка за съвместимост.

- i. Ако е посочен GUID на инициращ/родителски документ в преписката (DocParentID/DocumentGUID), търси документ с посочения GUID и според резултата:
 - (ЗР.4) Ако такъв документ не е открит, изпратеният документ се регистрира като инициращ на нова преписка.
 - (ЗР.5) Ако такъв документ е открит, изпратеният документ се регистрира към преписката, към която намереният документ принадлежи.
 - ii. Ако не е посочен GUID на инициращ/родителски документ в преписката (DocParentID/DocumentGUID):
 - (ЗР.6) Изпратеният документ се регистрира като инициращ на нова преписка.
 - iii. Според състоянието на регистрирания документ:
 - (ЗР.7) Ако работата по документа продължава:
 - установява статус (DocRegStatus) "Документът е регистрира" (DS_REGISTERED);
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на получения и регистриран документ;
 - установява очаквана дата за приключване на работата (DocExpectCloseDate), ако има такава.
 - (ЗР.8) Ако работата по документа е прекратена:
 - установява статус (DocRegStatus) "Работата по документа е прекратена" (DS_STOPPED);
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на получения и регистриран документ.
 - (ЗР.9) Ако работата по документа е приключена:
 - установява статус (DocRegStatus) "Работата по документа е приключена" (DS_CLOSED);
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на получения и регистриран документ.
4. Попълва допълнителните данни (DocAddData), ако има такива;
5. Връща съобщението-отговор.

Пояснения към регистрирането на документ

Като резултат от заявка за регистриране на документ, регистрирането му **може** да бъде отложено, отказано или извършено.

Регистрираният документ **трябва** да запазва своя GUID. Той **трябва** да се използва при проверка за дублиране на документа и при проверка на неговото състояние.

Регистрираният документ **може** или да запази своя номер, или да бъде регистриран под нов номер, в зависимост от действащите правила.

Елементът DocParentID винаги се попълва с данните за инициращия документ на преписката. При изпращане на инициращ документ от преписка до друга организация, двата елемента DocID и DocParentID са с еднакво съдържание.

Нека в организация А е регистрирана преписка, която съдържа инициращ документ Д1 и междинен документ Д2. Организация А изпраща до организация Б документа Д2 със

съобщение от вид "Заявка за регистриране на документ", като попълва GUID на документите по следния начин:

- DocID/DocumentGUID = Д2
- DocumentParentID/DocumentGUID = Д1

Организация Б получава съобщението от вид "Заявка за регистриране на документ" за документ Д2 и изготвя отговор под формата на документ Д3, който трябва да бъде изпратен до организация А. Тук се разглеждат два подслучая:

- **Д1 също е бил изпращан до Б.** Това означава, че в организация Б има вече регистрирана преписка с инициращ документ Д1. Организация Б изпраща до организация А създадения документ-отговор Д3 със съобщение от вид "Заявка за регистриране на документ", като попълва GUID на документите по следния начин:
 - DocID/DocumentGUID = Д3
 - DocumentParentID/DocumentGUID = Д1
- **Д1 не е бил изпращан до Б.** Тогава в процеса на получаване на документа в организация Б се създава преписка с инициращ документ Д2. Организация Б изпраща до организация А създадения документ-отговор Д3 със съобщение от вид "Заявка за регистриране на документ", като попълва GUID на документите по следния начин:
 - DocID/DocumentGUID = Д3
 - DocumentParentID/DocumentGUID = Д2

Организация А получава документа-отговор Д3. Той **трябва** да бъде обработен по следния начин:

- В базата данни се търси документ с GUID записан в елемента DocumentParentID/DocumentGUID (според горния пример съответно Д1 или Д2):
 - i. Ако съществува документ с такъв GUID, полученият документ се добавя към преписката, към която принадлежи.
 - ii. В противен случай се създава нова преписка, на която изпратеният документ става инициращ.

Заявление за проверка на състоянието на документ

Заявлението за проверка на състоянието на документ се използва за проверка при получателя за състоянието на изпратен до нея документ.

Заявлението за проверка на състоянието на документ се описва от XML обект от тип DocumentStatusRequestType, свойствата на който са:

- DocID (DocumentIdentificationType) – идентификатор на документа. Състои се от:
 - DocumentNumber (DocumentNumberType) – номер или DocumentURI (DocumentURI) – УРИ на документа при подателя;
 - DocumentGUID (GUIDType) – GUID на документа, споделен между подателя и получателя на документа.

Обработката на съобщение от този вид на *приложно ниво*, получателят **трябва** да следва следната процедура:

1. Подготвя съобщение-отговор от вид "Известие за състояние на документ" (DocumentResponseType), като попълва DocumentGUID с GUID на документа (DocumentGUID) от заявлението.
2. Търси документ с посочения GUID (DocumentGUID) и според резултата попълва останалите атрибути на съобщението-отговор, както следва:
 - (ПС.1)¹⁷ Ако документът не е открит:
 - установява статус (DocRegStatus) "Документът не е открит" (DS_NOT_FOUND);
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на документа със съответната стойност от заявлението.
 - (ПС.2) Ако документът е открит, но вече е бил получаван:
 - установява статус (DocRegStatus) "Документът вече е получен" (DS_ALREADY_RECEIVED);
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на получения и регистриран вече документ.
 - (ПС.4) Ако документът е открит, но още не е регистриран:
 - установява статус (DocRegStatus) "Документът очаква регистриране" (DS_WAIT_REGISTRATION);
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на документа със съответната стойност от заявлението.
 - (ПС.3) Ако документът е открит, но регистрирането му е отказано:
 - установява статус (DocRegStatus) "Регистрирането на документа е отказано" (DS_REJECTED);
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на документа със съответната стойност от заявлението;
 - установява причина за отказ от регистриране (RejectionReason) с въведената причина за отказ от регистриране.
 - (ПС.5) Ако документът е открит, регистриран и работата по него продължава:
 - установява статус (DocRegStatus) "Документът е регистриран" (DS_REGISTERED);
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на получения и регистриран документ;
 - установява очаквана дата за приключване на работата (DocExpectCloseDate), ако има такава.
 - (ПС.6) Ако документът е открит, регистриран и работата по него е прекратена:

¹⁷ Кодът изписан в скоби преди всеки един сценарий в комбинация с версията на протокола се използва, за да бъде идентифициран в технически задания, при провеждане на тестове и изготвяне на протоколи от проверка за съвместимост.

- установява статус (DocRegStatus) "Работата по документа е прекратена" (DS_STOPPED);
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на получения и регистриран документ.
- (ПС.7) Ако документът е открит, регистриран и работата по него е приключена:
- установява статус (DocRegStatus) "Работата по документа е приключена" (DS_CLOSED);
 - установява номер (DocumentNumber) или УРИ (DocumentURI) на получения и регистриран документ.
3. Попълва допълнителните данни (DocAddData), ако има такива;
4. Връща съобщението-отговор.

Известие за състояние на документ

Известието за състояние на документ се използва за известяване на подателя за номера, под който е регистриран изпратеният от нея документ, както и за неговото текущо състояние.

Известието за състояние на документ се използва в отговор на:

- Заявление за регистриране на документ;
- Заявление за проверка на състоянието на документ.

Известие за състояние на документ **трябва** да се изпраща и при всяка промяна в състоянието на документа (напр. регистриране, отказ от регистриране, приключване и др.).

Известието за състояние на документ се описва от XML обект от тип DocumentStatusResponseType, свойствата на който са:

- DocID (DocumentIdentificationType) – идентификатор на документа. Състои се от:
 - DocumentNumber (DocumentNumberType) – номер или DocumentURI (DocumentURI) – УРИ на документа при получателя;
 - DocumentGUID (GUIDType) – GUID на документа, споделен между подателя и получателя на документа.
- DocRegStatus (DocumentStatusType) – статус на документа. Представя стойност от изброим списък:
 - DS_WAIT_REGISTRATION – документът очаква регистриране;
 - DS_REGISTERED – документът е регистриран;
 - DS_STOPPED – работата по документа е прекратена;
 - DS_CLOSED – работата по документа е приключена;
 - DS_NOT_FOUND – документът не е открит;
 - DS_ALREADY_RECEIVED – документът вече е получен;
 - DS_REJECTED – регистрирането на документа е отказано.
- RejectionReason (xsd:string) – причина за отказ от регистриране (когато регистрирането на документа е отказано);
- DocExpectCloseDate (xsd:date) – очаквана дата за приключване на работата;

- DocAddData (AdditionalDataType) – допълнителни данни. Използва се за пренос на допълнителни метаданни незадължителни за обработка.

Обработката на съобщение от този вид на *приложно ниво*, получателят **трябва** да следва следната процедура:

1. (ИС.1)¹⁸ Ако документ с посочения GUID (DocumentGUID) не е открит, връща съобщение-отговор от вид "Известие за грешка" (ErrorMessageType) със следните попълнени атрибути:
 - GUID на съобщението (MessageGUID) – GUID на съобщението "Известие за състояние на документ";
 - Вид на грешката (ErrorType) – външна грешка (ERR_EXTERNAL);
 - Описание на грешката (ErrorDescription) – текстово описание на грешката.
2. Ако документ с посочения GUID (DocumentGUID) е открит:
 - (ИС.2) Ако статусът (DocRegStatus) е "Документът вече е получен" (DS_ALREADY_RECEIVED), отбелязва състоянието на документа и записва неговия номер или УРИ при получателя;
 - (ИС.3) Ако статусът (DocRegStatus) е "Документът очаква регистриране" (DS_WAIT_REGISTRATION), отбелязва състоянието на документа.
 - (ИС.4) Ако статусът (DocRegStatus) е "Регистрирането на документа е отказано" (DS_REJECTED), отбелязва състоянието на документа и записва причината за отказ от регистриране от неговия получател;
 - (ИС.5) Ако статусът (DocRegStatus) е "Документът е регистриран" (DS_REGISTERED), отбелязва състоянието на документа и записва неговия номер или УРИ при получателя, както и посочената очаквана дата на приключване на работата, ако е посочена такава;
 - (ИС.6) Ако статусът (DocRegStatus) е "Работата по документа е прекратена" (DS_STOPPED), отбелязва състоянието на документа и записва/обновява неговия или УРИ при получателя;
 - (ИС.7) Ако статусът (DocRegStatus) е "Работата по документа е приключена" (DS_CLOSED), отбелязва състоянието на документа и записва/обновява неговия или УРИ при получателя.
3. Приключва обработката.

Известие за грешка

Известието за грешка се използва за известяване на подателя за грешка възникнала по време на обработката на дадено съобщение.

Известието за грешка се описва от XML обект от тип ErrorMessageType, свойствата на който са:

¹⁸ Кодът изписан в скоби преди всеки един сценарий в комбинация с версията на протокола се използва, за да бъде идентифициран в технически задания, при провеждане на тестове и изготвяне на протоколи от проверка за съвместимост.

- MessageGUID (GUIDType) – GUID на съобщението, което е предизвикало грешката;
- ErrorType (ErrorKindType) – вид на грешката. Представява стойност от изброим списък:
 - ERR_INTERNAL – вътрешна грешка (напр. липса на връзка с БД);
 - ERR_EXTERNAL – външна грешка (напр. грешен формат на съобщението).
- ErrorDescription (xsd:string) – описание на грешката.

Обработката на съобщение от този вид на *приложно ниво*, получателят **трябва** да следва следната процедура:

1. (ИГ.1)¹⁹ Проверява дали GUID на съобщението предизвикало грешката (MessageGUID) съвпада с GUID на изпратено съобщение до същия участник съобщение. Ако не, обменът се счита за "**Неуспешен – Грешка при получателя**". Получателят **трябва** да отговори с "**Известие за грешка**" от вид "**Външна грешка**";
2. Проверява вида на грешката:
 - (ИГ.2) Ако грешката е "вътрешна", обменът се счита за "**Неуспешен – Грешка при получателя**";
 - (ИГ.3) Ако грешката е "външна", обменът се счита за "**Неуспешен – Грешка при подателя**".

V. СИГУРНОСТ НА ОБМЕНА НА СЪОБЩЕНИЯ

Сигурността на средата за обмен на съобщения се гарантира от следните негови характеристики:

1. **Използваният транспортен протокол е HTTPS (HTTP-върху-TLS) (с използване на TLS 1.2 или по-висока)**, който гарантира, че връзката не може да бъде "подслушвана" или манипулирана.
2. **Използваните цифрови сертификати използват 2048-битови RSAwithSHA256 ключове**, "разбиване" на които все още не е постигнато. Възможно е използването и на 4096-битови такива.
3. **Автентикацията и авторизацията се осъществява с цифрови сертификати** и всяка от комуниращите страни може да установи със сигурност коя е отсрещната страна и да откаже достъп до съответните ресурси и/или операции.
4. **Мрежовата архитектура на системата е peer-to-peer**, т.е. комуникацията не преминава през централизиран междинен сървър, който да евентуално да събира/обработва пренасяните данни или дори събира статистика кой участник с кого, колко и какви съобщения обменя.

¹⁹ Кодът изписан в скоби преди всеки един сценарий в комбинация с версията на протокола се използва, за да бъде идентифициран в технически задания, при провеждане на тестове и изготвяне на протоколи от проверка за съвместимост.

5. **Обменяните съобщения могат да бъдат удостоверявани за време²⁰**, с която независима трета страна удостоверява точния момент на създаване и подписване на електронните съобщения. Струва си да се отбележи, че при удостоверяване на време не е необходимо удостоверяващата страна да получава под каквато и да е форма съдържанието на съобщението.

VI. ПРИЛОЖЕНИЯ

Приложение 1. Описание на услугата на Регистъра

Вж.приложения файл eGovRegistry.wsdl.

Приложение 2. Описание на съобщенията на Регистъра

Вж.приложения файл eGovRegistry.xsd.

Приложение 3. Описание на услугата на участниците

Вж.приложения файл eGovEndpoint.wsdl.

Приложение 4. Описание на съобщенията между участниците

Вж.приложения файл eGovMessaging.xsd.

²⁰ **Препоръчително** е при подписването да бъде използван разширението XAdES, който дефинира старндартен начин за включване на удостоверение за време в подписаните XML документи.