РЕПУБЛИКА БЪЛГАРИЯ
Държавна агенция „Електронно управление“

Модел на интеграция с хоризонтална система за еАвтентикация

23.05.2018 г.

гр. София
2018 г.

Версия	Дата	Автор	Описание	Стр.
1.0	12.01.2018	Николай Минев	Първа версия на документа - дата на създаване	17
1.1	05.02.2018	Николай Минев	Сценарии за взаимодействие	17
1.8	03.04.2018	Николай Минев	Сценарии за взаимодействие	22
2.1	25.04.2018	Николай Минев	Сценарии за взаимодействие	21

Преглед и одобрение на документа:

Версия	Дата	Отговорник	Описание	Стр.
1.0		Николай Минев	Първа версия на документа	6
1.1	05.02.2018 г.	Николай Минев	Детайлно описание на сценарии за взаимодействие	17
2.1	10.05.2018 г.	Николай Минев	Детайлно описание на сценарии за взаимодействие	22
2.1		Висш експертен съвет	Версията на документа е утвърдена на заседание на ВЕС	22
2.1	17.05.2018	Съвет за интеграция на ИР	Версията на документа е утвърдена на заседание на Съвета	22

РЕЧНИК НА ИЗПОЛЗВАНИТЕ ТЕРМИНИ И ТЕХНИЧЕСКИ СЪКРАЩЕНИЯ

№		*Термин*
1.	***SAML***	***Security Assertion Markup Language***
2.	***SAML атестат***	***XML*** *– базирана услуга, съдържаща идентификационни данни за заявител на електронни услуги*
3.	***LDAP***	***Lightweight Directory Access Protocol***
4.	***XML***	***eXtensible Markup Language***
5.	***WSDL***	***Web Service Definition Language***
6.	***UDDI***	***Universal, Description, Discovery and Integration***
7.	***eIDAS възел***	*елемент (национално ниво) от схемите за електронна идентификация на държавите членки, включително и услуги за оперативна съвместимост със системите на държавите-членки на ЕС*
8.	***еАвтентикация***	***електронна автентикация –*** *хоризонтална система, чрез която се идентифицират лицата и информационните системи (всички участващи в електронното управление обекти и субекти) в електронния свят.*
9.	***еОтор***	***електронна оторизация -*** *хоризонтална система, която определя кой до какви ресурси на електронното управление (ЕУ) да има достъп, като въвежда строги централизирани политики и единен контрол на достъп до ресурсите, с които оперира електронното управление*
10.	***еВр***	***електронно връчване -*** *хоризонтална система, чрез която еднозначно удостоверяване на момента на изпращане, получаване и връчване, както и гарантиране на авторството и интегритета на същия*
11.	***еВал***	***електронно валидиране -*** *хоризонтална система, чрез която се прави проверка и потвърждаване на валидността на квалифициран електронен подпис, удостоверение за време (time stamp), електронно подписан документ в реално време, както и възможност за разпечатване на електронен документ, преобразуване на съдържанието на документ на хартиен носител в електронна форма*
12.	***Администратор на електронна идентичност***	*Регистрирани от Министъра на вътрешните работи „лица (администратори)“, които подпомагат дейността на органа за електронна идентификация*
13.	***Данни за електронна идентификация на лица***	*Набор от данни, които позволяват да се установи самоличността на физическо лице, вкл. в ролята му на законен представител на юридическо лице*
14.	***еИД***	***Електронен идентификатор*** *- уникален идентификатор на физическо лице, за който е издадено удостоверение за електронна идентичност, позволяващо еднопосочно еднозначно разпознаване на едно лицето в електронна среда с цел осигуряване на достъп до информационни системи или осигуряване на възможност за заявяване и изпълнение на електронни административни услуги*
15.	***Електронен печат***	*Данни в електронна форма, които се добавят към други данни в електронна форма или са логически свързани с тях, за да се гарантират произходът и целостта на последните*
16.	***Електронна идентификация***	*Процес на използване на данни в електронна форма за идентификация на лица, които данни представляват по уникален начин дадено физическо или юридическо лице, или физическо лице, представляващо юридическо лице.* *Съгл. Регламент (ЕС) № 910/2014 на Европейския парламент и на съвета от 23 юли 2014 година*

№		Термин
17.	***Електронна идентичност***	*Съвкупност от характеристики, записани в електронна форма, въз основа на които може да се направи еднозначно разграничаване на едно лице от други лица във виртуалната среда с цел осигуряване на достъп до информационни системи или осигуряване на възможност за извършване на електронни изявления*
18.	***Електронни административни услуги (ЕАУ)***	*Административните услуги, предоставяни на гражданите и организациите от административните органи, услугите, предоставяни от лицата, на които е възложено осъществяването на публични функции, както и обществените услуги, които могат да се заявяват и/или предоставят от разстояние чрез използването на електронни средства*
19.	***Квалифициран електронен подпис (КЕП)***	*Усъвършенстван електронен подпис, който е създаден от устройство за създаване на квалифициран електронен подпис и се основава на квалифицирано удостоверение за електронни подписи*
20.	***Орган за електронна идентификация***	*Орган за електронна идентификация е министърът на вътрешните работи, който издава удостоверения за електронна идентичност*
21.	***Секторен електронен идентификатор***	*Преобразуван посредством криптографски алгоритми електронен идентификатор, получен в процеса на електронна идентификация. Секторните електронни идентификатори може да се използват за идентифициране на физическите лица само в сектори, в които държавните органи предоставят на гражданите възможност да упражняват права по електронен път или да извършват електронни услуги, при което не се събират данни за гражданите от други органи и лица извън сектора. Секторите, в които се използват секторни електронни идентификатори се определят с решение на МС по предложение на председателя на Държавна агенция „Електронно управление“*
22.	***Средство за електронна идентификация***	*Материална и/или нематериална единица, която съдържа данни за електронна идентификация на лица*
23.	***Схема за електронна идентификация***	*Комплекс от информационни системи и техническа инфраструктура за електронна идентификация, при която средства за електронна идентификация се издават на физически лица и която позволява идентифициране на тези лица в лично или служебно качество или в качеството им на представляващи юридически лица.*
24.	***Титуляр на електронна идентичност***	*Титуляр на електронна идентичност е физическо лице, навършило 14-годишна възраст, на което е издадено удостоверение за електронна идентичност*
25.	***Удостоверение за електронна идентичност***	*Формализиран официален електронен документ, представен чрез общоприет стандарт и издаден с определен срок на валидност, съдържащ електронен идентификатор и други данни*
26.	***Център за електронна идентификация***	*Дирекция в структурата на Държавна агенция „Електронно управление“, която отговаря на изискванията на чл. 11, т. 1-3 от ЗЕИ*

Съдържание

1. Цел

Целта на настоящия документ е:

- Описание на структурата и функциите на системата за електронна автентикация, наричан за краткост в този документ еАвтентикация;
- Представяне на модел за интеграция на системата за еАвтентикация със средствата за електронна идентификация и сценариите за взаимодействие със съответстващите им доставчици на идентификация;
- Описание на функциите на еАвтентикация, свързани в основния процес по заявяване на електронни административни услуги (ЕАУ);
- Описание на взаимодействието на еАвтентикация с останалите хоризонтални и централизирани системи, предоставяни от Държавна агенция „Електронно управление“ (ДАЕУ) и информационните системи (ИС) на лицата, попадащи в обхвата на чл.1 ал.1 и ал.2 и чл.2 от Закона за електронното управление (ЗЕУ);
- Предоставяне на стандарт (задължителен за лицата по чл. 1 от ЗЕУ) за структурата, съдържанието и протокола, по който се генерира и обменя необходимата информация между ИС при електронна идентификация на потребителите им по електронен път, както и при взаимодействие система-система. Стандартът се одобрява от Съвета за интеграция на информационните ресурси, след което се утвърждава от Председателя на ДАЕУ. Стандартът е препоръчителен за ИС на останалите преки и непреки участници в електронното управление. Чрез стандарта и интеграцията с еАвтентикация се постига високо ниво на оперативна съвместимост, включително и при взаимодействие с ИС на лица от държавите членки на ЕС. Функционалността се осигурява чрез създаването и интеграцията на eIDAS възел, който ще се бъде създаден и ще се оперира от ДАЕУ.

2. Принципи

- Обслужва електронната идентификация на лицата при достъп до ресурсите на електронното управление;
- Защита и неприкосновеност на личния живот;
- Защита на идентификационните данни чрез използване на утвърдени стандарти.

3. Обхват

Документът е предназначен за ползване от всички лица по чл.1, ал.1 и ал. 2 и чл.2 от ЗЕУ при интеграция на ИС и при необходимост от електронна идентификация на физически и юридически лица. Интеграцията е задължителна при електронна идентификация на физически лица, юридически лица и административните органи при заявяване на електронни административни услуги. Всяка една от посочените групи взаимодействия за целите на електронната идентификация по определен модел.*

**Забележка*: *Системата за еАвтентикация ще бъде интегрирана с Националната схема за електронна идентификация (НСЕИД) на физически лица, която е в съответствие с Регламент ЕС 910/2014, след нейното утвърждаване от МВР като национален*

орган, водещ електронен регистър на удостоверенията за електронна идентичност, електронен регистър на електронни идентификатори, електронен регистър на администраторите на електронна идентичност, електронен регистър на центровете за електронна идентификация и електронен регистър на овластяванията.

3.1. Правна рамка

- Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронна трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО;
- Регламент за изпълнение (ЕС) 2015/1502 на Комисията от 8 септември 2015 г.за определяне на минимални технически спецификации и процедури за нивата на осигуреност за средствата за електронна идентификация съгласно член 8, параграф 3 от Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар;
- Закон за електронното управление;
- Закон за електронната идентификация.

3.2. Участници

3.2.1. Потребители

- Административни органи и техните структури, вкл. първичните администратори на данни;
- Лица и организации, осъществяващи публични функции и предоставящи обществени услуги;
- Физически и юридически лица със средства за електронна идентификация, издадени от български доставчици на идентификация;
- Физически и юридически лица със средства за електронна идентификация, издадени от доставчици на идентификация от държава членка на Европейския съюз.

3.2.2. Доставчици

- Лица по чл.1 ал.1 и ал. 2 и чл. 2 от ЗЕУ;
- Доставчици на удостоверителни услуги;
- Доставчици на идентификационни услуги (eIDProvider).

3.2.3. Софтуерни компоненти

Информационни системи и/или модули, информационна инфраструктура на лицата по чл.1 ал.1 и ал. 2 и чл. 2 от ЗЕУ, осигуряващи изпълнението на функционалностите.

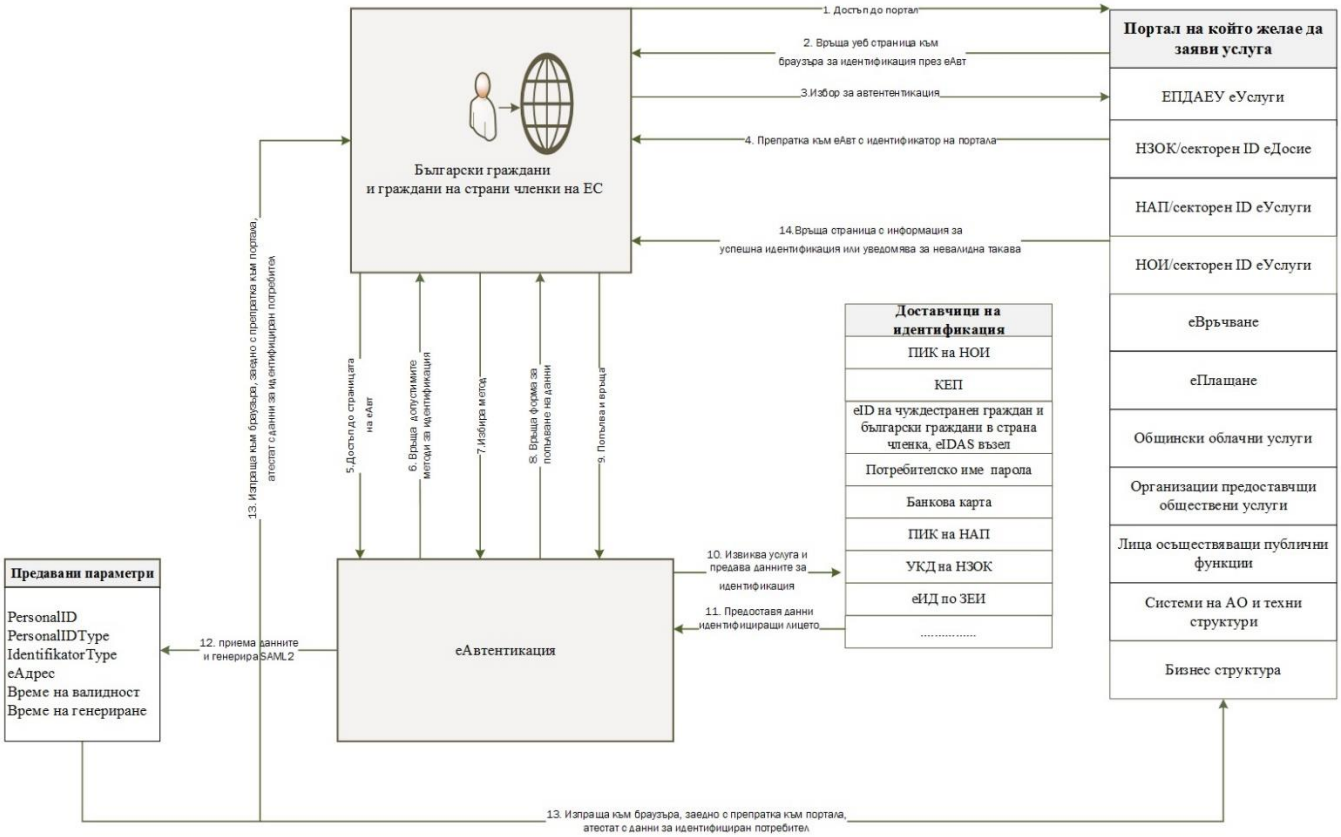
3.3. Функционалност

Системата за еАвтентикация предоставя SingleSign-On функция, като издава атестати, идентифициращи потребителите (ФЛ, ЮЛ или ИС) в информационната среда на електронното управление. Атестатите важат за времето, в което потребителят има активна сесия в рамките на средата на електронното управление, т.е. в системата, през която е осъществил вход и

идентификация. В рамките на сесията на потребителя атестатът се предава през защитен протокол „система-система“ към всяка следваща система, която участва в процеса, като на всяка стъпка може да бъде валидиран от еАвтентикация чрез автоматизирана услуга.

4. Модели на взаимодействие

На фиг. 1 е представен функционален модел на системата за еАвтентикация и начините на взаимодействие с доставчици на идентификация и на идентификационна услуга.



Фиг. 1. Модел на взаимодействия със системата за еАвтентикация

Сценарий:

1. Потребителят въвежда в браузъра електронния адрес на портала на административен орган, на който желае да заяви услуга или да достъпи ресурс. Браузърът изпраща **https** заявка към въведения адрес;
2. Порталът на административния орган връща уеб страница към браузъра и на потребителя се дава възможност да избере дали ще се идентифицира през еАвтентикация;
3. Потребителят избира електронна идентификация през еАвт и браузърът изпраща https заявка към портала на административния орган, съдържаща избора на потребителя;
4. Порталът на административния орган връща към браузъра препратка (redirect) със своя идентификатор към адреса на еАвтентикация.
5. Браузърът следва препратката и се обръща към страницата на еАвтентикация, като предава и идентификатора на портала на административния орган;

6. еАвтентикация връща страница със списък с допустимите методи за идентификация, който се визуализира в браузъра на потребителя;
7. Потребителят избира метод за електронна идентификация и браузърът изпраща заявка към еАвтентикация;
8. еАвтентикация връща форма, в която да бъдат попълнени данните за електронна идентификация на потребителя;
9. Потребителят попълва формата за електронна идентификация и браузърът изпраща данните към еАвтентикация;
10. еАвтентикация извиква автоматизирана услуга на доставчика на идентификация, съответстващ на средството, с което се идентифицира потребителят, като предава данните му за електронна идентификация (за средства за електронна идентификация, издадени от държава членка на ЕС, се извиква услуга от eIDAS възела);
11. Доставчикът на идентификация проверява данните за потребителя, извлича данните, определящи неговата идентичност (ЕГН, ЛНЧ, Имена и др.), с който той е регистриран и ги връща на еАвтентикация като резултат от автоматизираната услуга;
12. еАвтентикация приема данните от доставчика на идентификация, запазва ги и генерира SAML2 атестат, в който слага дискретна информация с идентичност на лицето. Атестатът е подписан и криптиран с асиметричен ключ, специфичен за портала на администрацията, за която се изисква автентикация. Алгоритъмът за криптиране следва да отговаря на минимални изисквания за сигурност на използвания алгоритъм SHA-256 с използването на симетрични ключове на базата на ECDH споразумение за размяна на ключове. Подписването на SAML атестата следва препоръчително да използва хеширащи алгоритми RSASSA-PSS(3072) или ECDSA (256). Така генерираният SAML2 атестат се изпраща към браузъра, заедно с препратка към портала на административния орган. За оптимална сигурност се препоръчва участниците в процеса на автентикация и порталът на администрацията да използват в рамките на комуникацията помежду си сертификати, базирани на алгоритми с елиптични криви ECDH и ECDSA. Алгоритмите предоставят голяма сигурност при малък размер на използвания ключ.
13. Браузърът следва препратката и изпраща към портала на административния орган получения SAML2 атестат;
14. Порталът на администрацията прочита SAML2 атестата, извършва необходимите валидации за автентичност и декриптиране на получения SAML2 атестат, проверява го за валидност и използва съдържащите се в атестата идентификационни данни за автентикация на потребителя, уведомява за успешната електронна автентикация и дава достъп до желаната услуга/ресурс. При неуспешна автентикация системата връща данни за идентификация със статус „Невалиден идентификатор“ на портала на административния орган, който изпраща към браузъра на потребителя страница, която го уведомява за неуспешната автентикация.

4.1. Общи положения

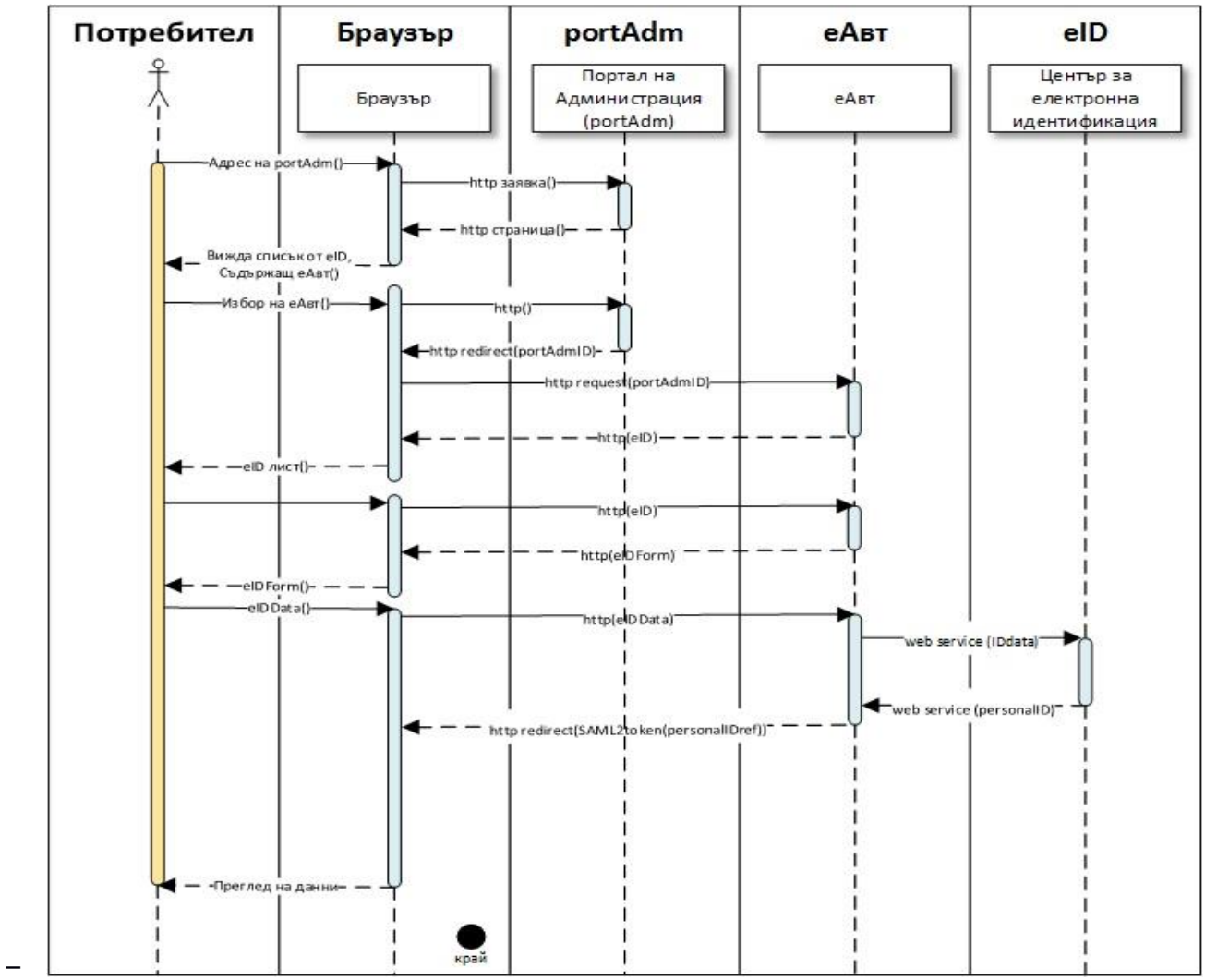
- Централните системи за заявяване на ЕАУ и ИС на лицата по чл. 1 и чл.2, ал.2 от ЗЕУ се интегрират с еАвтентикация по стандартизиран протокол, одобрен от Съвета за интеграция на информационните ресурси и утвърден от Председателя на ДАЕУ;
- Интеграцията на еАвтентикация с доставчици на идентификация се извършва по стандартизиран защитен протокол от тип „система-система“ в средата на електронното управление, одобрен от Съвета за интеграция на информационните ресурси и утвърден от Председателя на ДАЕУ.

- В атестата, издаван от системата за еАвтентикация, не се съдържат чувствителни данни за идентифицираните лица в чист текстов вид. Предаването на лични данни се осъществява само с криптирани и подписани съобщения на базата на споделени публични ключове (сертификати).

4.2. Електронна идентификация на физически и юридически лица със средства за еИД, издадени от национални доставчици на идентификация

Участници:

- Потребител – физическо лице, което желае да заяви електронна услуга или да получи достъп до ресурс на електронното управление в лично качество или като представител на юридическо лице;
- Браузър – софтуерен компонент, използван от потребителя за достъп до Интернет;
- Портал на администрация (portAdm) – уеб страница/портал, на който могат да бъдат заявявани електронни услуги и/или да бъдат достъпвани ресурси. Може да бъде сайт/портал на конкретен административен орган или ЕПДЕАУ;
- еАвтентикация – централна система на електронното управление, през която се извършва електронна идентификация на потребителя;
- Център за електронна идентификация (eIDProvider) – система на доставчици на идентификация, която извършва електронна идентификация на потребителя.
- На диаграмата по-долу е представено взаимодействието със системата за еАвтентикация при електронна идентификация на потребител, който желае да достъпи система на административен орган за заявяване на електронна услуга или достъп до ресурс.



Фиг. 2 Диаграма на процеса автентикация на физически и юридически лица

4.3. Електронна идентификация на физически и юридически лица със средства за еИД, издадени от доставчици на идентификация на държави членки (ДЧ) на ЕС

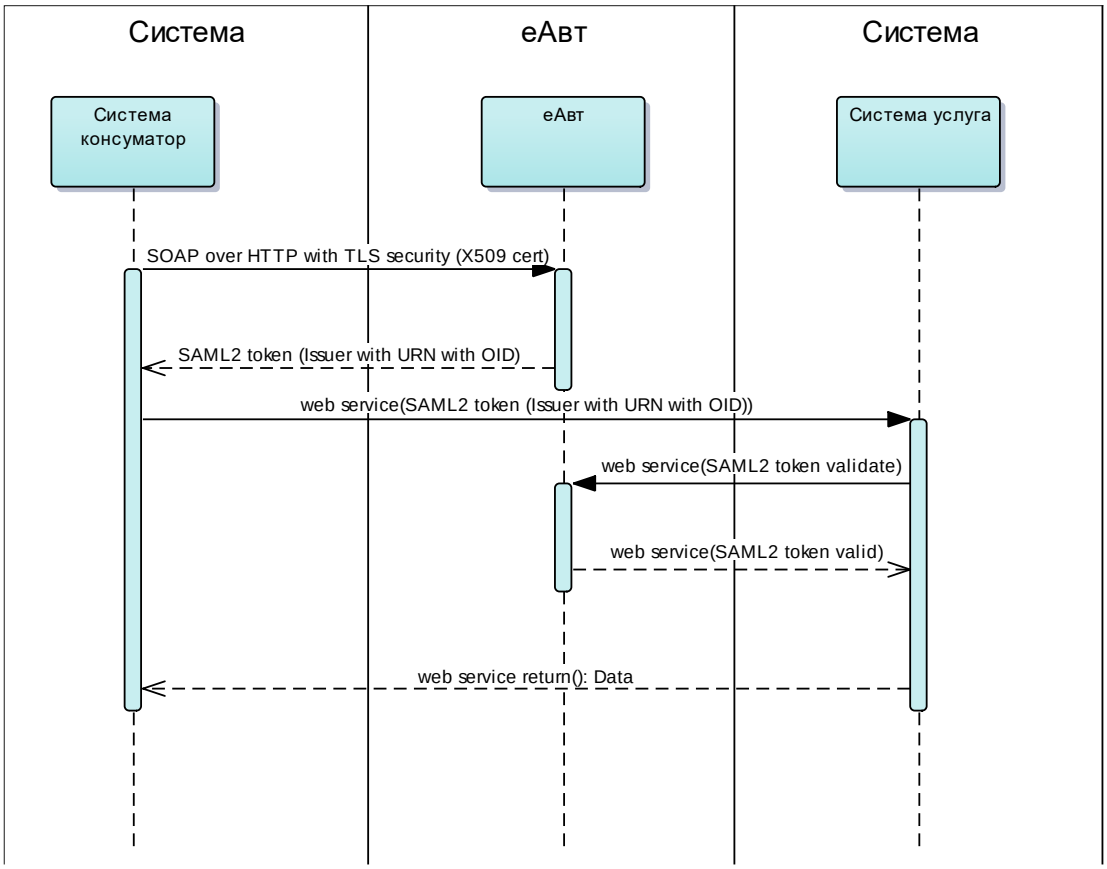
Граждани на други държави членки на ЕС и български граждани, постоянно или временно пребиваващи на територията на друга държава членка на ЕС, могат да използват своите средства за електронна идентификация за достъп до електронни административни услуги в Република България.

1. Модулът за еАвтентикация извиква автоматизирана услуга на eIDAS възела, като предава електронния идентификатор на потребителя;
2. eIDAS възелът идентифицира държавата, издател на електронния идентификатор, и го изпраща на съответния национален eIDAS възел на държавата членка на ЕС;

3. При успешна електронна идентификация eIDAS възелът е получил от съответния национален eIDAS възел на ДЧ данни за електронна идентификация и ги предава на системата за еАвтентикация.

4.4. Електронна идентификация на система при взаимодействие „система-система“ (S2S)

На диаграмата е показано взаимодействието със системата за еАвтентикация при електронна идентификация на система, която трябва да консумира автоматизирана услуга или да достъпи ресурс в рамките на електронното управление.



Фиг. 3. Диаграма на процеса при взаимодействие „система-система“ (S2S)

4.4.1. Участници:

- Система консуматор – информационна система, от която се осъществява достъп до автоматизирана услуга или ресурс на електронното управление;
- еАвтентикация – централна система на електронното управление, през която се извършва електронна идентификация на системата консуматор;
- Система услуга – информационна система, която предоставя достъп до автоматизирана услуга или ресурс на електронното управление.

4.4.2. Сценарий:

1. Системата консуматор извиква автоматизирана услуга на еАвтентикация, като подава своя цифров сертификат;
2. еАвтентикация проверява цифровия сертификат на системата консуматор, генерира SAML2 атестат, който да послужи за идентифицирането на консуматора пред системата доставчик на услуга и го изпраща на консуматора;
3. Системата консуматор извиква услуга на доставчика, като прилага SAML2 атестата;
4. Системата доставчик на услуга проверява SAML2 атестата и го валидира, като извиква автоматизирана услуга на еАвтентикация;
5. След валидацията на атестата системата, която предоставя услуга, връща резултат на системата консуматор.

**Забележки: (1)В сценариите са разгледани само случаите, при които идентификацията е успешна и в процеса не възникват грешки;*

(2) Сертификатите се издават от доверена PKI верига, поддържана от ДАЕУ.

5. Структура

5.1. Специфицираната структура в термините на SAML

Следва пример за SAML атестат: Assertion с обяснения. Редовете са номерирани, за да бъдат използвани за препратки. **Специфицираната структура в термините на SAML е следната:**

XML фрагмент, пример 01

```
/*01*/ <saml:Assertion
/*02*/       xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
/*03*/       xmlns:xs="http://www.w3.org/2001/XMLSchema"
/*04*/       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
/*05*/       ID="b07b804c-7c29-ea16-7300-4f3d6f7928ac"
/*06*/       Version="2.0"
/*07*/       IssueInstant="2004-12-05T09:22:05"
/*08*/ >
/*09*/       <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer>
/*10*/       <ds:Signature
/*11*/             xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
/*12*/       >...</ds:Signature>
/*13*/       <saml:Subject>
```

```
/*14*/                 <saml:NameID
/*15*/                         Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
/*16*/                 >3f7b3dcf-1674-4ecd-92c8-1544f346baf8</saml:NameID>
/*17*/                 </saml:SubjectConfirmation>
/*18*/         </saml:Subject>
/*19*/         <saml:Conditions
/*20*/                 NotBefore="2004-12-05T09:17:05"
/*21*/                 NotOnOrAfter="2004-12-05T09:27:05"
/*22*/         >
/*23*/                 <saml:AudienceRestriction>
/*24*/                         <saml:Audience>https://sp.example.com/SAML2</saml:Audience>
/*25*/                 </saml:AudienceRestriction>
/*26*/         </saml:Conditions>
/*27*/         <saml:AuthnStatement
/*28*/                 AuthnInstant="2004-12-05T09:22:00"
/*29*/         >
/*30*/                 <saml:AuthnContext>
/*31*/
        <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtecte
dTransport</saml:AuthnContextClassRef>
/*32*/                 </saml:AuthnContext>
/*33*/         </saml:AuthnStatement>
/*34*/         <saml:AttributeStatement>
/*35*/                 <saml:Attribute
/*38*/                         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
/*39*/                         Name="urn:oid:2.5.4.5"
/*40*/                         FriendlyName="serialNumber"
/*41*/                 />
/*35*/         <saml:Attribute FriendlyName="FamilyName" Name="urn:oid:X.X.X.X"
```

/*36*/ NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

/*37*/ <saml:AttributeValue xsi:type="eavt:FamilyNameType">Chalk</saml:AttributeValue>

/*38*/</saml:Attribute>

/*39*/<saml:Attribute FriendlyName="GivenName" Name="urn:oid:X.X.X.X"

/*40*/NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

/*41*/ <saml:AttributeValue xsi:type="eavt:GivenNameType">Sarah</saml:AttributeValue>

/*42*/</saml:Attribute>

/*43*/<saml:Attribute FriendlyName="DateOfBirth" Name="urn:oid:X.X.X.X"

/*44*/NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

/*45*/ <saml:AttributeValue xsi:type="eavt:DateOfBirthType">1970-05-28

/*46*/</saml:AttributeValue>

/*47*/</saml:Attribute>

/*48*/<saml:Attribute FriendlyName="UniqueIdentifier" Name="urn:oid:X.X.X.X"
/*49*/NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">

/*50*/ <saml:AttributeValue xsi:type="eavt:UniqueIdentifierType">

/*51*/PNOBG-1010101010</saml:AttributeValue>

/*52*/</saml:Attribute>

/*53*/ </saml:AttributeStatement>

/*54*/ </saml:Assertion>

Информацията, записана в примера, се чете така:

Удостоверение ("b07b804c-7c29-ea16-7300-4f3d6f7928ac"), издадено на "2004-12-05T09:22:05" от доставчик на самоличност (https://idp.example.org/SAML2) на субект (3f7b3dcf -1674-4ecd-92c8-1544f346baf8), за да послужи пред доставчик на услуги (https://sp.example.com/SAML2) в интервала от "2004-12-05T09:17:05" до "2004-12-05T09:27:05".

Следва описание на редовете с динамична информация.

„Динамична“ означава, че при сравнение на две различни удостоверения (SAML атестати) разликите ще се именно в тези редове:

Ред (05) е уникален идентификатор за удостоверението (SAML атестат). Използва се UUID стойност (128 бита число в HEX формат). Не се допускат повторения.

Ред (07) е време на създаване на удостоверението. Използва се UTC стойност(ден, час и времева зона).

Ред (09) е уникален идентификатор за доставчик на самоличност. Използва се URN с OID от регистър на ресурсите, раздавано на системите (например "urn:oid:2.16.100.1.1.1.1.16.4.2"). Като алтернатива може да се използва и общопризнат URL.

Редове (10-12) са криптографски подпис върху цялото удостоверение (SAML атестат).

Ред (13-18) са идентичност на субекта. Използва се UUID стойност (128 бита число в HEX формат).

Ред (16) е непрозрачен преходен идентификатор на субекта. Използва се UUID стойност (128 бита число в HEX формат). Идентичността на субекта е скрита поради съображения за неприкосновеност.

„Преходен“ означава, че в две различни удостоверения за един и същи субект ще се получат различни идентификатори за субекта.

„Непрозрачен“ означава, че в него не е кодиран идентификатор на субекта.

Ред (20) е началото на периода на валидност за удостоверението. Използва се UTC стойност (ден, час и времева зона). Препоръчва се разликата с времето на създаване на удостоверението да е положителна и не повече от няколко минути.

Ред (21) е краят на периода на валидност за удостоверението. Използва се UTC стойност (ден, час и времева зона). Препоръчва се разликата с началото на периода на валидност да е положителна и не повече от минута.

Ред (24) е уникален идентификатор на доставчик на услуги. Използва се URN с OID, раздавано на системите (например „urn:oid:2.16.100.1.1.1.1.16.4.2“). Като алтернатива може да се използва и общопризнат URL.

Редове (27-33) са информация за това кога и как субектът се е идентифицирал пред доставчика на самоличност.

Ред (28) е моментът на електронна идентификация на субекта. Използва се UTC стойност (ден, час и времева зона).

Ред (31) е код за начина на идентификация. Използва се URN. Стойностите са предефинирани в „Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0“и ако бъде предоставена единна схема с оценка на нивото на осигуреност на различните доставчици на идентичност. В полето ще се попълва стойност по схемата, дефинирана в eIDAS Levels of Assurance, съответно:

- http://eidas.europa.eu/LoA/low
- http://eidas.europa.eu/LoA/substantial
- http://eidas.europa.eu/LoA/high

(!) Схемите с кодовете за достъп на НАП, НЗОК и НОИ са вариант на парола през защитена сесия или „urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport“.

Редове (35-52) са допълнителна информация за субекта, която доставчик на услуги може да поиска от доставчик на самоличност.

Името на атрибута съответства на използвания в X509 сертификатите по eIDAS за електронна идентификация на Автор/Титуляр.

Очакваните стойности (една или повече) са в съответствие с ETSI EN 319 412-1(V1.1.0 от 2015-12) точки 5.1.3 и 5.1.4. По същата схема на човек с ЕГН „1111111111“ съответства на „PNOBG-1111111111“.

5.2. Атрибути

Атрибут	*Задълж.*	*Примерна стойност*	*тип*	*описание*	*Забележка*
serialNumber	ДА	_9ebc8854ec7f701da9749e87a801e5f2	URI	Референция на доставчик на идентичност	
FamilyName	НЕ	Ivanov	String	Фамилно име	Latin
GivenName	НЕ	Ivan	String	Име	Latin
UniqueIdentifier	ДА	PNOBG-1111111111	Complex	Уникален идентификатор в съответствие с ETSI	
DateOfBirth	НЕ	1979-01-01	Date	Дата на раждане	

XML със SAML saml:Attribute се съдържа в saml:AttributeStatement, а той се съдържа в saml:Assertion.

6. Доставчици на идентификация и средства за електронна идентификация

6.1. Нива на осигуреност

Нивото на осигуреност характеризира степента на надеждността и качеството на средствата за електронна идентификация в процеса на установяване на самоличността.

- Средствата за електронна идентификация имат три нива на осигуреност – „ниско“, „значително“ и „високо“, в съответствие с Регламент 910/2014 г., като критериите за определяне на нивото на осигуреност на електронния идентификатор са специфицирани в Регламент 1502/2015 г.;

- Председателят на ДАЕУ поддържа списък на средствата за електронна идентификация при достъп до ресурсите на електронното управление. Посочените средства могат да се използват и за други цели, ако страните се договорят за това;
- Съгласно чл.7в, т.21 от ЗЕУ, Председателят на ДАЕУ изгражда и поддържа национален Център за електронна идентификация и осъществява функции във връзка с електронната идентификация по ред, определен със Закона за електронната идентификация;
- Съгласно чл.7в, т.22 от ЗЕУ, Председателят на ДАЕУ осъществява правомощия по Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ, L 257/73 от 28 август 2014 г.), наричан по-нататък "Регламент (ЕС) № 910/2014;
- Съгласно чл.7в, т.1 от ЗЕУ, Председателят на ДАЕУ провежда държавната политика в областта на електронната идентификация.

6.2. Нива на осигуреност при достъп до електронни административни услуги (ЕАУ) и информация от регистри и бази данни

- Нивото на осигуреност на всеки ресурс от електронното управление се определя от неговия собственик, т.е. от административния орган, който го предоставя
- В регистъра за достъп до ресурсите на електронното управление за всеки информационен ресурс е установено предварително определеното по разработена от ДАЕУ методика за ниво на осигуреност.
- В Административния регистър, поддържан от Министерски съвет, е установено нивото на осигуреност на ЕАУ, като същите са достъпни през Регистър на ресурсите.

7. Стандарти и протоколи

В този раздел са описани протоколите, средите и каналите на взаимодействие и атрибутите, предавани в SAML2 атестата.

7.1. Стандарт за реализация на SSO

Възможно е въвеждането на SSO чрез употребата на session cookies или чрез портална сесия през Единния портал за достъп до електронни услуги, поддържан от ДАЕУ. Порталната сесия ще предоставя на потребителите изживяване с еднократен вход, ако достъпваните през портала ресурси изискват еднакво ниво на осигуреност. Вече автентикираното лице пред портала автоматично се преавтентикира при опити да достъпи нов ресурс.

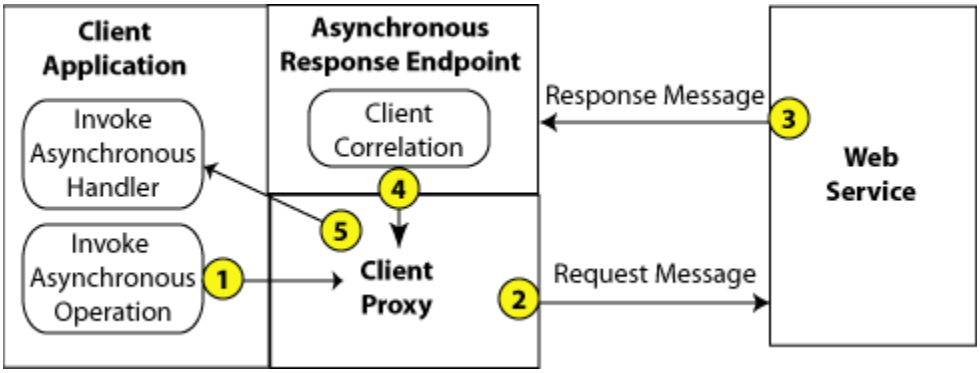
7.2. Протокол за интеграция между еАвтентикация и доставчик на идентификационни услуги

Комуникацията се осъществява посредством SOAP уеб услуги и използва протокол на базата на WSDL, отговарящ на изискванията и препоръките на WS-I Basic Profile 2.0. Това улеснява интеграцията на доставчици на идентичност, които използват разнородни програмни средства, като предоставя добре документиран протокол. За гарантиране на сигурността на предаваната

информация ще се използва сигурен канал за комуникация между системите на базата на TLS 1.2 с използването на доверени сертификати.

За автентикация на системите ще се използват средствата на еАвтентикация. Комуникацията в описания протокол ще се основава на криптирани и подписани XML съобщения с използване на стандарта WS-Security.

Протоколът ще предоставя асинхронен модел за комуникация с периодично запитване за отговор (polling). Целта на модела е да се предостави гъвкавост на различните доставчици на идентичност с различни методи на идентификация, които не могат да се извършват в синхронен режим.



Фиг. 4. Модел за асинхронна комуникация с периодично запитване за отговор

С цел осигуряване на комфорт при използване еАвтентикация, дефинира се ограничение, че една заявка не може да продължава повече от 60 секунди (като продължителността е конфигурирана). След изтичане на периода на изчакване еАвтентикация връща грешка, която указва изтекъл период на изчакване.

Предоставяните методи от еАвтентикация за интеграция с доставчици на идентичност са както следва:

- **identityCallback** – еАвтентикация предоставя възможност за допълнителна информация и/или потвърждение за целите на идентификацията. Извикването не е задължително и се осъществява в зависимост от нуждите на доставчика на идентичност. Методът предоставя възможност за голяма комбинация от мета-данни за покриване на максимален брой сценарии.

Предоставяните от доставчика на идентичност WSDL методи са както следва:

- **identityInquiry** – запитване за самоличността;
- **getResult** – получаване на резултат от идентификация.

7.3. Структура на предаваните съобщения

За максимална гъвкавост при размяната на съобщения е предвидена и допълнителна опционална стъпка за събиране на допълнителна идентифицираща информация от потребителя и/или други потвърждаващи действия.

Параметрите на методите за комуникация са както следва:

1. **identityInquiry**: като параметри приема

- relyingPartyId - уникален идентификатор на доставчик на услуги, OID от регистъра на ресурсите;
- RelyingPartyRequestId – уникален идентификатор на заявката. Създава се еАвтентикация и се използва за получаване на резултата;
- UserID – потребителско име/ПИК (незадължително поле);
- password – парола (незадължително поле).

Резултат: ResultStatus на заявката. Съдържа статус за грешка или за потвърждение и флаг при нужда от допълнителна информация, изискваща identityCallback.

2. **getResult** – параметри на метода

- RelyingPartyRequestId – уникален идентификатор на заявката.

Резултатът от изпълнението съдържа полета, нужни за издаване на SAML атестат от еАвтентикация. Полетата са както следва:

IdentityResponce:

- FamilyName – фамилно име на идентифицираното лице;
- GivenName – други имена на лицето;
- UniqueIdentifier – уникален идентификатор във формат съгласно ETSI EN 319 412-1;
- DateOfBirth – дата на раждане.

Всички полета са незадължителни с изключение на UniqueIdentifier.

3. **identityCallback** – методът е опционален и служи за получаване на допълнителна информация. За целта структурата на параметрите е с променлив размер, като всички параметри са незадължителни.

- RelyingPartyRequestId – уникален идентификатор на заявката;
- userDataForms <key [String], value[String]> - тук се предават нужните полета, изискващи данни от потребителя;
- BinaryResorce – ресурс за визуализация, който се предава с използването на MTOM механизъм.

Резултат: callbackResponce е с параметри както следва:

- Status – code за резултата от изпълнение;
- userDataForms <key [String], value[String]> - модифицираните от потребителя данни от формата за запитване.