DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

Popis eGON služby

E04 - robAutentizace

Typ dokumentace:	Technická
Autor:	Digitální a informační agentura
Účel:	Popis eGON služeb v rámci základních registrů

Verze:	01.00
Datum aktualizace:	25. 12. 2016
Počet stran:	9

Obsah

2 Účel dokumentu

Účelem tohoto dokumentu je především poskytnout orgánům veřejné moci, obecně uživatelům Základních registrů, jednoduchý a srozumitelný popis jak používat příslušnou eGON službu, včetně informací pro IT pracovníky orgánů veřejné moci. Změny provádí SZR.

3 Funkcionalita služby

Služba *E04 robAutentizace* zprostředkuje ověření identity fyzické osoby prostřednictvím elektronického identifikačního dokladu.

4 Základní informace o službě

Název služby	**robAutentizace**
Označení služby	**E04**
Verze služby	**V1**
Publikována v katalogu služeb od verze	
Platnost od	**1. 7. 2012**
Platnost do	
Stav služby	**Aktivní**
Nahrazena službou	
Nahrazuje službu	
Třída služby	S1
Dostupnost služby, potřebná oprávnění	**Veřejná služba, ověření dle registrace.**
Režim služby	Synchronní i asynchronní
SLA služby	SLA-01

5 Historie služby

Verze služby	**Aktuální stav verze**	**Publikovaná v produkčním prostředí**		**Popis změn oproti předchozí verzi**
		Od	**Do**	
V1	aktivní	1. 7. 2012		Prvotní verze

6 Účel služby - detailní popis

Služba *E04 robAutentizace* zprostředkuje ověření identity fyzické osoby prostřednictvím elektronického identifikačního dokladu a BOK tohoto dokladu.

7 Věcná pravidla vztahující se ke zpracování služby

7.1 Primární zpracování

Je provedeno ověření zašifrované hodnoty BOK elektronického dokladu. Služba vrací výsledek ověření správnosti šifrované hodnoty BOK na vstupu služby.

7.2 Referenční odkazy

Služba neprovádí žádné zpracování referenčních odkazů.

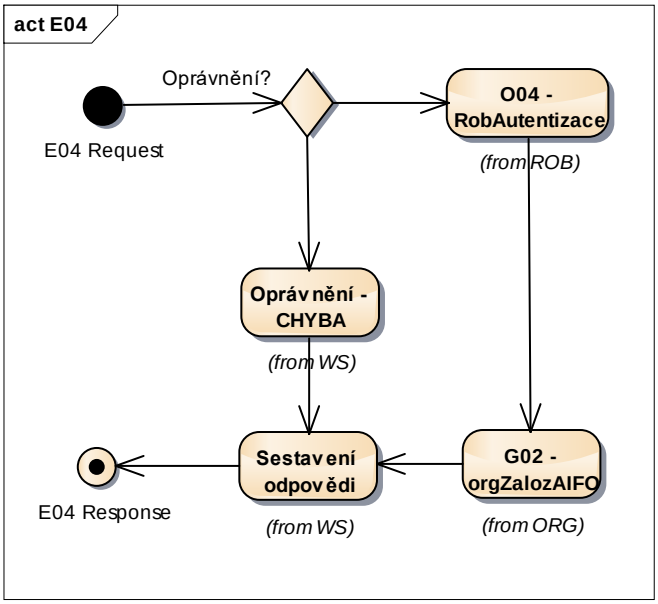
8 Rozpad eGon služby na primitivní služby

8.1 Seznam a popis využívaných primitivních služeb

V rámci zpracování jsou využívány následující interní služby:

- *O04 – robAutentizace* – služba zprostředkuje zjištění identity fyzické osoby prostřednictvím elektronického identifikačního dokladu.
- *G02 – orgZalozAIFO* - služba zprostředkuje překlad AIFOzdr na AIFOcil, nebo vygeneruje nové AIFO.

8.2 Workflow zpracování služby



9 Vstupní údaje

Vstupní údaje obsahují běžné položky definované v datovém typu *RrobAutentizaceType*. Bez správného vyplnění vstupních údajů nelze transakci zpracovat.

9.1 ZadostInfo

Položka *ZadostInfo* představuje standardní hlavičku datové zprávy dotazu, která je odesílána ke zpracování. Struktura a obsah hlavičky zprávy jsou dány datovým typem *ZadostInfoType*. Obsahuje údaje, které ISZR vyžaduje pro ověření přístupu ke službě. Povinné položky musí být vyplněny.

Položky *Subjekt, Uzivatel a DuvodUcel* musí být vždy vyplněny.

9.2 AutorizaceInfo

Pokud se uvádí na vstupu seznam údajů, je třeba specifikovat položky *Aifo*, *Doklad* a *Bok.*

9.3 Zadost

Položka *Zadost* slouží k detailní specifikaci požadavků na službu. Vstupní parametry jsou uvedeny v elementu *RobAutentizaceData*.

V tomto elementu se specifikují parametry autentizace. Minimální povolené kombinace jsou:

- *Cislo*, *Druh*

V parametrech je možné zadat i šifrovanou hodnotu BOK. Autentizace se vždy provádí podle všech zadaných parametrů v logickém součinu.

9.3.1 Šifrování BOK

Pro šifrování BOK je využito schéma využívající hybridní šifrování založené na šifrování zprávy symetrickým algoritmem, kterého klíč je následně zašifrován asymetrickým algoritmem

Do ROB je předáván zašifrovaný řetězec, který bude označován jako „**hlavní řetězec (HŘ)**“. Nezašifrovaný řetězec HŘ vznikne zřetězením následujících položek (zde symbolem || rozumíme pouze operaci zřetězení, nejedná se o znak vkládaný do řetězce):

HŘ = Čas v AIS || Kód agendy || Příznak operace || ID žádosti (volání WS) || Typ dokladu || Číslo dokladu || rezerva || BOK

V následující tabulce je uvedena velikost a vysvětlení jednotlivých položek tvořících HŘ. Všechny hodnoty použité v HŘ jsou známé nebo přímo generovány AIS volajícím webové služby. V HŘ není použit žádný oddělovač polí.

Položka	Popis	Velikost	Formát/hodnota
Čas v AIS	Jedná se o čas v UTC identifikující okamžik, kdy editorský AIS vytvořil zašifrovanou zprávu (a odeslal jí); za tímto účelem je vyžadována synchronizace hodin AIS se zdrojem přesného času	14B ASCII text	YYYYMMDDHHMMSS
Kód agendy	Kód agendy, která volá služby ROB	36B ASCII text	V případě kratšího BOKu je blok doplněn znakem mezera zleva.
Příznak operace	Příznak určující zdali je tento zašifrovaný blok dat ve volání služby ověřující nebo nastavující BOK	1B	‚0' … ověřování BOK ‚1' … nastavování BOK
ID žádosti	UUID žádosti, který byl vygenerován v AIS.	36B ASCII text	AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEEE
Typ dokladu	Druh elektronicky čitelného dokladu.	2B ASCII text	Např. hodnota 'ID'
Číslo dokladu	Číslo dokladu, ke kterému je nastavován BOK	9B ASCII text	
Rezerva		10B	
BOK	Samotná hodnota BOKu	10B ASCII text	V případě kratšího BOKu je blok doplněn znakem mezera zleva.

Pro **šifrování** vytvořeného **řetězce HŘ** je použito schéma založené na hybridním šifrování, které pro šifrování řetězce HŘ používá symetrický algoritmus AES s náhodně voleným symetrickým klíčem a nulovým IV a pro zašifrování tohoto symetrického klíče je použit asymetrický algoritmus RSA s veřejným klíčem ROB (ROB zveřejňuje svůj certifikát). Struktura zprávy odpovídá standardu PKCS#7 (PKCS#7 enveloped message, lze použít i CMS/PKCS#7). Jsou uplatňovány následující vstupní předpoklady:

Symetrický šifrovací algoritmus: AES-128 v CBC módu
Použití AES: šifrování řetězce HŘ s BOK
Délka vstupního bloku AES: 16 B (128 bitů)
Délka výstupního bloku AES: 16 B (128 bitů)
Schéma šifrování AES: AES128/CBC/PKCS7Padding
Velikost IV pro AES: 16B nulový IV

Délka vstupního textu:	128 B (14B čas v AIS + 36B kód agendy + 1B příznak operace + 36B ID žádosti + 2B typ dokladu + 9B číslo dokladu + 10B rezerva + 10B BOK + 10B PKCS7Padding)
Asymetrický šifrovací algoritmus:	RSA s délkou klíče 2048 bitů
Použití RSA:	šifrování symetrického klíče pro AES
Délka vstupního bloku RSA:	256B (2048 bitů)
Délka výstupního bloku RSA:	256B (2048 bitů)
Schéma šifrování RSA:	RSA/ECB/PKCS1Padding
Délka vstupního textu:	256B (16B délka AES klíče + 240B PKCS1Padding)
Formátování zprávy:	PKCS #7 Enveloped message (lze použít i CMS/PKCS7)
Velikost encMSG:	cca 560 B (odhad, reálně velikost mezi 400 B a 1000 B)

Při šifrování jsou použity následující skutečnosti:

- Klíč AES je generován náhodně pro každý řetězec HŘ. Jeho generování (a tím i jeho náhodnost) zajišťuje AIS volající služby. AIS je odpovědný za to, že nebude používat stejný klíč AES pro šifrování různých volání služeb.
- Pro šifrování algoritmem AES je použit nulový IV, který následně není se zašifrovaným řetězcem HŘ přenášen z AIS do ROB.
- Pro šifrování náhodně generovaného klíče AES je použit veřejný RSA klíč certifikátu ROB, který poskytne ROB všem AIS. Pro všechny AIS bude používán jeden certifikát ROB. Generování, uchovávání (zejména ochranu soukromého klíče) a správu tohoto certifikátu včetně jeho parametrů zajistí ROB (certifikát bude vydaný pravděpodobně CA ISZR a privátní klíč certifikátu bude uložený v ROB).
- Některé položky obsažené v řetězci HŘ jsou duplicitní s parametry volání webové služby a to z důvodu jejich následné kontroly v ROB, která je prováděna při zpracování zprávy. Tento přístup zamezuje použití vytvořeného řetězce HŘ v jiném volání služby.

Výsledná hodnota je pak vytvořena následovně:

- **encMSG = PKCS#7 (RSA (AES klíč), AES (HŘ))**

10 Kontroly při volání služby

Na vstupu jsou prováděny běžné kontroly na oprávnění při volání služby.

11 Příklad volání služby

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:cz:isvs:iszr:schemas:IszrRobAutentizace:v1"
xmlns:urn1="urn:cz:isvs:iszr:schemas:IszrAbstract:v1"
xmlns:urn2="urn:cz:isvs:reg:schemas:RegTypy:v1"
xmlns:urn3="urn:cz:isvs:rob:schemas:RobDotazyData:v1">
   <soapenv:Header/>
   <soapenv:Body>
      <urn:RobAutentizace>
```

```
         <urn1:ZadostInfo>
            <urn2:CasZadosti>2011-12-07T10:17:00.000Z</urn2:CasZadosti>
            <urn2:Agenda>A115</urn2:Agenda>
            <urn2:AgendovaRole>CR829</urn2:AgendovaRole>
            <urn2:Ovm>00007064</urn2:Ovm>
            <urn2:Ais>33</urn2:Ais>
            <urn2:Subjekt>Subjekt1</urn2:Subjekt>
            <urn2:Uzivatel>Uzivatel1</urn2:Uzivatel>
            <urn2:DuvodUcel>Důvod a Účel1</urn2:DuvodUcel>
            <urn2:AgendaZadostId>3c840744-942f-443e-9125-43af5a391cb8</urn2:AgendaZadostId>
            <urn2:IszrZadostId>3c840744-942f-443e-9125-43af5a391cb8</urn2:IszrZadostId>
         </urn1:ZadostInfo>
         <urn:Zadost>
            <urn:RobAutentizaceData>
               <urn3:Cislo>1</urn3:Cislo>
               <urn3:Druh>X</urn3:Druh>
            </urn:RobAutentizaceData>
         </urn:Zadost>
      </urn:RobAutentizace>
   </soapenv:Body>
</soapenv:Envelope>
```

12 Výstupní údaje

Výstupní údaje obsahují položky definované v datovém typu *robAutentizaceResponseType*.

12.1 OdpovedInfo

Struktura položky *OdpovedInfo* obsahuje údaje, které ISZR ale i AIS očekává k dokončení vyřízení požadavku. Struktura a obsah hlavičky zprávy jsou dány datovým typem *OdpovedInfoType*.

12.1.1 Stavy

Stav provedení služby je uveden v elementu *Status/VysledekKod*:

- OK – služba byla zpracována v pořádku
- CHYBA – zpracování není možné provést

Pokud skončí služba stavem *CHYBA* a jsou známy detailnější informace, jsou podrobnosti uvedeny v elementu *VysledekDetail*.

Stav CHYBA nastává v situacích:

Situace	**VysledekSubKod**	**Aplikační VysledekSubKod**	**Aplikační VysledekPopis**
Nenalezeno podle dokladu v ROB	APLIKACNI CHYBA	OBECNA CHYBA SLUZBY	CHYBA_0404: Doklad nebyl nalezen.
Nesprávně zašifrovaný BOK	APLIKACNI CHYBA	OBECNA CHYBA SLUZBY	CHYBA_0032: Neprovedla se konverze WS
Chyba v seznamu údajů	NENI OPRAVNENI	NENI OPRAVNENI	CHYBA_0403: Chybný seznam údajů.

Stav CHYBA dále může nastat v situacích, kdy službu nebylo možné z nějakého závažného důvodu vykonat nebo sestavit odpověď. Příklady situací, ve kterých vzniká tato chyba, je chybný vstup služby, nedostupnost databáze a podobně.

12.2 RobOdpoved

Položka je vyplněna, pokud bylo provedeno volání ROB. Výsledky zpracování v ROB jsou uvedeny v elementu *RobAutentizaceDataResponse. V odpovědi je uveden status ověření dle vstupních parametrů.*

13 Příklad odpovědi

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:autocont1="urn:cz:isvs:iszr:services:IszrRuianSouboryZmen:v1"
xmlns:abs="urn:cz:isvs:iszr:schemas:IszrAbstract:v1"
xmlns:e04="urn:cz:isvs:iszr:schemas:IszrRobAutentizace:v1"
xmlns:reg="urn:cz:isvs:reg:schemas:RegTypy:v1" xmlns:xlinl="http://www.w3.org/1999/xlink"
xmlns:rod="urn:cz:isvs:rob:schemas:RobDotazyData:v1"
xmlns:rob="urn:cz:isvs:rob:schemas:RobTypy:v1">
  <soapenv:Header />
  <soapenv:Body>
    <e04:RobAutentizaceResponse>
      <abs:OdpovedInfo>
        <reg:CasOdpovedi>2016-12-25T17:46:48.5446991+01:00</reg:CasOdpovedi>
        <reg:Status>
          <reg:VysledekKod>OK</reg:VysledekKod>
        </reg:Status>
        <reg:AgendaZadostId>b611f281-29ef-4d52-8d75-e271e827ebd2</reg:AgendaZadostId>
        <reg:IszrZadostId>98decdac-df2e-13c0-9513-17c1773a1001</reg:IszrZadostId>
      </abs:OdpovedInfo>
      <abs:MapaAifo lokalniAifoOd="2">
        <reg:PrevodAifo>
          <reg:LokalniAifo stavOvereniAifo="true">1</reg:LokalniAifo>
          <reg:GlobalniAifo>uQ9L7DIWroY9dQHNbK9DNR8=</reg:GlobalniAifo>
        </reg:PrevodAifo>
      </abs:MapaAifo>
      <e04:RobOdpoved>
        <e04:RobAutentizaceDataResponse>
          <rod:RobAplikacniStatus>
            <rob:VysledekRobKodType>OK</rob:VysledekRobKodType>
          </rod:RobAplikacniStatus>
          <rod:Aifo>1</rod:Aifo>
        </e04:RobAutentizaceDataResponse>
      </e04:RobOdpoved>
    </e04:RobAutentizaceResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

14 Notifikace změn

Služba není editační, notifikace změn pro ni není relevantní.

15 Chybová hlášení

Služba neobsahuje specifická chybová hlášení.

16 Odkazy na další dokumenty

16.1 Definice služby

WSDL služby: egon/wsdl/IszrRobAutentizace.wsdl
XSD služby: egon/xsd/IszrRobAutentizace.xsd