

Popis eGON služby

E345 - iszrOverCertifikat

| | | | |
|-----------------------|---|---------------------------|------------|
| Typ dokumentu: | Technická | Verze: | 1.00 |
| Autor: | Digitální a informační agentura | Datum aktualizace: | 05.12.2024 |
| Účel: | Popis eGON služeb v rámci základních registrů | Počet stran: | 8 |

Obsah

| | | |
|-----------|---|----------|
| 1 | Účel dokumentu..... | 3 |
| 2 | Funkcionalita služby..... | 3 |
| 3 | Základní informace o službě..... | 3 |
| 4 | Historie služby..... | 3 |
| 5 | Účel služby - detailní popis..... | 3 |
| 6 | Věcná pravidla vztahující se ke zpracování služby..... | 4 |
| 6.1 | Primární zpracování..... | 4 |
| 7 | Rozpad eGon služby na primitivní služby..... | 4 |
| 7.1 | Seznam a popis využívaných primitivních služeb..... | 4 |
| 7.2 | Workflow zpracování služby..... | 4 |
| 8 | Vstupní údaje..... | 5 |
| 8.1 | ZadostInfo..... | 5 |
| 8.2 | AutorizaceInfo..... | 5 |
| 8.3 | Zadost..... | 5 |
| 9 | Kontroly při volání služby..... | 5 |
| 10 | Příklad volání služby..... | 5 |
| 11 | Výstupní údaje..... | 6 |
| 11.1 | OdpovedInfo..... | 6 |
| 11.1.1 | Stavy..... | 6 |
| 11.2 | IszrOdpoved..... | 6 |
| 12 | Příklad odpovědi..... | 7 |
| 13 | Notifikace změn..... | 7 |
| 14 | Chybová hlášení..... | 7 |
| 15 | Odkazy na další dokumenty..... | 8 |
| 15.1 | Definice služby..... | 8 |
| 15.2 | Egon služby..... | 8 |

1 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 DIA.

2 Funkcionalita služby

Služba *E345 iszrOverCertifikat* slouží volajícím k validaci certifikátu a normalizaci údajů o certifikátu na základě odeslaného těla certifikátu.

3 Základní informace o službě

| | |
|--|---------------------------------|
| Název služby | iszrOverCertifikat |
| Označení služby | E345 |
| Verze služby | V1 |
| Publikována v katalogu služeb od verze | |
| Platnost od | 5. 12. 2024 |
| Platnost do | |
| Stav služby | Aktivní |
| Nahrazena službou | |
| Nahrazuje službu | |
| Třída služby | S4S |
| Dostupnost služby, potřebná oprávnění | Veřejná, ověření dle registrace |
| Režim služby | Synchronní |
| SLA služby | SLA-04 |

4 Historie služby

| Verze služby | Aktuální stav verze | Publikovaná v produkčním prostředí | | Popis změn oproti předchozí verzi |
|--------------|---------------------|------------------------------------|----|-----------------------------------|
| | | Od | Do | |
| V1 | Aktivní | 5. 12. 2024 | | Prvotní verze |
| | | | | |
| | | | | |
| | | | | |

5 Účel služby - detailní popis

Služba *E345 iszrOverCertifikat* slouží volajícím k validaci certifikátu a normalizaci údajů o certifikátu na základě odeslaného těla veřejné části certifikátu.

Cílem služby je jednak možnost ověřit, zda jde o kvalifikovaný certifikát ve smyslu nařízení *eIDAS*, a dále získat atributy certifikátu ve formátu, ve kterém jsou tyto informace uloženy v ROB.

6 Věcná pravidla vztahující se ke zpracování služby

Pro zpracování služby je zapotřebí oprávnění přístupu k ISZR.

6.1 Primární zpracování

ISZR na základě žádosti provede normalizaci a validaci souboru certifikátu.

V rámci validace se ověřuje, zda se jedná o kvalifikovaný certifikát ve smyslu nařízení *eIDAS*.

V rámci normalizace se z certifikátu extrahuje informace o sériovém čísle a vydavateli certifikátu ve formátu, který je kompatibilní s uložením těchto informací v ROB.

Poznámky:

- Pro ověření se využívá implementace nad knihovnu EU „DSS Digital Signature Services“: [https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eSignature+FAQ#eSignatureFAQ-DigitalSignatureServices\(DSS\)](https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eSignature+FAQ#eSignatureFAQ-DigitalSignatureServices(DSS))
- Zápis informací o certifikátu do ROB je prováděn prostřednictvím Portálu občana, který v rámci zápisu taktéž využívá tuto eGON službu.

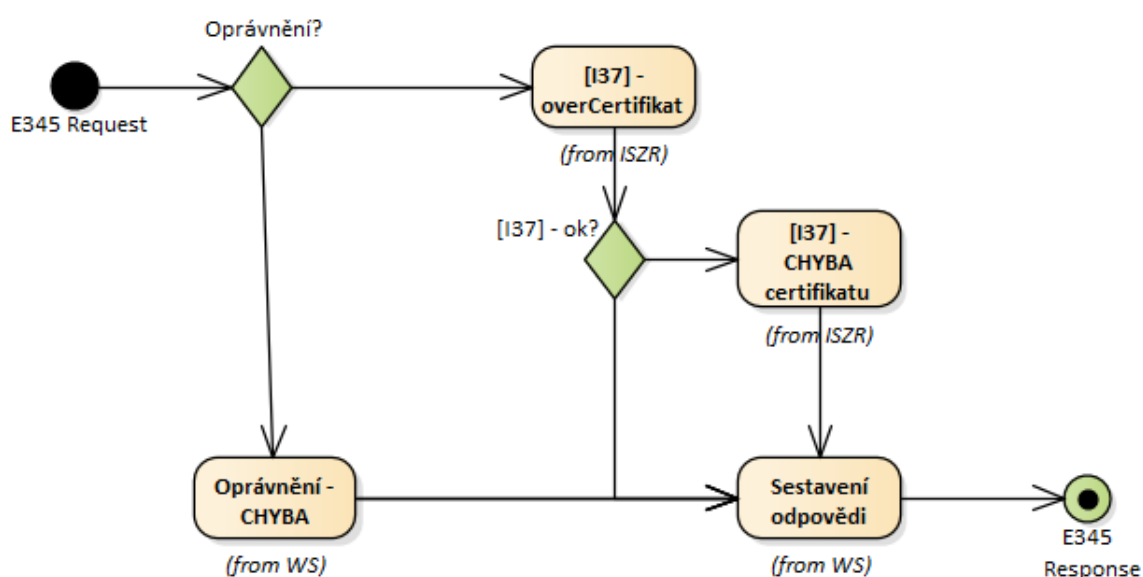
7 Rozpad eGon služby na primitivní služby

7.1 Seznam a popis využívaných primitivních služeb

V rámci zpracování jsou využívány následující interní služby:

- *I37 – iszrOverCertifikat* – normalizuje a ověřuje certifikát proti validátoru

7.2 Workflow zpracování služby



8 Vstupní údaje

Vstupní údaje obsahují standardní položky, definované v typu *IszrOverCertifikatType*. Bez správného vyplnění vstupních údajů nelze transakci zpracovat.

8.1 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.

8.2 AutorizaceInfo

Pro zpracování služby není ve volání nutné specifikovat položku *AutorizaceInfo*.

8.3 Zadost

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

Do elementu *TeloCertifikatu* volající vyplňuje veřejnou část certifikátu ve formě base64 řetězce.

9 Kontroly při volání služby

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

10 Příklad volání služby

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:cz:isvs:iszr:schemas:IszrOverCertifikat:v1"
xmlns:urn1="urn:cz:isvs:iszr:schemas:IszrAbstract:v1"
xmlns:urn2="urn:cz:isvs:reg:schemas:RegTypy:v1"
xmlns:urn3="urn:cz:isvs:iszr:schemas:IszrDataOverCertifikat:v1">
  <soapenv:Header/>
  <soapenv:Body>
    <urn:IszrOverCertifikat>
      <urn1:ZadostInfo>
        <urn2:CasZadosti>2012-05-14T00:00:00.000+02:00</urn2:CasZadosti>
        <urn2:Agenda>Axxx</urn2:Agenda>
        <urn2:AgendovaRole>CRxxx</urn2:AgendovaRole>
        <urn2:Ovm>ovm</urn2:Ovm>
        <urn2:Ais>ais</urn2:Ais>
        <urn2:Subjekt>Subjekt1</urn2:Subjekt>
        <urn2:Uzivatel>Uzivatel1</urn2:Uzivatel>
        <urn2:DuvodUcel>Duvod a Ucel1</urn2:DuvodUcel>
        <urn2:AgendaZadostId>e91f4c1a-5bf7-4a98-a8c5-451110ce680e</urn2:AgendaZadostId>
        <urn2:IszrZadostId>e91f4c1a-5bf7-4a98-a8c5-451110ce680e</urn2:IszrZadostId>
      </urn1:ZadostInfo>
      <urn:Zadost>
        <urn:IszrOverCertifikatData>
          <urn3:TeloCertifikatu>TmVxdWUgcG9ycm8gcXVpc3F1YW0gZXN0LCBxdWkgZG9sb3J1bSBpcHN1bSBxdWlhIGRvbG9yIH
          Np
          dCBhbWV0LCBjb25zZWNoZXRlcWVpYWRpcG1zY2kgdmVsaXQsIHN1ZCBxdWlhIG5vbiBudW1xdWFT
          IGVpdXMgbW9kaSB0ZW1wb3JhIGluY21kdW50IHV0IGxhYm9yZSB1dCBkb2xvcUgUgbWFnbmFtIGFs
          aXF1YW0gcXVhZXXhdCB2b2x1cHRhdGVtLiBEdWl1IHJpc3VzLiBBbG1xdWFTIGVYXQgdm9sdXRw
          YXQuIERvbmVjIHF1aXMgbm1iaCBhdCBmZWxpcyBjb25ndWUgY29tbW9kby4gTW9yYmkgbGVvIG1p
          LCBub251bW15IGVnZXQgdHJpc3RpcXV1IG5vbiwgcmhvbmN1cyBub24gbGVvLiBQcmFlc2VudCBp
          biBtYXVyaXMgZXUgdG9ydG9yIHBvcnR0aXRvciBhY2N1bXNhbi4gTnVsbGEgdHVycG1zIG1hZ25h
          LCBjdXJzdXMgc210IGFtZXQsIHN1c2NpcG10IGEsIGludGVyZHVtIGlkLCBmZWxpcy4gU2VkiHV0
```

```
IHB1cnNwaWNpYXRpcyB1bmRlIG9tbmlzIGlzdGUgYmF0dXMgZlY3Igc210IHZvbHVwdGF0ZW0g  
YWNjdXNhbncRpdW0gZG9sb3JlbXFlZSBsYXVkeW50aXVtLCB0b3RhbSBYZW0gYXB1cm1hbSwgZWFX  
dWUgaXBzYSBxdWFlIGFiIGlscG8gaW52ZW50b3JlIHZ1cm10YXRpcyBldCBxdWFzaSBhcmNoaXRl  
Y3RvIGJlYXRhZSB2aXRhZSBkaWN0YSBzdW50IGV4cGxpY2Fiby4gRnVzY2UgdGVsbHVzLiBEWlZ  
IHB1bH2pbmFyLiBQZWxsZW50ZXNxdWUgcHJldG11bSBsZWN0dXMgaWQgdHVycGlzLiBDdW0gc29j  
aWlZIG5hdG9xdWUgcGVuYXRpYnVzIGV0IG1hZ25pcyBkaXMgcGFydHVyaWVudCBtb250ZXMsIG5h  
c2NldHVyIHJpZGljdWx1cyBtdXMuIEV0aWFTIGRPyY3R1bSB0aW5jaWR1bnQgZGlhbS4gTmFtIGxp  
YmVybyB0ZWlwb3JlLCBjdW0gc29sdXRhIG5vYmlzIGVzdCB1bGlnZW5kaSBvcHRpbyBjdW1xdWUg  
bmloaWwgaWlwZWRpdCBxdW8gbWludXMgaWQgcXVvZCBtYXhpbWUgcGxhY2VhdCBmYWN1cmUgcG9z  
c2ltdXMsIG9tbmlzIHZvbHVwdGFzIGFzc3VtZW5kYSBlc3QsIG9tbmlzIGRvbG9yIHJlcGVsbGVu  
ZHVzLiBQZWxsZW50ZXNxdWUgc2FwaWVulG==</urn3:TeloCertifikatu>  
</urn:IszrOverCertifikatData>  
</urn:Zadost>  
</urn:IszrOverCertifikat>  
</soapenv:Body>  
</soapenv:Envelope>
```

11 Výstupní údaje

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

11.1 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*.

11.1.1 Stav

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* nebo *VAROVANI*, a jsou známy detailnější informace, jsou podrobnosti uvedeny v elementu *VysledekDetail*.

Stav *CHYBA* nastává v případech

- Nevalidní žádost
- Nevalidní data
- Obecná chyba služby

Stav *CHYBA* dále nastane v situaci, kdy službu nebylo možné z nějakého závažného důvodu vykonat nebo sestavit odpověď. Příkladem situace, ve které vzniká tato chyba, je například chybný vstup služby, nedostupnost databáze, nedostupnost validátoru a podobně.

11.2 IszrOdpoved

Obsahuje aplikační status s informací, zda interní zpracování proběhlo v pořádku.

V rámci výstupu služby jsou vydávány následující položky:

- *SerioveCisloCertifikatuHex* – sériové číslo certifikátu v hexadecimálním tvaru
- *Vydavatel* – vydavatel certifikátu
- *PlatnostOd* – datum začátku platnosti certifikátu
- *PlatnostDo* – datum konce platnosti certifikátu
- *KvalifikovanyPriVydani* – boolean informace zda byl certifikát kvalifikovaný při vydání
- *KvalifikovanyPriOvereni* – boolean informace zda byl certifikát kvalifikovaný při ověření

- *CasOvereni* – čas ověření
- *PopisKOvereniCertifikatu* – podrobný popis ověření certifikátu

12 Příklad odpovědi

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:autocont1="urn:cz:isvs:iszr:services:IszrOverCertifikat:v1"
xmlns:abs="urn:cz:isvs:iszr:schemas:IszrAbstract:v1"
xmlns:autocont2="urn:cz:isvs:iszr:schemas:IszrOverCertifikat:v1"
xmlns:reg="urn:cz:isvs:reg:schemas:RegTypy:v1" xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:autocont3="urn:cz:isvs:iszr:schemas:IszrDotazyData:v1"
xmlns:autocont4="urn:cz:isvs:iszr:schemas:IszrTypy:v1"
xmlns:autocont5="urn:cz:isvs:iszr:schemas:IszrDataOverCertifikat:v1">
  <soapenv:Header/>
  <soapenv:Body>
    <autocont2:IszrOverCertifikatResponse>
      <abs:OdpovedInfo>
        <reg:CasOdpovedi>2024-11-01T12:16:32.5593456+01:00</reg:CasOdpovedi>
        <reg:Status>
          <reg:VysledekKod>OK</reg:VysledekKod>
        </reg:Status>
        <reg:AgendaZadostId>e91f4c1a-5bf7-4a98-a8c5-451110ce680e</reg:AgendaZadostId>
        <reg:IszrZadostId>71faada0-e638-1418-9154-192dc0b8b000</reg:IszrZadostId>
      </abs:OdpovedInfo>
      <autocont2:IszrOdpoved>
        <autocont2:IszrOverCertifikatDataResponse>
          <autocont3:IszrAplikacniStatus>
            <autocont4:VysledekIszrKodType>OK</autocont4:VysledekIszrKodType>
          </autocont3:IszrAplikacniStatus>

          <autocont5:SerioveCisloCertifikatuHex>0166ABC2</autocont5:SerioveCisloCertifikatuHex>
          <autocont5:Vydavatel>cn=postsignum qualified ca 4,o=česká pošta\,
s.p.,2.5.4.97=ntrcz-47114983,c=cz</autocont5:Vydavatel>
          <autocont5:PlatnostOd>2024-10-11T16:45:41</autocont5:PlatnostOd>
          <autocont5:PlatnostDo>2025-10-31T16:45:41</autocont5:PlatnostDo>
          <autocont5:KvalifikovanyPriVydani>1</autocont5:KvalifikovanyPriVydani>
          <autocont5:KvalifikovanyPriOvereni>1</autocont5:KvalifikovanyPriOvereni>
          <autocont5:CasOvereni>2024-11-01T12:16:32</autocont5:CasOvereni>

          <autocont5:PopisKOvereniCertifikatu>DotNetValid|QEuValidationDone|QEuTimeDifferenceOk|QEuQualifi
cationAtIssueOk|QEuQualificationAtVerifyOk</autocont5:PopisKOvereniCertifikatu>
        </autocont2:IszrOverCertifikatDataResponse>
      </autocont2:IszrOdpoved>
    </autocont2:IszrOverCertifikatResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

13 Notifikace změn

Služba není editační, notifikace změn pro ni není relevantní.

14 Chybová hlášení

Služba neobsahuje specifická chybová hlášení.

15 Odkazy na další dokumenty

15.1 Definice služby

WSDL služby: [egon/wsd/IszrOverCertifikat.wsdl](#)

XSD služby: [egon/xsd/IszrOverCertifikat.xsd](#)

15.2 Egon služby

[DIA_popis_eGON_sluzeb_E344_iszrRobCtiPodleCertifikatu.doc](#)