Vybudování IS DMVS

Popis služby R1b - Služba pro údržbu autentizačních certifikátů

pro verzi 2.0.2

Historie změn dokumentu

Verze	Datum	Autor	Změny
1	14.9.2022	ACE	
2	23.3.2023	ACE	Změna příkladů volání služby kvůli změně formátu UID

Obsah

1 R1b Služba pro údržbu autentizačních certifikátů 3
1.1 Charakteristika služby 3
1.2 Historie změn služby 3
1.3 Detailní popis služby 3
1.4 Operace služby 4
1.4.1 nahrajCertifikat 4
1.4.2 zneplatniCertifikat 6
1.5 Varovná hlášení a chyby 7
1.6 Odkazy na další dokumenty 7

1 R1b Služba pro údržbu autentizačních certifikátů

1.1 Charakteristika služby

Skupina	Správa údajů o subjektech
Kód služby	R1b
Business název služby	Služba pro údržbu autentizačních certifikátů
Název služby	R1bUdrzbaCertifikatu
Stručný popis služby	Služba umožňuje vložení nebo zneplatnění autentizačních certifikátů pro WS, kterými se subjekty autentizují vůči WS rozhraní IS DMVS.
Poskytuje	IS DMVS
Užívá (volá)	Registrovaný subjekt
Typ služby	WS Synchronní
Verze služby	1
Platnost od	-
Platnost do	-
Stav služby	Produkce
Nahrazena službou	-
Nahrazuje službu	-

1.2 Historie změn služby

Verze služby	**Aktuální stav verze**	**Publikovaná v produkčním prostředí**		**Publikovaná v integračním prostředí**		**Popis změn oproti předchozí verzi**
		Od	**Do**	**Od**	**Do**	
1	Produkce	3.5.2024		3.4.2023		

1.3 Detailní popis služby

Služba R1bUdrzbaAutentizacnichCertifikatu je rozdělena na dvě operace. První operace na vstupu příjme certifikát a označení subjektu, ke kterému má být certifikát nahrán. Druhá

operace přijme certifikát k zneplatnění a označení subjektu, u kterého má být certifikát zneplatněn. Výstupem první i druhé operace je potvrzení zpracování.

Věcná pravidla vztahující se ke zpracování služby

Předpokladem úspěšného provedení operace pro přidání certifikátu je zadání ID existujícího subjektu a validní certifikát. Certifikát musí být vydaný jednou z následujících CA:

- První certifikační autorita, a. s.,
- Česká pošta, s. p. / PostSignum,
- eIdentity, a. s.

Předpokladem pro úspěšné provedení operace pro zrušení certifikátu je zadání ID existujícího subjektu a certifikát, který je k tomuto subjektu v IS DMVS evidován.

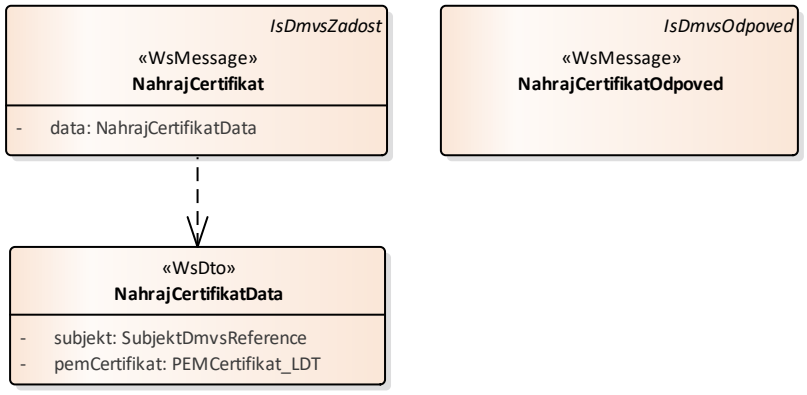
Autorizace

Subjekt může nahrávat a zneplatňovat pouze svoje certifikáty.

1.4 Operace služby

1.4.1 nahrajCertifikat

Tato operace přijme ID subjektu a autentizační certifikát v PEM formátu. Služba zkontroluje existenci subjektu s daným ID v systému a v případě nevalidního ID končí s chybou. Obdobně se zkontroluje, zda již není certifikát registrován, validita certifikátu, vydavatel certifikátu a případně se vrátí chyba. Pokud je vstup validní, pak se zaslaný certifikát přiřadí k subjektu. Všechny dosavadní existující certifikáty pro tento subjekt zůstávají v platnosti.



Vstupní údaje

Vstupní zpráva *NahrajCertifikat* obsahuje ID subjektu a nahrávaný certifikát ve formátu PEM.

Výstupní údaje

Odpověď první operace *NahrajCertifikatOdpoved* vrací v hlavičce výsledek požadavku.

Kontroly při volání služby

Na vstupu jsou prováděny běžné kontroly na existenci odkazovaných entit a oprávnění při volání služby. Dále jsou prováděny tyto kontroly:

- Kontrola vydávající CA.
- Kontrola, zda již certifikát není zaregistrován.

Příklad volání služby

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:cz:isvs:dmvs:isdmvs:schemas:R1bUdrzbaCertifikatu:v1"
xmlns:urn1="urn:cz:isvs:dmvs:common:schemas:Messages:v1"
xmlns:urn2="urn:cz:isvs:dmvs:common:schemas:Subjekty:v1">
   <soapenv:Header/>
   <soapenv:Body>
      <urn:NahrajCertifikat>
         <urn1:Hlavicka>
            <urn1:UidZadosti>fc6bbe85-8ed7-4fbc-b886-b2fd9547c369</urn1:UidZadosti>
         </urn1:Hlavicka>
         <urn:Data>
            <urn:Subjekt>
               <urn2:Id>SUBJ-00000000</urn2:Id>
            </urn:Subjekt>
            <urn:PemCertifikat>-----BEGIN CERTIFICATE-----
MIIEDjCCAfYCAw9CQDANBgkqhkiG9w0BAQsFADBWMQswCQYDVQQGEwJYWDEVMBMGA1UEBwwMRGVmYXVsdCBDaXR5MRwwGgYDV
QQKDBNEZWZhdWx0IENvbXBhbnkgTHRkMRIwEAYDVQQDDAlsb2NhbGhvc3QwHhcNMjIwMjIyMTAwMzQwWhcNMjQxMTE4MTAwMz
QwWjBCMQswCQYDVQQGEwJYWDEVMBMGA1UEBwwMRGVmYXVsdCBDaXR5MRwwGgYDVQQKDBNEZWZhdWx0IENvbXBhbnkgTHRkMII
BIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3Ql6wFDuXUYGDFZ69fz7moc+Edshk3eMgvVEWQXgT8skfwblfXJppEET
TCyK2H+qEP5imG7nFGkAYG6GYnRYB2ZsJqFvmaSs8dMk6yZPwpC+8bEKyaF2iZ0zEwngC9T2AJACJ026bwWhTwMTCeS4Sq+8a
6X57SGScs7LfMyPEBaFh0uOjdoJ7CWVe9LU4HkDWHJBBMRZjw4eazLyckn9+jVz4zCAV0fSGDc7n96eczJKx4dEOJuHswDRt0
r9Wwdp4L7pnQKoRQ5x+A35AGfNE8q4wrw28u4K37AZxGol2R1g5H9VGiIco3DQF605wWUW4v/62WhJv7VMivn6GIGsmQIDAQA
BMA0GCSqGSIb3DQEBCwUAA4ICAQBQa0mEWgdZzzvGPwRbVzyL+F/nSkmpIH4gTLwLgItfAW3jTl2E2MAi1x0OlH2dD/9gB0Be
8J7nROwuBmoRcgH1k7kze9ZkcnHMYXBxTmELG2J0CT/s913htNK5lU8tLvtkX/L31h9kLEKYLMySyNbLB8nnsFPNA/BnZ3NNv
5f2WROEuW/utymjlOjtEIQY+jIQB13yQzQelsGHwsgslm9mE5VFXvirsZnpM29snVcYwHWMq2tPCs3I6LzUjZ8w35Ayc1cHZL
wHSIxO5fdImHBxeCF9/WKGcc6iSKiIa1T6mqg2cMe4XmiCiuMy7IZSsim9aX/LQriXI8XdMZOgyhalDQzAyhZtNLWAK/jJ0i3
Wl5lK0c2RcIJAMm6yYdyGAA+bZ8Biiz2zy0DBn1CNBdmZN4HpyyVc2mHJYj8ltHOUxGR2yWI7ShiNYx/cuJYK0gvexNGNkVRr
3LDeaPMrDB3fYBAosVrtRbkzR7pCAWBhNLOvBgSGHG5TyLLtGqzA7Ej24GeHKIF/ohyVRf9oNNqVJTc9P/ACyWD8U/sQlILqV
a+ifNmk4apvdjGMoHMSiHHuf/mipvA/0Ad7GINy1YVJ48hivn4BJpn3BMlyFEEdGDIKz2ZSogIZ1tF+hpzgjPWwpBIJPwzMJb
Sml/sVInJaleoh+Xu0cvbtx2asSckocA==-----END CERTIFICATE-----</urn:PemCertifikat>
         </urn:Data>
      </urn:NahrajCertifikat>
   </soapenv:Body>
</soapenv:Envelope>
```

Příklad odpovědi

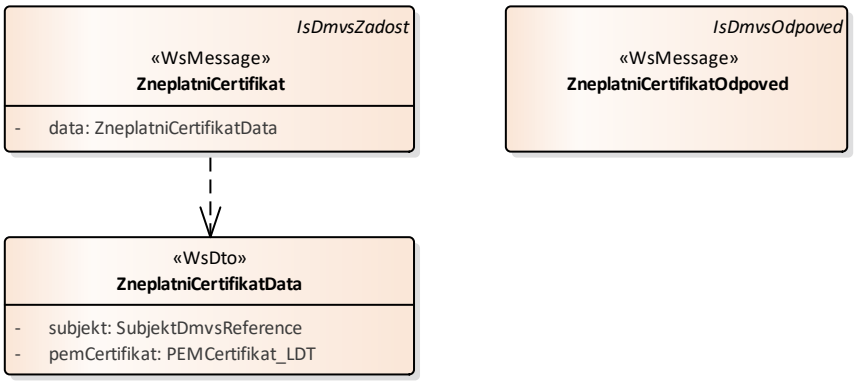
```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <ns21:NahrajCertifikatOdpoved xmlns:ns3="urn:cz:isvs:dmvs:common:schemas:Messages:v1"

xmlns:ns21="urn:cz:isvs:dmvs:isdmvs:schemas:R1bUdrzbaCertifikatu:v1">
         <ns3:Hlavicka>
            <ns3:UidOdpovedi>4081ffa1-7695-4caf-9df7-7b8aa841c257</ns3:UidOdpovedi>
            <ns3:Vysledek stav="OK">
               <ns3:UidZadosti>fc6bbe85-8ed7-4fbc-b886-b2fd9547c369</ns3:UidZadosti>
               <ns3:Hlaseni>
                  <ns3:Hlaseni kod="1000" typ="Informace">
                     <ns3:Zprava>Požadovaná akce byla úspěšně provedena</ns3:Zprava>
                  </ns3:Hlaseni>
```

```
            </ns3:Hlaseni>
         </ns3:Vysledek>
      </ns3:Hlavicka>
   </ns21:NahrajCertifikatOdpoved>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

1.4.2 zneplatniCertifikat

Tato operace přijme ID subjektu a autentizační certifikát v PEM formátu. Služba zkontroluje existenci subjektu s daným ID v systému a v případě nevalidního ID končí s chybou. Obdobně se zkontroluje validita certifikátu a případně se vrátí chyba. Pokud přijatý certifikát není uložen v systému pro přijaté ID subjektu, pak je navrácena chyba. Pokud je přijatý certifikát v systému uložen pro přijaté ID subjektu, pak je uložený certifikát zneplatněn.



Vstupní údaje

Vstupní zpráva *NahrajCertifikat* obsahuje ID subjektu a certifikát k zneplatnění ve formátu PEM.

Výstupní údaje

Odpověď první operace *NahrajCertifikatOdpoved* vrací v hlavičce výsledek požadavku.

Kontroly při volání služby

Na vstupu jsou prováděny běžné kontroly na existenci odkazovaných entit a oprávnění při volání služby. Dále jsou prováděny tyto kontroly:

- Kontrola, zda je certifikát u daného subjektu registrován.

Příklad volání služby

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:urn="urn:cz:isvs:dmvs:isdmvs:schemas:R1bUdrzbaCertifikatu:v1"
xmlns:urn1="urn:cz:isvs:dmvs:common:schemas:Messages:v1"
xmlns:urn2="urn:cz:isvs:dmvs:common:schemas:Subjekty:v1">
   <soapenv:Header/>
```

```
   <soapenv:Body>
      <urn:ZneplatniCertifikat>
         <urn1:Hlavicka>
            <urn1:UidZadosti>fc6bbe85-8ed7-4fbc-b886-b2fd9547c369</urn1:UidZadosti>
         </urn1:Hlavicka>
         <urn:Data>
            <urn:Subjekt>
               <urn2:Id>SUBJ-00000000</urn2:Id>
            </urn:Subjekt>
            <urn:PemCertifikat>-----BEGIN CERTIFICATE-----
MIIEDjCCAfYCAw9CQDANBgkqhkiG9w0BAQsFADBWMQswCQYDVQQGEwJYWDEVMBMGA1UEBwwMRGVmYXVsdCBDaXR5MRwwGgYDV
QQKDBNEZWZhdWx0IENvbXBhbnkgTHRkMRIwEAYDVQQDDAlsb2NhbGhvc3QwHhcNMjIwMjIyMTAwMzQwWhcNMjQxMTE4MTAwMz
QwWjBCMQswCQYDVQQGEwJYWDEVMBMGA1UEBwwMRGVmYXVsdCBDaXR5MRwwGgYDVQQKDBNEZWZhdWx0IENvbXBhbnkgTHRkMII
BIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3Ql6wFDuXUYGDFZ69fz7moc+Edshk3eMgvVEWQXgT8skfwblfXJppEET
TCyK2H+qEP5imG7nFGkAYG6GYnRYB2ZsJqFvmaSs8dMk6yZPwpC+8bEKyaF2iZ0zEwngC9T2AJACJ026bwWhTwMTCeS4Sq+8a
6X57SGScs7LfMyPEBaFh0uOjdoJ7CWVe9LU4HkDWHJBBMRZjw4eazLyckn9+jVz4zCAV0fSGDc7n96eczJKx4dEOJuHswDRt0
r9Wwdp4L7pnQKoRQ5x+A35AGfNE8q4wrw28u4K37AZxGol2R1g5H9VGiIco3DQF605wWUW4v/62WhJv7VMivn6GIGsmQIDAQA
BMA0GCSqGSIb3DQEBCwUAA4ICAQBQa0mEWgdZzzvGPwRbVzyL+F/nSkmpIH4gTLwLgItfAW3jTl2E2MAi1x0OlH2dD/9gB0Be
8J7nROwuBmoRcgH1k7kze9ZkcnHMYXBxTmELG2J0CT/s913htNK5lU8tLvtkX/L31h9kLEKYLMySyNbLB8nnsFPNA/BnZ3NNv
5f2WROEuW/utymjlOjtEIQY+jIQB13yQzQelsGHwsgslm9mE5VFXvirsZnpM29snVcYwHWMq2tPCs3I6LzUjZ8w35Ayc1cHZL
wHSIxO5fdImHBxeCF9/WKGcc6iSKiIa1T6mqg2cMe4XmiCiuMy7IZSsim9aX/LQriXI8XdMZOgyhalDQzAyhZtNLWAK/jJ0i3
Wl5lK0c2RcIJAMm6yYdyGAA+bZ8Biiz2zy0DBn1CNBdmZN4HpyyVc2mHJYj8ltHOUxGR2yWI7ShiNYx/cuJYK0gvexNGNkVRr
3LDeaPMrDB3fYBAosVrtRbkzR7pCAWBhNLOvBgSGHG5TyLLtGqzA7Ej24GeHKIF/ohyVRf9oNNqVJTc9P/ACyWD8U/sQlILqV
a+ifNmk4apvdjGMoHMSiHHuf/mipvA/0Ad7GINy1YVJ48hivn4BJpn3BMlyFEEdGDIKz2ZSogIZ1tF+hpzgjPWwpBIJPwzMJb
Sml/sVInJaleoh+Xu0cvbtx2asSckocA==-----END CERTIFICATE-----</urn:PemCertifikat>
         </urn:Data>
      </urn:ZneplatniCertifikat>
   </soapenv:Body>
</soapenv:Envelope>
```

Příklad odpovědi

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <ns21:ZneplatniCertifikatOdpoved xmlns:ns3="urn:cz:isvs:dmvs:common:schemas:Messages:v1"

xmlns:ns21="urn:cz:isvs:dmvs:isdmvs:schemas:R1bUdrzbaCertifikatu:v1">
         <ns3:Hlavicka>
            <ns3:UidOdpovedi>f99917e9-8f4d-43e7-a641-136c3eb16c01</ns3:UidOdpovedi>
            <ns3:Vysledek stav="OK">
               <ns3:UidZadosti>fc6bbe85-8ed7-4fbc-b886-b2fd9547c369</ns3:UidZadosti>
               <ns3:Hlaseni>
                  <ns3:Hlaseni kod="1000" typ="Informace">
                     <ns3:Zprava>Požadovaná akce byla úspěšně provedena</ns3:Zprava>
                  </ns3:Hlaseni>
               </ns3:Hlaseni>
            </ns3:Vysledek>
         </ns3:Hlavicka>
      </ns21:ZneplatniCertifikatOdpoved>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

1.5 Varovná hlášení a chyby

Služba neprodukuje žádná specifická hlášení. Obecná hlášení jsou specifikována v souboru CUZK_DMVS_zakladni_principy_chovani_sluzeb.pdf.

1.6 Odkazy na další dokumenty

WSDL služby:

dmvs-ws-api/isdmvs-ws-api/wsdl/R1bUdrzbaCertifikatu/R1bUdrzbaCertifikatu-v1.wsdl

XSD služby:

dmvs-ws-api/isdmvs-ws-api/xsd/IsDmvsWsApiV1/R1bUdrzbaCertifikatu/R1bUdrzbaCertifikatu-v1.xsd
dmvs-ws-api/isdmvs-ws-api/xsd/IsDmvsWsApiV1/R1bUdrzbaCertifikatu/NahrajCertifikatData-v1.xsd
dmvs-ws-api/isdmvs-ws-api/xsd/IsDmvsWsApiV1/R1bUdrzbaCertifikatu/NahrajCertifikatOdpoved-v1.xsd
dmvs-ws-api/isdmvs-ws-api/xsd/IsDmvsWsApiV1/R1bUdrzbaCertifikatu/NahrajCertifikat-v1.xsd
dmvs-ws-api/isdmvs-ws-api/xsd/IsDmvsWsApiV1/R1bUdrzbaCertifikatu/ZneplatnitCertifikatData-v1.xsd
dmvs-ws-api/isdmvs-ws-api/xsd/IsDmvsWsApiV1/R1bUdrzbaCertifikatu/ZneplatnitCertifikatOdpoved-v1.xsd
dmvs-ws-api/isdmvs-ws-api/xsd/IsDmvsWsApiV1/R1bUdrzbaCertifikatu/ZneplatnitCertifikat-v1.xsd

Základní principy chování služeb a společné prvky služeb:

CUZK_DMVS_zakladni_principy_chovani_sluzeb.pdf