CONFIDENTIAL
30.10.2026

SAMLINK VARMENNEPALVELU

PALVELUKUVAUS OHJELMISTOTALOILLE

samlink

A Kyndryl Company

Sisällysluettelo

1. Johdanto 3
2. Asiakasohjelmiston varmennehaun käyttötapaukset 3
3. getCertificate-operaatio 4
   3.1 SenderId 4
   3.2 RequestId 4
   3.3 Timestamp 4
   3.4 ApplicationRequest 4
4. CertApplicationRequest 4
   4.1 CustomerId 4
   4.2 Timestamp 4
   4.3 Environment 4
   4.4 SoftwareId 4
   4.5 Command 4
   4.6 ExecutionSerial 4
   4.7 Encryption 5
   4.8 EncryptionMethod 5
   4.9 Compression 5
   4.10 CompressionMethod 5
   4.11 Service 5
   4.12 Content 5
   4.13 TransferKey 5
   4.14 SerialNumber 5
   4.15 Signature 5
5. CertApplicationResponse 5
   5.1 CustomerId 5
   5.2 Timestamp 5
   5.3 ResponseCode ja ResponseText 5
   5.4 ExecutionSerial 6
   5.5 Encrypted 6
   5.6 EncryptionMethod 6
   5.7 Compressed 6
   5.8 CompressionMethod 6
   5.9 CustomerExtension 6
   5.10 Certificates 6
      5.10.1 Certificate 6

5.10.1.1 Name 6
5.10.1.2 Certificate 6
5.10.1.3 CertificateFormat 6
5.11 Signature 6
6. LIITTEET 7
7. Esimerkkiviestit 7
7.1 Pyyntösanoma 7
7.2 Vastaussanoma 8

1. Johdanto

WSDL kuvaa, minkälaisia sanomia Samlinkin varmennehakupalvelussa voidaan lähettää ja vastaanottaa. WSDL:ssä on kuvattu kolme operaatiota:

- getCertificate
- getServiceCertificates
- revokeCertificate

Samlinkin järjestelmäratkaisu tukee ainoastaan getCertificate-operaatiota.

Samlinkin varmennehakupalvelun SOAP-sanomassa ei käytetä salausta eikä pakkausta. Samlinkin

järjestelmäratkaisu ei tue pakkausta, koska palvelussa kulkevat viestit ovat tyypillisesti pieniä.WSDL:ssä ApplicationRequest sisältää Base64-koodatun CertApplicationRequestin, jonka skeema on kuvattu CertApplicationRequest_20090422.xsd:ssä (liite 2). Vastaussanoman ApplicationResponse sisältää Base64-koodatun CertApplicationResponsen, jonka skeema on kuvattu CertApplicationResponse_20090422.xsd:ssä (liite 3).

Tämä dokumentti kuvaa Samlinkin varmennehakupalvelun getCertificate-operaation ja sen CertApplicationRequest- ja CertApplicationResponse-elementtien käyttötapoja.

2. Asiakasohjelmiston varmennehaun käyttötapaukset

Asiakasohjelmistossa pitää ensimmäisellä kerralla luoda PKI-avainpari. Avainparin avulla luodaan varmennepyyntö (CSR), joka lähetetään Samlinkille WS-kanavassa siten, että ensimmäisellä kerralla asiakas käyttää tunnistautumisessa kertakäyttöistä salasanaa (TransferKey) ja seuraavilla kerroilla voimassa olevaa varmennetta.

Jo aiemmin haetun ja voimassa olevan varmenteen voi hakea uudestaan samalla CSR:llä. Kun varmenne on voimassa alle 60 päivää, niin asiakas voi hakea uuden varmenteen, kunhan varmennepyyntö on luotu uudella avainparilla. Vanhalla avainparilla ei voi hakea uutta varmennetta.

Uuden varmenteen voi hakea vain, jos varmennetta ei ole vielä haettu tai nykyinen varmenne on alle 60 päivää voimassa. Jos varmennetta yritetään uusia edellä mainittujen ehtojen vastaisesti tuloksena, on virhe seuraavan taulukon mukaisesti:

avain	**käyttäjä**	**voimassaoloaika**	**kuvaus**
uusi	uusi	ei varmennetta	Normaali uuden luominen
uusi	vanha	alle60	Normaali uusinta
uusi	vanha	yli60	VIRHE: Varmennetta ei saa vielä uusia
vanha	uusi	alle60	VIRHE: Virheellinen käyttäjätieto
vanha	uusi	yli60	VIRHE: Virheellinen käyttäjätieto
vanha	vanha	alle60	VIRHE: Yksityinen avain pitää generoida uudestaan

vanha	vanha	yli60	Palautetaan vanha varmenne

3. getCertificate-operaatio

Alla on selitetty tarkemmin SOAP viestin elementit yksitellen.

3.1 SenderId

Viestin lähettäjän yksilöivä tunniste ja käyttäjätunnus, joka on luovutettu yritykselle sopimuksen allekirjoituksen yhteydessä.Arvo on sama kuin myöhemmin kuvattava CertApplicationRequestin CustomerId-elementissä ja varmennepyynnön Surname-kentässä (SN).

3.2 RequestId

Lähetyksen yksilöivä tunniste, jonka tarkoitus on helpottaa ongelmien selvitystyötä. Samlinkilla ei tarkisteta, onko tunnistetta käytetty aikaisemmin.

3.3 Timestamp

Aikaleima, joka kertoo milloin Application Request Header on luotu.

3.4 ApplicationRequest

Sisältää Base64-koodattuna CertApplicationRequestin.

4. CertApplicationRequest

4.1 CustomerId

Varmenteen allekirjoituspyynnön tekijän yksilöivä tunniste ja käyttäjätunnus, joka on luovutettu yritykselle sopimuksen allekirjoituksen yhteydessä.

Arvo on sama kuin aiemmin kuvatussa SenderId-elementissä ja varmennepyynnön Surnamekentässä (SN).

4.2 Timestamp

Skeemassa pakollinen. Arvoa ei käytetä.

4.3 Environment

Arvo: PRODUCTION Testiominaisuutta ei käytetä.

4.4 SoftwareId

Ohjelmiston tarkka tunniste, jonka tarkoitus on helpottaa ongelmien selvitetystyötä.

4.5 Command

Arvo: GetCertificate

4.6 ExecutionSerial

Ei käytetä

4.7 Encryption
Ei käytetä

4.8 EncryptionMethod
Ei käytetä

4.9 Compression
Ei käytetä

4.10 CompressionMethod
Ei käytetä

4.11 Service
Skeemassa pakollinen. Käytetään oletusarvoa ISSUER.

4.12 Content
Base64-koodattu varmenteen allekirjoituspyyntö (PKCS#10).

4.13 TransferKey
Ensimmäisellä kerralla käytettävä kertakäyttöinen salasana (8+8). Ensimmäinen osio luovutetaan yritykselle sopimuksen allekirjoituksen yhteydessä, toinen osio saapuu erikseen postissa. Kun asiakas on vastaanottanut allekirjoitetun varmenteen, käytetään varmennetta (Signature-elementti) asiakkaan tunnistamisessa, jolloin TransferKey-elementtiä ei saa enää esiintyä. WS-kanavassa kertakäyttöinen salasana merkataan käytetyksi, kun allekirjoitettu varmenne lähtee asiakkaalle.

4.14 SerialNumber
Ei käytetä

4.15 Signature
Ensimmäisellä kerralla asiakas tunnistautuu käyttämällä kertakäyttöistä salasanaa (TransferKeyelementti). Sen jälkeen TransferKey-elementtiä ei enää käytetä ja vaan tunnistus tapahtuu XMLallekirjoituksen avulla.

5. CertApplicationResponse

5.1 CustomerId
Asiakkaan CertApplicationRequestissä käyttämä tunniste.

5.2 Timestamp
Aikaleima, joka kertoo milloin CertApplicationResponse on luotu.

5.3 ResponseCode ja ResponseText

ResponseCode	ResponseText

0	OK
5	TUNTEMATON SOVELLUSPYYNTÖ
6	VARMENNETTA EI SAA VIELÄ UUSIA
7	VIRHEELLINEN KÄYTTÄJÄTIETO
8	YKSITYINEN AVAIN PITÄÄ GENEROIDA UUDESTAAN
12	AINEISTON MUODOLLINEN TARKISTUS EPÄONNISTUI
26	TEKNINEN VIRHE
30	TUNNISTUS EPÄONNISTUI

5.4 ExecutionSerial
Ei käytetä.

5.5 Encrypted
Ei käytetä.

5.6 EncryptionMethod
Ei käytetä.

5.7 Compressed
Ei käytetä.

5.8 CompressionMethod
Ei käytetä.

5.9 CustomerExtension
Ei käytetä.

5.10 Certificates
Sisältää yhden Certificate-elementin.

5.10.1 Certificate
Sisältää Name-, Certificate- ja CertificateFormat-elementit.

5.10.1.1 Name
Varmenteen subjekti esim.

SURNAME=9923233, CN=YRITYS AB, O=Aineistopalvelut-Samlink, C=FI

5.10.1.2 Certificate
Base64-koodattu allekirjoitettu varmenne (X509v3).

5.10.1.3 CertificateFormat
Arvo: X509

5.11 Signature
Samlink lisää XML-allekirjoituksen kaikille viesteille. Asiakkaan tulee varmistaa allekirjoituksen oikeellisuus.

6. LIITTEET

Liitteet ladattavissa Samlinkin kotisivuilta

- Varmennepalvelun WSDL-dokumentaatio
- CertApplicationRequest.xsd schema
- CertApplicationResponse.xsd schema

7. Esimerkkiviestit

7.1 Pyyntösanoma

```
<soapenv:Envelope xmlns:opc="http://mlp.op.fi/OPCertificateService" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Header>
    </soapenv:Header>
    <soapenv:Body wsu:Id="id-3" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <opc:getCertificatein>
            <opc:RequestHeader>
                <opc:SenderId>99415033</opc:SenderId>
                <opc:RequestId>12345678</opc:RequestId>
                <opc:Timestamp>2016-05-04T08:12:26.30</opc:Timestamp>
            </opc:RequestHeader>
            <opc:ApplicationRequest>PD94bWwgdmVyc2lvbj0iMS4wIj8+...
            WNhdGlvblJlcXVlc3Q+</opc:ApplicationRequest>
        </opc:getCertificatein>
    </soapenv:Body>
</soapenv:Envelope>
```

7.2 Vastaussanoma

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
        xmlns:cer="http://mlp.op.fi/OPCertificateService">
        <soapenv:Header>
                <wsse:Security soapenv:mustUnderstand="1"
                        xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
                        <wsu:Timestamp wsu:Id="Timestamp-c8599f50-342d-4fb5-9031-53d5cdb045eb"
                                xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
                                <wsu:Created>2016-05-04T05:12:27Z</wsu:Created>
                                <wsu:Expires>2016-05-04T05:17:27Z</wsu:Expires>
                        </wsu:Timestamp>
                        <wsse:BinarySecurityToken
                                wsu:Id="SecurityToken-2f291284-dfcf-4ebc-a192-aa2ca14d720e"
                                EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
                                ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
                                xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">MIIFETCCAvmgAwIBAgIQUHFBQ1tAv...IQW1tDtk=
                        </wsse:BinarySecurityToken>
                        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                                <SignedInfo>
                                        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
                                        <Reference URI="#Timestamp-c8599f50-342d-4fb5-9031-53d5cdb045eb">
                                                <Transforms>
                                                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                                                </Transforms>
                                                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                                                <DigestValue>57KNPysmumFct7yiRUosf3uyfJc=</DigestValue>
                                        </Reference>
                                        <Reference URI="#Body-b1b9dbf7-9980-4867-9fda-f9479a73441c">
                                                <Transforms>
                                                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
                                                </Transforms>
                                                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                                                <DigestValue>8ipUWG+6e0J6i94gydmIiR3lWyo=</DigestValue>
                                        </Reference>
                                </SignedInfo>
                                <SignatureValue>DvB+0cy2laidmg2THNx5jF5HiL05TH27AqLoLI+ZGm...r9BqgSIg==
                                </SignatureValue>
                                <KeyInfo>
                                        <wsse:SecurityTokenReference xmlns="">
                                                <wsse:Reference
                                                        URI="#SecurityToken-2f291284-dfcf-4ebc-a192-aa2ca14d720e"
                                                        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3" />
                                        </wsse:SecurityTokenReference>
                                </KeyInfo>
                        </Signature>
                </wsse:Security>
        </soapenv:Header>
        <soapenv:Body wsu:Id="Body-b1b9dbf7-9980-4867-9fda-f9479a73441c"
                xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
                <cer:getCertificateout>
                        <cer:ResponseHeader>
                                <cer:SenderId>99415033</cer:SenderId>
                                <cer:RequestId>12345678</cer:RequestId>
                                <cer:Timestamp>2016-05-04T08:12:27+03:00</cer:Timestamp>
                                <cer:ResponseCode>0</cer:ResponseCode>
                                <cer:ResponseText>OK</cer:ResponseText>
                        </cer:ResponseHeader>
                        <cer:ApplicationResponse>PD94bWwgdmVyc2lvbj0iMS4...BvbnNlPg==
                        </cer:ApplicationResponse>
                </cer:getCertificateout>
        </soapenv:Body>
</soapenv:Envelope>
```