FICOM RY:N SOVELTAMISOHJE ETSI:N MSS-STANDARDEILLE V2.0

Versio	Kuvaus
1.0	Alkuperäinen versio.
1.1	WSDL:n edellyttämä MSS_Signature-elementti lisätty viestiformaatin kuvaukseen ja viestiesimerkkeihin (puuttuivat myös ETSI TS 102 204:n esimerkeistä). Viitteisiin lisätty WSDL. Tuki organisaatiovarmenteille lisätty SignatureProfileen.
1.2	Lisätty tuki viestintätavalle ”asynkroninen client-server”. Lisätty tuki operaatiolle MSS_StatusQuery. Lisätty tuki testivarmenteille SignatureProfileen. Risuaidat (#) poistettu käyttäjäkokemuksesta. UserIdentifier-elementin formaattia korjattu. DataToBeSigned-elementin enkoodausta korjattu. Korostettu, että tapahtuma”numero” alkaa joko kirjaimella tai alaviivalla (NCName).
2.0	Allekirjoitusprofiilit uusittu täysin. Allekirjoitusvastauksien StatusDetail-elementtiin varattu paikka lisäarvopalvelujen vastaussanomille. Uudet lisäarvopalvelut AE-validointi ja PersonIdentity. Lisäarvopalvelu SessionID nimetty uudelleen palveluksi EventID. UserIdentifier-elementin tuki poistettu (tämän korvaa PersonIdentity-palvelu). Kirjoitettu auki tuetut MSS_Format/MimeType/Encoding/SignatureProfile-yhdistelmät. Uusi MSS_Format PKCS1. 505-statuskoodi lisätty testi-identiteeteille. Lisätty statuskoodien ekstensiot (liite C). Synkronista viestintätapaa ei suositella.

Sisältö

1 Johdanto

Tämä dokumentti määrittelee FiCom ry:n puitteissa laaditun FiCom Mobile Signature Service – suosituksen (jatkossa ”FiCom-suositus”).

FiCom-suositus on soveltamisohje ETSI:n Mobile Signature Service -standardeille. Dokumentin kuvaamien tekniikoiden, käytäntöjen, rajoitusten ja laajennusten mukaisesti voidaan toteuttaa eri palveluntuottajien kesken Suomessa mobiili allekirjoituspalvelu, joka käsittää:

- ETSI TS 102 204-yhteensopivan palveluntarjoaja-rajapinnan matkapuhelimella tehdylle allekirjoitukselle ja käyttäjän mobiilitunnistamiselle
- ETSI TS 102 207-yhteensopivan eri matkapuhelinverkkojen välisen allekirjoitusvierailun (mobile signature roaming)
- yhtenäisen, operaattorista riippumattoman käyttäjäkokemuksen
- turvallisuutta ja käytettävyyttä parantavat, ETSI-standardeja täydentävät lisäpalvelut

Soveltamisohje ei rajoita ohjeen ulkopuolella olevien lisätoiminnallisuuksien tarjoamista. Soveltamisohje ei kuvaa MSS palvelun teknistä toteutusta, liiketoimintamalleja eikä kaupallisia ehtoja.

Solvetamisohjeen ymmärtämisen kannalta on suositeltavaa perehtyä myös alkuperäisiin standardien määrittelyihin sekä SOAP 1.2 ja WSDL 1.1 -määrittelyihin.

Soveltamisohjetta päivitetään FiCom ry:n toimesta.

2 Viitteet

FiCom-suositus nojaa seuraaviin tekniikoihin.

ETSI
TS 102 204; TR 102 206; TS 102 207:
http://portal.etsi.org/docbox/EC_Files/ EC_Files/ts_102204v010104p.pdf
http://portal.etsi.org/docbox/EC_Files/ EC_Files/tr_102206v010103p.pdf
http://portal.etsi.org/docbox/EC_Files/ EC_Files/ts_102207v010103p.pdf

W3C
XML Schema Part 1; Part 2:
http://www.w3.org/TR/xmlschema-1/
http://www.w3.org/TR/xmlschema-2/
SOAP Version 1.2 Part 0: Primer; Part 1: Messaging Framework; Part 2: Adjuncts:
http://www.w3.org/TR/2003/REC-soap12-part0-20030624/
http://www.w3.org/TR/2003/REC-soap12-part1-20030624/
http://www.w3.org/TR/2003/REC-soap12-part2-20030624/
XMLSignature:
http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/
WSDL 1.1:
http://www.w3.org/TR/wsdl

RSA Laboratories
PKCS#7: Cryptographic Message Syntax Standard:
http://www.rsasecurity.com/rsalabs
RFC 5652: Cryptographic Message Syntax: neljäs revisio PKCS#7 määrityksestä

OASIS
Security Assertion Markup Language (SAML) v2.0:
http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

3 Lyhenteet ja määritelmät

MSS-standardi	Mobile Signature Service standard. ETSI TS 102 204:ssä kuvattu standardi, joka määrittää Palveluntarjoajan rajapinnan mobiiliin allekirjoituspalveluun. Termi viittaa osaksi myös ETSI TS 102 207:ssa kuvattuun allekirjoitusvierailu-standardiin.
FiCom-suositus	Ks. Johdanto.
Käyttäjä	Allekirjoituslaitteen haltija. Palveluntarjoajan ja kotioperaattorin eli HMSSP:n asiakas.
AP	Palveluntarjoaja (Application Provider). Käyttäjän allekirjoituksen tarvitseva toimija. AE:n asiakas.
AP_ID	Palveluntarjoajan yhteystieto MSSP:iden järjestelmissä.
AP_PWD	Paveluntarjoajan salasana AE:n järjestelmässä.
MSSP	Mobile Signature Service Provider. Tässä dokumentissa MSSP viittaa toimijaan, joka tarjoaa HMSSP-palveluja Käyttäjille sekä mahdollisesti AE-palveluja Palveluntarjoajille ja/tai RE-palveluja AE:ille. Tyypillinen tällainen toimija on mobiilivarmennepalveluja tarjoava operaattori.
AE	Acquiring Entity. Toimija, joka tarjoaa Palveluntarjoajalle web service -rajapinnan FiCom-suosituksen mukaiseen mobiiliin allekirjoituspalveluun. Kommunikoi Käyttäjän kotioperaattorin (HMSSP) kanssa tarvittaessa allekirjoitusvierailua hyödyntäen.
RE	Routing Entity. Entiteetti, joka reitittää liikennettä AE:n ja HMSSP:n välillä. RE voi olla AE- tai HMSSP-järjestelmien komponentti tai kolmannen toimijan erillinen järjestelmä.
HMSSP	Home MSSP. Käyttäjän kotioperaattori.
VE	Verifying Entity. Reitittävä entiteetti (RE), joka lisäksi vastaa tapahtuman validoinnista.
Mobiili allekirjoitus	Matkapuhelimella tai mobiililla päätelaitteella tehtävä julkisen avaimen menetelmään (PKI) perustuva digitaalinen allekirjoitus, jota voidaan käyttää erilaisiin varmennuspalveluihin kuten mm. sähköisten allekirjoituksiin, henkilön sähköiseen tunnistamiseen ja käyttäjän vahvaan todentamiseen.

4 FiCom-suositus lyhyesti

ETSI:n MSS–standardit tuntevalle oheinen luettelo kertoo tiivistetysti FiCom-suosituksessa valitut tekniikat, käytännöt, rajoitukset ja laajennukset. Käytetyt termit selviävät myös tästä dokumentista.

1. Tuetut viestintätavat ovat synkroninen client-server (ei suositella) ja asynkroninen client-server. Viestintätapaa asynkroninen server-server ei toistaiseksi tueta.
2. Kaikkien viestin reitittämiseen osallistuvien entiteettien välinen vahva molemminpuolinen tunnistus ja salaus.
3. AP:n yhteystieto (AP_ID) sekä AP:n päätelaitteella näytettävä nimi luodaan AP:n ja AE:n välisessä palvelusopimuksessa. Sopimusta tehtäessä AP:lle luodaan myös salasana (AP_PWD). Tämän jälkeen AP omistaa luodun AP_ID:n ja se säilyy, vaikka AP myöhemmin siirtyisi käyttämään toisen AE:n rajapintaa. AE välittää AP_ID:n ja AP:n nimen kaikille HMSSP:ille.
4. Päätelaitteella näytettävä AP:n nimi ei ole sama kuin AP_ID.
5. AP:n ja AE:n välillä vahva molemminpuolinen tunnistus ja viestiliikenteen salaus, salasanan (AP_PWD) lisäksi.
6. Tuetut viestiformaatit MSS_SignatureReq, MSS_SignatureResp, MSS_StatusReq, MSS_StatusResp, MSS_ReceiptReq ja MSS_ReceiptResp.
7. Suositus jättää tässä versiossa huomiotta MSS-palvelun rekisteröintiviestit. Käyttäjien rekisteröintiprosessi jätetään kunkin HMSSP:n sisäiseksi asiaksi.
8. XML-allekirjoitettuja palveluviestejä ei toistaiseksi tueta.
9. Käyttäjä ja HMSSP löydetään yksinomaan MSISDN:n perusteella, hyödyntäen numeron siirrettävyysresursseja.
10. Palvelupyynnöissä tuetut merkistöt UTF-8, GSM ja UCS2, päätelaitteella tuetut merkistöt GSM 03.38 ja UCS2. Käytettävissä ainoastaan GSM 03.38-merkistöön kuuluvat UTF-8 merkit.
11. HMSSP:t tarjoavat kuusi eri allekirjoituspalvelua:
    - anonyymi tunnistaminen
    - tunnistaminen
    - selväkielisen sisällön sähköinen allekirjoitus
    - tiivistetyn sisällön sähköinen allekirjoitus
    - suostumuksen antaminen
    - operaattoripalvelu tunnistamiseen
12. Tarjotuille allekirjoituspalveluille on kullekin oma allekirjoitusprofiilinsa. Allekirjoitusprofiilia käytetään suoraan halutun palvelun osoittamiseen.
13. Käyttäjä voi kieltää minkä tahansa allekirjoitusprofiilin käytön omalla matkapuhelinliittymällään.
14. MSS-standardin laajennuksina lisäarvopalveluja (AdditionalServices):
    - matkapuhelimen häirinnän esto
    - tapahtumatunnus, joka yhdistää asiointikanavan istunnon tunnistustapahtumaan
    - AE:n suorittama validointi
    - Käyttäjän kielipreferenssi
    - PersonIdentity-palvelu
15. Yhtenäinen käyttäjäkokemus: allekirjoituspyyntöjen muoto standardoitu.
16. Sähköisen allekirjoituksen formaattina base64-enkoodattu PKCS#7 tai PKCS#1 täydennettynä käyttäjän varmenteella.
17. Järjestelmäkellon ajastaminen NTP-palvelun avulla on AE:lle, RE:lle ja HMSSP:lle pakollista. AP:lle se on suositeltavaa.

5 Allekirjoitustapahtuman kulku

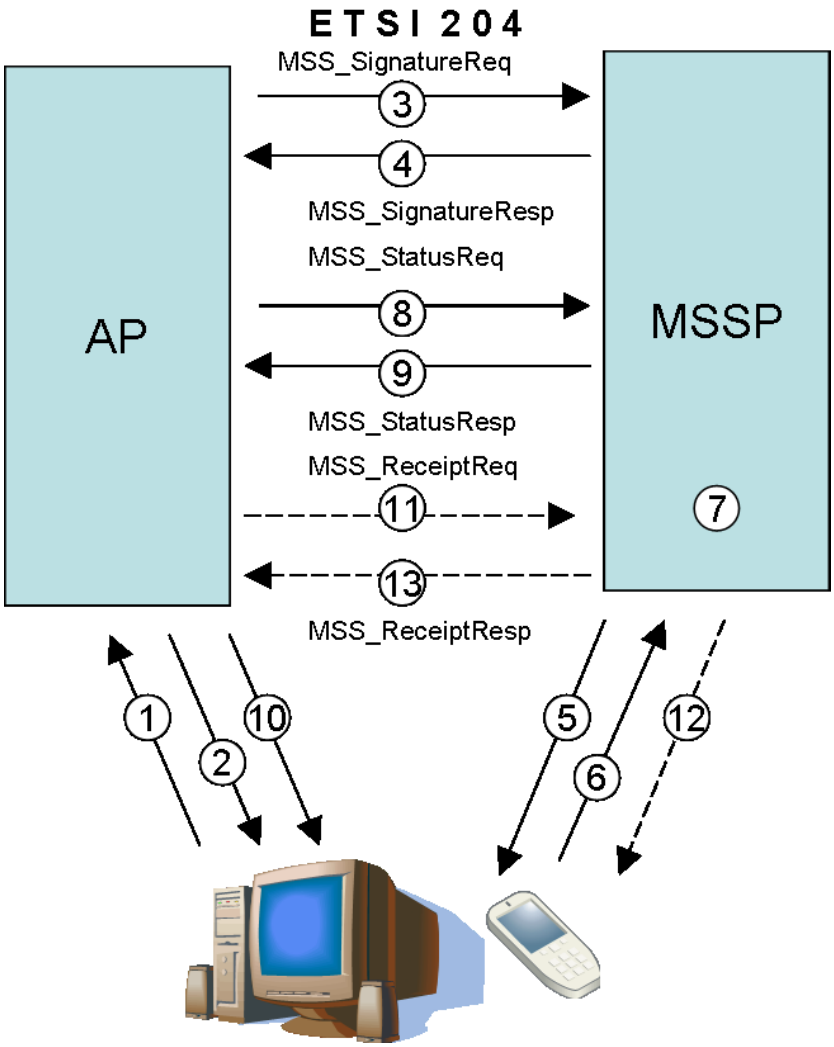
ETSI TS 102 204 –määrityksessä kuvataan kolme vaihtoehtoista viestintätapaa: synkroninen, asynkroninen client-server ja asynkroninen server-server.

FiCom-suositus tukee viestintätapaa asynkroninen client-server. Asynkronista server-server viestintää ei toistaiseksi tueta, ja synkronista viestintätapaa ei suositella käytettävän, koska se kuluttaa tarpeettomasti AP:n ja MSSP:n järjestelmäresursseja. Seuraavassa kuvataan tapahtuman kulku tuetussa viestintätavassa. Tässä luvussa käsitteellä ”MSSP” tarkoitetaan yleisesti kaikkien operaattorien muodostamaa allekirjoitusvierailuja hyödyntävää järjestelmää. ETSI:n MSS-standardien eräs päätavoite on piilottaa allekirjoitusvierailujen monimutkaisuus Palveluntarjoajalta, jotta AP:n järjestelmien kannalta kommunikointi näyttää tapahtuvan yksittäisen MSSP:n kanssa, joka kattaa kaikkien Käyttäjien mobiililiittymät.

5.1 Asynkroninen client-server viestintätapa

Asynkronisessa client-server viestinnässä allekirjoitustapahtuma koostuu seuraavista palveluviesteistä: **allekirjoituspyyntö**, pyynnön käsittelyn tilaa tiedusteleva **statuskysely** ja siihen liittyvä **statusvastaus,** sekä optionaalinen **kuittauspyyntö** ja siihen liityvä **kuittausvastaus**. Tapahtuma koostuu useista toisiaan seuraavista HTTP-istunnoista, jotka avataan aina AP:n järjestelmästä käsin. Viestintätapa on synkroniseen viestintään nähden hyödyllinen siten, että AP saa varhain viitetiedon allekirjoitustapahtumaan ja palvelujärjestelmä voi käyttää kaikkia keinojaan palvelun korkean luotettavuuden aikaansaamiseksi.

Turhan ruuhkan välttämiseksi AP:n on suositeltavaa tehdä ensimmäinen statuskyselynsä 20 sekuntia allekirjoituspyynnön lähettämisen jälkeen ja toistaa kysely 5 sekunnin välein kunnes HMSSP palauttaa AP:lle statusvastauksen, joka ilmaisee allekirjotustapahtuman päättymisen.



1. Käyttäjä avaa istunnon AP:n palvelimelle. Ilmenee tarve sisäänkirjautumiseen tai sähköisen dokumentin allekirjoittamiseen. Käyttäjä syöttää matkapuhelinnumeronsa ja häirinnän estokoodinsa palveluntarjoajan palvelimelle.
2. AP näyttää Käyttäjälle asiointikanavassa opasteen, joka ohjaa Käyttäjän tarkkailemaan allekirjoituskanavaa (matkapuhelinta). Opasteessa kerrotaan Käyttäjälle allekirjoitustapahtuman tapahtumatunnus.
3. AP lähettää allekirjoituspyynnön (MSS_SignatureReq) AE:lle jonka web service-rajapintaan AP on integroitunut. AE tunnistaa vahvasti AP:n. Pyynnön lisäarvopalvelu-osassa AP voi pyytää HMSSP:tä toimittamaan Käyttäjän identiteettiin liittyviä lisätietoja.
4. Vastaanotettuaan allekirjoituspyynnön ja generoituaan sille MSSP-tapahtumanumeron, AE palauttaa tapahtumanumeron AP:lle. Vastausviestissä (MSS_SignatureResp) AE kertoo tapahtuman olevan vielä kesken.
5. AE varmistaa, että AP:n pyytämä allekirjoituspalvelu ja lisäarvopalvelut ovat palvelusopimuksen mukaisia. AE prosessoi allekirjoituspyynnön ja ohjaa sen Käyttäjän HMSSP:lle. (Kuvassa kokonaisuus kuvataan yhtenä MSSP:nä, sillä AP:n kannalta koko AE:n takainen maailma on läpinäkyvä.) HMSSP tarkistaa Käyttäjän häirinnänestokoodin ja varmistaa, että AP:n pyytämä allekirjoituspalvelu ja lisäarvopalvelut ovat käyttäjän sallimia. HMSSP toimittaa allekirjoituspyynnön käyttäjän matkapuhelimelle.
6. Käyttäjä varmistaa, että matkapuhelimella tapahtuman esittelyssä näytettävä tapahtumatunnus täsmää asiointikanavassa kerrotun tapahtumatunnuksen kanssa. Sitten Käyttäjä allekirjoittaa tapahtuman syöttämällä pyydetyn SPIN-koodin. Tuloksena syntyy Käyttäjän sähköinen allekirjoitus, joka toimitetaan HMSSP:lle.
7. HMSSP koostaa sähköisestä allekirjoituksesta PKCS#7-standardin mukaisen sähköisen allekirjoitusviestin, joka liitetään osaksi allekirjoitusvastausta (MSS_StatusResp). HMSSP

prosessoi AP:n pyytämät lisäarvopalvelut ja liittää sähköiseen allekirjoitusviestiin lisäarvopalvelujen vastaukset AP:lle (esimerkiksi Käyttäjän identiteettiin liittyviä lisätietoja).
8. Lähetettyään allekirjoituspyynnön kyselee AP määrätyin väliajoin allekirjoitusvastauksen valmistumista (MSS_StatusReq).
9. HMSSP validoi sähköisen allekirjoituksen. HMSSP tiedottaa AP:ta allekirjoituspyynnön tilasta statusvastauksessa (MSS_StatusResp). (Myös AE voi validoida. Ks. AE-validointi.) Kun allekirjoitus on valmis, se toimitetaan AP:lle statusvastauksen osana.
10. AP prosessoi saamansa allekirjoitusvastauksen. AP yhdistää toisiinsa sähköisessä allekirjoituksessa identifioidun Käyttäjän ja käyttäjän AP:n omassa käyttäjäkannassa. Käyttäjä on autentikoitu. Mikäli AP käyttää asiointikanavassa esim. itseään päivittävää web-sivua, AP voi nyt muuttaa sivun sisällön sellaiseksi, että käyttäjän selain ohjautuu autentikointia vaatineeseen sisältöön.
11. Halutessaan AP voi lähettää Käyttäjälle tunnistuskanavassa vielä kuittauksen tapahtuman onnistumisesta (MSS_ReceiptReq).
12. AP:n kuittausviesti toimitetaan käyttäjälle samalla tavalla kuin allekirjoituspyyntö.
13. AP:lle toimitetaan vahvistus kuittausviestin toimittamisesta (MSS_ReceiptResp).

6 Palveluntarjoajan rajapinta

6.1 Yleinen viestirakenne

Palveluntarjoajan (AP:n) ja AE:n välinen viestirajapinta toteutetaan joukolla ETSI:n määrittämiä MSS-palveluviestejä. Tuetuissa viestintätavoissa viestinnän kukin vaihe etenee käytännössä siten, että AP lähettää AE:lle palvelupyynnön ja saa pyyntöön AE:lta palveluvastauksen. AP:n palvelupyyntö on aina HTTP POST Request ja AE:n vastausviesti on HTTP Response.

MSS-palveluviestit on käärittyä HTTP-viestin sisältönä välitettäviin SOAP-kirjekuoriin. SOAP-kirjekuoret koostuvat otsikkoelementistä (env:Header) ja sisältöelementistä (env:Body).

6.1.1 SOAP Header

SOAP Header –elementti on optionaalinen. Se on hyödyllinen etupäässä XML-allekirjoitusten toteuttamisessa, ja FiCom suositus ei huomioi XML-allekirjoituksia.

6.1.2 SOAP Body

SOAP Body -elementti on pakollinen, ja se sisältää jonkin seuraavista viestityypin määrittävistä elementeistä:

- MSS_SignatureReq (operaatio: MSS_Signature)
- MSS_SignatureResp (operaatio: MSS_Signature)
- MSS_StatusReq (operaatio: MSS_Status)
- MSS_StatusResp (operaatio: MSS_Status)
- MSS_ReceiptReq (operaatio: MSS_Receipt)
- MSS_ReceiptResp (operaatio: MSS_Receipt)

Näistä kukin edelleen sisältää kyseiselle viestityypille ominaiset attribuutit ja alielementit. WSDL 1.1 –määrityksen mukaisesti varsinainen viestielementti on vielä käärittyä ”operaation” nimen kertovaan elementtiin. (Ks. esimerkki alla.)

6.1.3 Nimiavaruudet

SOAP Envelopen määrittävä elementti varaa oman nimiavaruutensa:

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
```

Sisältöelementin viestityypin määrittävä elementti varaa nimiavaruudet ETSI:n MSS-standardin määrityksille ja tarvittaessa XML-allekirjoituksen määrityksille sekä FiCom-suosituksen määrittämille allekirjoituspyyntöjen lisäarvopalveluille:

```
<MSS_ReceiptReq xmlns=http://uri.etsi.org/TS102204/v1.1.2#
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:fi="http://mss.ficom.fi/TS102204/v1.0.0#" ...>
```

6.1.4 Viestirakenteen esimerkki

Ohessa on kuvattu esimerkki yleisestä viestirakenteesta. Jäljempänä esitetään kustakin MSS-palveluviestistä vielä omat esimerkkinsä, ilman optionaalista otsikkoelementtiä. W3C ei suosittele XML-kommenttien käyttöä todellisessa viestiliikenteessä.

```
POST /MSS_Signature HTTP/1.0
Host: mss.teliasonera.com
Content-Type: application/soap+xml; charset="utf-8"
Content-Length: ...

<?xml version="1.0"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
   <!- Otsikkoelementti on optionaalinen -->
   <env:Header>
   </env:Header>
   <!- Sisältöelementti on pakollinen -->
   <env:Body>
       <-! Operaation nimi -->
      <MSS_Signature>
         <!- MSS-palveluviesti -->
         <MSS_SignatureReq ...>
            . . .
         </MSS_SignatureReq>
      </MSS_Signature>
   </env:Body>
</env:Envelope>
```

6.1.5 Suosituksen ulkopuoliset viestityypit

FiCom-suositus *ei* huomioi seuraavia MSS-standardin määrittelemiä viestityyppejä:

- MSS_RegistrationReq
- MSS_RegistrationResp
- MSS_ProfileReq
- MSS_ProfileResp
- MSS_HandshakeReq
- MSS_HandshakeResp

6.1.6 Virhetiedotus

Jos tapahtuman aikana havaitaan mikä tahansa virhetilanne, Palveluntarjoajalle palautetaan statuskoodi SOAP FAULT-viestinä. Virheilmoitusviestin rakenne kuvataan myöhempänä varsinaisten palveluviestien jälkeen.

6.2 Allekirjoituspyyntö (MSS_SignatureReq)

Allekirjoituspyynnön viestikuvauksessa käydään palveluviestin attribuutit ja elementit läpi syvimmin, ja osaan näistä kuvauksista viitataan muiden MSS-palveluviestien kuvauksissa.

Palveluntarjoajan AE:lle lähettämä allekirjoituspyyntö sisältää seuraavat tiedot:

- Viestintätapa (synkroninen tai asynkroninen client-server viestintä)
- Tapahtuman sallittu kesto eli ”timeout”
- Palveluntarjoajan yhteystieto (AP_ID)
- Käyttäjän yhteystieto (MSISDN)
- Aikaleima
- Allekirjoitettava sisältö (DTBS)
- Palveluntarjoajan edellyttämä allekirjoitusprofiili = AP:n pyytämä palvelu
- Lisäpalvelut, kuten haittakäytön esto ja identiteettitiedot

6.2.1 MSS_SignatureReq: attribuutit

Nimi	Arvo	Kuvaus	Vaadittu
MajorVersion	”1”	Rajapinnan yläversio, tällä hetkellä 1.	Kyllä
MinorVersion	”1”	Rajapinnan alaversio, tällä hetkellä 1.	Kyllä
MessagingMode	”asynchClient Server” tai ”synch”	Viestintätapa, tällä hetkellä aina joko ”asynchClientServer” (suositus) tai “synch”.	Kyllä
ValidityDate	DateTime	AP:n määräämä aikaraja, jonka jälkeen keskeneräinen tapahtuma on hylättävä. Ilmoitetaan absoluuttisena aikaleimana. Esim. ”2003-06-25T21:32:00Z”.	Ei
TimeOut	Integer	AP:n määräämä aikaraja, jonka jälkeen keskeneräinen tapahtuma on hylättävä. Ilmoitetaan sekunteina tapahtuman alkamisesta.	Ei

6.2.1.1 MajorVersion ja MinorVersion

Käytetyn MSS-rajapinnan versio on tällä hetkellä 1.1. Mikäli AP:n asettama versionumero poikkeaa tästä, AE palauttaa AP:lle statuskoodin 108 (INCOMPATIBLE_INTERFACE).

6.2.1.2 MessagingMode

FiCom-suositus takaa tuettavan toistaiseksi asynkronista client-server viestintää. Tukea asynkroniselle server-server viestinnälle ei taata.

Jos AE tai HMSSP ei tue Palveluntarjoajan pyytämää viestintätapaa, kyseinen MSSP palauttaa AP:lle statuskoodin 101 (WRONG_PARAM).

6.2.1.3 ValidityDate ja TimeOut

Palveluntarjoaja voi halutessaan asettaa käynnistämälleen tapahtumalle aikarajan, jonka kuluttua umpeen AE:n on keskeytettävä tapahtuma. Aikarajan puuttuessa käytetään AE:n oletusarvoista TimeOutia, joka on 5 minuuttia. Aikarajan voi asettaa joko absoluuttisena aikaleimana (ValidityDate) tai sekunteina tapahtuman alkamishetkestä (TimeOut). (Ks. http://www.w3.org/TR/xmlschema-2/#dateTime) Oletusarvoisen tai AP:n asettaman aikarajan kuluttua umpeen HMSSP keskeyttää tapahtuman ja lähettää AP:lle statuskoodin 208 (EXPIRED_TRANSACTION).

FiCom-suositus edellyttää, että kaikki AE:t ja HMSSP:t käyttävät NTP-palvelua järjestelmäkellojensa ajastukseen. Myös AP:n suositellaan ajastavan kellonsa NTP:n avulla. NTP (Network Time Protocol) on kuvattu dokumentissa RFC 5905.

6.2.1.4 Esimerkki: MSS_SignatureReq–elementin attribuutit

```
<MSS_SignatureReq xmlns="http://uri.etsi.org/TS102204/v1.1.2#" MajorVersion="1"
MinorVersion="1" MessagingMode="synch" ValidityDate="2003-06-25T21:32:00Z">
```

6.2.2 MSS_SignatureReq: elementit

Nimi	Kuvaus	Vaadittu
AP_Info	Palveluntarjoajan yhteystieto sekä AP:n tapahtumalle antama tapahtumanumero ja aikaleima.	Kyllä
MSSP_Info	Elementin arvo jätetään normaalisti tyhjäksi.	Kyllä
MobileUser	Loppukäyttäjän yhteystieto, toistaiseksi aina elementti muotoa: <MSISDN>+358123456789</MSISDN> missä matkapuhelinnumeron alkuosa +358 (Suomessa) on pakollinen, eli noudatetaan kansainvälistä numeroformaattia.	Kyllä
DataToBeSigned	Allekirjoitettava teksti, max. 160 merkkiä.	Kyllä
DataToBeDisplayed	Käyttäjälle näytettävä teksti, max. 110 merkkiä.	Ei
MSS_Format	Pyydettävän allekirjoituksen formaatti, esim. <mssURI>http://uri.etsi.org/TS102204/v1.1.2#PKCS7</mssURI>	Ei
SignatureProfile	Käytettävä allekirjoitusprofiili eli valittu palvelu.	Kyllä*
AdditionalServices	Allekirjoitustapahtumaan liittyvät lisäpalvelut. FiCom on määrittänyt muutamia lisäpalveluja, jotka lisäävät Loppukäyttäjän tietoturvaa ja käyttömukavuutta.	Kyllä*

*MSS-standardia tiukempi vaatimus

6.2.2.1 AP_Info

Elementti AP_Info sisältää seuraavat attribuutit:

Nimi	Arvo	Kuvaus	Vaadittu
AP_ID	anyURI	Palveluntarjoajan yksikäsitteinen URI-tyyppinen tunnus jolla AP on rekisteröity käyttämään AE:n palveluja. Esim. ”http://mss.teliasonera.com/mssURI/OyCompanyAb”	Kyllä
AP_TransID	NCName	Palveluntarjoajan luoma yksikäsitteinen tapahtuma-id. Tätä id:tä ei yleensä tarvita synkronisessa viestinvälityksessä, mutta se on silti generoitava standardin kunnioittamiseksi. Id:n ensimmäinen merkki on joko kirjain tai alaviiva (’_’).	Kyllä
AP_PWD	String	Palveluntarjoajan tunnistamisessa käytetty salasana.	Kyllä
Instant	DateTime	Palveluntarjoajan luoma aikaleima allekirjoituspyynnön lähettämishetkelle.	Kyllä

AP_ID

FiCom-suositus edellyttää, että AE ja Palveluntarjoaja tunnistavat toisensa vahvasti esim. TLS-kättelyn avulla. Tämän lisäksi tarvitaan mekanismi, jolla AE esittelee AP:n kotioperaattorille (HMSSP) allekirjoitusvierailun yhteydessä. AP_ID on yksikäsitteinen URI, jonka AE saattaa AP:n tiedoksi osana palvelusopimusta, ja jonka avulla muutkin toimijat kuin AE tunnistavat

yksikäsitteisesti tapahtuman käynnistäneen Palveluntarjoajan. AP_ID:tä *ei* näytetä Käyttäjälle vaan se on MSSP:iden keskinäiseen kommunikointiin tarkoitettu tieto. Yksikäsitteisyyden takaamiseksi AP_ID noudattaa muotoa ”http://<AE-kohtainen URIn alkuosa>/<AP:n nimi>”. AP_ID:n maksimipituus on 64 merkkiä. Esimerkiksi ”http://mss.teliasonera.com/mssURI/OyCompanyAb”, missä ”teliasonera.com/mssURI” yksilöi AE:n nimiavaruuden ja ”OyCompanyAb” on AP:n nimi AE:n hallinnoimassa nimiavaruudessa.

Mikäli AP_ID ei ole asetettu AE:n ohjeiden mukaiseksi, AE palauttaa AP:lle statuskoodin 104 (UNAUTHORIZED_ACCESS). Jos HMSSP ei tunnista Palveluntarjoajaa AP_ID:n perusteella, HMSSP palautaa Palveluntarjoajalle statuskoodin 104 (UNAUTHORIZED_ACCESS).

AP_TransID

Palveluntarjoajan tulee liittää jokaiseen lähettämäänsä allekirjoituspyyntöön tapahtumanumero. Hyvä tapa edellyttää, että jokainen generoitu tapahtumanumero on Palveluntarjoajan omien järjestelmien kannalta uniikki viimeisen kuukauden aikaikkunan sisällä. AE valvoo tätä yksikäsitteisyyttä. Tapahtumanumerossa sallitaan numeroiden lisäksi mm. kirjaimia mutta ei kaksoispisteitä. (Ks. http://www.w3.org/TR/xmlschema-2/#NCName). Tapahtumanumeron maksimipituus on 19 merkkiä.

Jos tapahtumanumero puuttuu pyynnöstä, AE palauttaa AP:lle statuskoodin 102 (MISSING_PARAM).

AP_PWD

FiCom-suositus edellyttää erillistä Palveluntarjoajan vahvaa tunnistusta, joten MSS-standardissa kuvattua Palveluntarjoajan salasanaa ei sinänsä enää tarvita. Salasana on kuitenkin standardin vaatimusten kunnioittamiseksi oltava käytössä.

Jos allekirjoituspyynnöstä puuttuu salasana, tai AP ei esitä AE:n edellyttämää salasanaa, AE palauttaa AP:lle statuskoodin 104 (UNAUTHORIZED_ACCESS).

Instant

Palveluntarjoajan tulee liittää allekirjoituspyyntöönsä aikaleima, joka ilmaisee pyynnön lähettämishetken. (Ks. http://www.w3.org/TR/xmlschema-2/#dateTime) Vastaavasti HMSSP/AE tulee merkitsemään vastausviestiinsä aikaleiman.

Jos AP:n aikaleima puuttuu pyynnöstä, AE palauttaa AP:lle statuskoodin 102 (MISSING_PARAM).

AP_URL (ei käytössä)

MSS-standardi määrittelee optinaalisen tiedon AP_URL, jota käytetään viestintätavassa ”asynkroninen server-server” vastausviestin reitittämiseen Palveluntarjoajalle. FiCom-suositus ei toistaiseksi huomioi tätä parametria.

Esimerkki: AP_Info –elementin attribuutit

```
<AP_Info AP_ID="http://mss.teliasonera.com/mssURI/oycompanyab" AP_TransID="A1203"
AP_PWD="1AP-PWD2" Instant="2003-06-24T21:32:00Z"/>
```

6.2.2.2 MSSP_Info

Palveluntarjoajan tulee MSS-standardin mukaan merkitä allekirjoituspyyntöön elementti MSSP_Info ja sille elementti MSSP_ID. Jälkimmäisen elementin voi kuitenkin allekirjoituspyynnössä nomaalisti jättää tyhjäksi, sillä AP:n ei tarvitse tietää mille HMSSP:lle allekirjoituspyyntö on osoitettu.

```
<MSSP_Info>
    <MSSP_ID/>
</MSSP_Info>
```

Jos elementti MSSP_Info tai sen sisältämä elementti MSSP_ID puuttuvat allekirjoituspyynnöstä, AE palauttaa AP:lle statuskoodin 102 (MISSING_PARAM). Jos AP on antanut MSSP_ID:lle arvon ja AE ei jostain syystä kelpuuta tätä arvoa, AE palauttaa AP:lle statuskoodin 101 (WRONG_PARAM). AE:lle sopiessaankin parametrin arvo saattaa aiheuttaa myöhempiä reititysongelmia, joita ilmaistaan statuskoodeilla 750-780.

6.2.2.3 MobileUser

Loppukäyttäjän yhteystietona suositellaan käytettävän matkapuhelinnumeroa (MSISDN). Matkapuhelinnumeron perusteella on Suomessa selvitettävissä Käyttäjän kotioperaattori (HMSSP) numeron siirrettävyyspalvelun avulla. Muita MSS-standardin kuvaamia Käyttäjän yhteystietoja FiCom-suositus ei takaa tuettavan tässä versiossa. Puhelinnumero vaaditaan kansainvälisessä numeroformaatissa (Suomessa merkitsee etuliitettä +358).

```
<MobileUser>
    <MSISDN>+358123456789</MSISDN>
</MobileUser>
```

Jos Käyttäjän yhteystieto puuttuu, AE ei kykene yhteystiedon perusteella päättelemään HMSSP:tä, tai HMSSP ei yhteystiedon perusteella tunnista Käyttäjää, vastaavasti AE tai HMSSP palauttaa AP:lle statuskoodin 105 (UNKNOWN_CLIENT). Jos HMSSP tunnistaa Käyttäjän, muttei jostain syystä tavoita Käyttäjää, HMSSP palauttaa AP:lle statuskoodin 209 (OTA_ERROR).

6.2.2.4 DataToBeSigned

Elementissä välitetään Käyttäjän allekirjoitettavaksi osoitettu sisältö. Sisältö on joko:

- selväkielistä, ihmisen luettavaa sopimustekstiä
- mielivaltaisen binaaritiedon tiiviste
- pitkä satunnaisluku eli tunnistushaaste

Allekirjoitettavaan sopimussisältöön on suositeltavaa sisällyttää aikaleima tai muu selväkielinen tapahtuman yksilöivä tunniste.

Tunnistushaastetta ei näytetä Käyttäjälle lainkaan, vaan haasteen sijaan näytetään tunnistustapahtuman vakiomuotoinen kuvaus.

Allekirjoitettavan sisällön maksimipituus on 160 merkkiä. Jos allekirjoituspyynnön sisältö on tätä pidempi, HMSSP palauttaa AP:lle statuskoodin 103 (WRONG_DATA_LENGTH). Allekirjoitettavat tiivisteet ovat käytännössä 20-64 oktettia pitkiä.

Elementillä on varsinaisen allekirjoitettavan sisällön lisäksi kaksi attribuuttia, jotka kertovat sisällön formaatin:

Nimi	Arvo	Kuvaus	Vaadittu
MimeType	string	Allekirjoitettavan sisällön MIME-tyyppi	Ei
Encoding	string	Käytetty merkistö.	Ei

MimeType

Allekirjoitettavan sisällön MIME-tyypit on lueteltu seuraavassa taulukossa..

Jos HMSSP ei hyväksy AP:n ilmoittamaa MIME-tyyppiä, HMSSP palauttaa AP:lle statuskoodin 107 (INAPPROPRIATE_DATA).

Encoding

Allekirjoitettavan sisällön enkoodaus. Mikäli allekirjoitetaan tunnistushaaste tai tiiviste, voidaan Encoding-tyypiksi astettaa ”base64”. Tällöin voidaan elementin arvoksi asettaa haasteen tai tiivisteen arvo (raakatavuina) base64-enkoodattuna. Selväkielisellä tekstillä tuettuja enkoodauksia ovat mm. UTF-8.

Jos HMSSP ei hyväksy AP:n ilmoittamaa merkistöä, HMSSP palauttaa AP:lle statuskoodin 107 (INAPPROPRIATE_DATA).

Oheinen taulukko kuvaa MimeType/Encoding yhdistelmiä, joita FiCom-suositus takaa tuettavan. Muita yhdistelmiä ei sallita.

MimeType	Encoding	Kuvaus	MSS_ Format	Signa Profil
text/plain	UTF-8	Geneerinen selväkielisen tekstin allekirjoitus. AP lähettää tekstin UTF-8-merkistössä, HMSSP konvertoi sen GSM 03.38-merkistöön.	PKCS1 PKCS7	A,S
text/plain;UTF-8	base64	Base64-enkoodattu selväkielisen UTF-8-tekstin allekirjoitus. HMSSP base64-dekodaa tekstin ja konvertoi sen GSM 03.38-merkistöön.	PKCS1 PKCS7	A,S
text/plain;gsm	base64	Base64-enkoodattu selväkielisen GSM 03.38-tekstin allekirjoitus. HMSSP base64-dekoodaa tekstin ja säilyttää alkuperäisen merkistön.	PKCS1 PKCS7	A,S
text/plain;ucs2	base64	Base64-enkoodattu selväkielisen UCS2-tekstin allekirjoitus. HMSSP base64-dekoodaa tekstin ja säilyttää alkuperäisen merkistön.	PKCS1 PKCS7	A,S
application/octet-stream	base64	AP:n tuottaman tunnistehaasteen allekirjoitus. AP muodostaa tunnistehaasteen (esimerkiksi AP_TransID:n binääriesitys) ja lähettää sen base64-enkoodattuna DTBS-elementissä. HMSSP base64-dekoodaa haasteen ja tuottaa siitä PKCS#7-allekirjoituksen.	PKCS7	A
application/octet-stream	base64	AP:n tuottaman MessageDigestin allekirjoitus. AP tiivistää allekirjoitettavan sisällön SHA1- tai SHA256-tiivistealgoritmilla ja tuottaa RSAES-PKCS1-v1_5 –standardin mukaisen DER-enkoodatun DigestInfo-rakenteen (MessageDigest).AP lähettää rakenteen base64-enkoodattuna DTBS-elementissä. HMSSP base64-dekoodaa MessageDigestin ja tuottaa MessageDigestistä PKCS#1-allekirjoituksen ilman autentikoituja attribuutteja.	PKCS1	A,D
application/x-sha1	base64	SHA1-tiivistetyn binaaridatan allekirjoitus. AP tiivistää allekirjoitettavan sisällön SHA1-tiivistealgoritmilla ja lähettää rakenteen base64-enkoodattuna DTBS-elementissä. HMSSP base64-dekoodaa tiivistetyn sisällön, lisää sisältöön autentikoituna attribuuttina ”random noncen”, tiivistää täydennetyn sisällön ja tuottaa lopputuloksesta MessageDigestin. Edelleen HMSSP tuottaa MessageDigestista allekirjoituksen, AP:n pyytämän formaatin mukaisesti.	PKCS1 PKCS7	A,D
application/x-sha256	base64	Kuten edellä, mutta käyttäen SHA256-tiivistealgoritmia SHA1:n sijasta.	PKCS1 PKCS7	A,D

*A=tunnistus, S=selväkielisen sanoman sähköinen allekirjoitus, suostumus, D=tiivisteen allekirjoitus

Huom! Jos allekirjoitetaan selväkielistä sanomaa käyttäen UTF-8-merkistöä, HMSSP tekee allekirjoitettavalle sisällölle muunnoksen XML-lomakkeen UTF-8 –merkistöstä päätelaitteen GSM 03.38-merkistöön. Merkkimuunnos tehdään tehokkuussyistä. Palveluntarjoajan on huomioitava HMSSP:n tekemä merkkimuunnos validoidessaan allekirjoituksen itse. Allekirjoitettava sanoma ei muunnoksessa sisällöllisesti muutu, mikäli sanoma ei sisällä GSM 03.38-merkistöön kuulumattomia merkkejä. Liitteessä D on lueteltu GSM 03.38-merkistön symbolit ja niitä vastaavat UTF-8-merkistön symbolit. AP:n tulee luonnollisesti rajoittaa käyttämänsä UTF-8-merkit liitteen D luettelemiin merkkeihin. Jos liitteen D ulkopuolisia merkkejä esiintyy, HMSSP palauttaa AP:lle statuskoodin 107 INAPPROPRIATE_DATA.

Esimerkki tunnistushaasteesta:

```
<DataToBeSigned MimeType="application/octet-stream" Encoding="base64">
```

```
   TWFuIGlzIGRpc3R=
</DataToBeSigned>
```

Esimerkki tiivistämättömästä sopimuksesta:

```
<DataToBeSigned MimeType="text/plain" Encoding="UTF-8">
   Vahvistan muutokset OyCompanyAb:n käyttäjäprofiilissani: uusi postitusosoite
x ; uusi puhelinnumero y.
</DataToBeSigned>
```

Esimerkki tiivisteestä:

```
<DataToBeSigned MimeType="application/octet-stream" Encoding="base64">
   TWFuIGlzIGRpc3Rpbmd1aXNoQA9=
</DataToBeSigned>
```

6.2.2.5 DataToBeDisplayed

FiCom-suositus ei salli tätä elementtiä (ks. poikkeus alla). Kun allekirjoitetaan tiivistettä (bittijonoa) tarkoitukseen varatulla SignatureProfilella, Käyttäjälle näytettävä tiiviste muokataan heksadesimaaliesitykseksi siten kuin on kuvattu dokumentissa Mobiilivarmennepalvelun palvelukuvaus; mutta HMSSP tekee tämän muotoilun automaattisesti AP:n puolesta, eikä DTDB-elementtiä siis käytetä.

Jos DTBD-elementti on mukana AP:n pyynnössä, HMSSP palauttaa AP:lle statuskoodin 101 (WRONG_PARAM).

Huom! Operaattorin tunnistuspalvelussa (ks. SignatureProfile) DataToBeDisplayed on vaadittu elementti eikä kielletty elementti. Jos DTBD-elementti puuttuu tässä käyttötapauksessa, HMSSP palauttaa AP:lle statuskoodin 102 (MISSING_PARAM).

6.2.2.6 MSS_Format

Allekirjoituksen formaatti on joko PKCS#7 tai PKCS#1. Näistä jälkimmäinen on FiComin määrittämä formaatti, joka sisältää PKCS#1-allekirjoituksen yhdessä käyttäjän mobiilivarmenteen kanssa. (Lisää PKCS#1-allekirjoitusformaatista ks. viestityypin MSS_SignatureResp elementin MSS_Signature kuvaus.)

FiCom-suositus *ei* takaa muita allekirjoitusformaatteja tuettavan.

PKCS#7:

```
<MSS_Format>
       <mssURI>http://uri.etsi.org/TS102204/v1.1.2#PKCS7</mssURI>
</MSS_Format>
```

PKCS#1:

```
<MSS_Format>
       <mssURI>http://mss.ficom.fi/TS102204/v1.0.0#PKCS1</mssURI>
</MSS_Format>
```

6.2.2.7 SignatureProfile

SignatureProfile-elementti kertoo, mitä allekirjoituspalvelua Palveluntarjoaja pyytää HMSSP:lta. Toistaiseksi FiCom-suositus huomioi allekirjoitusprofiili-tiedon seuraavasti. FiCom määrittelee kuusi eri palvelua: anonyymi tunnistaminen, käyttäjän tunnistaminen, selväkielisen sisällön allekirjoittaminen, tiivistetyn sisällön allekirjoittaminen, suostumuksen antaminen. FiCom on määrittänyt neljä allekirjoitusprofiilia, joiden URI:t suoraan kertovat, mitä palvelua AP edellyttää.

FiCom-suosituksen huomioimat allekirjoitusprofiilit ovat:

1. anonyymi tunnistaminen

```
<SignatureProfile>
   <mssURI>http://mss.ficom.fi/TS102206/v1.0.0/anonymous-profile.xml</mssURI>
</SignatureProfile>
```

2. tunnistaminen

```
<SignatureProfile>
   <mssURI>http://mss.ficom.fi/TS102206/v1.0.0/authentication-
profile.xml</mssURI>
</SignatureProfile>
```

3. selväkielisen sisällön sähköinen allekirjoitus

```
<SignatureProfile>
   <mssURI>http://mss.ficom.fi/TS102206/v1.0.0/signature-profile.xml</mssURI>
</SignatureProfile>
```

4. tiivistetyn sisällön sähköinen allekirjoitus

```
<SignatureProfile>
   <mssURI>http://mss.ficom.fi/TS102206/v1.0.0/digestive-signature-
profile.xml</mssURI>
</SignatureProfile>
```

5. suostumuksen antaminen

```
<SignatureProfile>
   <mssURI>http://mss.ficom.fi/TS102206/v1.0.0/consent-profile.xml</mssURI>
</SignatureProfile>
```

6. operaattorin tunnistuspalvelu (operaattorin sisäinen palvelu)

Huom! Operaattorin tunnistuspalvelussa DataToBeDisplayed on vaadittu elementti eikä kielletty elementti.

```
<SignatureProfile>
   <mssURI>http://mss.ficom.fi/TS102206/v1.0.0/operauth-profile.xml</mssURI>
</SignatureProfile>
```

Jos Palveluntarjoaja ei merkitse allekirjoitusprofiilia palvelupyyntöönsä, HMSSP olettaa allekirjoitusprofiilin 1 (tunnistaminen).

Jos Palveluntarjoajan edellyttämä allekirjoitusprofiili on jotakin muuta, HMSSP generoi statuskoodin 109 (UNSUPPORTED_PROFILE). Jos Käyttäjä on kieltänyt palvelupyynnöt Palveluntarjoajan edellyttämällä allekirjoitusprofiililla, HMSSP palauttaa AP:lle statuskoodin 109 (UNSUPPORTED_PROFILE)

6.2.2.8 AdditionalServices

Tämä elementti kuvataan jäljempänä kohdassa Lisäarvopalvelut.

6.2.2.9 SignatureProfileComparison (ei käytössä)

FiCom-suosituksen käsittämien allekirjoitusprofiilien puitteissa käytännössä ainoa mielekäs arvo tälle MSS-standardin mukaan optionaaliselle tiedolle on ”exact”. Koska ko. arvo on myös standardin määrittämä oletusarvo, FiCom-suositus ei huomioi elementtiä.

Jos Palveluntarjoaja on liittänyt tämän tiedon mukaan allekirjoituspyyntöön ja antanut tiedolle muun arvon kuin ”exact”, FiCom-suositus ei ota kantaa siihen miten HMSSP reagoi. Mutta mikäli HMSSP generoi AP:lle virheilmoituksen, sen statuskoodi on 109 (UNSUPPORTED_PROFILE).

6.2.2.10 KeyReference (ei käytössä)

FiCom-suositus ei huomioi tätä MSS-standardin optionaalista elementtiä. Allekirjoituslaitteen valinta tai laitteen tietyn varmenteen valinta määräytyy suoraan Palveluntarjoajan edellyttämän allekirjoitusprofiilin perusteella (SignatureProfile). FiCom suosii tätä käytäntöä siksi, että yksityiskohtaisten allekirjoitusprofiilien laatiminen ja päivittäminen helpottuu jos jokaisella allekirjoituslaitteella ja laitteen palvelulla (varmenteella) on oma erillinen profiilinsa.

Jos Palveluntarjoaja on liittänyt mukaan KeyReference –tiedon, FiCom-suositus ei ota kantaa siihen, miten HMSSP tähän tietoon suhtautuu. Mutta mikäli HMSSP generoi AP:lle virheilmoituksen, sen statuskoodi on 404 (NO_KEY_FOUND).

6.2.3 Lisäarvopalvelut

ETSI:n MSS-standardissa on mahdollista määritellä lisäarvopalveluja, jotka allekirjoituspyynnön elementteinä noudattavat muotoa:

```
<AdditionalServices>
   <Service>
      <Description>
         <mssURI>(service 1 URI)</mssURI>
      </Description>
      <(param1)>(parameter 1 value)</(param1)>
      <(param2)>(parameter 2 value)</(param2)>
      . . .
   </Service>
   <Service>
      <Description>
         <mssURI>(service 2 URI)</mssURI>
      </Description>
      <(param1)>(parameter 1 value)</(param1)>
      <(param2)>(parameter 2 value)</(param2)>
      . . .
   </Service>
    . . .
</AdditionalServices>
```

Jokaisella lisäarvopalvelulla on siten yksilöivä URI ja optionaalisesti yksi tai useampi vapaasti määriteltävä parametri. Lisäksi ETSI sallii kullekin lisäarvopalvelulle elementin Entity, jolla AP voi edellyttää tietyn toimijan vastaavan lisäarvopalvelun toteutuksesta. FiCom-suositus ei kuitenkaan elementtiä Entity huomioi, sillä FiComin määrittelemät lisäpalvelut toteuttaa aina HMSSP.

FiCom-suositus käsittää seuraavan taulukon mukaiset lisäarvopalvelut:

Nimi	URI	Vaadittu
Tapahtumatunnus	http://mss.ficom.fi/TS102204/v1.0.0#eventId	Kyllä
Häirinnän estokoodi	http://mss.ficom.fi/TS102204/v1.0.0#noSpam	Kyllä*
AE-validointi	http://mss.ficom.fi/TS102204/v1.0.0#validate	Ei
PersonIdentity	http://mss.ficom.fi/TS102204/v1.0.0#personIdentity	Ei
Kielipreferenssi	http://mss.ficom.fi/TS102204/v1.0.0#userLang	Ei

* Voidaan korvata AP:n itse toteuttamalla vahvalla tai heikolla tunnistamisella, mutta itse lisäarvopalvelun kuvaavan elementin on oltava aina läsnä.

Lisäarvopalvelujen käyttötarkoitus on kuvattu syvemmin suomalaisten teleoperaattorien toimittamassa dokumentissa Mobiilivarmennepalvelun palvelukuvaus.

6.2.3.1 Tapahtumatunnus

Tapahtumatunnuksen tarkoitus on helpottaa mobiilivarmennustapahtuman yhdistämistä vastaavaan asiointikanavan tapahtumaan..Tapahtumatunnus näytetään Käyttäjälle molemmissa kanavissa samanaikaisesti (mikäli se on mahdollista näyttää asiointikanavassa).

Lisäarvopalvelulla on aina yksi parametri, elementti nimeltä EventID. Elementin arvo on mielivaltainen merkkijono.

```
<Service>
   <Description>
      <mssURI>http://mss.ficom.fi/TS102204/v1.0.0#eventId</mssURI>
   </Description>
   <EventID xmlns="http://mss.ficom.fi/TS102204/v1.0.0#>14521412</EventID>
</Service>
```

Mikäli tapahtumatunnus puuttuu, HMSSP palauttaa AP:lle statuskoodin 102 (MISSING_PARAM).

6.2.3.2 Häirinnän estokoodi

Häirinnän estokoodin tarkoitus on estää Käyttäjän matkapuhelimen asiaton härintä. Käyttäjä kertoo asiointikanavassa häirinnän estokoodinsa AP:lle, joka toimittaa sen edelleen HMSSP:lle. Mikäli koodi ei täsmää Käyttäjän profiiliin tallennetun koodin kanssa, HMSSP kieltäytyy palvelemasta palvelupyyntöä.

Lisäarvopalvelulla on aina yksi parametri, elementti nimeltä NoSpamCode. Elementin arvo on vähintään kolmimerkkinen numeroiden ja kirjainten jono. Ensimmäisen merkin on oltava kirjain. Sillä on myös optionaalinen attribuutti nimeltä verify, jonka mahdolliset arvot ovat "yes" tai "no".

```
<Service>
   <Description>
      <mssURI>http://mss.ficom.fi/TS102204/v1.0.0#noSpam</mssURI>
   </Description>
   <NoSpamCode xmlns="http://mss.ficom.fi/TS102204/v1.0.0#">A1B2</NoSpamCode>
</Service>
```

Elementin arvo voi olla myös tyhjä, merkkinä siitä että Käyttäjä on valinnut olla hyödyntämättä häirinnän estoa. (Tällöin Käyttäjän häirinnänestokoodin on vastaavasti oltava poistettuna käytöstä HMSSP:n käyttäjäprofiilissa.)

```
<Service>
   <Description>
      <mssURI>http://mss.ficom.fi/TS102204/v1.0.0#noSpam</mssURI>
```

```
    </Description>
    <NoSpamCode xmlns=”http://mss.ficom.fi/TS102204/v1.0.0#”></NoSpamCode>
</Service>
```

Jos Palveluntarjoajan järjestelmässä mobiiliallekirjoituksia edeltää aina heikko tai vahva tunnistus, tai häirinnän estokoodi on kertaalleen kysytty, koodia ei tarvitse kysyä Käyttäjältä. **Tällöin AP:n tulee liittää elementin NoSpamCode attribuutti ”verify” ja sen arvona ”no”**, mikä pyytää HMSSP:tä ohittamaan häirinnän estokoodin tarkistuksen. Tällöin elementin arvolla ei ole merkitystä.

```
<Service>
    <Description>
        <mssURI>http://mss.ficom.fi/TS102204/v1.0.0#noSpam</mssURI>
    </Description>
    <NoSpamCode verify="no"
xmlns=”http://mss.ficom.fi/TS102204/v1.0.0#”></NoSpamCode>
</Service>
```

Mikäli tämä lisäarvopalvelu puuttuu allekirjoituspyynnöstä, HMSSP palauttaa AP:lle statuskoodin 102 (MISSING_PARAM). Jos palvelupyynnön estokoodi ei täsmää HMSSP:n käyttäjäprofiilin koodin kanssa, HMSSP palautta AP:ll statuskoodin 101 (WRONG_PARAM).

6.2.3.3 AE-validointi

Validate-palvelulla Palveluntarjoaja voi pyytää AE:ta tekemään tapahtumalle erillisen validoinnin, HMSSP:n tekemän validoinnin lisäksi. AE:n validointitulos kirjataan erilliseen lisäarvopalvelun vastauselementtiin (ks. AE;n validointivastaus jäljempänä).

6.2.3.4 PersonIdentity

PersonIdentity-palvelulla Palveluntarjoaja voi pyytää HMSSP:tä toimittamaan allekirjoitusvastauksessa sellaisia henkilötietoja, jotka eivät löydy Käyttäjän mobiilivarmenteesta, sekä mahdollisesti toimittamaan myös mobiilivarmenteen tietoja ”valmiiksi parsittuna”. Pyydetyt henkilötiedot yksilöidään URI-nimillä. Allaolevassa esimerkissä Palveluntarjoaja pyytää HMSSP:ltä henkilötunnusta ja postiosoitetta.

6.2.3.4.1 Henkilötietokysely

Henkilötietokysely on SAML2 attribuuttikysely, seuraavilla käyttöohjeilla.

Samlp:AttributeQuery sisältää aina seuraavat pakolliset kentät [SAML2 Core, luku 3].

Kentän nimi	Käyttöohje
ID	Pakollinen [Saml2Core, 3.2.1]. Arvona esimerkiksi AP_TransID:n kopio.
Version	Pakollinen [Saml2Core, 3.2.1]. Arvona ”2.0”.
IssueInstant	Pakollinen [Saml2Core, 3.2.1]. Arvona esimerkiksi MSS-viestin Instantin kopio.
Subject ja Subject.NameID	Pakollinen [SAML2Core, 3.3.2.1]. Subject on se henkilö, jonka henkilötietoja nyt kysytään. AP ei lähtökohtaisesti tiedä Subjectista muuta kuin puhelinnumeron, eikä puhelinnumero ole henkilötietojen todellinen hakuehto. AP kirjoittaa Subject–kentän siten, että se sisältää tyhjän NameID –kentän.

Henkilötietokyselyn varsinainen sisältö on luettelo niistä henkilön attribuuteista, jotka palveluntarjoaja haluaa tunnistuspyynnön vastauksessa tietoonsa. Seuraava taulukko luettelee URI-nimetyt attribuutit, joita FiCom-suositus takaa tuettavan. Palveluntarjoaja kuvaa attribuutit vain niiden teknisillä URI-nimillä.

Attribuutin nimi	Kuvaus
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#hetu	Vastaussanomassa on käyttäjän henkilötunnus. Palvelu vaatii erillisen sopimuksen. Tietotyyppi xs:string
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#satu	Käyttäjän varmenteessa oleva käyttäjän sähköinen asiointitunnus. Tietotyyppi xs:string
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#address	Käyttäjän osoite, joka on tallennettu operaattorin järjestelmään. Semantiikka: JHS 106 Tietotyyppi fi:PostalAddress
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#age	Käyttäjän ikä vuosina. Tietotyyppi xs:integer
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#ageClass	Onko käyttäjä täyttänyt 18 vuotta? Arvojoukko true/false. Tietotyyppi xs:boolean
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#email	Käyttäjän sähköpostiosoite Tietotyyppi xs:string
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#gender	Käyttäjän sukupuoli. M=mies F=nainen. Tietotyyppi xs:string
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#givenName	Käyttäjän varmenteessa oleva käyttäjän etunimitieto. (Käyttäjän kaikki etunimet, esim. Teemu Tapani.) Tietotyyppi xs:string
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#surName	Käyttäjän varmenteessa oleva käyttäjän sukunimitieto. (Esim. Nykänen) Tietotyyppi xs:string
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#subject	Käyttäjän varmenteen Subject-kentän arvo. Tietotyyppi xs:string
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#validUntil	Käyttäjän varmenteen viimeinen voimassaolo. Tietotyyppi xs:dateTime

Henkilötiedot palautetaan tavalla, joka on kuvattu viestityypin MSS_SignatureResp elementin Status kohdalla.

6.2.3.4.2 Esimerkki PersonIdentity-palvelun SAML2-attribuuttikyselystä

```
<Service>
   <Description>
     <mssURI>http://mss.ficom.fi/TS102204/v1.0.0#personIdentity</mssURI>
   </Description>
   <samlp:AttributeQuery ID="id-20090817105401849"
       Version="2.0"
       IssueInstant="2009-08-17T10:54:01.849+03:00"
       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
       xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     <saml:Subject>
        <saml:NameID/>
     </saml:Subject>
     <saml:Attribute
        Name="http://mss.ficom.fi/TS102204/v1.0.0/PersonID#hetu"/>
     <saml:Attribute
        Name="http://mss.ficom.fi/TS102204/v1.0.0/PersonID#address"/>
```

```
    </samlp:AttributeQuery>
</Service>
```

6.2.3.5 **Kielipreferenssi**

Kielipreferenssillä kerrotaan HMSSP:lle, millä kielellä AP haluaa tarjota palvelua.

Lisäarvopalvelulla on aina yksi parametri, elemetti nimeltä UserLang. Elementin arvo on ISO-639-1 määrityksen mukainen kaksikirjaiminen kielikoodi, esim. ”fi”, ”sv”, ”en”. FiCom-suositus takaa, että tämä lisäarvopalvelu syntaktisesti hyväksytään, mutta palvelun implementointi ja tarkemmat käyttöohjeet ovat HMSSP-kohtaisia.

```
<Service>
   <Description>
      <mssURI>http://mss.ficom.fi/TS102204/v1.0.0#userLang</mssURI>
   </Description>
   <UserLang xmlns=”http://mss.ficom.fi/TS102204/v1.0.0#”>fi</UserLang>
</Service>
```

6.2.4 Esimerkki: allekirjoituspyyntö

Ohessa lyhentämätön ja kommentoitu esimerkki, joka kokoaa yhdeksi viestiksi kuvatut allekirjoituspyynnön attribuutit ja elementit.

```
POST /MSS_Signature HTTP/1.0
Host: mss.teliasonera.com
Content-Type: application/soap+xml; charset="utf-8"
Content-Length: ...

<?xml version="1.0"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
<env:Body>
   <!- WSDL:n edellyttämä wrapper-elementti -->
   <MSS_Signature>

   <!- Allekirjoituspyyntö alkaa, huomaa nimiavaruuksien varaus -->
   <MSS_SignatureReq xmlns="http://uri.etsi.org/TS102204/v1.1.2#"
xmlns:fi="http://mss.ficom.fi/TS102204/v1.0.0#" MajorVersion="1" MinorVersion="1"
MessagingMode="synch">

      <!- Palveluntarjoajan yhteystieto, tapahtumanumero ja aikaleima -->
      <AP_Info AP_ID="http://mss.teliasonera.com/mssURI/oycompanyab"
AP_TransID="A1203" AP_PWD="ssl" Instant="2003-06-24T21:32:00Z"/>

      <!- Acquiring Entityn yhteystieto -->
      <MSSP_Info>
         <MSSP_ID>
            <URI>http://mss.teliasonera.com</URI>
         </MSSP_ID>
      </MSSP_Info>

      <!- Loppukäyttäjän yhteystieto -->
      <MobileUser>
         <MSISDN>+358123456789</MSISDN>
      </MobileUser>

      <!- Allekirjoitettava tunnistushaaste -->
      <DataToBeSigned MimeType="text/plain" Encoding="UTF-8">
         24F56B879D6ADF71027E65A7095D1162EAF17C7A
      </DataToBeSigned>

      <!- Allekirjoitusprofiili eli valittu allekirjoituspalvelu -->
      <SignatureProfile>
         <mssURI>http://mss.ficom.fi/TS102206/v1.0.0/authentication-profile.xml
</mssURI>
      </SignatureProfile>

      <!- Lisäarvopalvelut -->
      <AdditionalServices>
         <Service>
            <Description>
               <mssURI>http://mss.ficom.fi/TS102204/v1.0.0#eventId</mssURI>
            </Description>
            <fi:EventID>A1B2</fi:EventID>
         </Service>
         <Service>
            <Description>
               <mssURI>http://mss.ficom.fi/TS102204/v1.0.0#noSpam</mssURI>
            </Description>
            <fi:NoSpamCode>A1B2</fi:NoSpamCode>
         </Service>
```

```
      </AdditionalServices>

   </MSS_SignatureReq>
   </MSS_Signature>
</env:Body>
</env:Envelope>
```

6.3 Allekirjoitusvastaus (MSS_SignatureResp)

Allekirjoitusvastauksen luo HMSSP. Vastaus reititetään AE:n kautta Palveluntarjoajalle. Palveluntarjoaja saa vastauksen samassa HTTP-istunnossa, jossa lähetti allekirjoituspyynnön (synkroninen viestintä) tai viimeisen statuskyselyn (asynkroninen client-server viestintä). Mikäli käytetään asynkronista client-server viestintää, allekirjoitusvastaus palautetaan välittömästi ja status-tiedossa kerrotaan tapahtuman olevan kesken 504 (OUTSTANDING_TRANSACTION). Virhetilanteissa, joissa AE ei kykene toimittamaan allekirjoituspyyntöä edelleen HMSSP:lle, allekirjoitusvastauksen luo virhekoodeineen AE itse.

Allekirjoitusvastaus sisältää seuraavat tiedot:

- Palveluntarjoajan yhteystieto
- Allekirjoitusvastauksen luoneen MSSP:n yhteystieto
- Käyttäjän yhteystieto
- Aikaleima
- Tapahtuman loppustatus
- mahdolliset lisäarvopalvelujen vastausviestit

Allekirjoituksen onnistuttua lisäksi:

- HMSSP:n noudattama allekirjoitusprofiili
- Sähköinen allekirjoitus

6.3.1 MSS_SignatureResp: attribuutit

Nimi	Arvo	Kuvaus	Vaadittu
MajorVersion	”1”	Rajapinnan yläversio, tällä hetkellä 1.	Kyllä
MinorVersion	”1”	Rajapinnan alaversio, tällä hetkellä 1.	Kyllä
MSSP_TransID	NCName	MSSP:n generoima tapahtumanumero.	Kyllä

6.3.1.1 MajorVersion ja MinorVersion

Käytetyn MSS-rajapinnan versio on tällä hetkellä 1.1.

6.3.1.2 MSSP_TransID

HMSSP:n on liitettävä vastaukseen *omalta* kannaltaan yksikäsitteinen tapahtumanumero. (Sallittu merkistö ks. http://www.w3.org/TR/xmlschema-2/#NCName) Tapahtumanumeron maksimipituus on 19 merkkiä.

Esimerkki: MSS_SignatureResp–elementin attribuutit

```
<MSS_SignatureResp xmlns="http://uri.etsi.org/TS102204/v1.1.2#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" MajorVersion="1"
MinorVersion="1" MSSP_TransID="B653">
```

6.3.2 MSS_SignatureResp: elementit

Nimi	Kuvaus	Vaadittu
AP_Info	Kopioidaan suoraan pyynnöstä (MSS_SignatureReq).	Kyllä

MSSP_Info	MSSP:n yhteystieto. Käytetään URI-muotoa.	Kyllä
MobileUser	Kopioidaan suoraan pyynnöstä (MSS_SignatureReq).	Kyllä
Status	Tapahtuman loppustatus.	Kyllä
SignatureProfile	Käytetty allekirjoitusprofiili.	Ei*
MSS_Signature	Sähköinen allekirjoitus.	Ei*

*virhetilanteissa ei yleensä voida liittää mukaan

6.3.2.1 AP_Info

Elementti on suora kopio AP:n lähettämän allekirjoituspyynnön (MSS_SignatureReq) samannimisestä elementistä.

6.3.2.2 MSSP_Info

Allekirjoitusvastauksessa MSSP_Info kertoo HMSSP:n identiteetin. MSSP:n tulee käyttää URI-muotoista esitystapaa identiteettinsä kirjaamiseen (alielementissä nimeltä MSSP_ID). Esityksen maksimipituus on 64 merkkiä. MSSP:n on lisäksi annettava MSSP_Info –elementille attribuutti ”Instant”. Attribuutti saa arvokseen aikaleiman, joka kertoo allekirjoitusvastauksen lähettämishetken. (Ks. http://www.w3.org/TR/xmlschema-2/#dateTime) Esimerkki URI-tyyppisestä identiteetistä:

```
<MSSP_Info Instant="2003-06-24T21:33:00Z">
   <MSSP_ID>
      <URI>http://mss.elisa.fi</URI>
   </MSSP_ID>
</MSSP_Info>
```

6.3.2.3 MobileUser

Elementti on suora kopio AP:n lähettämän allekirjoituspyynnön (MSS_SignatureReq) samannimisestä elementistä.

6.3.2.4 Status

Elementti kertoo tapahtuman statuksen (synkronisessa viestinnässä loppustatuksen). Elementti koostuu MSS-standardin mukaisesta statuskoodista (StatusCode), jolla on pakollinen integer-tyyppinen attribuutti Value, optionaalisesta statusviestistä (StatusMessage) sekä optionaalisesta lisäelementistä (StatusDetail).

Statusviesti on arvoltaan aina MSS-standardissa kerrottu, statuskoodia vastaava nimi; nämä nimet on lueteltu dokumentin liitteissä.

StatusDetail sisältää elementin ServiceResponse, joka jakaantuu ServiceResponse-nimisiin alielementteihin käytettyjen lisäarvopalvelujen mukaisesti. Lisäarvopalvelujen vastausviestit on kuvattu jäljempänä.

```
<Status>
   <StatusCode Value="500"/>
   <StatusMessage>SIGNATURE</StatusMessage>
   <StatusDetail>
      <fi:ServiceResponses>
         <fi:ServiceResponse>
            <fi:Description>
               <mssURI>http://uri.etsi.org/TS102204/v1.1.2#validate</mssURI>
            </fi:Description>
            <fi:Entity>
               <mssURI>http://ae.elisa.fi</mssURI>
            </fi:Entity>
            <fi:Status>
               <mss:StatusCode Value="502"/>
               <mss:StatusMessage>VALID_SIGNATURE</mss:StatusMessage>
            </fi:Status>
         </fi:ServiceResponse>
         <fi:ServiceResponse>
            <fi:Description>
               <mssURI>
                  http://mss.ficom.fi/TS102204/v1.0.0#personIdentity
               </mssURI>
            </fi:Description>
            <samlp:Response
               ID="id-20090817105401849"
               ...
            </samlp:Response>
         </fi:ServiceResponse>
         ...
      </fi:ServiceResponses>
   </StatusDetail>
</Status>
```

Statuskoodien arvoissa noudatetaan oheisia MSS-standardin sääntöjä:

Asynkronisessa client-server viestintätavassa HMSSP kuittaa tapahtuman vastaanotetuksi (mutta ei vielä valmiiksi) statuskoodilla 100 (REQUEST_OK). Kun HMSSP on onnistunut koostamaan sähköisen allekirjoituksen, HMSSP validoi tapahtuman (HMSSP:n lisäksi myös AE voi validoida tapahtuman, mikäli Palveluntarjoaja pyytää tällaista lisäarvopalvelua. Ks. AE-validointivastaus jäljempänä.)

Jos tapahtuman validoija

- toteaa sähköisen allekirjoituksen validiksi, statuskoodi on 502 (VALID_SIGNATURE)
- toteaa sähköisen allekirjoituksen validiksi muilta osin, mutta Käyttäjän varmenteen tietosisältö ei täytä allekirjoitusprofiilissa määritettyjä lisäehtoja, statuskoodi on 505 (CONSTRAINT_MISMATCH)
  - lisäehtovirhe voi olla esimerkiksi varmennepolitiikan tunnisteen puuttuminen tai tunnisteen ei-sallittu arvo
- havaitsee allekirjoittajan joutuneen sulkulistalle, statuskoodi on 501 (REVOKED_CERTIFICATE)
- havaitsee sähköisen allekirjoituksen virheelliseksi tai varmenteen vanhentuneen, statuskoodi on 503 (INVALID_SIGNATURE)

6.3.2.5 AE:n validointivastaus

Vastuu allekirjoitustapahtumien validoinnista on normaalisti HMSSP:lla. HMSSP:n lisäksi myös AE voi halutessaan validoida allekirjoitustapahtuman. AE merkitsee validoinnin antaman

loppustatuksen StatusDetail-elementin sisältämäksi ServiceReseponseksi, missä lisäarvopalvelun tunniste on:

http://uri.etsi.org/TS102204/v1.1.2#validate

(Ks. esimerkki edellä.)

Jos HMSSP on validoinut allekirjoitustapahtuman ja kirjannut statuskoodin 501 (REVOKED_SIGNATURE) tai 503 (INVALID_SIGNATURE), AE saa jättää tapahtuman validoimatta ja AE:n tulee toistaa HMSSP:n raportoima statuskoodi.

Jos HMSSP on validoinut tapahtuman ja kirjannut statuskoodin 502 (VALID_SIGNATURE), 424 (CRL_EXPIRED) tai 425 (ERROR_CERTIFICATE), AE validoi tapahtuman ja kirjaa statuskoodiksi oman validointinsa mukaisen statuksen.

6.3.2.6 PersonIdentity-lisäarvopalvelun vastaus

PersonIdentity-lisäarvopalvelun vastausviesti kirjataan StatusDetail-elementin sisältämäksi ServiceResponseksi, missä lisäarvopalvelun tunniste on:

http://mss.ficom.fi/TS102204/v1.0.0#personIdentity

(Ks. esimerkki edellä.)

PersonIdentity-lisäarvopalvelun vastaus on SAML2 vastausviesti, seuraavilla soveltamisohjeilla.

Samlp:Response sisältää aina seuraavat pakolliset kentät [SAML2 Core, luku 3].

Kentän nimi	Käyttöohje
ID	Pakollinen. Arvona henkilötietokyselyn ID-kentän kopio.
Version	Pakollinen. Arvona ”2.0”.
IssueInstant	Pakollinen. Arvona se hetki, jolloin SAML2-palvelu loi vastauksen. Tämä voi poiketa MSS-vastausviestin aikaleimasta.
Status ja Status.StatusCode	Pakollinen. Status-kentässä on pakollisena sisältönä StatusCode-arvo. Sen arvojoukko on seuraavassa taulukossa.

SAMLP-statuskoodi	Kuvaus
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#ok	Henkilötietohaku onnistui.
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#partialFailure	Henkilötietohaku epäonnistui osittain. Vastauksessa voi silti olla se osa henkilötiedoista, jotka palvelu onnistui selvittämään.
http://mss.ficom.fi/TS102204/v1.0.0/PersonID#failure	Henkilötietohaku epäonnistui kokonaan.

Pakollisten tietojen lisäksi henkilötietovastauksessa on henkilötiedot attribuutteina esitettynä Henkilötietokysely-luvun taulukon kuvaamalla tavalla.

Vastauksen samlp:Response elementti on HMSSP:n allekirjoittama vastauksen sisäisellä XML-allekirjoituksella [XML Signature, SAML2 Core luku 5]. Allekirjoitus sisältää ds:X509Certificate elementeissä allekirjoitukseen käytetyn varmenteen ja mahdollisen varmennepolun HMSSP:n juurivarmentajaan asti.

6.3.2.7 Esimerkki PersonIdentity-lisäarvopalvelun SAML2-assertiosta

```
<fi:ServiceResponse>
   <Description>
     <mssURI>http://mss.ficom.fi/TS102204/v1.0.0#personIdentity</mssURI>
   </Description>
   <samlp:Response ID="id-20090817105442102"
       Version="2.0"
       IssueInstant="2009-08-17T10:54:42.102+03:00"
       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
       xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
       <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
         <ds:SignedInfo>
             <ds:CanonicalizationMethod
                 Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
             <ds:SignatureMethod
                 Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
             <ds:Reference URI="#RnlmcdL2pmTIvZ7c">
                 <ds:Transforms>
                     <ds:Transform
               Algorithm="http://www.w3.org/2000/09/xmldsig#envelopedsignature"/>
                     <ds:Transform
                             Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                         <InclusiveNamespaces
                             PrefixList="#default samlp saml ds"
                             xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                     </ds:Transform>
                 </ds:Transforms>
                 <ds:DigestMethod
                     Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                 <ds:DigestValue>TliIDRiYWMgOGIwNyAwNTIxCg==</ds:DigestValue>
             </ds:Reference>
         </ds:SignedInfo>
         <ds:SignatureValue>
             OTYyOCAw...
         </ds:SignatureValue>
         <ds:KeyInfo>
             <ds:X509Data>
                 <ds:X509Certificate>
                     AwYzA2IGQ...
                 </ds:X509Certificate>
                 <ds:X509Certificate>
                     AwYzAOTli...
                 </ds:X509Certificate>
             </ds:X509Data>
         </ds:KeyInfo>
     </ds:Signature>
     <samlp:Status>
        <samlp:StatusCode
           Value="http://mss.ficom.fi/TS102204/v1.0.0/PersonID#ok">
        </samlp:StatusCode>
     </samlp:Status>
     <saml:Subject>
       <saml:NameID/>
     </saml:Subject>
     <saml:Attribute
        Name="http://mss.ficom.fi/TS102204/v1.0.0/PersonID#hetu">
       <saml:AttributeValue type="xs:string">141175-112P</saml:AttributeValue>
     </saml:Attribute>
     <saml:Attribute
        Name="http://mss.ficom.fi/TS102204/v1.0.0/PersonID#address">
       <saml:AttributeValue>
```

```
          <fi:PostalAddress>
            <fi:Name>Sanna Perkiö</fi:Name>
            <fi:StreetAddress>Malminrinne 5 A 12</fi:StreetAddress>
            <fi:PostalCode>00100</fi:PostalCode>
            <fi:Town>Helsinki</fi:Town>
            <fi:Country>Finland</fi:Country>
          </fi:PostalAddress>
        </saml:AttributeValue>
      </saml:Attribute>
    </samlp:Response>
</fi:ServiceResponse>
```

6.3.2.8 SignatureProfile

Elementillä HMSSP kertoo Palveluntarjoajalle, mitä allekirjoitusprofiilia käytettiin. FiCom-suosituksessa tämä elementti on suora kopio AP:n lähettämän allekirjoituspyynnön samannimisestä tiedosta.

6.3.2.9 MSS_Signature

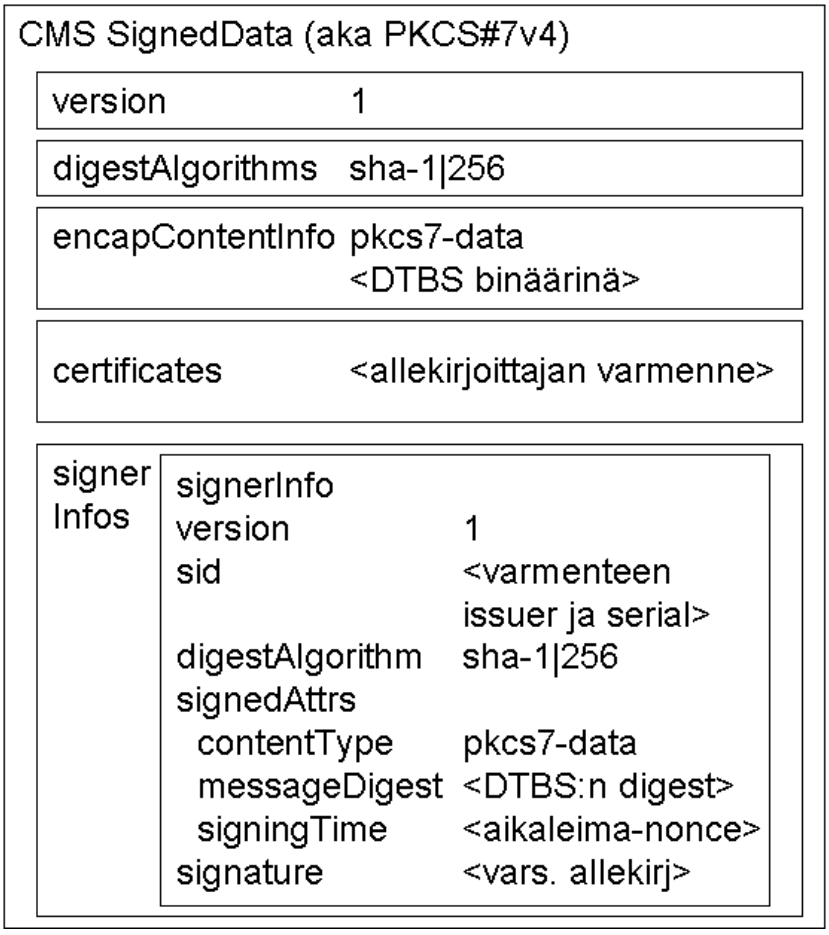
HMSSP:n koostama Käyttäjän sähköinen allekirjoitus on jompikumpi seuraavista:

- **PKCS#7**-standardin mukainen allekirjoitusviesti, joka on **base64**-enkoodattu
- **PKCS#1**-standardin mukainen allekirjoitus yhdessä käyttäjän mobiilivarmenteen kanssa, jotka on **base64**-enkoodattu erillisiin elementeihin (ks. esimerkki alla)

FiCom-suositus *ei* takaa HMSSP:n tukevan muita allekirjoitusformaatteja.

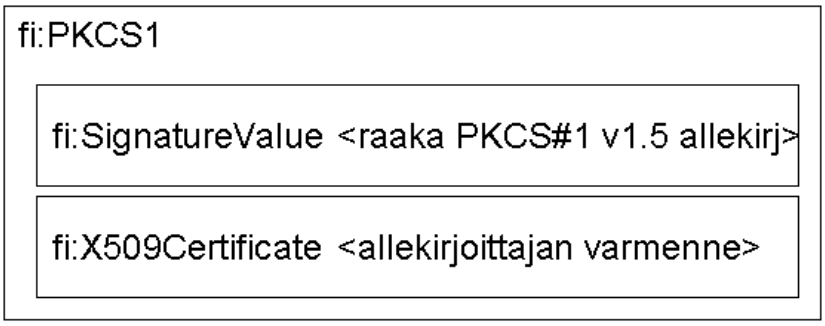
PKCS#7:

```
<MSS_Signature>
   <Base64Signature>ExTOCTrERKqKs+HY1lZfC5Xwd4SqjIXhPwWpHL6TPw2Fu7LtjMkxdEv42jgu
CMBYEGM97sdn23Ewz0NtG7RGRrVaU6Do5B5XfnRr827+bCoZ+Ll8Jgj1ft6PmZXzecDUzTC17QM6tS4+L
WDzTIWq/Qhdeie5b9k6U/EOvqd0wek=</Base64Signature>
</MSS_Signature>
```


CMS SignedData (aka PKCS#7v4)
version 1
digestAlgorithms sha-1|256
encapContentInfo pkcs7-data
<DTBS binäärinä>
certificates <allekirjoittajan varmenne>
signer Infos
signerInfo
version 1
sid <varmenteen issuer ja serial>
digestAlgorithm sha-1|256
signedAttrs
contentType pkcs7-data
messageDigest <DTBS:n digest>
signingTime <aikaleima-nonce>
signature <vars. allekirj>

PKCS#1:

```
<MSS_Signature>
  <fi:PKCS1 >
<fi:SignatureValue>Jbzj3d2HGmAVeFmcTSEfoZEmPk9uSZs65+gtFdzTP0SuazBJ6ym9SqDKcuqRvH
4WuvurUCgiuyo81bpK0w5pxhIHSBNz...</fi:SignatureValue >
<fi:X509Certificate>MIIDmDCCAoCgAwIBAgIDAI2rMA0GCSqGSIb3DQEBBQUAMEwxCzAJBgNVBAYTA
kZJ…</fi:X509Certificate>
  </ fi:PKCS1>
</MSS_Signature>
```



PKCS#1 on määritelty dokumentissa RFC 2437: RSA Cryptography Specifications Version 2.0

PKCS#7 on määritelty dokumentissa RFC 5652: Cryptographic Message Syntax.

Base64-enkoodaus on määritelty mm. W3C:n suosituksessa:
http://www.w3.org/TR/xmlschema-2/#base64Binary

6.3.3 Esimerkki: allekirjoitusvastaus

```
HTTP/1.0 200 OK
Content-Type: application/soap+xml; charset="utf-8"
Content-Length: ...

<?xml version="1.0"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
   <env:Body>
      <MSS_Signature>

      <!- Allekirjoitusvastaus alkaa -->
      <MSS_SignatureResp xmlns="http://uri.etsi.org/TS102204/v1.1.2#"
MajorVersion="1" MinorVersion="1" MSSP_TransID="B653">

         <!- Palveluntarjoajan yhteystieto, tapahtumanumero ja aikaleima -->
         <AP_Info AP_ID=" http://mss.teliasonera.com/mssURI/oycompanyab"
AP_TransID="A1203" AP_PWD="ssl" Instant="2003-06-24T21:32:00Z"/>

         <!- Vastauksen luojan yhteystieto (HMSSP/AE) -->
         <MSSP_Info Instant="2003-06-24T21:32:28Z">
            <MSSP_ID>
               <URI>http://mss.elisa.fi</URI>
            </MSSP_ID>
         </MSSP_Info>

         <!- Loppukäyttäjän yhteystieto -->
         <MobileUser>
            <MSISDN>+358123456789</MSISDN>
         </MobileUser>

         <!- Sähköinen allekirjoitus -->
         <MSS_Signature>
            <Base64Signature>
ExTOCTrERKqKs+HY1lZfC5Xwd4SqjIXhPwWpHL6TPw2Fu7LtjMkxdEv42jguCMBYEGM97sdn23Ewz0NtG
7RGRrVaU6Do5B5XfnRr827+bCoZ+Ll8Jgj1ft6PmZXzecDUzTC17QM6tS4+LWDzTIWq/Qhdeie5b9k6U/
EOvqd0wek=
            </Base64Signature>
         </MSS_Signature>

         <!- Tapahtuman loppustatus -->
         <Status>
            <StatusCode Value="502"/>
            <StatusMessage>VALID_SIGNATURE</StatusMessage>
            <StatusDetail>
               <fi:ServiceResponses>

               <!-- Tämä on AE:n tuottama validointikuitti -->
                  <fi:ServiceResponse>
                     <fi:Description>
                        http://uri.etsi.org/TS102204/v1.1.2#validate
                     </fi:Description>
                     <fi:Entity>
                        <mss:URI>http://askonae.methics.fi</mss:URI>
                     </fi:Entity>
                     <fi:Status>
                        <mss:StatusCode Value="502"/>
                        <mss:StatusMessage>VALID_SIGNATURE</mss:StatusMessage>
                     </fi:Status>
                  </fi:ServiceResponse>
               </fi:ServiceResponses>
            </mss:StatusDetail>
```

```
          </Status>

       </MSS_SignatureResp>
       </MSS_Signature>
    </env:Body>
</env:Envelope>
```

6.4 Statuskysely (MSS_StatusReq)

Statuskyselyllä Palveluntarjoaja tiedustelee aiemmin lähettämänsä palvelupyynnön valmistumista HMSSP:ltä asynkronisessa client-server viestinnässä. Statuskysely toistetaan Palveluntarjoajan järjestelmästä kunnes tapahtuman status on jokin muu kuin ”käsittely kesken” (504 OUTSTANDING_TRANSACTION). Kutakin statuskyselyä varten avataan erillinen HTTP-istunto, mutta TCP-protokollan tasolla Palveluntarjoajaa suositellaan käyttämään persistenttejä yhteyksiä esimerkiksi 5 minuutin ”idle timeoutilla” eli aikakatkaisulla AP:n järjestelmien puolelta mikäli TCP-kanavassa ei ole liikennettä 5 minuutin aikana.

HMSSP-järjestelmien tarpeettoman kuormittamisen välttämiseksi Palveluntarjoajaa suositellaan tekemään ensimmäinen statuskysely vasta 20 sekuntia sen jälkeen kun on saanut HMSSP:ltä kuittauksen allekirjoituspyynnön vastaanottamisesta (MSS_SignatureResp). Lisäksi samaa tapahtumaa koskevia kyselyjä ei suositella toistettavaksi tiheämmin kuin kerran 5 sekunnissa. Jälkimmäinen rajoitus perustuu siihen, että statuskyselyt aiheuttavat turhaa kuormaa silloin kun tapahtuma päättyy Käyttäjästä johtuvaan timeoutiin.

6.4.1 MSS_StatusReq: attribuutit

Nimi	Arvo	Kuvaus	Vaadittu
MajorVersion	”1”	Rajapinnan yläversio, tällä hetkellä 1.	Kyllä
MinorVersion	”1”	Rajapinnan alaversio, tällä hetkellä 1.	Kyllä
MSSP_TransID	NCName	HMSSP:n generoima tapahtumanumero.	Kyllä

6.4.1.1 MajorVersion ja MinorVersion

Käytetyn MSS-rajapinnan versio on tällä hetkellä 1.1. Mikäli AP:n asettama versionumero poikkeaa tästä, AE palauttaa AP:lle statuskoodin 108 (INCOMPATIBLE_INTERFACE).

6.4.1.2 MSSP_TransID

Attribuutti sisältää tapahtumanumeron, jonka Palveluntarjoaja sai aiemmin tapahtuman allekirjoitusvastauksessa HMSSP:ltä, eli kopio elementin MSS_SignatureResp attribuutista MSSP_TransID. Tällä numerolla Palveluntarjoaja kohdistaa statuskyselyn alunperin käynnistämäänsä allekirjoitustapahtumaan.

Jos tapahtumanumero puuttuu, tai HMSSP ei jostain syystä kykene yhdistämään statuskyselyä allekirjoitustapahtumaan, HMSSP palauttaa AP:lle statuskoodin 101 (WRONG_PARAM).

Esimerkki: MSS_StatusReq–elementin attribuutit

Esimerkin toinen rivi sisältää viittauksen XMLSignature-määrityksiin, jotka mahdollistavat XML-allekirjoitetut kuitit.

```
<MSS_StatusReq xmlns="http://uri.etsi.org/TS102204/v1.1.2#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" MajorVersion="1" MinorVersion="1"
MSSP_Trans_ID="B653">
```

6.4.2 MSS_StatusReq: elementit

Nimi	Kuvaus	Vaadittu
AP_Info	Palveluntarjoajan yhteystieto sekä AP:n tapahtumalle antama tapahtumanumero ja aikaleima.	Kyllä
MSSP_Info	MSSP_ID –kenttään kopio MSS_SignatureResp –viestin MSSP_ID –kentästä.	Kyllä

6.4.2.1 AP_Info

Elementti on suora kopio AP:n aiemmin lähettämän allekirjoituspyynnön (MSS_SignatureReq) samannimisestä elementistä. Kuittauspyynnölle on kuitenkin annettava aikaleima, eli elementin AP_Info attribuutti Instant on uusittava vastaamaan statuskyselyn lähettämishetkeä.

6.4.2.2 MSSP_Info

Elementti sisältää kopion MSS_SignatureResp –viestin MSSP_ID –elementistä.

6.4.3 Esimerkki: statuskysely

Huomaa, että kuittauspyynnön aikaleima on uusittu ja WSDL-operaation nimi on muutettu verrattuna allekirjoituspyyntö-esimerkkiin.

```
HTTP/1.0 200 OK
Content-Type: application/soap+xml; charset="utf-8"
Content-Length: ...

<?xml version="1.0"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
   <env:Body>

      <MSS_StatusQuery>

      <!- Statuskysely alkaa -->
      <MSS_StatusReq xmlns="http://uri.etsi.org/TS102204/v1.1.2#"
MajorVersion="1" MinorVersion="1" MSSP_TransID="B653">

         <!- Palveluntarjoajan yhteystieto, tapahtumanumero ja aikaleima -->
         <AP_Info AP_ID="http://mss.teliasonera.com/mssURI/oycompanyab"
AP_TransID="A204" AP_PWD="ssl" Instant="2003-06-24T21:32:31Z"/>

         <!- HMSSP:n yhteystieto -->
         <MSSP_Info>
            <MSSP_ID>
               <URI>http://mss.teliasonera.com</URI>
            </MSSP_ID>
         </MSSP_Info>
      </MSS_StatusReq>

      </MSS_StatusQuery>
   </env:Body>
</env:Envelope>
```

6.5 Statusvastaus (MSS_StatusResp)

Statusvastauksessa HMSSP kertoo Palveluntarjoajalle tämän käynnistämän allekirjoitustapahtuman tilanteen.

6.5.1 MSS_StatusResp: attribuutit

Nimi	Arvo	Kuvaus	Vaadittu
MajorVersion	”1”	Rajapinnan yläversio, tällä hetkellä 1.	Kyllä
MinorVersion	”1”	Rajapinnan alaversio, tällä hetkellä 1.	Kyllä

6.5.1.1 MajorVersion ja MinorVersion

Käytetyn MSS-rajapinnan versio on tällä hetkellä 1.1.

6.5.2 MSS_StatusResp: elementit

Nimi	Kuvaus	Vaadittu
AP_Info	Palveluntarjoajan yhteystieto sekä AP:n tapahtumalle antama tapahtumanumero ja aikaleima.	Kyllä
MSSP_Info	AE:n yhteystieto.	Kyllä
MobileUser	Loppukäyttäjän yhteystieto, toistaiseksi aina elementti muotoa: <MSISDN>+358x01234567</MSISDN> missä matkapuhelinnumeron alkuosa +358 (Suomessa) on pakollinen, eli noudatetaan kansainvälistä numeroformaattia.	Kyllä
MSS_Signature	Sähköinen allekirjoitus.	Ei
Status	Tapahtuman loppustatus.	Kyllä

6.5.2.1 AP_Info ja MSSP_Info

Elementit ovat identtisiä allekirjoituspyynnön (MSS_SignatureReq) samannimisten elementtien kanssa.

6.5.2.2 MobileUser

Elementti on identtinen allekirjoituspyynnön (MSS_SignatureReq) samannimisen elementin kanssa.

6.5.2.3 MSS_Signature

Elementti on identtinen allekirjoitusvastauksen (MSS_SignatureResp) samannimisen elementin kanssa.

6.5.2.4 Status

Elementti kertoo allekirjoitustapahtuman tämänhetkisen statuksen. Jos tapahtuman käsittely on edelleen kesken, HMSSP palauttaa AP:lle statuskoodin 504 (OUTSTANDING_TRANSACTION). Jos tapahtuman käsittely on valmis, elementti on identtinen allekirjoitusvastauksen (MSS_SignatureResp) samannimisen elementin kanssa.

6.5.3 Esimerkki: statusvastaus

```
HTTP/1.0 200 OK
Content-Type: application/soap+xml; charset="utf-8"
Content-Length: ...

<?xml version="1.0"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
   <env:Body>
      <MSS_StatusQuery>

      <!- Statusvastaus alkaa -->
      <MSS_StatusResp xmlns="http://uri.etsi.org/TS102204/v1.1.2#"
MajorVersion="1" MinorVersion="1" MSSP_TransID="B653">

         <!- Palveluntarjoajan yhteystieto, tapahtumanumero ja aikaleima -->
         <AP_Info AP_ID=" http://mss.teliasonera.com/mssURI/oycompanyab"
AP_TransID="A1203" AP_PWD="ssl" Instant="2003-06-24T21:32:31Z"/>

         <!- Vastauksen luojan yhteystieto (HMSSP/AE) -->
         <MSSP_Info Instant="2003-06-24T21:32:36Z>
            <MSSP_ID>
               <URI>http://mss.elisa.fi</URI>
            </MSSP_ID>
         </MSSP_Info>

         <!- Loppukäyttäjän yhteystieto -->
         <MobileUser>
            <MSISDN>+358123456789</MSISDN>
         </MobileUser>

         <!- Tapahtuman status -->
         <Status>
            <StatusCode Value="504"/>
            <StatusMessage>
               OUTSTANDING_TRANSACTION
            </StatusMessage>
         </Status>
      </MSS_StatusResp>

      </MSS_StatusQuery>
   </env:Body>
</env:Envelope>
```

6.6 Kuittauspyyntö (MSS_ReceiptReq)

Kuittauspyynnön avulla Palveluntarjoa voi allekirjoitustapahtuman jälkeen halutessaan lähettää Käyttäjän matkapuhelimelle kuittauksen tapahtuman onnistumisesta tai epäonnistumisesta.

6.6.1 MSS_ReceiptReq: attribuutit

Nimi	Arvo	Kuvaus	Vaadittu
MajorVersion	”1”	Rajapinnan yläversio, tällä hetkellä 1.	Kyllä
MinorVersion	”1”	Rajapinnan alaversio, tällä hetkellä 1.	Kyllä
MSSP_TransID	NCName	MSSP:n generoima tapahtumanumero.	Kyllä

6.6.1.1 MajorVersion ja MinorVersion

Käytetyn MSS-rajapinnan versio on tällä hetkellä 1.1. Mikäli AP:n asettama versionumero poikkeaa tästä, AE palauttaa AP:lle statuskoodin 108 (INCOMPATIBLE_INTERFACE).

6.6.1.2 MSSP_TransID

Attribuutti sisältää tapahtumanumeron, jonka Palveluntarjoaja sai aiemmin tapahtuman allekirjoitusvastauksessa HMSSP:ltä, eli kopio elementin MSS_SignatureResp attribuutista MSSP_TransID. Tällä numerolla Palveluntarjoaja kohdistaa kuittauspyynnön aiempaan allekirjoitustapahtumaan.

Jos tapahtumanumero puuttuu, tai HMSSP ei jostain syystä kykene yhdistämään kuittauspyyntöä allekirjoitustapahtumaan, HMSSP palauttaa AP:lle statuskoodin 101 (WRONG_PARAM).

Esimerkki: MSS_ReceiptReq–elementin attribuutit

Esimerkin toinen rivi sisältää viittauksen XMLSignature-määrityksiin, jotka mahdollistavat XML-allekirjoitetut kuitit.

```
<MSS_ReceiptReq xmlns="http://uri.etsi.org/TS102204/v1.1.2#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" MajorVersion="1" MinorVersion="1"
MSSP_Trans_ID="B653">
```

6.6.2 MSS_ReceiptReq: elementit

Nimi	Kuvaus	Vaadittu
AP_Info	Palveluntarjoajan yhteystieto sekä AP:n tapahtumalle antama tapahtumanumero ja aikaleima.	Kyllä
MSSP_Info	AE:n yhteystieto.	Kyllä
MobileUser	Loppukäyttäjän yhteystieto, toistaiseksi aina elementti muotoa: <MSISDN>+358123456789</MSISDN> missä matkapuhelinnumeron alkuosa +358 (Suomessa) on pakollinen, eli noudatetaan kansainvälistä numeroformaattia.	Kyllä
Status	Tapahtuman loppustatus.	Ei
Message	Palveluntarjoajan kuittausviesti Käyttäjälle.	Ei
SignedReceipt	Palveluntarjoajan sähköisesti allekirjoittama kuitti.	Ei

6.6.2.1 AP_Info ja MobileUser

Elementit ovat suoria kopioita AP:n aiemmin lähettämän allekirjoituspyynnön (MSS_SignatureReq) samannimisistä elementeistä. Kuittauspyynnölle on kuitenkin annettava aikaleima, eli elementin AP_Info attribuutti Instant on uusittava vastaamaan kuittauspyynnön lähettämishetkeä.

6.6.2.2 MSSP_Info

Elementti sisältää kopion MSS_SignatureResp –viestin MSSP_ID –elementistä.

6.6.2.3 Status

Tapahtuman loppustatus. Elementti on suora kopio tapahtuman allekirjoitusvastauksessa (MSS_SignatureResp) Palveluntarjoajalle toimitetusta samannimisestä elementistä.

6.6.2.4 Message

Käyttäjälle osoitettu kuittausviesti. Viesti voi olla vapaamuotoinen kuitti tehdystä transaktiosta tai yleisempi, tapahtuman loppustatuksen kertova kuittausviesti. Elementillä on samat attribuutit ja pituusrajoitus kuin allekirjoituspyynnön elementillä DataToBeSigned.

6.6.2.5 SignedReceipt

Käyttäjälle osoitettu AP:n allekirjoittama kuittausviesti. FiCom-suositus ei ota kantaa tämän tiedon käyttöön. AP ohjeistaa Käyttäjän asiointikanavaa pitkin mikäli käyttää tätä tietoa. Yleensä kyse on sähköisesti allekirjoitetusta Messagen tiivisteestä; allekirjoituksen tarkistamiseen tarvittu AP:n julkinen avain voidaan kertoa asiointikanavassa.

6.6.3 Esimerkki: kuittauspyyntö

Huomaa, että kuittauspyynnön aikaleima on uusittu verrattuna allekirjoituspyyntö-esimerkkiin.

```
HTTP/1.0 200 OK
Content-Type: application/soap+xml; charset="utf-8"
Content-Length: ...

<?xml version="1.0"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
   <env:Body>

      <MSS_Receipt>

      <!- Kuittauspyyntö alkaa -->
      <MSS_ReceiptReq xmlns="http://uri.etsi.org/TS102204/v1.1.2#"
MajorVersion="1" MinorVersion="1" MSSP_TransID="B653">

         <!- Palveluntarjoajan yhteystieto, tapahtumanumero ja aikaleima -->
         <AP_Info AP_ID=" http://mss.teliasonera.com/mssURI/oycompanyab"
AP_TransID="A204" AP_PWD="ssl" Instant="2003-06-24T21:32:31Z"/>

         <!- HMSSP:n yhteystieto -->
         <MSSP_Info>
            <MSSP_ID>
               <URI>http://mss.teliasonera.com</URI>
            </MSSP_ID>
         </MSSP_Info>

         <!- Loppukäyttäjän yhteystieto -->
         <MobileUser>
            <MSISDN>+358123456789</MSISDN>
         </MobileUser>

         <!- Tapahtuman loppustatus -->
         <Status>
            <StatusCode Value="502"/>
            <StatusMessage>
               VALID_SIGNATURE
            </StatusMessage>
         </Status>

         <!- Käyttäjän päätelaitteella näkyvä viesti -->
         <Message>
            Tervetuloa Yritys Oy:n asiakaspalveluun.
         </Message>

      </MSS_ReceiptReq>
      </MSS_Receipt>
   </env:Body>
</env:Envelope>
```

6.7 Kuittausvastaus (MSS_ReceiptResp)

6.7.1 MSS_ReceiptResp: attribuutit

Nimi	Arvo	Kuvaus	Vaadittu
MajorVersion	”1”	Rajapinnan yläversio, tällä hetkellä 1.	Kyllä
MinorVersion	”1”	Rajapinnan alaversio, tällä hetkellä 1.	Kyllä

6.7.1.1 MajorVersion ja MinorVersion

Käytetyn MSS-rajapinnan versio on tällä hetkellä 1.1.

6.7.2 MSS_ReceiptResp: elementit

Nimi	Kuvaus	Vaadittu
AP_Info	Palveluntarjoajan yhteystieto sekä AP:n tapahtumalle antama tapahtumanumero ja aikaleima.	Kyllä
MSSP_Info	AE:n yhteystieto.	Kyllä
Status	Tapahtuman loppustatus.	Ei

6.7.2.1 AP_Info ja MSSP_Info

Elementit ovat identtisiä allekirjoituspyynnön (MSS_SignatureReq) samannimisten elementtien kanssa.

6.7.2.2 Status

Elementti kertoo kuittauspyynnön onnistumisen tai epäonnistumisen. Jos kuittauspyyntö toimitettiin Käyttäjän päätelaitteelle, HMSSP palauttaa AP:lle statuskoodin 100 (REQUEST_OK). Jos AE tai HMSSP ei tunne Käyttäjää, AP:lle palautetaan statuskoodi 105 (UNKNOWN_CLIENT). Jos HMSSP ei tavoita Käyttäjää, HMSSP voi palauttaa AP:lle statuskoodin 209 (OTA_ERROR). Jos HMSSP ei tunnista MSSP_TransID:ta, HMSSP palauttaa AP:lle statuskoodin 101 (WRONG_PARAM).

6.7.3 Esimerkki: kuittausvastaus

```
HTTP/1.0 200 OK
Content-Type: application/soap+xml; charset="utf-8"
Content-Length: ...

<?xml version="1.0"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
   <env:Body>
      <MSS_Receipt>

      <!- Kuittausvastaus alkaa -->
      <MSS_ReceiptResp xmlns="http://uri.etsi.org/TS102204/v1.1.2#"
MajorVersion="1" MinorVersion="1" MSSP_TransID="B653">

         <!- Palveluntarjoajan yhteystieto, tapahtumanumero ja aikaleima -->
         <AP_Info AP_ID=" http://mss.teliasonera.com/mssURI/oycompanyab"
AP_TransID="A1203" AP_PWD="ssl" Instant="2003-06-24T21:32:31Z"/>

         <!- Vastauksen luojan yhteystieto (HMSSP/AE) -->
         <MSSP_Info Instant="2003-06-24T21:32:36Z>
            <MSSP_ID>
               <URI>http://mss.elisa.fi</URI>
            </MSSP_ID>
         </MSSP_Info>

         <!- Tapahtuman loppustatus -->
         <Status>
            <StatusCode Value="100"/>
            <StatusMessage>
               REQUEST_OK
            </StatusMessage>
         </Status>

      </MSS_ReceiptResp>
      </MSS_Receipt>
   </env:Body>
</env:Envelope>
```

6.8 Virheilmoitusviesti (SOAP FAULT)

ETSI TS 102 204:n mukaisesti FiCom-suositus nojaa SOAP 1.2 –määrityksen standardiin virhetiedotusmekanismiin. Entiteetti, joka havaitsee virhetilanteen tahpahtuman aikana (AE, RE tai HMSSP), keskeyttää tapahtuman ja reitittää MSS-palvelun vastausviestin sijasta palveluntarjoajalle SOAP FAULT-viestin. Seuraavassa kuvataan viestin rakenne.

Lisätietoja SOAP FAULT –viesteistä:
http://www.w3.org/TR/2003/REC-soap12-part0-20030624/#L11549

Elementti	Alielementti		Arvo	Kuvaus
Code	Value		“env:Receiver” tai “env:Sender”	SOAP 1.2 –määrityksen mukainen virhekoodi.
	Subcode	Value	Integer	MSS-palvelun virhekoodi.
Reason	Text		reasontext	MSS-palvelun virhekoodin selite.
Node			anyURI	Virheen havainneen entiteetin URI.
Role			anyURI	Virheen havainneen entiteetin rooli.

6.8.1 Code

Elementti sisältää alielementit Value ja Subcode.

Alielementti Value sisältää SOAP 1.2 –määrityksen mukaisen statuskoodin (pääkoodi). Koodi on käytännössä joko env:Sender tai env:Receiver. Liitteessä C on kerrottu kumpaa koodia kussakin virhetilanteessa käytetään. SOAP 1.2 määrittelee myös koodit env:VersionMismatch, env:MustUnderstand ja env:DataEncodingUnknown. FiCom-suositus ei huomioi näitä koodeja, eikä niitä pitäisi tarvita, jos kaikki toimijat noudattavat suosituksen mukaista SOAP-versiota ja palveluviestirakenteita sekä käyttävät UTF-8-merkistöä läpi viestirakenteen. Palveluntarjoajan kannalta virheen todellinen syy selviää MSS-palvelun statuskoodista eikä SOAP-tason pääkoodista.

Alielementti Subcode koostuu alielementistä Value, joka sisältää MSS-palvelun statuskoodin (alikoodi). Alikoodit on kuvattu liitteessä C selitteineen. Edempänä MSS-viestirakenteiden kuvauksissa on kerrottu alikoodien konkreettiset soveltamisohjeet. SOAP 1.2 sallii alikoodien upottamisen toistensa sisään. FiCom-suosituksessa ylimmän tason Subcode-elementillä ilmaistaan ETSI 204-standardin määrittelemä alikoodi ja seuraavan tason Subcode-elementillä FiComin määrittämä tarkempi alikoodi.

Alielementin Value arvo on muotoa

```
<env:Value>fi:_(virhekoodi)</env:Value>
```

6.8.2 Reason

Elementin ainoa alielementti Text sisältää MSS-palvelun statuskoodia vastaavan selitteen.

6.8.3 Detail

Elementti kertoo virhetilannetta tarkentavan selitteen, joka voi olla vapaa teksti tai alielementtejä sisältävä rakenne.

6.8.4 Node

Elementti kertoo virhetilanteen havainneen entiteetin URI:n.

6.8.5 Role

Elementti kertoo virhetilanteen havainneen entiteetin roolin. Rooli on jokin seuraavista:

http://uri.etsi.org/TS102207/v1.1.3#role_AcquiringEntity
http://uri.etsi.org/TS102207/v1.1.3#role_HomeMSSP
http://uri.etsi.org/TS102207/v1.1.3#role_IdentityIssuer
http://uri.etsi.org/TS102207/v1.1.3#role_RoutingEntity
http://uri.etsi.org/TS102207/v1.1.3#role_VerifyingEntity

6.8.6 Esimerkki: SOAP FAULT

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
  <env:Body>
    <env:Fault>
      <env:Code>
        <env:Value>env:Receiver</env:Value>
        <env:Subcode>
          <env:Value>fi:_208</env:Value>
        </env:Subcode>
      </env:Code>
      <env:Reason>
        <env:Text xml:lang="en">EXPIRED_TRANSACTION</env:Text>
      </env:Reason>
      <env:Node>mss.elisa.fi</env:Node>
      <env:Role>http://uri.etsi.org/TS102207/v1.1.3#role_HomeHMSSP</env:Role>
    </env:Fault>
  </env:Body>
</env:Envelope>
```

Liite A: XML Schema (ETSI)

FiCom-suositus on sopusoinnussa oheisen ETSI 102 204-standardin viestirakenteet määrittelevän XML Scheman kanssa.

```
<xs:schema targetNamespace="http://uri.etsi.org/TS102204/v1.1.2#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
xmlns:mss="http://uri.etsi.org/TS102204/v1.1.2#"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:env="http://www.w3.org/2003/05/soap-envelope"
elementFormDefault="qualified">
   <xs:import namespace="http://www.w3.org/2000/09/xmldsig#"/>
   <xs:import namespace="http://www.w3.org/2001/04/xmlenc#"/>
   <xs:import namespace="http://www.w3.org/2003/05/soap-envelope"/>

   <xs:complexType name="MessageAbstractType" abstract="true">
      <xs:sequence>
         <xs:element name="AP_Info">
            <xs:complexType>
               <xs:attribute name="AP_ID" type="xs:anyURI" use="required"/>
               <xs:attribute name="AP_TransID" type="xs:NCName"
use="required"/>
               <xs:attribute name="AP_PWD" type="xs:string" use="required"/>
               <xs:attribute name="Instant" type="xs:dateTime" use="required"/>
               <xs:attribute name="AP_URL" type="xs:anyURI" use="optional"/>
            </xs:complexType>
         </xs:element>
         <xs:element name="MSSP_Info">
            <xs:complexType>
               <xs:sequence>
                  <xs:element name="MSSP_ID" type="mss:MeshMemberType"/>
               </xs:sequence>
               <xs:attribute name="Instant" type="xs:dateTime" use="optional"/>
            </xs:complexType>
         </xs:element>
      </xs:sequence>
      <xs:attribute name="MajorVersion" type="xs:integer" use="required"/>
      <xs:attribute name="MinorVersion" type="xs:integer" use="required"/>
   </xs:complexType>

   <xs:element name="MSS_SignatureReq" type="mss:MSS_SignatureReqType"/>
   <xs:complexType name="MSS_SignatureReqType">
      <xs:complexContent>
         <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
               <xs:element name="MobileUser" type="mss:MobileUserType"/>
               <xs:element name="DataToBeSigned" type="mss:DataType"/>
               <xs:element name="DataToBeDisplayed" type="mss:DataType"
minOccurs="0"/>
               <xs:element name="SignatureProfile" type="mss:mssURIType"
minOccurs="0"/>
               <xs:element name="AdditionalServices" minOccurs="0">
                  <xs:complexType>
                     <xs:sequence>
                        <xs:element name="Service"
type="mss:AdditionalServiceType" maxOccurs="unbounded"/>
                     </xs:sequence>
                  </xs:complexType>
               </xs:element>
               <xs:element name="MSS_Format" type="mss:mssURIType"
minOccurs="0"/>
```

```
                <xs:element name="KeyReference" type="mss:KeyReferenceType"
minOccurs="0"/>
                <xs:element name="SignatureProfileComparison"
type="mss:SignatureProfileComparisonType" minOccurs="0"/>
            </xs:sequence>
            <xs:attribute name="ValidityDate" type="xs:dateTime"
use="optional"/>
            <xs:attribute name="TimeOut" type="xs:positiveInteger"
use="optional"/>
            <xs:attribute name="MessagingMode" type="mss:MessagingModeType"
use="required"/>
         </xs:extension>
      </xs:complexContent>
   </xs:complexType>

   <xs:element name="MSS_SignatureResp" type="mss:MSS_SignatureRespType"/>
   <xs:complexType name="MSS_SignatureRespType">
      <xs:complexContent>
         <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
               <xs:element name="MobileUser" type="mss:MobileUserType"/>
               <xs:element name="MSS_Signature" type="mss:SignatureType"
minOccurs="0"/>
               <xs:element name="SignatureProfile" type="mss:mssURIType"
minOccurs="0"/>
               <xs:element name="Status" type="mss:StatusType"/>
            </xs:sequence>
            <xs:attribute name="MSSP_TransID" type="xs:NCName" use="required"/>
         </xs:extension>
      </xs:complexContent>
   </xs:complexType>

   <xs:element name="MSS_StatusReq" type="mss:MSS_StatusReqType"/>
   <xs:complexType name="MSS_StatusReqType">
      <xs:complexContent>
         <xs:extension base="mss:MessageAbstractType">
            <xs:attribute name="MSSP_TransID" type="xs:NCName" use="required"/>
         </xs:extension>
      </xs:complexContent>
   </xs:complexType>

   <xs:element name="MSS StatusResp" type="mss:MSS StatusRespType"/>
   <xs:complexType name="MSS_StatusRespType">
      <xs:complexContent>
         <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
               <xs:element name="MobileUser" type="mss:MobileUserType"/>
               <xs:element name="MSS_Signature" type="mss:SignatureType"
minOccurs="0"/>
               <xs:element name="Status" type="mss:StatusType"/>
            </xs:sequence>
         </xs:extension>
      </xs:complexContent>
   </xs:complexType>

   <xs:element name="MSS_RegistrationReq" type="mss:MSS_RegistrationReqType"/>
   <xs:complexType name="MSS_RegistrationReqType">
      <xs:complexContent>
         <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
               <xs:element name="MobileUser" type="mss:MobileUserType"/>
               <xs:element name="EncryptedData" type="xenc:EncryptedType"
minOccurs="0"/>
```

```
                <xs:element name="EncryptResponseBy" type="xs:anyURI"
minOccurs="0"/>
                <xs:element name="CertificateURI" type="xs:anyURI"
minOccurs="0"/>
                <xs:element name="X509Certificate" type="xs:base64Binary"
minOccurs="0"/>
                <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
             </xs:sequence>
          </xs:extension>
       </xs:complexContent>
   </xs:complexType>

   <xs:element name="MSS_RegistrationResp" type="mss:MSS_RegistrationRespType"/>
   <xs:complexType name="MSS_RegistrationRespType">
       <xs:complexContent>
          <xs:extension base="mss:MessageAbstractType">
             <xs:sequence>
                <xs:element name="Status" type="mss:StatusType"/>
                <xs:element name="EncryptedData" type="xenc:EncryptedType"
minOccurs="0"/>
                <xs:element name="CertificateURI" type="xs:anyURI"
minOccurs="0"/>
                <xs:element name="X509Certificate" type="xs:base64Binary"
minOccurs="0"/>
                <xs:element name="PublicKey" type="xs:base64Binary"
minOccurs="0"/>
             </xs:sequence>
          </xs:extension>
       </xs:complexContent>
   </xs:complexType>

   <xs:element name="MSS_ProfileReq" type="mss:MSS_ProfileReqType"/>
   <xs:complexType name="MSS_ProfileReqType">
       <xs:complexContent>
          <xs:extension base="mss:MessageAbstractType">
             <xs:sequence>
                <xs:element name="MobileUser" type="mss:MobileUserType"/>
             </xs:sequence>
          </xs:extension>
       </xs:complexContent>
   </xs:complexType>

   <xs:element name="MSS_ProfileResp" type="mss:MSS_ProfileRespType"/>
   <xs:complexType name="MSS_ProfileRespType">
       <xs:complexContent>
          <xs:extension base="mss:MessageAbstractType">
             <xs:sequence>
                <xs:element name="SignatureProfile" type="mss:mssURIType"
minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="Status" type="mss:StatusType"/>
             </xs:sequence>
          </xs:extension>
       </xs:complexContent>
   </xs:complexType>

   <xs:element name="MSS_ReceiptReq" type="mss:MSS_ReceiptReqType"/>
   <xs:complexType name="MSS_ReceiptReqType">
       <xs:complexContent>
          <xs:extension base="mss:MessageAbstractType">
             <xs:sequence>
                <xs:element name="MobileUser" type="mss:MobileUserType"/>
                <xs:element name="Status" type="mss:StatusType" minOccurs="0"/>
                <xs:element name="Message" type="mss:DataType" minOccurs="0"/>
```

```
                <xs:element name="SignedReceipt" type="ds:SignatureType"
minOccurs="0"/>
             </xs:sequence>
             <xs:attribute name="MSSP_TransID" type="xs:NCName" use="required"/>
          </xs:extension>
       </xs:complexContent>
    </xs:complexType>

    <xs:element name="MSS_ReceiptResp" type="mss:MSS_ReceiptRespType"/>
    <xs:complexType name="MSS_ReceiptRespType">
       <xs:complexContent>
          <xs:extension base="mss:MessageAbstractType">
             <xs:sequence>
                <xs:element name="Status" type="mss:StatusType"/>
             </xs:sequence>
          </xs:extension>
       </xs:complexContent>
    </xs:complexType>

    <xs:element name="MSS_HandshakeReq" type="mss:MSS_HandshakeReqType"/>
    <xs:complexType name="MSS_HandshakeReqType">
       <xs:complexContent>
          <xs:extension base="mss:MessageAbstractType">
             <xs:sequence>
                <xs:element name="SecureMethods">
                   <xs:complexType>
                      <xs:attribute name="MSS_Signature" type="xs:boolean"
use="required"/>
                      <xs:attribute name="MSS_Registration" type="xs:boolean"
use="required"/>
                      <xs:attribute name="MSS_Notification" type="xs:boolean"
use="required"/>
                      <xs:attribute name="MSS_ProfileQuery" type="xs:boolean"
use="required"/>
                      <xs:attribute name="MSS_Receipt" type="xs:boolean"
use="required"/>
                      <xs:attribute name="MSS_Status" type="xs:boolean"
use="required"/>
                   </xs:complexType>
                </xs:element>
                <xs:element name="Certificates">
                   <xs:complexType>
                      <xs:sequence>
                         <xs:element name="Certificate" type="xs:base64Binary"
minOccurs="0" maxOccurs="unbounded"/>
                      </xs:sequence>
                   </xs:complexType>
                </xs:element>
                <xs:element name="RootCAs">
                   <xs:complexType>
                      <xs:sequence>
                         <xs:element name="DN" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/>
                      </xs:sequence>
                   </xs:complexType>
                </xs:element>
                <xs:element name="SignatureAlgList">
                   <xs:complexType>
                      <xs:sequence>
                         <xs:element name="Algorithm" type="mss:mssURIType"
minOccurs="0" maxOccurs="unbounded"/>
                      </xs:sequence>
                   </xs:complexType>
                </xs:element>
```

```
            </xs:sequence>
         </xs:extension>
      </xs:complexContent>
   </xs:complexType>

   <xs:element name="MSS_HandshakeResp" type="mss:MSS_HandshakeRespType"/>
   <xs:complexType name="MSS_HandshakeRespType">
      <xs:complexContent>
         <xs:extension base="mss:MessageAbstractType">
            <xs:sequence>
               <xs:element name="SecureMethods">
                  <xs:complexType>
                     <xs:attribute name="MSS_Signature" type="xs:boolean"
use="required"/>
                     <xs:attribute name="MSS_Registration" type="xs:boolean"
use="required"/>
                     <xs:attribute name="MSS_Notification" type="xs:boolean"
use="required"/>
                     <xs:attribute name="MSS_ProfileQuery" type="xs:boolean"
use="required"/>
                     <xs:attribute name="MSS_Receipt" type="xs:boolean"
use="required"/>
                     <xs:attribute name="MSS_Status" type="xs:boolean"
use="required"/>
                  </xs:complexType>
               </xs:element>
               <xs:element name="MatchingMSSPCertificates">
                  <xs:complexType>
                     <xs:sequence>
                        <xs:element name="Certificate" type="xs:base64Binary"
minOccurs="0" maxOccurs="unbounded"/>
                     </xs:sequence>
                  </xs:complexType>
               </xs:element>
               <xs:element name="MatchingAPCertificates">
                  <xs:complexType>
                     <xs:sequence>
                        <xs:element name="Certificate" type="xs:base64Binary"
minOccurs="0" maxOccurs="unbounded"/>
                     </xs:sequence>
                  </xs:complexType>
               </xs:element>
               <xs:element name="MatchingSigAlgList">
                  <xs:complexType>
                     <xs:sequence>
                        <xs:element name="Algorithm" type="mss:mssURIType"
minOccurs="0" maxOccurs="unbounded"/>
                     </xs:sequence>
                  </xs:complexType>
               </xs:element>
            </xs:sequence>
            <xs:attribute name="MSSP_TransID" type="xs:NCName" use="required"/>
         </xs:extension>
      </xs:complexContent>
   </xs:complexType>

   <xs:complexType name="MobileUserType">
      <xs:sequence>
         <xs:element name="IdentityIssuer" type="mss:MeshMemberType"
minOccurs="0"/>
         <xs:element name="UserIdentifier" type="xs:string" minOccurs="0"/>
         <xs:element name="HomeMSSP" type="mss:MeshMemberType" minOccurs="0"/>
         <xs:element name="MSISDN" type="xs:string" minOccurs="0"/>
      </xs:sequence>
```

```
   </xs:complexType>

   <xs:complexType name="DataType">
      <xs:simpleContent>
         <xs:extension base="xs:string">
            <xs:attribute name="MimeType" type="xs:string" use="optional"/>
            <xs:attribute name="Encoding" type="xs:string" use="optional"/>
         </xs:extension>
      </xs:simpleContent>
   </xs:complexType>

   <xs:simpleType name="SignatureProfileComparisonType">
      <xs:restriction base="xs:string">
         <xs:enumeration value="exact"/>
         <xs:enumeration value="minimum"/>
         <xs:enumeration value="better"/>
      </xs:restriction>
   </xs:simpleType>

   <xs:simpleType name="MessagingModeType">
      <xs:restriction base="xs:string">
         <xs:enumeration value="synch"/>
         <xs:enumeration value="asynchClientServer"/>
         <xs:enumeration value="asynchServerServer"/>
      </xs:restriction>
   </xs:simpleType>

   <xs:complexType name="DigestAlgAndValueType">
      <xs:sequence>
         <xs:element name="DigestMethod" type="ds:DigestMethodType"
minOccurs="0"/>
         <xs:element name="DigestValue" type="ds:DigestValueType"/>
      </xs:sequence>
   </xs:complexType>

   <xs:complexType name="mssURIType">
      <xs:sequence>
         <xs:element name="mssURI" type="xs:anyURI"/>
         <xs:element name="DigestAlgAndValue" type="mss:DigestAlgAndValueType"
minOccurs="0"/>
         <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
   </xs:complexType>

   <xs:complexType name="MeshMemberType">
      <xs:sequence>
         <xs:element name="DNSName" type="xs:string" minOccurs="0"/>
         <xs:element name="IPAddress" type="xs:string" minOccurs="0"/>
         <xs:element name="URI" type="xs:anyURI" minOccurs="0"/>
         <xs:element name="IdentifierString" type="xs:string" minOccurs="0"/>
      </xs:sequence>
   </xs:complexType>

   <xs:complexType name="KeyReferenceType">
      <xs:sequence>
         <xs:element name="CertificateURL" type="xs:anyURI" minOccurs="0"
maxOccurs="unbounded"/>
         <xs:element name="CertificateIssuerDN" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/>
         <xs:element name="HashOfUsersPublicKey"
type="mss:DigestAlgAndValueType" minOccurs="0" maxOccurs="unbounded"/>
         <xs:element name="HashOfCAPublicKey" type="mss:DigestAlgAndValueType"
minOccurs="0" maxOccurs="unbounded"/>
```

```
            <xs:any namespace="##other" processContents="lax"/>
         </xs:sequence>
      </xs:complexType>

      <xs:complexType name="SignatureType">
         <xs:choice>
            <xs:element name="XMLSignature" type="ds:SignatureType"/>
            <xs:element name="Base64Signature" type="xs:base64Binary"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0"/>
            <!-- this can also be an advanced XML Signature-->
         </xs:choice>
      </xs:complexType>

      <xs:element name="MSS_MessageSignature">
      <xs:complexType>
         <xs:sequence>
            <xs:element ref="ds:Signature"/>
         </xs:sequence>
         <xs:attribute ref="env:role" use="required"/>
         <xs:attribute ref="env:mustUnderstand" use="required"/>
      </xs:complexType>
      </xs:element>

      <xs:complexType name="AdditionalServiceType">
         <xs:sequence>
            <xs:element name="Description" type="mss:mssURIType"/>
            <xs:element name="Entity" type="mss:MeshMemberType" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
         </xs:sequence>
      </xs:complexType>

      <xs:complexType name="StatusType">
         <xs:sequence>
            <xs:element name="StatusCode" type="mss:StatusCodeType"/>
            <xs:element name="StatusMessage" type="xs:string" minOccurs="0"/>
            <xs:element name="StatusDetail" type="mss:StatusDetailType"
minOccurs="0"/>
         </xs:sequence>
      </xs:complexType>

      <xs:complexType name="StatusCodeType">
         <xs:sequence>
            <xs:element name="StatusCode" type="mss:StatusCodeType" minOccurs="0"/>
         </xs:sequence>
         <xs:attribute name="Value" type="xs:integer" use="required"/>
      </xs:complexType>

      <xs:complexType name="StatusDetailType">
         <xs:sequence>
            <xs:any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
         </xs:sequence>
      </xs:complexType>
</xs:schema>
```

Liite B: XML Schema (FiCom)

FiCom-suosituksessa kuvatut lisäarvopalvelut määritellään oheisessa XML Schemassa.

```
<xs:schema targetNamespace="http://mss.ficom.fi/TS102204/v1.0.0#"
           xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:mss="http://uri.etsi.org/TS102204/v1.1.2#"
           xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
           elementFormDefault="qualified">

  <xs:import namespace="http://uri.etsi.org/TS102204/v1.1.2#"
        schemaLocation="MSS-plus.xsd"/>
  <xs:import namespace="urn:oasis:names:tc:SAML:2.0:protocol"
            schemaLocation="saml-schema-protocol-2.0.xsd"/>

  <xs:element name="PKCS1">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="SignatureValue" type="xs:base64Binary"/>
        <xs:element name="X509Certificate" type="xs:base64Binary"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:element name="NoSpamCode">
    <xs:complexType>
      <xs:simpleContent>
        <xs:extension base="xs:string">
          <xs:attribute name="verify" type="xs:string" default="yes"/>
        </xs:extension>
      </xs:simpleContent>
    </xs:complexType>
  </xs:element>

  <xs:element name="EventID" type="xs:string"/>
  <xs:element name="SessionID" type="xs:string"/>

  <xs:element name="UserLang" type="xs:string" default="fi"/>

  <xs:element name="ServiceResponses">
    <xs:complexType>
      <xs:sequence>
   <xs:element name="ServiceResponse" maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Description" type="mss:mssURIType"/>
              <xs:element name="Entity" type="mss:MeshMemberType" minOccurs="0"/>
         <xs:element name="Status" type="mss:StatusType" minOccurs="0"/>
              <xs:element ref="samlp:Response" minOccurs="0"/>
              <xs:any namespace="##other" processContents="lax" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

</xs:schema>
```

Liite C: Statuskoodit

FiCom-suositus huomioi seuraavat ETSI:n määrittelemät statuskoodit. Luetteloista on jätetty pois mm. asynkroniseen viestintätapaan ja suosituksen ulkopuolisiin viestityyppeihin liittyvät koodit.

Ensimmäinen luettelo sisältää mahdolliset SOAP FAULT –rakenteessa AP:lle palautettavat virhekoodit. Jälkimmäinen luettelo sisältää MSS_SignatureResp- ja MSS_ReceiptResp-viestien Status-elementissä palautettavat statuskoodit.

HMSSP ei välttämättä kykene havaitsemaan tapahtuman keskeytymistä päätelaitteella (statuskoodit 401-406). Tällöin HMSSP odottaa kunnes aikaraja kuluu umpeen ja palauttaa statuskoodin 208 (EXPIRED_TRANSACTION). HMSSP saattaa toisaalta kyetä kertomaan virhetilanteelle tarkemman syyn kuin mitä voidaan ilmaista ETSI:n määrittämillä statuskoodeilla; tällainen HMSSP voi palauttaa SOAP FAULT-viestirakenteen Detail-elementissä ongelmaa tarkentavan statuskoodin, ”tarkenteen”. FiCom-suosituksen mukaiset tarkenteet on mainittu luettelossa, ja luetteloa seuraa tarkennetta hyödyntävä viestiesimerkki.

Koodeja 423, 424 ja 600-603 ei FiCom-suosituksessa huomioida lainkaan.

Koodit 700-780 ovat allekirjoitusvierailun aikana kirjattuja virhekoodeja. Näiden tarkempi semantiikka noudattaa ETSI TS 102 207 –määritystä. Kyse on lähes aina palveluntarjoajasta riippumattomasta järjestelmävirheestä. Poikkeuksena koodi 720 silloin, jos palveluntarjoaja on asettanut tapahtumalle kohtuuttoman lyhyen umpeutumisajan.

SOAP FAULT –viestien statuskoodit (env:Sender)

Koodi		Selite	Kuvaus
101		WRONG_PARAM	Yksi tai useampi palvelupyynnön parametreistä on virheellinen.
	1011	Invalid NoSpamCode	AP:n välittämä häirinnän estokoodi ei täsmää HMSSP:n koodin kanssa.
	1012	Missing NoSpamCode	AP:n välittämä tyhjä häirinnän estokoodi ei täsmää HMSSP:n koodin kanssa.
	1013	Illegal MessagingMode	AE ei tue AP:n käyttämää viestintätapaa.
	1014	Unknown AdditionalService	MSSP ei tunnista yhtä tai useampaa AP:n pyytämää lisäarvopalvelua.
	1015	DataToBeDisplayed not supported	HMSSP ei tue DataToBeDisplayed-elementtiä.
	1016	Unsupported MimeType and/or Encoding	HMSSP ei tue pyydettyä DTBS:n MimeTypea ja/tai Encodingia pyydetylle allekirjoitusprofiilille.

	1017	MSS_Format unsupported for MimeType, Encoding and/or SignatureProfile	HMSSP ei tue pyydettyä allekirjoitusformaattia pyydetylle MimeTypelle, Encodingille ja/tai allekirjoitusprofiilille.
102		MISSING_PARAM	Yksi tai useampi palvelupyynnön vaadituista parametreista puuttuu.
	1021	DataToBeDisplayed missing	HMSSP:n vaatima elementti DataToBeDisplayed puuttuu.
103		WRONG_DATA_LENGTH	Elementin DataToBeSigned arvo on sallittua lyhyempi tai pidempi.
104		UNAUTHORIZED_ACCESS	AP:ta ei tunneta, annettu salasana ei kelpaa, AP pyytää lisäarvopalvelua johon sillä ei ole käyttöoikeutta tai AP pyytää SignatureProfilea tai lisäarvopalvelua tai PersonIdentity-palvelun attribuuttia jonka käytön Käyttäjä on kieltänyt.
	1041	User-disabled SignatureProfile	AP pyytää SignatureProfilea jonka käytön Käyttäjä on kieltänyt.
	1042	User disabled AdditionalService	AP pyytää lisäarvopalvelua tai PersonIdentity-palvelun attribuuttia jonka käytön Käyttäjä on kieltänyt.
	1043	Service suspended	Käyttäjän käyttöoikeus palveluun on estetty.
105		UNKNOWN_CLIENT	AE tai HMSSP ei tunne Käyttäjää, jota palvelupyyntö koskee.
	1051	Malformatted user identifier	Käyttäjän yhteystieto on väärin muotoiltu.
	1052	User identifier does not exist	Tuntematon Käyttäjä.
	1053	Unregistered user	Käyttäjää ei ole rekisteröity.
	1054	Incompatible SIM card	Käyttäjän SIM-kortti ei sovellu palveluun.

107		INAPPROPRIATE_DATA	AP on antanut elementille DataToBeSigned, DataToBeDisplayed tai Message MIME-tyypin tai enkoodauksen, jota HMSSP ei tue.
108		INCOMPATIBLE_INTERFACE	AE tai HMSSP ei tue AP:n kertomaa rajapinnan versionumerota.
701		A Roaming Header block is missing.	Tapahtuma keskeytynyt allekirjoitusvierailussa ilmenneen teknisen ongelman vuoksi.
702		An Identity Issuer Header block is missing.	
703		A Home MSSP Header block is missing.	
710		Appropriate input information is missing.	
720		The validity date of the transaction has expired.	Tapahtuman aikaraja umpeutunut palvelupyynnön reitityksen aikana.

SOAP FAULT –viestien statuskoodit (env:Receiver)

109		UNSUPPORTED_PROFILE	AP on määritellyt allekirjoitusprofiilin, jota HMSSP ei tue.
208		EXPIRED_TRANSACTION	Tapahtuman aikaraja on ylittynyt.
	2081	Server timeout	Palvelin ei reagoinut aikarajan puitteissa
	2082	User timeout	Käyttäjä ei reagoinut aikarajan puitteissa
209		OTA_ERROR	HMSSP ei tavoittanut Käyttäjää. Matkapuhelin suljettu tai yhteysongelma.
	2091	Unknown OTA Error	Tuntematon OTA-virhe
	2092	Card not found (OTA DB)	Korttia ei löydy OTA-kannasta
	2093	ME Communication Error	Puhelimen aiheuttama virhe OTA-viestinnässä
	2094	Invalid capabilities	SIM-sovelluksen ominaisuudet eivät riitä pyynnön täyttämiseen
401		USER_CANCEL	Käyttäjä on peruuttanut tapahtuman.

	4011	User Cancel	Käyttäjä on peruuttanut tapahtuman.
	4012	Incorrect PoP	Käyttäjä syötti väärän PoP-koodin
	4013	Postponed signature	Käyttäjä on siirtänyt tapahtumaa
402		PIN_NR_BLOCKED	Allekirjoittaminen päätelaitteella epäonnistunut.
	4021	PIN blocked	
403		CARD_BLOCKED	
	4031	PUK blocked	
	4032	PIN blocked	
404		NO_KEY_FOUND	
	4041	Requested Key not found	
	4042	Incorrect key usage	
405		NO_URL_FOUND	
406		PB_SIGNATURE_PROCESS	
407		REGISTRATION_NOK	Virhe rekisteröintiprosessin aikana
	4071	Unknown Registration Error	Tuntematon Virhe rekisteröintiprosessin aikana
	4072	Registration Failed on Server	Virhe pavelimessa rekisteröintiprosessin aikana
	4073	Registration Failed on SIM	Virhe SIM-kortilla rekisteröintiprosessin aikana
422		NO_CERT_FOUND	Käyttäjän allekirjoitus onnistui, mutta allekirjoitusta vastaavaa varmennetta ei voitu liittää mukaan.
423		CRL_PB	
424		CRL_EXPIRED	AE:n CRL-kopio on vanhentunut ja CRL-päivitys epäonnistuu.
425		ERROR_CERTIFICATE	AE:n validoinnissa varmenne todettu vialliseksi.
750		Unable to provide Routing Entity services.	Tapahtuma keskeytynyst allekirjoitusvierailussa ilmenneen teknisen ongelman vuoksi.
760		Unable to provide Identity Issuer services.	
770		Unable to provide Verifying Entity services.	
780		Unable to provide services.	

900		INTERNAL_ERROR	Tuntematon ongelma.
	9001	Unknown Internal error	Tuntematon ongelma.
	9002	Server Error	Palvelin ongelma
	9003	SIM Application error	SIM-sovellus virhetilassa
	9004	SIM Configuration error	SIM-sovellus konfiguroitu väärin
	9005	DTBD missing	DTBD puuttuu
	9006	Invalid key length	Avaimen pituus väärä
	9007	Invalid hash type	Tuntematon/ei tuettu hash-tyyppi tai algoritmi
	9008	Invalid Key Algorithm	Väärä avaintyyppi

MSS-viestien statuskoodit

Koodi	Nimi	Kuvaus
100	REQUEST_OK	Kuittauspyyntö toimitettu käyttäjälle.
500	SIGNATURE	Sähköinen allekirjoitus on koostettu. Allekirjoitusta ei ole vielä validoitu.
501	REVOKED_ CERTIFICATE	Sähköinen allekirjoitus on koostettu, mutta Käyttäjän varmenne on sulkulistalla. Huom. varmenteen ekspiroituminen ilmaistaan koodilla 503.
502	VALID_SIGNATURE	Sähköinen allekirjoitus on koostettu ja todettu validiksi.
503	INVALID_SIGNATURE	Sähköinen allekirjoitus on koostettu, mutta allekirjoitus on validoinnissa todettu vialliseksi tai varmenne on ekspiroitunut.
504	OUTSTANDING_TRANSACTIO N	Allekirjoitusvastaus ei ole vielä valmis.
505	CONSTRAINT_MISMATCH	Tapahtuma on muutoin validi, mutta käyttäjän varmenne ei täytä sille allekirjoitusprofiilissa määritettyjä lisäehtoja. Kyse on todennäköisesti testivarmenteesta. (FiCom-spesifi statuskoodi.)

Esimerkki: SOAP FAULT (tarkenteen kanssa)

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
 <soapenv:Body>
  <soapenv:Fault>
   <soapenv:Code>
    <soapenv:Value>soapenv:Receiver</soapenv:Value>
    <soapenv:Subcode>
        <soapenv:Value>fi:_101</soapenv:Value>
        <soapenv:Subcode>
            <soapenv:Value>fi:1014</soapenv:Value>
        </soapenv:Subcode>
    </soapenv:Subcode>
   </soapenv:Code>
   <soapenv:Reason>
    <soapenv:Text xml:lang="en">User cancel</soapenv:Text>
   </soapenv:Reason>
  </soapenv:Fault>
 </soapenv:Body>
</soapenv:Envelope>
```

Liite D: GSM 03.38-merkistö

Oheinen taulukko sisältää päätelaitteella käytettävän GSM 03.38-merkistön, sekä vastaavat Unicode–merkistön UCS16 ja UTF-8 merkkikoodit.

Hex	Dec	Character name	Character	UCS16 Char	UTF-8 Hex
0x00	0	COMMERCIAL AT	@	\u0040	0x40
0x01	1	POUND SIGN	£	\u00A3	0xC2A3
0x02	2	DOLLAR SIGN	$	\u00A4	0xC2A4
0x03	3	YEN SIGN	¥	\u00A5	0xC2A5
0x04	4	LATIN SMALL LETTER E WITH GRAVE	è	\u00A8	0xC3A8
0x05	5	LATIN SMALL LETTER E WITH ACUTE	é	\u00A9	0xC3A9
0x06	6	LATIN SMALL LETTER U WITH GRAVE	ù	\u00B9	0xC3B9
0x07	7	LATIN SMALL LETTER I WITH GRAVE	ì	\u00AC	0xC3AC
0x08	8	LATIN SMALL LETTER O WITH GRAVE	ò	\u00B2	0xC3B2
0x09	9	LATIN SMALL LETTER C WITH CEDILLA	Ç	\u00C7	0xC387
0x0A	10	LINE FEED		\u000A	0x0A
0x0B	11	LATIN CAPITAL LETTER O WITH STROKE	Ø	\u00C8	0xC398
0x0C	12	LATIN SMALL LETTER O WITH STROKE	ø	\u00F8	0xC3B8
0x0D	13	CARRIAGE RETURN		\u000D	0x0D
0x0E	14	LATIN CAPITAL LETTER A WITH RING ABOVE	Å	\u00C5	0xC385
0x0F	15	LATIN SMALL LETTER A WITH RING ABOVE	å	\u00E5	0xC3A5
0x10	16	GREEK CAPITAL LETTER DELTA	Δ	\u0394	0xCE94
0x11	17	LOW LINE	_	\u005F	0x5F
0x12	18	GREEK CAPITAL LETTER PHI	Φ	\u03A6	0xCEA6
0x13	19	GREEK CAPITAL LETTER GAMMA	Γ	\u0393	0xCE93
0x14	20	GREEK CAPITAL LETTER LAMBDA	Λ	\u039B	0xCE9B
0x15	21	GREEK CAPITAL LETTER OMEGA	Ω	\u03A9	0xCEA9
0x16	22	GREEK CAPITAL LETTER PI	Π	\u03A0	0xCEA0
0x17	23	GREEK CAPITAL LETTER PSI	Ψ	\u03A8	0xCEA8
0x18	24	GREEK CAPITAL LETTER SIGMA	Σ	\u03A3	0xCEA3
0x19	25	GREEK CAPITAL LETTER THETA	Θ	\u0398	0xCE98
0x1A	26	GREEK CAPITAL LETTER XI	Ξ	\u039E	0xCE9E
0x1B	27	ESCAPE TO EXTENSION TABLE			
0x1B0A	27 10	FORM FEED		\u000C	0x0C
0x1B14	27 20	CIRCUMFLEX ACCENT	^	\u005E	0x5E
0x1B28	27 40	LEFT CURLY BRACKET	{	\u007B	0x7B
0x1B29	27 41	RIGHT CURLY BRACKET	}	\u007D	0x7D
0x1B2F	27 47	REVERSE SOLIDUS (BACKSLASH)	\	\u005C	0x5C
0x1B3C	27 60	LEFT SQUARE BRACKET	[	\u005B	0x5B
0x1B3D	27 61	TILDE	~	\u007E	0x7E
0x1B3E	27 62	RIGHT SQUARE BRACKET	]	\u005D	0x5D
0x1B40	27 64	VERTICAL BAR	|	\u007C	0x7C
0x1B65	27 101	EURO SIGN	€	\u20AC	0xE282AC
0x1C	28	LATIN CAPITAL LETTER AE	Æ	\u00C6	0xC386
0x1D	29	LATIN SMALL LETTER AE	æ	\u00E6	0xC3A6
0x1E	30	LATIN SMALL LETTER SHARP S (German)	ß	\u00DF	0xC39F
0x1F	31	LATIN CAPITAL LETTER E WITH ACUTE	É	\u00C9	0xC389
0x20	32	SPACE		\u0020	0x20
0x21	33	EXCLAMATION MARK	!	\u0021	0x21
0x22	34	QUOTATION MARK	"	\u0022	0x22

0x23	35	NUMBER SIGN	#	\u0023	0x23
0x24	36	CURRENCY SIGN	¤	\u00A4	0xC2A4
0x25	37	PERCENT SIGN	%	\u0025	0x25
0x26	38	AMPERSAND	&	\u0026	0x26
0x27	39	APOSTROPHE	'	\u0027	0x27
0x28	40	LEFT PARENTHESIS	(	\u0028	0x28
0x29	41	RIGHT PARENTHESIS	)	\u0029	0x29
0x2A	42	ASTERISK	*	\u002A	0x2A
0x2B	43	PLUS SIGN	+	\u002B	0x2B
0x2C	44	COMMA	,	\u002C	0x2C
0x2D	45	HYPHEN-MINUS	-	\u002D	0x2D
0x2E	46	FULL STOP	.	\u002E	0x2E
0x2F	47	SOLIDUS (SLASH)	/	\u002F	0x2F
0x30	48	DIGIT ZERO	0	\u0030	0x30
0x31	49	DIGIT ONE	1	\u0031	0x31
0x32	50	DIGIT TWO	2	\u0032	0x32
0x33	51	DIGIT THREE	3	\u0033	0x33
0x34	52	DIGIT FOUR	4	\u0034	0x34
0x35	53	DIGIT FIVE	5	\u0035	0x35
0x36	54	DIGIT SIX	6	\u0036	0x36
0x37	55	DIGIT SEVEN	7	\u0037	0x37
0x38	56	DIGIT EIGHT	8	\u0038	0x38
0x39	57	DIGIT NINE	9	\u0039	0x39
0x3A	58	COLON	:	\u003A	0x3A
0x3B	59	SEMICOLON	;	\u003B	0x3B
0x3C	60	LESS-THAN SIGN	<	\u003C	0x3C
0x3D	61	EQUALS SIGN	=	\u003D	0x3D
0x3E	62	GREATER-THAN SIGN	>	\u003E	0x3E
0x3F	63	QUESTION MARK	?	\u003F	0x3F
0x40	64	INVERTED EXCLAMATION MARK	¡	\u00A1	0xC2A1
0x41	65	LATIN CAPITAL LETTER A	A	\u0041	0x41
0x42	66	LATIN CAPITAL LETTER B	B	\u0042	0x42
0x43	67	LATIN CAPITAL LETTER C	C	\u0043	0x43
0x44	68	LATIN CAPITAL LETTER D	D	\u0044	0x44
0x45	69	LATIN CAPITAL LETTER E	E	\u0045	0x45
0x46	70	LATIN CAPITAL LETTER F	F	\u0046	0x46
0x47	71	LATIN CAPITAL LETTER G	G	\u0047	0x47
0x48	72	LATIN CAPITAL LETTER H	H	\u0048	0x48
0x49	73	LATIN CAPITAL LETTER I	I	\u0049	0x49
0x4A	74	LATIN CAPITAL LETTER J	J	\u004A	0x4A
0x4B	75	LATIN CAPITAL LETTER K	K	\u004B	0x4B
0x4C	76	LATIN CAPITAL LETTER L	L	\u004C	0x4C
0x4D	77	LATIN CAPITAL LETTER M	M	\u004D	0x4D
0x4E	78	LATIN CAPITAL LETTER N	N	\u004E	0x4E
0x4F	79	LATIN CAPITAL LETTER O	O	\u004F	0x4F
0x50	80	LATIN CAPITAL LETTER P	P	\u0050	0x50
0x51	81	LATIN CAPITAL LETTER Q	Q	\u0051	0x51
0x52	82	LATIN CAPITAL LETTER R	R	\u0052	0x52
0x53	83	LATIN CAPITAL LETTER S	S	\u0053	0x53
0x54	84	LATIN CAPITAL LETTER T	T	\u0054	0x54
0x55	85	LATIN CAPITAL LETTER U	U	\u0055	0x55
0x56	86	LATIN CAPITAL LETTER V	V	\u0056	0x56
0x57	87	LATIN CAPITAL LETTER W	W	\u0057	0x57

0x58	88	LATIN CAPITAL LETTER X	X	\u0058	0x58
0x59	89	LATIN CAPITAL LETTER Y	Y	\u0059	0x59
0x5A	90	LATIN CAPITAL LETTER Z	Z	\u005A	0x5A
0x5B	91	LATIN CAPITAL LETTER A WITH DIAERESIS	Ä	\u00C4	0xC384
0x5C	92	LATIN CAPITAL LETTER O WITH DIAERESIS	Ö	\u00D6	0xC396
0x5D	93	LATIN CAPITAL LETTER N WITH TILDE	Ñ	\u00D1	0xC391
0x5E	94	LATIN CAPITAL LETTER U WITH DIAERESIS	Ü	\u00DC	0xC39C
0x5F	95	SECTION SIGN	§	\u00A7	0xC2A7
0x60	96	INVERTED QUESTION MARK	¿	\u00BF	0xC2BF
0x61	97	LATIN SMALL LETTER A	a	\u0061	0x61
0x62	98	LATIN SMALL LETTER B	b	\u0062	0x62
0x63	99	LATIN SMALL LETTER C	c	\u0063	0x63
0x64	100	LATIN SMALL LETTER D	d	\u0064	0x64
0x65	101	LATIN SMALL LETTER E	e	\u0065	0x65
0x66	102	LATIN SMALL LETTER F	f	\u0066	0x66
0x67	103	LATIN SMALL LETTER G	g	\u0067	0x67
0x68	104	LATIN SMALL LETTER H	h	\u0068	0x68
0x69	105	LATIN SMALL LETTER I	i	\u0069	0x69
0x6A	106	LATIN SMALL LETTER J	j	\u006A	0x6A
0x6B	107	LATIN SMALL LETTER K	k	\u006B	0x6B
0x6C	108	LATIN SMALL LETTER L	l	\u006C	0x6C
0x6D	109	LATIN SMALL LETTER M	m	\u006D	0x6D
0x6E	110	LATIN SMALL LETTER N	n	\u006E	0x6E
0x6F	111	LATIN SMALL LETTER O	o	\u006F	0x6F
0x70	112	LATIN SMALL LETTER P	p	\u0070	0x70
0x71	113	LATIN SMALL LETTER Q	q	\u0071	0x71
0x72	114	LATIN SMALL LETTER R	r	\u0072	0x72
0x73	115	LATIN SMALL LETTER S	s	\u0073	0x73
0x74	116	LATIN SMALL LETTER T	t	\u0074	0x74
0x75	117	LATIN SMALL LETTER U	u	\u0075	0x75
0x76	118	LATIN SMALL LETTER V	v	\u0076	0x76
0x77	119	LATIN SMALL LETTER W	w	\u0077	0x77
0x78	120	LATIN SMALL LETTER X	x	\u0078	0x78
0x79	121	LATIN SMALL LETTER Y	y	\u0079	0x79
0x7A	122	LATIN SMALL LETTER Z	z	\u007A	0x7A
0x7B	123	LATIN SMALL LETTER A WITH DIAERESIS	ä	\u00E4	0xC3A4
0x7C	124	LATIN SMALL LETTER O WITH DIAERESIS	ö	\u00F6	0xC3B6
0x7D	125	LATIN SMALL LETTER N WITH TILDE	ñ	\u00F1	0xC3B1
0x7E	126	LATIN SMALL LETTER U WITH DIAERESIS	ü	\u00FC	0xC3BC
0x7F	127	LATIN SMALL LETTER A WITH GRAVE	à	\u00E0	0xC3A0