AS Sertifitseerimiskeskus

DigiDocService spetsifikatsioon

Dokumendi versioon: 2.123
Viimati uuendatud 01.03.2009
Kirjeldatav teenuse versioon: 2.3.30

Sisukord

1 Dokumendi muudatuste ajalugu

Ver.	Kuupäev	Muutja	Täiendused
2.123	19.12.08	Ahto Jaago, Urmo Keskel	- Lisatud peatükk „Nõuded ja soovitused teenuse kasutamisel“ - Lisatud meetodi CheckCertificate kirjeldus - Lisatud punkt „ID-kaardiga “ - Täiendatud kirjeldusi meetodite StartSession, MobileAuthenticate, MobileAuthenticateStatus, AddDataFile ning andmestruktuuri DataFileInfo juures - Parandatud punkti 6.2.1 juures olevat joonist ja tegevuste kirjeldusi
2.122	23.04.07	Urmo Keskel	- Lisatud GetMobileCertificate meetodi kirjeldus. - Korrigeeritud teksti.
2.120	02.03.07	Urmo Keskel	- Lisatud täiendavad staatused meetodi GetMobileAuthenticateStatus ja GetStatusInfo vastustesse. - Täiendatud SOAP veakoodide loetelu. - Parameetrite nimetused nüüd kõikjal suure algustähega (Sesscode, Status, jne). - DataFileAttribute ja DataFileInfo->Attributes elementide nimetused viidud keeleliselt korrektseteks.
2.112	13.02.07	Urmo Keskel	- Muudetud asünkroonset tagasisaatmist - Lisatud WaitSignature parameetrid meetoditele GetMobileAuthenticateStatus ja GetStatusInfo. - Lisatud ChallangeID MobileSign ja - MobileCreateSignature meetodite vastustele. - Lisatud SOAP veakoodide esialgsed kirjeldused. - Lisatud ServiceName parameeter MobileSign meetodile.
2.110	22.01.07	Urmo Keskel	Muudetud MobileCreateSignature päringu kirjeldust (FileInfo elemendile lisatud DigestType parameeter, lisatud failiversiooni parameeter), asynchServerServer režiim viidud kaheks: asynchServerServerJMS ja asynchServerServerSOAP.
2.109	13.12.06	Urmo Keskel	Kirjeldatud asynchServerServer režiimis vastuste saatmine; Lisatud meetodite MobileCreateSignature ja GetMobileCreateSignatureStatus kirjeldused.
2.108	24.11.06	Urmo Keskel	Pisimuudatused GetMobileAuthenticateStatus päringu kirjelduses
2.107	16.10.06	Urmo	- Mobiilautentimise ja isikutuvastuse

		Keskel	päringutele lisatud riigi kood; GetMobileAuthenticateStatus lisatud parameeter WaitSignature; - MobileAuthenticate päringule lisatud parameeter ServiceName; - MobileAuthenticate meetodi MessageToDisplay parameeter nüüd mittekohustuslik.
2.006	26.05.06	Urmo Keskel	Kirjeldatud mobiilautentimise päringud ja lisatud mobiiliga isikutuvastuse toimingu jadadiagramm.
2.005	03.05.06	Urmo Keskel	Muudetud meetodeid StartSession ja MobileSign, lisatud signatureProfile parameeter. Lisatud ajatempleid ja tühisusnimekirju puudutavad meetodid. Dokumentatsioonist eemaldatud näitepäringud.
2.004	10.11.05	Urmo Keskel	GetSignedDocInfo päringu viidud teenuse versioonis 1.000 olnud kujule, lisatud meetodi GetStatusInfo kirjeldus. Lisatud peatükk “Teenuse muudatuste ajalugu”.
2.003	31.10.05	Urmo Keskel	Esimene versioon, baseerub Veiko Sinivee koostatud dokumendil “DigiDocService teenuse mudel ja spetsifikatsioon”

2 Viited

	Viide
[1] RFC3275	(Extensible Markup Language) XML-Signature Syntax and Processing. March 2002.
[2] ETSI TS 101 903	XML Advanced Electronic Signatures (XAdES). February 2002.
[3] DigiDoc vorming	http://www.sk.ee/file.php?id=144
[4] SOAP	Simple Object Access Protocol http://www.w3.org/TR/soap/
[5] Time Formats	The W3C note Date and Time Formats *http://www.w3.org/TR/NOTE-datetime*, September 1997
[6] ETSI TS 102 204	Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface. V.1.1.4, August 2003.
[7] RFC 3161	Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP), August 2001

3 Mõisted

Mõiste	Kirjeldus
Algfail, Andmefail	Suvalises vormingus andmefail, mida hakatakse allkirjastama.
Allkirjastamine	Tekstis käsitletud kui „digitaalse allkirja moodustamine Digitaalallkirja Seaduse mõistes“. Toiming sisaldab lisaks signeerimisele kehtivuskinnituse võtmist
Kontrollkood	Mobiil-ID’ga allkirjastamisel ja autentimisel kasutatav nelja kohaline number, mis krüptograafiliselt seotud allkirjastava räsiga. Kontrollkood kuvatakse nii allkirjastamist/autentimist võimaldavas rakenduses kui telefoni ekraanil, võimaldamaks kasutajal veenduda allkirjastamise / autentimispäringu autentsuses.
MSSP	Mobile Signature Service Provider – mobiilallkirjastamise teenuse pakkuja. Kirjeldatud standardis ETSI TS 102 204 [6].
Mobiil-ID	ID-kaardiga analoogiline autentimise ja digitaalallkirjastamise teenus. Mobiil-ID kasutaja omab spetsiaalset SIM kaarti, millel on kasutaja salajased võtmed. Autentimisel või allkirjastamisel edastatakse signeeritav räsi üle GSM võrgu telefoni ja kasutaja peab allkirjastamise teostamiseks sisestama telefoni autentimise/allkirjastamise PIN koodi. Signeerimise järgselt saadetakse tekkinud tulem teenusesse.
Rakenduse pakkuja	DigiDocService teenuse tarbija, pakub kasutajale allkirjastamist, allkirjade verifitseerimist või autentimist võimaldavat rakendust.

Mõiste	Kirjeldus
Räsi, Räsikood	Signeeritav andmehulk, mis on krüptograafiliselt seotud allkirjastatavate algfailide ja muude allkirja parameetritega
Signeerimine	Privaatvõtme rakendamine lähtetekstile. Tulemuseks on „signatuur“.
Teenuse pakkuja	DigiDocService teenuse pakkuja.
Verifitseerimine	Digitaalallkirjastatud andmekogumi allkirja(de) kontroll.

4 Sissejuhatus

DigiDocService on SOAP põhine veebiteenus võimaldamaks võimalikult lihtsalt autentimise, digitaalallkirjastamise ja allkirjade verifitseerimise funktsionaalsust siduda teiste infosüsteemidega.

Teenust on võimalik kasutada erinevatelt arenduskeskkondadest/platvormidelt, millel on SOAP 1.0 RPC-encoded tugi.

Teenuse poolt pakutav funktsionaalsus:

- Isikusamasuse kontroll Mobiil-ID’ga
- Sertifikaatide kehtivuse kontroll (isikusamasuse kontroll ID-kaardi ja muu kiipkaardiga)
- DigiDoc failide moodustamine
- Digitaalallkirjastamine Mobiil-ID’ga
- Digitaalallkirjastamine ID-kaardi (ja muu kiipkaardiga)
- Digitaalallkirjastatud failide (DigiDoc) sisu ja allkirjade kehtivuse kontroll.

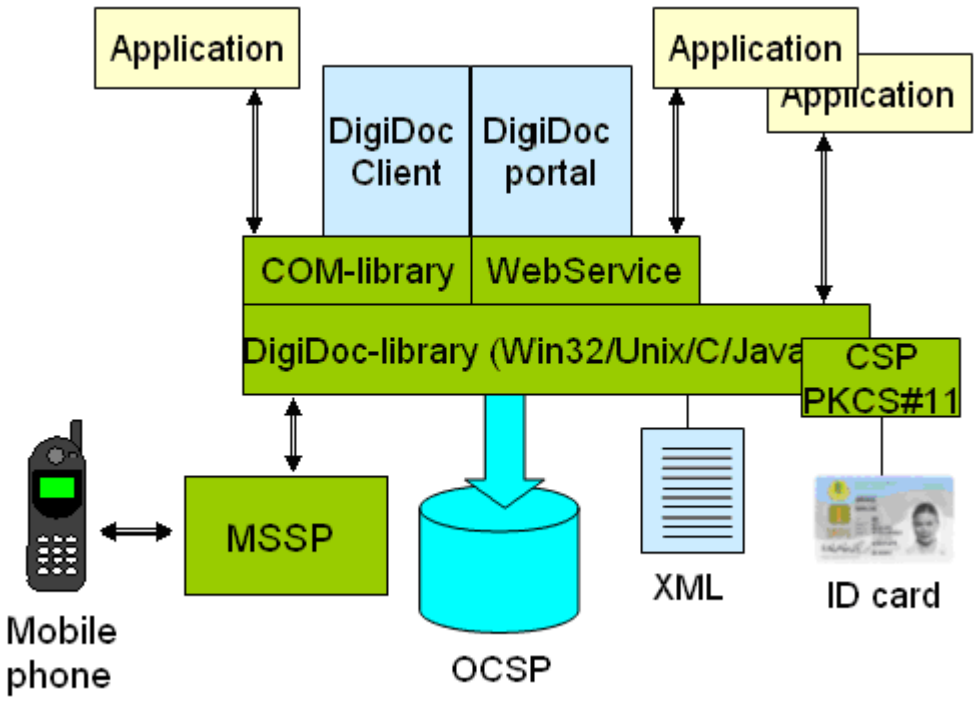
Teenusele ligipääsu võimaldatakse IP aadressi põhiselt, teenuse kasutamiseks tuleb rakenduse pakkujal sõlmida leping AS Sertifitseerimiskeskusega, teenuse kasutamise maksumus sõltub allkirjastamise ja autentimise päringute arvust kuus ja ühelt rakenduselt tulevatest üheaegsete päringute arvust.

DigiDocService toetab järgmisi digitaalallkirjastatud dokumendiformaate: SK-XML 1.0, DIGIDOC-XML 1.1, DIGIDOC-XML 1.2, DIGIDOC-XML 1.3.

4.1 DigiDocist

DigiDoc on terviksüsteem digitaalallkirjastatud dokumentide tekitamiseks ja verifitseerimiseks. DigiDoc koosneb failiformaadist, baasteekidest, veebiteenusest, veebiteenuse abiteekidest ja lõppkasutaja rakendustest nagu DigiDoc Client ja DigiDoc portaal.

DigiDoci arhitektuur:

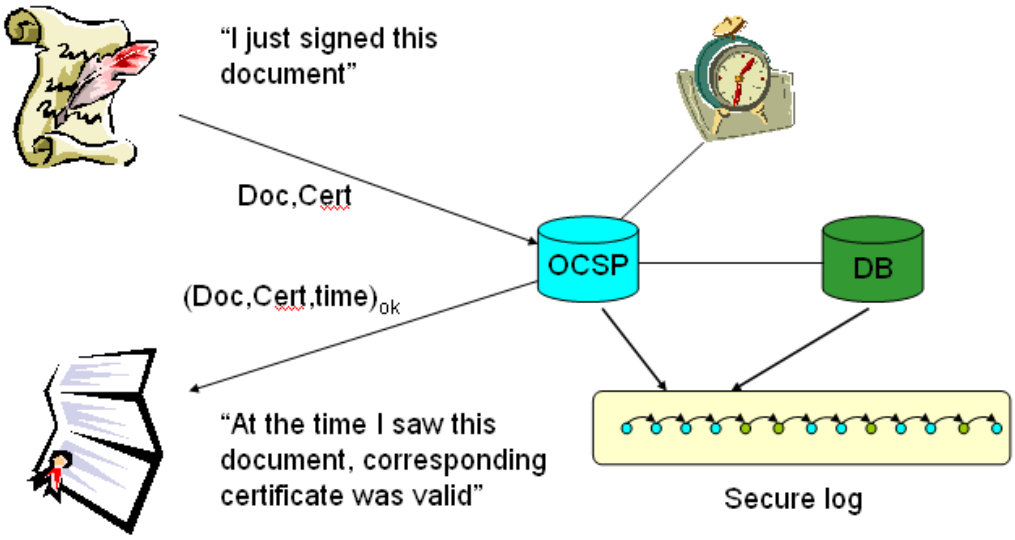


4.2 DigiDoci turvamudel

Üks suuremaid väljakutseid digitaalallkirjastamise süsteemides on digitaalallkirja kehtivuse kontroll pikka aega pärast allkirja andmist. Sageli jäetakse allkirja kehtivuse kontrollija hooleks veenduda, et allkirjastamise hetkel oli allkirjastaja sertifikaat kehtiv.

DigiDoc ja OpenXAdES ideoloogia on teistmoodi üles ehitatud – allkirjastaja sertifikaadi kehtivuse tõestus (kehtivuskinnitus) hangitakse allkirjastamise käigus. See kinnitus saadakse OCSP(Online Certificate Statud Protocol) serverilt ja talletatakse allkirjastatud dokumendis.

Allkirjastatava dokumendi räsi (mis on otseselt seotud allkirjastatava dokumendiga) sisaldub OCSP päringus ja vastuses. See annab võimaluse tõlgendada positiivset OCSP kehtivuskinnituse teenuse vastust, kui “ajal, mil ma nägin seda allkirjastatud dokumenti, antud allkirjastaja sertifikaat oli kehtiv”.



Ülaltoodud joonis iseloomustab OCSP serverit kui e-notarit kinnitamaks allkirjade kehtivust. Infrastruktuuri poolelt antud usaldusmudel vajab standardset OCSP kehtivuskinnituse teenust, allkirjastatav räsi on OCSP päringus paigutatud "nonce" väljale.

Et tagada värskeim info sertifikaadi kehtivuse kohta, peab OCSP kehtivuskinnituse teenus töötama "reaalajas", mis tähendab:

- Sertifikaadi kehtivusinfo võetakse aktiivsest sertifikaatide andmebaasist, mitte perioodiliselt uuendatavast sertifikaatide tühisusnimekirjast (CRL);
- OCSP vastuses sisaldub aeg on õige (nii täpne kui võimalik).

Saavutamaks pikaajalist allkirjade kehtivust, on võetud kasutusele turvalogi. Kõik OCSP vastused ja muutused sertifikaatide kehtivuses logitakse turvaliselt garanteerimaks antud digitaalallkirjade kehtivuse isegi pärast sertifikaatide väljaandja (CA) või OCSP serveri privaatvõtme ilmsikstulekut.

On oluline märkida, et täiendavad ajatemplid ei ole vajalikud rakendades ülaltoodud mudelit:

- Allkirjastamise aeg ja allkirjastamise kehtivuskinnituse aeg on määratud OCSP vastuses;
- Turvalogi garanteerib allkirjade pikaajalise kehtivuse ilma vajaduseta arhiveerimisajatemplite järgi.

4.3 DigiDoc failiformaat

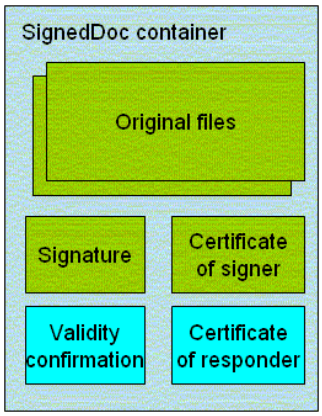
Digitaalallkirjastatud failide formaat baseerub ETSI TS 101 903 standardile, mida kutsutakse "XML Advanced Electronic Signatures (XAdES)". Antud standard kirjeldab digitaalallkirjastatud dokumentide struktuuri erinevatel täiendava kehtivuskinnituse info sisalduvuse tasemetel .

Võttes aluseks ülaltoodud usaldusmudeli, vastab DigiDoc XAdES profiilile “XAdES-X-L”-ile, kuid RFC 3161 ajatemplite asemel kasutatakse nn “ajamärgist” (allkirjastamise ametlik aeg on fikseeritud OCSP kehtivuskinnituse ajaga).

Antud profiil:

- Võimaldab allkirjaga siduda järgnevad allkirjastatavad atribuudid:
  - Allkirjastamiseks kasutatav sertifikaat
  - Allkirjastamise aeg
  - Allkirjastamise asukoht
  - Allkirjastaja roll või resolutsioon
- Allkirjas sisaldub allkirjastaja sertifikaadi kehtivuse info
  - OCSP vastus
  - OCSP serveri sertifikaat

Antud mudeli tulemusena on võimalik allkirja kehtivust kontrollida ilma täiendava infota – allkirja kontrollija peab usaldama allkirjastaja sertifikaadi väljaandjat ja OCSP serveri sertifikaati. Näiteks DigiDoc kliendi puhul tähendab see, et antud sertifikaadid peavad olema Windowsi sertifikaadihoidlas.



DigiDoc konteineris sisalduvad algfailid (failid, mis allkirjastati). Allkirjad, mis on seotud allkirjastatud faili(de)-ga, kusjuures igas allkirjas sisaldub allkirjasta sertifikaat, kehtivuskinnitus ja kehtivuskinnituse teenuse sertifikaat.

DigiDoc süsteem kasutab ülaltoodud mudelile vastavate failide puhul “ddoc” laiendit.

.ddoc failide süntaks on kirjeldatud detailselt failiformaati kirjeldavas dokumendis [3] DigiDoc vorming.

5 Nõuded ja soovitused rakenduse pakkujale

5.1 Nõuded digitaalallkirjastamisele

- Tulenevalt „Digitaalallkirja seadusest“ peab digitaalallkiri koos selle kasutamise süsteemiga:
  1) võimaldama üheselt tuvastada isiku, kelle nimel allkiri on antud;
  2) võimaldama kindlaks teha allkirja andmise aja;
  3) siduma digitaalallkirja andmetega sellisel viisil, mis välistab võimaluse tuvastamatult muuta andmeid või nende tähendust pärast allkirja andmist.
- Kasutajad peavad olema PIN2 sisestamise eelselt informeeritud digitaalallkirjastamisega kaasnevatest õiguslikest tagajärgedest;
- Tuleb rakendada meetmeid selleks, et allkirjastatavad andmed oleksid allkirjastajale üheselt tõlgendatavad;
- Kasutajal peab olema võimalik veenduda allkirjastatavate andmete ja allkirjale lisatavate atribuutide (allkirjastamise asukoht, roll/resolutsioon) õigsuses juhul, kui neid kasutatakse;

- Tuleb tagada, et kasutajale allkirjastamise eelselt esitatud andmed vastavad tegelikult allkirjastatavatele andmetele
- Kasutajale peab olema kättesaadav digitaalallkirjastamise järgselt tekkinud digitaalallkirjastatud fail.

5.2 Soovitused Mobiil-ID toimingute käivitamiseks

Mobiil-ID toimingute käivitamine on võimalik kasutades DigiDocService meetodeid MobileAuthenticate, MobileSign ja MobileCreateSignature. Kõikide nende meetodite korral on sisendparameetriteks Mobiil-ID kasutaja telefoninumber ja/või isikukood.

Ainult telefoninumbri kasutamise eelisteks on:

- Kasutatavuse poolelt kõige parem;
- Ei ole soovitatav kasutada ainukese identifikaatorina turvakriitilistes süsteemides kuna telefoninumbrid on avalikud ning on võimalik Mobiil-ID päringute saatmine kolmandatele isikutele.

Isikukoodi ja telefoninumbri mõlema kasutamise eelised on:

- Kasutaja eksimuse (sisestab näiteks telefoninumbri või isikukoodi mõne numbri valesti) tõttu on peaaegu välistatud, et päring saadetakse valele telefonile;
- Raskendatud on spämmimine, kuna isikukoodid ei ole avalikud;
- Tulenevalt e-teenuse loogikast võib kasutajalt isikukoodi sisendparameetrina kasutamise asemel kasutada ka muud väärtust, mille põhjal e-teenus teab kasutaja isikukoodi (näiteks kasutajatunnus, mis on infosüsteemis seotud isikukoodiga).

Mobiil-ID toimingute käivitamisel on igal e-teenusel soovitatav rakendada meetmeid (IP piirangud, spämmimist takistavad sisendparameetrid), mis teeksid võimatuks e-teenuse kaudu massilise Mobiil-ID autentimise või allkirjastamise päringute saatmise. Juhul, kui ühe teenuse kaudu tehakse üheaegselt tavapärasest määrast ja lepinguga tagatud määrast tunduvalt rohkem päringuid, on SK sunnitud, tagamaks teiste e-teenuste teenindamise, piirama päringute mahtu ületavale teenusele ligipääsu.

Mobiil-ID toimingute käigus peab Mobiil-ID toimingut tegev rakendus selgelt kuvama või edastama muul üheselt mõistetaval viisil kasutajale kontrollkoodi ja paluma kasutajal enne telefoni Mobiil-ID PIN koodi sisestamist kontrollida rakenduses kuvatava kontrollkoodi kokkulangemist telefoni ekraanil kuvatavaga. Kui kontrollkoodid on erinevad, tuleb toiming katkestada.

5.3 Tehnilised nõuded ja soovitused

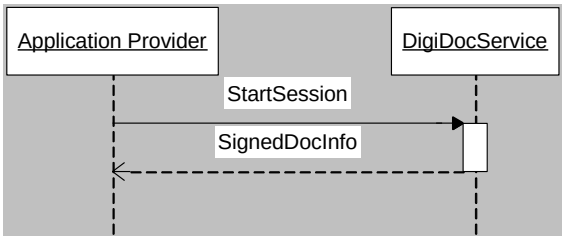
- ID-kaardi ja Mobiil-ID-ga digitaalallkirjastamist ning autentimist võimaldavatest rakendustes soovitame tungivalt kasutada brauseri ja veebiserveri vahelises suhtluses krüpteeritud andmesidet (HTTPS ühendus).
- Mobiil-ID'ga autentimisel või allkirjastamisel tuleb rakendusel küsida teenusest regulaarselt toimingu olekuinfot (ehk pollida teenust), kaugel mobiiltelefoni kasutaja autentimise või allkirjastamisega jõudnud on.

Juhul, kui mobiiliga allkirjastamist/autentimist tehakse veebirakendusest, on soovitatav veebilehel kasutada Ajax vahendeid, et olekuinfo järjekordsel küsimisel ei peaks lehte alati tervenisti uuesti laadima.

6 Peamised kasutusjuhud

6.1 DigiDoc faili verifitseerimine

Digitaalallkirjastatud dokumendi verifitseerimiseks kõige lihtsam moodus on kasutada StartSession päringut (kirjeldatud peatükis 8.1) väärtustades SigDocXML parameeter. Juhul, kui soovitakse saada ainult ülevaadet DigiDoc-i sisust ja edasisi allkirja lisamisi andmefailide/sertifikaatide lugemisi plaanis ei ole, on otstarbekas StartSession päring välja kutsuda bHoldSession parameetri väärtus oleks “false”. Sel juhul ei ole hilisemalt vajalik algatatud sessiooni sulgemine. StartSession päring tagastab allkirjastatud dokumendi info SignedDocInfo struktuurina, kust on välja loetavad allkirjastatud dokumendi olulisemad parameetrid.

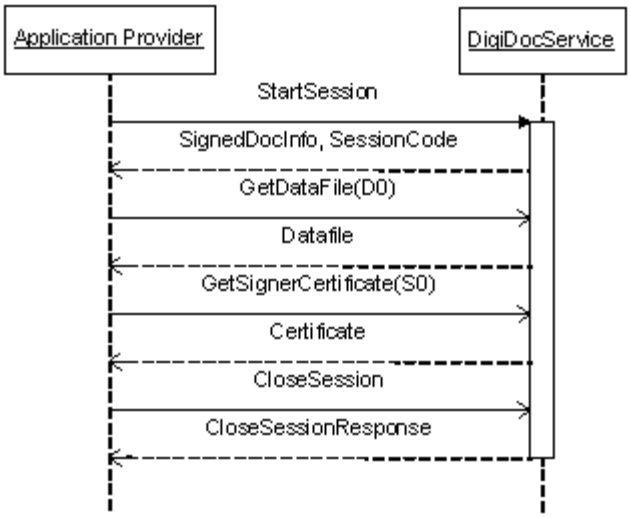


Kui StartSession kutsutakse välja bHoldSession parameetri väärtusega “true”, siis dokumendi verifitseerimise järgselt on võimalik pärida allkirjastatud dokumendi täiendavaid elemente:

- Andmefaili infot – GetDataFile meetod;
- Allkirjastaja sertifikaati – GetSignerCertificate meetod;
- Allkirja kehtivuskinnitust – GetNotary meetod;
- Kehtivuskinnituse sertifikaati – GetNotaryCertificate meetod.

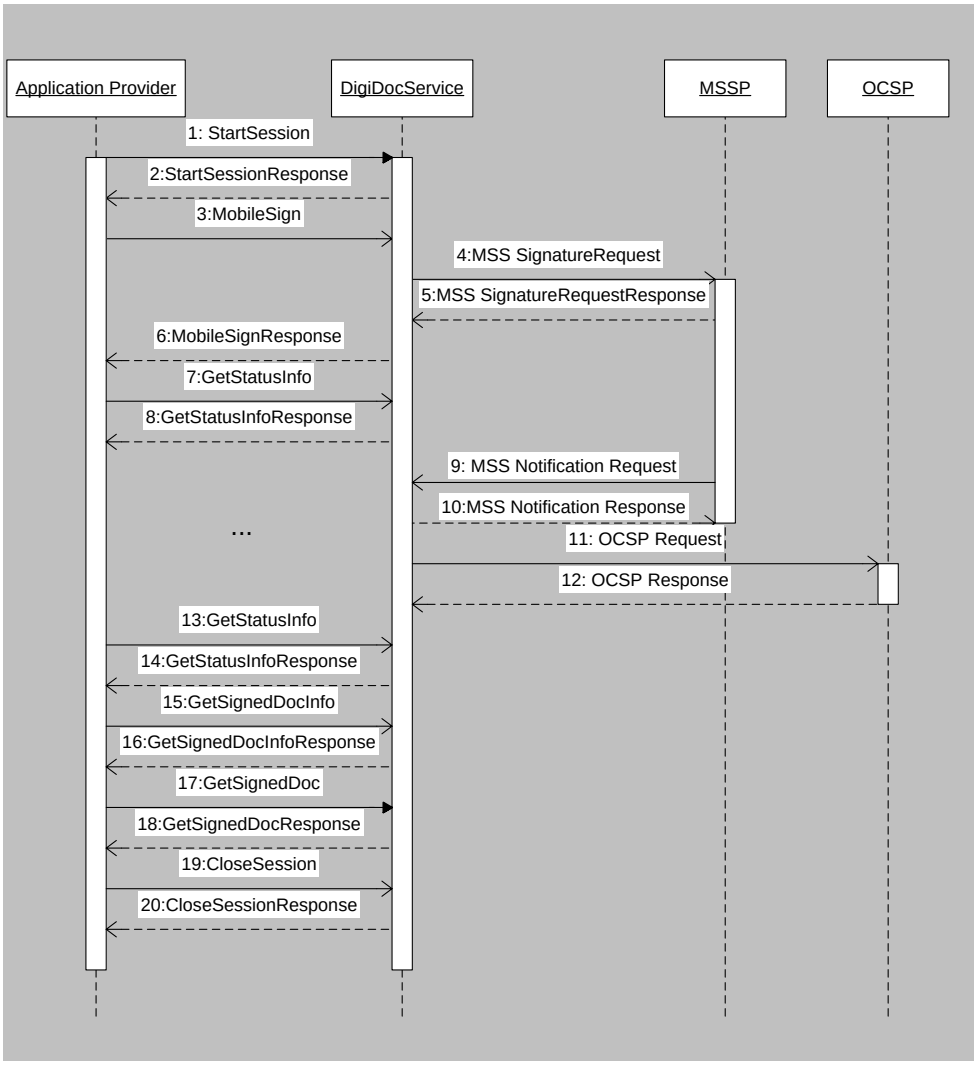
StartSessioni kasutamisel bHoldSession=true korral on vajalik hiljem sessioon CloseSession meetodiga sulgeda.

Näidis kasutusjuhu jadadiagramm:


Application Provider
DigiDocService
StartSession
SignedDocInfo, SessionCode
GetDataFile(D0)
Datafile
GetSignerCertificate(S0)
Certificate
CloseSession
CloseSessionResponse

6.2 Allkirjastamine

6.2.1 Mobiiliga Allkirjastamine asünkroonselt Client-Server režiimis



1. Teenust kasutav rakendus saadab StartSession päringu käigus allkirjastamist vajavad failid (DigiDoc faili või algfailid).
2. StartSession päringu tulemusena tagastatakse muuhulgas loodud sessiooni identifikaator, mida tuleb kasutada järgnevates päringus.
3. Allkirjastamise käivitamiseks saadab rakendus MobileSign päringu. Kui soovitakse allkirjastada korraga mitut algfaili on võimalik enne MobileSign päringu saatmist AddDataFile päringuga lisada täiendavaid andmefaile.
4. DigiDocService edastab signeerimispäringu MSSP teenusele, kes omakorda edastab selle telefonioperaatori kaudu kasutaja telefonile.
5. MSSP tagastab kas veakoodi või info päringu täitmise kohta.
6. DigiDocService tagastab teenust kasutavale rakendusele MobileSign päringu vastuse, milleks on kas veakood või info signeerimispäringu õnnestumise kohta.

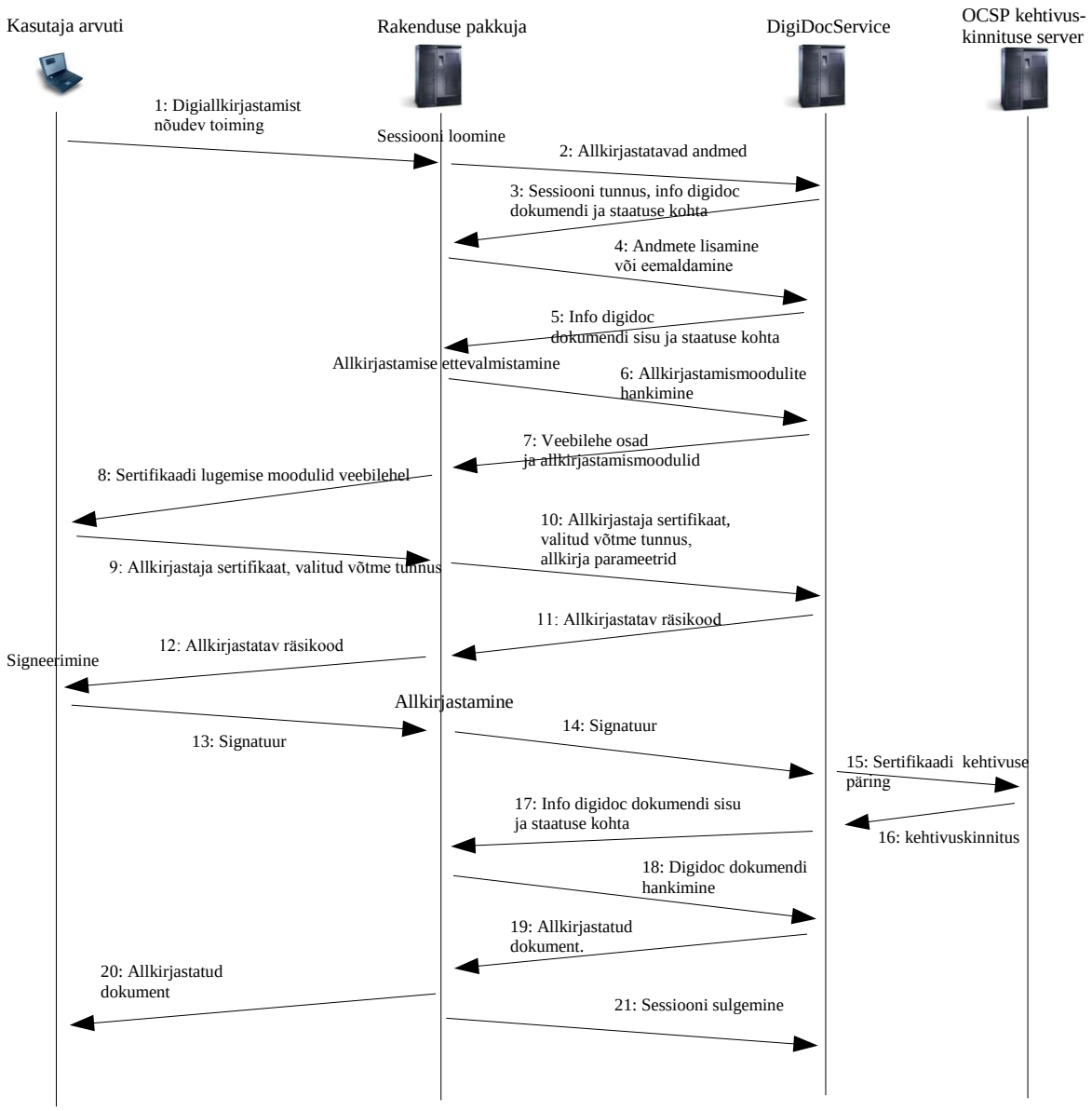
7, 8. Järgnevalt peab asünkroonse client-server režiimi korral rakendus saatma regulaarselt mingi väikese intervalli (näiteks mõne sekundi) järel

DigiDocService'le GetStatusInfo päringu kuni signeerimise toiming on kas õnnestunud või ebaõnnestunud.

9. MSSP teenus saadab signeerimise õnnestumise/ebaõnnestumise kohta teate. Kui signeerimine õnnestub, saadetakse DigiDocServicele ka signatuur.
10. DigiDocService tagastab MSSP-le info signatuuri kättesaamise kohta
11. Saanud kätte signatuuri, teeb DigiDocService OCSP kehtivuskinnituse teenusesse päringu allkirjastaja sertifikaadi kehtivuse kohta.
12. Kehtivuskinnituse teenus tagastab kehtivuskinnituse. Sessioonis olevale DigiDoc failile lisatakse allkiri, mis sisaldab muuhulgas signatuuri ja kehtivuskinnitust.
13. Teenusele tehakse järjekordne GetStatusInfo päring
14. Seekord tagastab GetStatusInfo vastuse signeerimistoimingu õnnestumise või ebaõnnestumise kohta
15. Teenust kasutava rakenduse poolt tehakse GetSignedDocInfo päring dokumendi staatuse kohta.
16. DigiDocService tagastab info dokumendi staatuse, sealhulgas allkirja lisamise õnnestumise koha.
17. Rakendus küsib GetSignedDoc meetodiga allkirjastatud DigiDoc faili sisu.
18. DigiDocService tagastab DigiDoc fail. Juhul, kui StartSession päringu käigus ei edastatud teenusele andmefailide sisu, tuleb teenust kasutaval rakendusel ise DigiDoc konteinerisse lisada andmefailide sisu.
19. Rakendus sulgeb CloseSession päringuga sessiooni.
20. Teenus kustutab sessioonis oleva info ja tagastab vastuse sessiooni eduka sulgemise kohta.

6.2.2 Kiipkaardiga allkirjastamine

Käesolev näide on toodud digitaalallkirjastamist võimaldava veebilehe näitel.



1. Digitaalallkirjastamist pakkuva rakenduse kasutaja on valinud mingi toimingu, mis eeldab andmete allkirjastamist. Kasutaja alustab allkirjastamise protsessi, klõpsates rakenduse pakkuja veebiteenuses vastavat nuppu või linki.

2. Allkirjastamiseks valitud andmed saadetakse StartSession päringuga DigiDocService-le - sellega algatatakse uus sessioon. Iga sessioon on seotud ühe (allkirjastatud) dokumendiga. Ühes allkirjastatud dokumendis

võib aga olla mitu andmekogumit (algfaili). Rakendus saadab teenusele kas:

a. allkirjastatava faili;
b. allkirjastatava faili metainfo ja räsi (faili sisu on eemaldatud);
c. puhul kogu allkirjastatava konteineri või
d. puhul allkirjastatava konteineri, millest on eemaldatud andmefailide keha(d) (eemaldatud on DataFile märgiste vahele jääv faili sisu).

Allkirjastamiseks vajalike andmete saatmise viisid on täpsemalt kirjeldatud peatükis 8.1. StartSession päringu käigus vastuvõetud andmed talletatakse sessioonis.

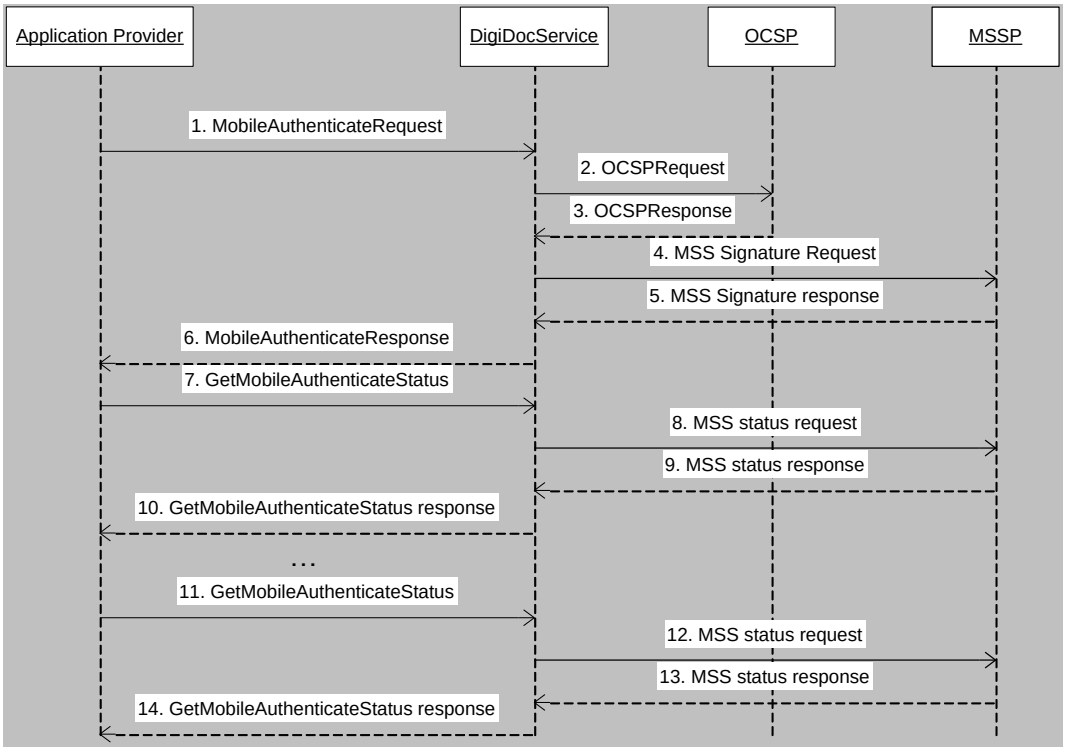
3. Rakendusele tagastatakse SessionCode, mis võimaldab sessioonis olevate andmetega järgmisi toiminguid teostada.
4. 4,5 Enne allkirjastamist võib rakendus lisada täiendavaid andmefaile (AddDataFile päring või eemaldada mõne andmefaili (RemoveDataFile päring) või teostada sessioonis olevate andmetega muid toiminguid.
5. Toimingute järgselt tagastatakse hetkel sessioonis oleva dokumendi info.
6. Allkirjastamise protsessi alustamiseks saadab rakenduse pakkuja DigiDocServicele päringu allkirja ettevalmistamiseks vajalike moodulite hankimiseks (päring GetSignatureModules). Moodulid on vajalikud, et veebilehel oleks võimalik allkirjastaja kiipkaardilt (nt. ID-kaardilt) allkirjastamise sertifikaat välja lugeda ja teenusele edastada. Komponentidest on kasutusel ActiveX moodul IE ja Java applet Mozilla/Netscape/Firefoxi jaoks. Viimane variant toetab ka Linux/Mac keskkonnas allkirjastamist.
7. Rakenduse pakkujale tagastatakse vajalikud allkirjastamismoodulid.
8. Allkirjastamismoodulid on integreeritud allkirjastamist pakkuvale veebilehele, muuhulgas võidakse veebilehel kasutaja käest küsida rolli/resolutsiooni ja allkirjastamise asukoha infot. Lehel olevad allkirjastamise komponent (ActiveX moodul või Java applet) loeb allkirjastaja kiipkaardilt sertifikaadi info.
9. Allkirjastaja kiipkaardilt on välja loetud sertifikaat edastatakse koos muude kasutaja poolt sisestatud allkirja atribuutidega allkirjastamise funktsionaalsust pakkuvasse veebiserverisse.
10. Allkirja parameetrid edastatakse DigiDocServicele kasutades PrepareSignature päringut.
11. DigiDocService lisab sessioonis olevale dokumendile uue allkirja info – allkirjasta sertifikaadi ja allkirja parameetrid ning arvutab välja räsi, mille allkirjastaja peab signeerima ja saadab selle rakenduse pakkujale PrepareSignature vastuses.
12. Allkirjastatav räsi kuvatakse koos allkirjastamise mooduliga kasutajale. Kasutaja vajutab lehel olevat allkirjastamise nuppu, mispeale allkirjastamismoodul toimetab ära signeerimise operatsiooni, sh küsib PINi. Moodustatud signatuur pannakse vormi peidetud väljale ja saadetakse allkirjastamisfunktsionaalsust pakkuvale veebilehele.
13. Signatuur edastatakse signeerimist pakkuvale veebiserverile (rakenduse pakkujale).
14. Signatuur edastatakse DigiDocServicele FinalizeSignature päringuga.
15. DigiDocService kontrollib allkirjastaja sertifikaadi kehtivust OCSP kehtivuskinnituse teenusest.
16. OCSP kehtivuskinnituse server tagastab allkirja kehtivuskinnituse.

17. Kui kinnitus oli positiivne, st allkirjastaja sertifikaat kehtis, lisab DigiDocService kogu info (allkirjastaja signatuuri ja kehtivuskinnituse) moodustatavale allkirjale. Nüüd on sessioonis olev DigiDocile lisatud allkiri terviklik. DigiDocService tagastab SignedDocInfo digitaalallkirjastamist pakkuvale rakendusele.
18. Rakendus pärib GetSignedDoc päringuga DigiDoc faili sisu.
19. DigiDocService tagastab sessioonis oleva DigiDoc dokumendi, milles sisaldub ka lisatud allkiri.
20. Kasutajat informeeritakse, et allkirjastamine on edukalt lõpetatud ja kasutaja saab allkirjastatud DigiDoc faili alla laadida oma arvutisse. NB! Juhul kui StartSession ja AddDataFile päringutes ei saadetud serverisse andmefailide sisu (variandid b ja d) on vajalik teenusest saadud DigiDoc faili andmefailide kehade lisamine. <DataFile> märgisest tuleb muuta ära ContentType, eemaldada viide räsikoodile ja lisada <DataFile> märgiste vahele andmefailide sisud Base64 kujul. Võimaluse korral kontrollitakse täiendavalt allkirjade kehtivust ja faili terviklikkust.
21. Viimase sammuna on digitaalallkirjastamist pakkuv rakendus viisakas ja sulgeb CloseSession päringuga sessiooni, mispeale teenus kustutab sessiooni käigus talletatud andmed.

6.3 Autentimine

6.3.1 Mobiil-ID autentimine asünkroonselt klient-server režiimis

Kasutusjuht kirjeldab Mobiil-ID'ga kasutaja autentimist.



1. Rakendus saadab DigiDocServicele MobileAuthenticate päringu käigus autentimiseks vajalikud andmed (kasutaja info, autentimisel kasutajale kuvatav tekst, keel)
2. Teenus saadab OCSP kehtivuskinnituse teenusele kasutaja autentimiseks sertifikaadi kehtivuse päringu.
3. OCSP kehtivuskinnituse teenus tagastab info autentija sertifikaadi kehtivuse kohta. Kui sertifikaat kehtib, suundutakse sammu 4 juurde, vastasel juhul sammu 6 juurde.
4. DigiDocService saadab MSSP teenuse kaudu kasutaja telefonile autentimispäringu.
5. MSSP tagastab kas veakoodi või info autentimispäringu saatmise õnnestumise kohta.
6. Sõltuvalt sellest, kas autentija sertifikaat kehtis ja autentimispäringu edastamine õnnestus, tagastatakse rakenduse pakkujale positiivne või negatiivne vastus; positiivses vastuses sisaldub ka info autenditava isiku kohta.
7. Sõltuvalt kasutatavast režiimist hakkab rakenduse pakkuja küsima perioodiliselt allkirjastamistoimingu staatust või ootab staatusinfo automaatset saatmist DigiDocService poolt. Antud näide käsitleb teenuse kasutamist klient-server režiimis, mistõttu rakenduse pakkuja peab perioodiliselt saatma DigiDocServicele autentimistoimingu staatuse küsimise päringu: *GetMobileAuthenticateStatus*.
8. DigiDocService pärib omakorda MSSP teenuselt autentimisetoimingu staatust.
9. MSSP teenus vastab autentimispäringu staatuse kohta.
10. Info autentimistoimingu staatuse kohta saadetakse edasi rakenduse pakkujale.
11. 12. 13. 14 jne sammudes korratakse 7, 8, 9, 10 sammudes tehtud toimingut niikaua, kuni saabub veainfo või positiivne vastus autentimistoimingu õnnestumise kohta.

6.3.2 ID-kaardiga autentimine

ID-kaardiga autentise ühe osana - autentimissertifikaadi kehtivusinfo küsimiseks - saab kasutada teenuse meetodit CheckCertificate.

7 Autentimisega seotud teenuse päringud ja vastused

Kõik päringud ja vastused on RPC-encoded kujul, kasutatakse UTF-8 kodeeringut.

7.1 MobileAuthenticate

Meetod Mobiil-ID autentimise protsessi käivitamiseks.

Meetodi täitmisel kontrollitakse esmalt tuvastatava isiku Mobiil-ID digitaalset isikutuvastamist võimaldava sertifikaadi kehtivust. Sertifikaadi kehtivuse korral edastatakse autentija telefonile autentimispäring, vastasel korral tagastatakse viga. Päringu tulemusena tagastatakse rakendusele autenditava kasutaja info,

autentijale kuvatav kontrollkood ning rakenduse pakkuja soovi korral ka isikutuvastusesertifikaat ja selle kehtivusinfo.

Päring:

Parameeter	Tüüp	K	Kirjeldus
IDCode	String	+	Autenditava isiku isikukood
Country	String(2)	+	Isikukoodi välja andnud riik, kasutatakse ISO 3166 2 tähelisi riigikoode (näiteks: EE).
PhoneNo	String	-	Autentidava isiku telefoninumber koos riigikoodiga kujul +xxxxxxxxx (näiteks +3706234566), juhul kui telefoninumber on määratud, ei pea IDCode ja Country parameetrid olema määratud. Kui on määratud nii PhoneNo kui ka IDCode parameetrid, kontrollitakse telefoninumbri vastavust isikukoodile ja mittevastavuse korral tagastatakse SOAP veakood 301.
Language	String(3)	+	Telefonile kuvatavate teadete keel. Kasutatakse: 3-tähelisi koode suurtähtedes. Võimalikud variandid: (EST,ENG,RUS).
ServiceName	String(20)	+	Autentimisel telefonil kuvatav teenuse nimetus, maksimaalne pikkus 20 tähemärki. Eelnevalt on vajalik kasutatava teenuse nimetuse kokkuleppimine teenuse pakkujaga.
MessageToDisplay	String(40)	-	Täiendav tekst, mis autentimise PIN-i küsimise eelselt lisaks teenuse nimetuse kasutaja telefonile kuvatakse. Maksimaalne pikkus 40 tähemärki.
SPChallenge	String(20)	-	Rakenduse pakkuja poolt genereeritud juhuslik 10 baidine tekst, mis on osa autentimise käigus kasutaja poolt signeeritavast sõnumist. Edastatakse HEX stringina. **NB!** Suurema turvalisuse huvides on soovitatav elle välja alati täita, iga kord erineva juhusliku väärtusega
MessagingMode	String	+	Autentimise toimingu vastuse tagastamise viis. Võimalikud variandid: - "asynchClientServer" – rakendus teeb pärast MobileAuthenticate meetodi väljakutsumist täiendavaid staatuspäringuid (kasutades meetodit *GetMobileAuthenticateStatus*). - "asynchServerServer" – toimingu lõppemisel või vea tekkimisel saadetakse vastus kliendirakendusele asünkroonselt (vt. parameeter AsyncConfiguration).
AsyncConfiguration	Integer	-	Määrab asünkroonselt vastuse tagasisaatmise konfiguratsiooni. Antud parameetri väärtust kasutatakse ainult juhul kui MessagingMode on "asynchServerServer". Konfiguratsioon lepitakse kokku teenuse kasutaja ja teenuse pakkuja vahel. Hetkel on toetatud vastuse tagasi saatmine kasutades Java Message Services (JMS) liidest.
ReturnCertData	Boolean	-	Kui väärtus on "TRUE", tagastatakse vastuses

			autenditava isiku sertifikaat. Sertifikaat on vajalik, kui rakenduse pakkuja soovib talletada ja iseseisvalt kontrollida signatuuri korrektsust ja kehtivusinfot.
ReturnRevocationData	Boolean	-	Väärtuse “TRUE” korral tagastatakse sertifikaadi kehtivusinfo vastuses RevocationData väljal.

Vastus:

Välja nimetus	Tüüp	Kirjeldus
Sesscode	Integer	loodud sessiooni identifikaator
Status	String	Toimingu edukal täitmisel “OK” **NB!** Antud toimingule “OK” vastuse saamine ei tähenda, et kasutaja on tuvastatud – kasutaja autentimiseks tuleb teha täiendavad staatusepäringud kuni autentimistoimingu olek on “USER_AUTHENTICATED”. Juhul, kui meetodi väljakutsel juhtub viga, tagastatakse SOAP veaobjekt. SOAP veaobjektide kirjeldus ja veakoodid on toodud peatükis 9.4.
UserIDCode	String	Autenditava isiku isikukood. Väärtus võetakse isikutuvastuse sertifikaadi eraldusnime “Serial Number” väljalt.
UserGivenname	String	Autenditava isiku eesnimi. Väärtus võetakse isikutuvastuse sertifikaadi eraldusnime G (Given name) väljalt.
UserSurname	String	Autenditava isiku perekonnanimi. Väärtus võetakse isikutuvastuse sertifikaadi eraldusnime SN (Surname) väljalt.
UserCountry	String(2)	Autenditava isiku riik, kasutatakse ISO 3166 2 tähelisi riigikoode. Väärtus võetakse isikutuvastuse sertifikaadi eraldusnime C (Country) väljalt.
UserCN	String	Autenditava isiku isikutuvastuse sertifikaadi põhinimi. Väärtus võetakse isikutuvastuse sertifikaadi eraldusnime CN (Common Name) väljalt.
CertificateData	String	Autenditava isiku isikutuvastuse sertifikaat Base64 kujul (tagastatakse ainult juhul, kui päringus ReturnCertData väärtus on “TRUE”, vastasel korral tagastatakse tühi string.
ChallengeID	String	4 tähemärgiline kontrollkood, mis arvutatakse kasutaja telefonile signeerimiseks saadetava Challenge väärtuse põhjal. Antud kontrollkood tuleb mobiilautentimist võimaldaval rakendusel kuvada kasutajale ja selle kaudu on võimalik kasutajal veenduda päringu autentsuses. **NB!** Mobiil-ID autentimise rakendus peab paluma kasutajal kontrollida rakenduses ja telefonil kuvatava kontrollkoodi kokkulangevust.
Challenge	String	Kasutaja poolt autentimisel allkirjastatav sõnum, koosneb rakenduse looja poolt saadetud sõnumist (SPChallange, 10 baiti) ja teenuse poolt lisatust (samuti 10 baiti). Tagastatakse vaid juhul, kui päringus

		SPChallenge väli on väärtustatud.
RevocationData	String	Sertifikaadi kehtivusinfo (OCSP kehtivuskinnituse teenuse vastus) Base64 kujul. Tagastatakse ainult juhul, kui päringus ReturnRevocationData parameetri väärtus on “TRUE”, vastasel korral tagastatakse tühi string.

Kui kasutatakse AsynchClientServer režiimi, tuleb pärast vastuse saamist hakata teenusele saatma GetMobileAuthenticateStatus päringuid veendumaks, et kasutaja sisestab isikutuvastuse PIN-i ja saab tuvastatud.

NB! Enne esimese staatuse päringu saatmist on soovitatav oodata vähemalt 15 sekundit kuna autentimise protsess ei saa tehniliste ja inimlike piirangute tõttu kiiremini lõppeda.

Juhul, kui kasutatakse “asynchServerServer” režiimi saadetakse autentimise toimingu lõppemisel automaatselt teenuse kasutajale vastavalt kokku lepitud konfiguratsioonile.

Asünkroonselt tagasi saadetav vastus on XML kujul ja selle struktuur on:

Välja nimetus	Tüüp	Kirjeldus
Sesscode	Integer	Vastusega seotud sessiooni identifikaator
Status	String	Toimingu staatuskood. Toimingu õnnestumisel “USER_AUTHENTICATED”. Teised võimalikud olekud on kirjeldatud GetMobileAuthenticateStatus päringu vastuses.
Data	String	Autentimise käigus moodustatud signatuur PKCS#1 konteinerina Base64 kujul. Tagastatakse ainult juhul, kui teenuse kasutaja on ette andnud SPChallange, vastasel juhul on väärtus tühi.

7.2 GetMobileAuthenticateStatus

Antud meetodit kasutatakse sünkroonses režiimis Mobiil-ID autentimise toimingu staatuse pärimiseks.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	Sessiooni identifikaator (kasutada väärtust, mis tagastati MobileAuthenticate vastuses).
WaitSignature	Boolean	+	Kui TRUE, siis päringule enne vastust ei tagastata, kui telefonilt on signatuuri väärtus saabunud, või on juhtunud viga. FALSE korral tagastatakse kohe vastus ja rakendus peab GetMobileAuthenticate meetodi väikese viite (2-10 sekundit) järel uuesti välja kutsuma.

Vastus:

Parameeter	Tüüp	Kirjeldus
Status	String	Mobiilautentimise protsessi olek: - OUTSTANDING_TRANSACTION– autentimine alles toimub; - USER_AUTHENTICATED – isik autenditud; - NOT_VALID – toiming on lõppenud, kuid kasutaja poolt tekitatud signatuur ei ole kehtiv. - EXPIRED_TRANSACTION – sessioon on aegunud; - USER_CANCEL – kasutaja katkestas; - MID_NOT_READY - Mobiil-ID funktsionaalsus ei ole veel kasutatav, proovida mõne aja pärast uuesti - PHONE_ABSENT – telefon ei ole levis; - SENDING_ERROR – Muu sõnumi saatmise viga (telefon ei suuda sõnumit vastu võtta, sõnumikeskus häiritud); - SIM_ERROR – SIM rakenduse viga; - INTERNAL_ERROR – teenuse tehniline viga
Signature	String	Autentimise käigus moodustatud signatuur PKCS#1 konteinerina Base64 kujul. Tagastatakse ainult juhul, kui MobileAuthenticate päringus oli määratud SPChallange, vastasel juhul on väärtus tühi. **NB!** Suurema turvalisuse huvides on rakenduse loojal soovitatav signatuuri verifitseerida, kasutades selleks allkirjastatavat sõnumit (väli Challenge MobileAuthenticate meetodi vastusest, millest 10 esimest baiti peab olema DigiDocService'it kasutava rakenduse poolt ette antud SPChallange), avalikku võtit kasutaja autentimissertifikaadist ning arvutatud signatuuri. Signatuur on arvutatud RSA algoritmi järgi.

Kui vastuses on Status väärtus ei ole OUTSTANDING_TRANSACTION, siis meetodi välja kutsumise järgselt sessioon suletakse.

7.3 CheckCertificate

Antud meetodit saab kasutada SK välja antud sertifikaatide (sealhulgas ID-kaardi ja Digitempli sertifikaatide) kehtivusinfo kontrollimiseks – mugavamaks täienduseks senisele võimalusele küsida sertifikaatide kehtivusinfot kehtivuskinnitusteenuse (OCSP) käest. Lisaks tagastab meetod (olulisemate) sertifikaadiväljade väärtused.

Lisaks tagastab meetod kehtivusinfot SK kehtivuskinnituse teenuse poolt teenindatavate välismaiste sertifitseerijate sertifikaatide kohta. Teenindatavate välismaiste sertifitseerijate loetelu on toodud http://www.sk.ee/certs/proxyocsp/.

Päring:

Parameeter	Tüüp	K	Kirjeldus

Certificate	String	+	Kontrollitava sertifikaadi andmed BASE 64 kujul. Sertifikaadi andmed võivad sisaldada ka sertifikaadi PEM formaadile omaseid „---BEGIN CERTIFICATE---„ ja „---END CERTIFICATE---„ ridu
ReturnRevocationData	Boolean	-	Väärtuse TRUE korral tagastatakse sertifikaadi kehtivusinfo vastuses RevocationData väljal.

Vastus:

Välja nimetus	Tüüp	Kirjeldus
Sesscode	Integer	loodud sessiooni identifikaator
Status	String	Sertifikaadi kehtivusinfo. - GOOD – sertifikaat kehtib - REVOKED – sertifikaat on tühistatud - UNKNOWN – sertifikaati ei ole kunagi välja antud või on tegu tundmatu sertifitseerijaga - EXPIRED – sertifikaat on aegunud (lõpu kuupäev on vanem kui hetkekuupäev) - SUSPENDED – sertifikaat on peatatud
UserIDCode	String	Sertifikaadiomaniku isikukood. SK poolt välja antud sertifikaatide korral võetakse väärtus sertifikaadi eraldusnime “Serial Number” väljalt.
UserGivenname	String	Sertifikaadiomaniku eesnimi. Väärtus võetakse sertifikaadi eraldusnime G (Given name) väljalt.
UserSurname	String	Sertifikaadiomaniku perekonnanimi. Väärtus võetakse sertifikaadi eraldusnime S (Surname) väljalt.
UserCountry	String(2)	Sertifikaadiomaniku riik, kasutatakse ISO 3166 2-tähelisi riigikoode. Väärtus võetakse sertifikaadi eraldusnime C (Country) väljalt.
UserOrganisation	String	Sertifikaadiomaniku organisatsioon, väärtus võetakse sertifikaadi eraldusnime O (Organisation) väljalt.
UserCN	String	Sertifikaadi põhinimi. Väärtus võetakse sertifikaadi eraldusnime CN (Common Name) väljalt.
Issuer	String	Sertifikaadi väljaandja (Issueri) eraldusnimi (CN).
KeyUsage	String	Sertifikaadiga seotud (salajase) võtme kasutusalad
EnhancedKeyUsage	String	Võtme laiendatud kasutusalad
RevocationData	String	Sertifikaadi kehtivusinfo (OCSP kehtivuskinnituse teenuse vastus) Base64 kujul. Tagastatakse ainult juhul, kui päringus ReturnRevocationData parameetri väärtus on TRUE, vastasel korral tagastatakse tühi string.

Tagastatavad väärtused on UTF8 kodeeringus.

8 Digitaalallkirjastamisega seotud teenuse meetodid

8.1 StartSession

Enamasti alustatakse transaktsiooni veebiteenusega kasutades StartSession meetodit. Startsession päringu käigus saadetakse teenusele andmefail, mille põhjal soovitakse moodustada DigiDoc fail, või siis juba valmis DigiDoc fail, millele soovitakse lisada allkirja, kontrollida DigiDoc faili sisu või eraldada andmefaili sisu. Startsession päringu käigus tagastatakse unikaalne sessiooni identifikaator, mis tuleb lisada kõigile antud transaktsiooni käigus teostatud toimingutele.

Startsession päringu parameetrid:

- **SigningProfile –** Parameeter määramaks allkirjastamisel tekitatava allkirja omadusi. (Näiteks, kas allkiri sisaldab lisaks OCSP kehtivuskinnitusele veel täiendavaid ajatempleid). Sama parameetriga määratakse ka milliseid nõudeid esitatakse allkirjadele allkirjade verifitseerimisel. Vaikeprofiili kasutamiseks tuleb parameeter väärtustada tühja stringiga. Antud teenuse versioonis parameetri väärtust ignoreeritakse.
- **SigDocXML** – DigiDoc dokument XML kujul, mis on viidud HTML escaped kujule. Näiteks “<DataFile>” peab olema viidud kujule „<DataFile>“.
- **bHoldSession** – lipp, mis määrab kas StartSession päringu käigus saadetud andmeid hoida sessioonis või kustutada teenusele saadetud info kohe pärast vastuse tagastamist.
- **Datafile** - antud element võimaldab StartSession päringu käigus saata teenusele andmefail, mille põhjal moodustatakse DigiDoc konteiner. Näiteks cv.pdf saatmisel tekitatakse cv.ddoc mis sisaldab esialgu ainsa andmefailina cv.pdf-i. Datafile struktuur on kirjeldatud käesolevas dokumendis peatükis 9.3. Andmefaili lisamisel ei ole vajalik määrata faili identifikaatorit.
  Vaikimisi tekitatakse DIGIDOC-XML 1.3 fail, kui soovitakse kasutada mõnda muud failiformaati, tuleks kõigepealt välja kutsuda meetod CreateSignedDoc

NB! Teenusele ei tohi saata korraga SigDocXML kui ka Datafile andmeid, kuna nad on üksteist välistavad.

Päringu vastusena tagastatav info:

- **Status** – Väärtus „OK“ või veastring.
- **Sesscode** – Sessiooni kood, mida kasutatakse antud transaktsiooni edasistes päringutes.
- **SignedDocInfo** – Juhul, kui StartSession päring sisaldas andmefaili või DigiDoc faili, tagastatakse vastuses SignedDocInfo struktuur käesoleva dokumendi peatükis 9.1 esitatud kujul.

Töökiiruse huvides on soovitatav teenusesse mitte saata tervet andmefaili, vaid saata ainult andmefaili info ja andmefaili räsi – ja seda mõlemal juhul: andmefailide saatmise korral (kui kasutatakse StartSession’i Datafile parameetrit) ning ka teenusele Digidoc konteineri saatmisel (kui kasutatakse StartSession’i SigDocXML parameetrit). Allpool on mõlema juhu kohta selgitavad näited.

Näide – Andmefaili asemel räsikoodi saatmine allkirjastamiseks

Olgu soov digitaalallkirjastada 42-baidine (sh 2 CRLF reavahetust) tekstifail test.txt, järgmise sisuga:

This is a test file
secondline
thirdline

Koostame järgmise, **kanoniseeritud*** kujul, xml-elemendi, kus väärtus „VGhpcyBpcyBhIHRlc3QgZmlsZQ0Kc2Vjb25kbGluZQ0KdGhpcmRsaW5l“ on andmefaili sisu Base64 kujul ning lõpumärgendi </DataFile> ees on reavahetus (mis on Digidoc-teekide spetsiifiline nõue):

<DataFile xmlns="http://www.sk.ee/DigiDoc/v1.3.0#"
ContentType="EMBEDDED_BASE64" Filename="test.txt" Id="D0"
MimeType="text/plain"
Size="42">VGhpcyBpcyBhIHRlc3QgZmlsZQ0Kc2Vjb25kbGluZQ0KdGhpcmRsa
W5l
</DataFile>

Eeldusel, et xml-is on kanoniseerimise tõttu reavahetused CRLF (\r\n) asendatud reavahetustega LF (\n), andmefail on Base64 kujul 64-sümboli pikkuste ridadena ning DataFile elemendi väärtused (sh atribuutide väärtused) on UTF8 kodeeringus, arvutame SHA1 räsi üle kogu DataFile xml-elemendi, saame HEX-kujul stringi „b7c7914ab293811e0f0002932d85860a3b934890“ – selle konverteerime binary-stringiks ehk järjestikuste baitide jadaks: 0xb7, 0xc7, 0x91, ..., 0x90, mille viime Base64 kujule ja saame väärtuse „t8eRSrKTgR4PAAKTLYWGCjuTSJA=“.

PHP-s käiks viimase väärtuse saamine järgmiselt:
base64_encode(pack("H*", "b7c7914ab293811e0f0002932d85860a3b934890"));

Koostame StartSession Datafile parameetri täitmiseks andmestruktuuri (olgu nimega $inputData) järgmiste väärtustega:

Filename=“test.txt“
MimeType=“text/plain“
ContentType=“HASHCODE“
Size=42
DigestType=“SHA1“
DigestValue=“t8eRSrKTgR4PAAKTLYWGCjuTSJA=“

Saadame StartSession meetodiga andmestruktuuri teenusele:

StartSession(„“, „“, TRUE, $inputData);

Järgnevalt sooritatakse teenuse vastu toiminguid allkirjastatavate failide täiendavaks lisamiseks (vt. meetodit AddDataFile), digitaalallkirja lisamiseks jne. Lõpuks küsitakse digitaalallkirjastatud konteiner teenuselt meetodiga GetSignedDoc.

Saadud konteineris tuleb xml element <DataFile ... ContentType="HASHCODE" ... Id="D0" ... > ... </DataFile> asendada eelnevalt koostatud xml elemendiga:

<DataFile xmlns="http://www.sk.ee/DigiDoc/v1.3.0#"
ContentType="EMBEDDED_BASE64" Filename="test.txt" Id="D0"
MimeType="text/plain"
Size="42">VGhpcyBpcyBhIHRlc3QgZmlsZQ0Kc2Vjb25kbGluZQ0KdGhpcmRsa
W5l
</DataFile>

Nüüd peaks olema valmis digidoc formaadile vastav konteiner.

* Kanoniseeritud xml-i kohta loe siit: http://www.w3.org/TR/xml-c14n

Näide – Digidoc konteineri saatmine teenusesse nii, et andmefail on asendatud räsikoodiga

Näiteks kui DigiDoc konteineris on DataFile blokk kujul:

<DataFile xmlns="http://www.sk.ee/DigiDoc/v1.3.0#"
ContentType="EMBEDDED_BASE64" Filename="test.txt" Id="D0"
MimeType="text/plain"
Size="42">VGhpcyBpcyBhIHRlc3QgZmlsZQ0Kc2Vjb25kbGluZQ0KdGhpcmRsa
W5l
</DataFile>

ja teenusele ei soovita andmefaili sisu saata, tuleks blokk asendada alljärgnevaga:

<DataFile xmlns="http://www.sk.ee/DigiDoc/v1.3.0#"
ContentType="HASHCODE" Filename="test.txt" Id="D0" MimeType="text/plain"
Size="42" DigestType="sha1"
DigestValue="t8eRSrKTgR4PAAKTLYWGCjuTSJA="></DataFile>

Kui teenusesse on saadetud andmefailide sisu asemel räsi, tuleb teenusest (näiteks peale konteineri verifitseerimist või allkirjade lisamist) DigiDoc faili tagasi saamisel andmefaili sisaldav <DataFile> element tagasi asendada.

8.2 CloseSession

CloseSessioni päringuga lõpetatakse transaktsioon. Päringu tulemusena kustutatakse kogu antud sessioonijooksul serverisse talletatud info. Pärast CloseSession päringu kasutamist tuleb uue sessiooni algatamiseks teha uuesti StartSession päring. Alati on soovitatav transaktsioon CloseSession päringuga lõpetada. Kui rakendus sessiooni ise ei lõpeta, siis lõpetatakse sessioon automaatselt timeout´i saabumisel.

Päringu parameetrid:

- **Sesscode** –aktiivse sessiooni identifikaator.

Vastuse parameetrid:

- **Status** - kui sessiooni sulgemine õnnestub, on antud parameetri väärtuseks OK.

Kui sessiooni sulgemine mingil põhjusel ebaõnnestub tagastatakse SOAP-FAULT objekt.

8.3 CreateSignedDoc

CreateSignedDoc päringut kasutatakse uue DigiDoc konteineri loomiseks juhul, kui rakendus soovib määrata moodustatava konteineri formaati ja versiooni. CreateSignedDoc päringu moodustamise järgselt tuleb lisada AddDataFile päringuga andmed ja seejärel on võimalik fail allkirjastada.

Päringu parameetrid:

- **Sesscode** –aktiivse sessiooni identifikaator.
- **Format** – loodava dokumendikonteineri formaat (hetkel toetatud DIGIDOC-XML)
- **Version** – loodava dokumendikoneineri formaadi versiooninumber (hetkel DIGIDOC-XML-i puhul toetatud versioonid 1.1,1.2, 1.3)

DigiDoc formaatide kirjeldused leiab http://www.sk.ee/digidoc.

Päringu vastuses sisaldub järgmine info:

- **Status** – toimingu vastuskood, kui toiming õnnestus on vastuskood “OK”.
- **SignedDocInfo** – Sessioonis oleva DigiDoc konteineri struktuur andmefaili lisamise järgselt. SignedDocInfo struktuur on kirjeldatud käesolevas dokumendis peatükis 9.1.

Kui antud formaadi ja versiooninumbrina päringu parameetrites kasutatakse ebasobivat kombinatsiooni, tagastatakse SOAP veaobjekt veateatega “**Invalid format & version combination!**”.

8.4 AddDataFile

AddDataFile päring võimaldab sessioonis olevale DigiDoc konteinerile lisada täiendava algfaili. Kui StartSession käigus on lisatud üks andmefail, kuid kasutaja soovib ühe DigiDoc konteineri sees allkirjastada mitut andmefaili, siis saab antud meetodiga enne allkirjastamist lisada ülejäänud algfailid.
NB! Andmefaili lisamine on võimalik ainult nende DigiDoc failide puhul, millele ei ole lisatud ühtegi allkirja.

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator.
- **Filename** – andmefaili nimi ilma teekonnata.
- **MimeType** – algandmete andmetüüp.
- **ContentType** – Andmefaili sisu tüüp (HASHCODE, EMBEDDED_BASE64)
  - **HASHCODE** – teenusele ei saadeta tervet andmefaili sisu, vaid ainult üle andmete arvutatud räsikood*. Räsikoodi arvutamise algoritm on määratud parameetris *DigestType* ja räsikood edastatakse parameetrina *DigestValue.*
  - **EMBEDDED_BASE64 –** Faili sisu on esitatud Base64 kujul Content parameetris.

- **Size** – tegeliku algandmefaili suurus baitides.
- **DigestType** - algandmefaili räsikoodi tüüp. Esialgu toetatakse vaid sha1 tüüpi. Nõutud vaid HASHCODE tüüpi faili puhul.
- **DigestValue** – algandmefaili räsikoodi* väärtus Base64 kujul. Nõutud vaid HASHCODE tüüpi faili puhul.
- **Attributes** - Suvaline hulk muid atribuute (metaandmed), mis lisatakse DigiDoc faili koosseisu <Datafile> plokki atribuutideks kujul <nimi>="<väärtus>".
- **Content** - andmefaili sisu Base64 kujul, täidetakse vaid EMBEDDED_BASE64 ContentType korral.

* Vaata näidist, kuidas algandmefailist räsi arvutada ning teenusele saata, punktist 8.1

Vastus päringule:

- **Status** – toimingu vastuskood, kui toiming õnnestus on vastuskood “OK”.
- **SignedDocInfo** – Sessioonis oleva DigiDoc konteineri struktuur andmefaili lisamise järgselt. SignedDocInfo struktuur on kirjeldatud peatükis 9.1.

8.5 MobileSign

MobileSign meetod käivitab sessioonis oleva DigiDoc faili allkirjastamise Mobiil-ID’ga.

MobileSign meetodi kasutamiseks peab sessioonis olevale DigiDoc konteineris olema vähemalt üks andmefail.

Kui soovitakse mobiiliga allkirja anda ilma DigiDoc faili loomata või teenusesse saatmata, tuleks kasutada antud meetodi asemel MobileCreateSignature meetodit.

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator
- **SignerIDCode** - Allkirjastaja isikukood;
- **SignersCountry –** Isikukoodi välja andnud riik, kasutatakse ISO 3166 2 tähelisi riigikoode (näiteks: EE);
- **SignerPhoneNo –** allkirjastava isiku telefoninumber koos riigikoodiga kujul +xxxxxxxxx (näiteks +3706234566). Mittekohustuslik, juhul kui telefoninumber on määratud, ei pea IDCode ja Country parameetrid olema määratud. Kui on määratud nii PhoneNo kui ka IDCode parameetrid, kontrollitakse telefoninumbri vastavust isikukoodile ja mittevastavuse korral tagastatakse SOAP veakood 301.
- **ServiceName -** Teenuse kasutaja ja pakkuja vahel eelnevalt kokku lepitud teenuse nimetus. Kohustuslik, maksimaalne pikkus 20 tähemärki
- **AdditionalDataToBeDisplayed** –Allkirjastamise käigus telefonil kuvatav lisatekst. Mittekohustuslik, maksimaalne pikkus 50 tähemärki.
- **Language** – Allkirjastaja telefonile kuvatavate teadete keel. Kasutatakse ISO 639: 3-tähelisi koode suurtähtedes, kohustuslik.
- **Role -** Allkirjastaja sisestatud rolli või resolutsioon, mittekohustuslik

- **City** – Allkirjastamise asukoha linna nimi, mittekohustuslik.
- **StateOrProvince** – Allkirjastamise asukoha maakonna nimi, mittekohustuslik.
- **PostalCode** – Allkirjastamise asukoha postiindeks, mittekohustuslik.
- **CountryName** – Allkirjastamise asukoha riiginimi, mittekohustuslik
- **SigningProfile –** Parameeter määramaks allkirjastamisel tekitatava allkirja omadusi. (Näiteks, kas allkiri sisaldab lisaks OCSP kehtivuskinnitusele veel täiendavaid ajatempleid). Vaikemäärangute kasutamiseks tuleb parameeter väärtustada tühja stringiga. Antud teenuse versioonis parameetri väärtust ignoreeritakse.
- **MessagingMode** - Määrab mis režiimis tagastatakse MobileSign päringu vastus. Võimalikud variandid on:
  - "asynchClientServer" – Rakenduse pakkuja teeb pärast MobileSign päringut täiendavaid staatusepäringuid.
  - "asynchServerServer" – Signeerimistoimingu lõppemisel või vea tekkimisel saadetakse vastus kliendirakendusele asünkroonselt vastavalt AsyncConfiguration parameetris määratud konfiguratsioonile.
- **AsyncConfiguration** – Määrab asünkroonselt vastuse tagasisaatmiseks kasutatava konfiguratsiooni. Antud parameetri väärtust kasutatakse ainult juhul kui MessagingMode on "asynchServerServer". Konfiguratsioon lepitakse kokku teenuse kasutaja ja teenuse pakkuja vahel.
- **ReturnDocInfo –** kui väärtus "true", tagastatakse päringu tulemusena DigiDoc faili info.
- **ReturnDocData – "**true" väärtuse korral tagastatakse DigiDoc dokument HTMLescaped kujul.

Päringu vastusena tagastatav info:

- **Status** – väärtus „OK" või veastring.
- **StatusCode** – 0 kui toiming õnnestus, vastasel korral veakood.
- **ChallengeID** - 4 numbriline kontrollkood, mis arvutatakse signeeritava räsi põhjal. Antud kontrollkood tuleb mobiilallkirjastamist võimaldaval rakendusel kuvada kasutajale ja selle kaudu on võimalik kasutajal veenduda päringu autentsuses (sama kontrollkoodi kuvab ka telefon PIN2 küsimisel).

Kui kasutatakse asynchClientServer režiimi tuleb pärast antud päringu vastuse saamist hakata teenusele saatma GetStatusInfo päringuid veendumaks, et allkirjastamine on lõpule jõudnud.

NB! Enne esimese staatuse päringu saatmist on soovitatav oodata vähemalt 15 sekundit kuna autentimise protsess ei saa tehniliste ja inimlike piirangute tõttu kiiremini lõppeda.

Juhul, kui kasutatakse "asynchServerServer" režiimi saadetakse allkirjastamise toimingu lõppemisel automaatselt teenuse kasutajale vastavalt kokku lepitud konfiguratsioonile.

Asünkroonselt tagasi saadetav vastus on XML kujul ja selle struktuur on:

Välja nimetus	Tüüp	Kirjeldus

Sesscode	Integer	Vastusega seotud sessiooni identifikaator
Status	String	Toimingu staatuskood. Toimingu õnnestumisel “OK”. Teised võimalikud olekud on kirjeldatud GetSignedDocInfo päringu vastuses Status väljal.
Data	String	a) Kui mobiilallkirjastamise päringu käivitanud meetodis oli ReturnDocInfo elemendi väärtus “true”, siis on antud parameetri väärtuseks sessioonis oleva allkirjastatud faili struktuur XML-ina vastavalt käesolevas dokumendis peatükis 9.1 esitatud kujul b) Kui mobiilallkirjastamise päringu käivitanud meetodis oli ReturnDocInfo väärtus “false” ja ReturnDocData elemendi väärtuseks “true”, siis on antud parameetri väärtuseks sessioonis olev DigiDoc fail HTML encoded kujul. c) Kui päringus on nii ReturnDocInfo kui ReturnDocData väärtused “false” on antud parameetri väärtus tühi.

8.6 GetStatusInfo

GetStatusInfo meetod on mõeldud teenusest sessiooni olekuinfo saamiseks.

GetStatusInfo päringut kasutatakse peamiselt mobiilallkirjastamise puhul asünkroonses Client-Server režiimis allkirjastamise protsessi olekuinfo pärimiseks (pollimiseks).

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	Aktiivse sessiooni identifikaator
ReturnDocInfo	Boolean	+	“true” väärtuse korral tagastatakse vastuses sessioonis oleva dokumendi info SignedDocInfo plokis.
WaitSignature	Boolean	+	Kui TRUE, siis päringule enne vastust ei tagastata kui telefonilt on signatuuri väärtus saabunud või on juhtunud viga. FALSE korral tagastatakse koheselt vastus ja GetStatusInfo väljakutset tuleb natukese aja pärast (2-10 sekundit) korrata.

Päringu vastus:

Parameeter	Tüüp	Kirjeldus
Status	String	Viimase toimingu staatuse kood. Mobiilallkirjastamise puhul: - REQUEST_OK – sõnum täitmiseks vastu võetud; - EXPIRED_TRANSACTION – saabus timeout, enne kui kasutaja jõudis allkirjastada; - USER_CANCEL - kasutaja katkestas telefonil allkirjastmise; - SIGNATURE - allkirjastamine edukalt lõpetatud;

		- NOT_VALID - tekkinud signatuur ei valideeru; - OUTSTANDING_TRANSACTION – toiming kestab, staatuse päringut tuleb korrata; - MID_NOT_READY - telefoni Mobiil-ID funktsionaalsus ei ole veel kasutatav, proovida mõne aja pärast uuesti; - PHONE_ABSENT – sõnumi saatmine ebaõnnestus, telefon ei ole levis; - SENDING_ERROR – muu sõnumi saatmise viga (telefon ei suuda sõnumit vastu võtta, sõnumikeskus häiritud); - SIM_ERROR – SIM rakenduse viga; - INTERNAL_ERROR – muu tehniline viga.
StatusCode	String	Viimasena välja kutsutud toimingu olekukood
SignedDocInfo	SignedDocInfo	Juhul, kui GetStatusInfo päringus oli parameetri ReturnDocInfo väärtus “true”, tagastatakse sessioonis oleva allkirjastatud faili struktuur vastavalt käesolevas dokumendis peatükis 9.1 esitatud kujul.

8.7 GetSignedDocInfo

GetSignedDocInfo päring on mõeldud teenusest hetkel sessioonis oleva (allkirjastatud) dokumendi ja selle olekuinfo saamiseks.

Päringu parameetrid on:

- **Sesscode** – aktiivse sessiooni identifikaator

Päringu vastusena tagastatav info:

- **Status** – väärtus „OK“ või veastring
- **SignedDocInfo** - sessioonis oleva allkirjastatud faili struktuur vastavalt käesolevas dokumendis peatükis 9.1 esitatud kujul.

8.8 GetSignedDoc

GetSignedDoc päringuga saadakse veebiteenusest tagasi allkirjastatud dokument. Dokumenti sisu on HTML-encoded kujul. Kui lisaks allkirjastatud dokumendile soovitakse saada struktureeritud kujul dokumendi infot, tuleb kasutada GetSignedDocInfo päringut.

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator

Vastus päringule:

- **Status** – väärtus „OK“ või veastring
- **SignedDocData** – Sessioonis oleva allkirjastatud dokument XML kujul. Kuna XML märgised on viidud HTMLencoded kujule, siis tuleks enne faili salvestamist failisüsteemi või andmebaasi teha HTML decode teisendus.

8.9 GetDataFile

GetDataFile päring on allkirjastatud failist algfaili pärimiseks. Näiteks kui laadida StartSession päringuga teenusesse allkirjastatud fail, siis GetDataFile päringuga on võimalik kõik algfailid ükshaaval välja lugeda.

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator
- **DataFileId** – andmefaili identifikaator. Kujul Dxx, kus xx on faili järjenumber. Sessioonis oleva allkirjastatud failis sisalduvate algfailide identifikaatorid on kättesaadavad SignedDocInfo struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks StartSession või GetSignedDocInfo päringu tulemusena.

Päringu vastus:

- **Status** – päringu õnnestumise korral „OK“
- **DataFileData** – Algandmefaili info DataFileInfo stuktuurina, mis on kirjeldatud käesolevas dokumendis peatükis 9.3. Andmefailid tagastatakse samal kujul, nagu nad teenusele StartSession või AddDataFile meetoditega edastati, st. kui teenusele saadeti andmefaili sisu, siis antud meetod tagastab ka andmefaili bloki nii, et DfData väljal on andefaili sisu Base64 kujul. Juhul, kui teenusele edastati vaid andmefaili räsi, siis tagastab ka antud meetod andmefaili kohta vaid räsi.

Kui proovitakse pärida andmefaili, mida ei eksisteeri, tagastatakse SOAP-i vea objekt veateatega “**No such DataFile!**”.

8.10 RemoveDataFile

RemoveDataFile päring võimaldab DigiDoc konteinerist eemaldada algfaili. NB! andmefaili eemaldamine on võimalik vaid siis kui konteiner ei sisalda mitte ühtegi allkirja. Kui dokumendile on lisatud üks või rohkem allkirja, siis andmefaili eemaldamine võimalik ei ole.

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator
- **DataFileId** – andmefaili identifikaator. Kujul Dxx, kus xx on faili järjenumber. Sessioonis oleva allkirjastatud failis sisalduvate algfailide identifikaatorid on kättesaadavad *SignedDocInfo* struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks *StartSession* või *GetSignedDocInfo* päringu tulemusena.

Päringu vastus:

- **Status** – päringu õnnestumise korral „OK“
- **SignedDocInfo** – Sessioonis oleva DigiDoc-i info algfaili eemaldamise järgselt. SignedDocInfo struktuur on kirjeldatud peatükis 9.1.

Juhul, kui allkirja eemaldamine ei õnnestu tagastatakse SOAP veaobjekt. Näiteks kui proovitakse eemaldada faili allkirjastatud dokumendilt, tagastatakse viga “Cannot change a signed doc”.

8.11 RemoveSignature

RemovesSignature päring võimaldab Sessioonis olevalt allkirjastatud faililt eemaldada allkirja. Päringu tulemusena tagastatakse SignedDocInfo eemaldatud allkirjaga kujul.

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator
- **SignatureId** – allkirja unikaalne tunnus. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber (näiteks S0, S1 jne.). Sessioonis oleva allkirjastatud failis sisalduvate allkirjade tunnused on kättesaadavad SignedDocInfo struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks StartSession või GetSignedDocInfo päringu tulemusena.

Päringu vastus:

- **Status** – päringu õnnestumise korral „OK“.
- **SignedDocInfo** – Sessioonis oleva DigiDoc-i info allkirja eemaldamise järgselt. SignedDocInfo struktuur on kirjeldatud käesolevas dokumendis peatükis 9.1.

Juhul, kui allkirja eemaldamine ei õnnestu tagastatakse SOAP veaobjekt veateatega.Võimalikud veateated:

- **Must supply Signature id**! – allkirja identifikaator on määramata
- **No such Signature!** – päringu parameetriks olevale allkirja identifikaatorile vastavat allkirja ei leitud

8.12 GetSignersCertificate

Allkirjastaja sertifikaadi päring. Päring võimaldab soovi korral (näiteks kasutajale kuvamiseks) teenuse kasutajal lugeda DigiDoc failist välja allkirjastaja sertifikaadi.

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator
- **SignatureId** – allkirja, mille allkirjastaja sertifikaati soovitakse pärida, identifikaator. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber (näiteks S0, S1 jne.). Sessioonis oleva allkirjastatud failis sisalduvate allkirjade tunnused on kättesaadavad SignedDocInfo struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks StartSession või GetSignedDocInfo päringu tulemusena.

Päringu vastus:

- **Status** – päringu õnnestumise korral „OK“
- **CertificateData** – päritud sertifikaat stringina Base64 kujul (PEM formaadis).

Juhul, kui sertifikaadi tagastamine ei õnnestu tagastatakse SOAP veaobjekt veateatega. Võimalikud veateated:

- **Must supply Signature id!** – allkirja identifikaator on määramata.
- **No such Signature!** – päringu parameetriks olevale allkirja identifikaatorile vastavat allkirja ei leitud.

8.13 GetNotarysCertificate

Päringu tulemusena tagastatakse määratud allkirja kehtivuskinnituse allkirjastaja sertifikaat (OCSP serveri sertifikaat).

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator
- **SignatureId** – allkirja unikaalne tunnus. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber (näiteks S0, S1 jne.). Sessioonis oleva allkirjastatud failis sisalduvate allkirjade tunnused on kättesaadavad SignedDocInfo struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks StartSession või GetSignedDocInfo päringu tulemusena.

Päringu vastus:

- **Status** – päringu õnnestumise korral „OK“
- **CertificateData** – päritud sertifikaat stringina Base64 kujul (PEM formaadis).

Juhul, kui sertifikaadi tagastamine ei õnnestu tagastatakse SOAP veaobjekt veateatega.Võimalikud veateated:

- **Must supply Signature id!** – allkirja identifikaator on määramata.
- **No such Signature!** – päringu parameetriks olevale allkirja identifikaatorile vastavat allkirja ei leitud.
- **No notary for this Signature**! – päringu parameetriks oleval allkirjal ei ole kehtivuskinnitust.

8.14 GetNotary

Antud päring võimaldab teenuselt saada määratud allkirja kehtivuskinnitus.

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator
- **SignatureId** – allkirja unikaalne tunnus. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber (näiteks S0, S1 jne.). Sessioonis oleva allkirjastatud failis sisalduvate allkirjade tunnused on kättesaadavad SignedDocInfo struktuuris. Antud struktuur tagastatakse teenuse kasutajale näiteks StartSession või GetSignedDocInfo päringu tulemusena.

Päringu vastus:

- **Status** – päringu õnnestumise korral „OK“.
- **OcspData** – OCSP kehtivuskinnitus Base64 kujul.

Juhul, kui kehtivuskinnituse hankimine ei õnnestu tagastatakse SOAP veaobjekt veateatega. Võimalikud veateated**:**

- **Must supply Signature id!** – allkirja identifikaator on määramata.
- **No such Signature!** – päringu parameetriks olevale allkirja identifikaatorile vastavat allkirja ei leitud.
- **No notary for this Signature!** – päringu parameetriks oleval allkirjal ei ole kehtivuskinnitust.

8.15 GetVersion

Päring võimaldab kontrollida teenuse töötamist ja saada teada teenuse versiooni. Päringul parameetrid puuduvad.

Vastuse struktuur:

- **Name** – teenuse nimetus (hetkel DigiDocService).
- **Version** – teenuse versioon kujul x.x.x (näiteks 1.0.3) Versiooni kõige suurem järk märgib põhjalikke muudatusi teenuses, versiooni numbri teine järk kirjeldab muudatusi, mille tulemusena võib muutuda teenuse protokoll ja viimane järk kirjeldab pisiparandusi, mis protokolli ei muuda.
- **Libname –** kasutatava baasteegi nimetus.
- **Libver –** kasutava baasteegi versioon.

8.16 PrepareSignature

Päring kiipkaardiga allkirjastamise korral allkirja ettevalmistamiseks. Päringu tulemusena lisatakse sessioonis olevale DigiDoc konteinerile uus nö. poolik allkiri ning tagastatakse uue allkirja unikaalne tunnus ja allkirjastatav räsikood, mis tuleks teenust kasutava rakenduse poolt edastada kasutaja arvutis olevale signeerimisprogrammile (enamasti ActiveX või Java Applet).

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator
- **SignersCertificate** – allkirjasta sertifikaat binaarselt kujult (DER) viiduna HEX stringi kujule. Enamasti sertifikaat antakse õigel kujul kasutaja arvutis oleva signeerimisprogrammi (ActiveX või Java Applet) poolt.
- **SignersTokenId** – kiipkaardil privaatvõtme pesa identifkaator, väärtus määratakse signeerimisprogrammi poolt allkirjastaja sertifikaadi väljalugemisel ja edastatakse signeerimisprogrammile signeerimistoimingu teostamisel.
- **Role -** Allkirjastaja poolt sisestatud rolli või resolutsiooni tekst
- **City -** Allkirjastamise asukoha linna nimi
- **State -** Allkirjastamise asukoha maakonna nimi
- **PostalCode** - Allkirjastamise asukoha postiindeks
- **Country** - Allkirjastamise asukoha riiginimi
- **SigningProfile** – Parameeter määramaks allkirjastamisel tekitatava allkirja omadusi. (Näiteks, kas allkiri sisaldab lisaks OCSP kehtivuskinnitusele veel täiendavaid ajatempleid). Vaikemäärangute kasutamiseks tuleb parameeter väärtustada antud parameeter tühja stringiga. Antud teenuse versioonis parameetri väärtust ignoreeritakse.

Allkirjastamise asukohainfo küsib enamasti allkirjastamisrakendus kasutajalt ning edastav DigiDocServicele. Rolli ja allkirjastamise asukoha info sisestamine ei ole kohustuslik.

Päringu vastus:

- **Status** – päringu õnnestumise korral „OK“.
- **SignatureId –** uue loodava allkirja unikaalne tunnus. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber (näiteks S0, S1 jne.). Antud tunnust kasutades on võimalik hiljem allkiri kustutada või pärida allkirja atribuute (allkirjastaja sertifikaat, kehtivuskinnituse sertifikaat, kehtivuskinnitus).
- **SignedInfoDigest –** Allkirjastatav räsikood HEX string kujul.

Juhul, kui kehtivuskinnituse tagastamine ei õnnestu tagastatakse SOAP veaobjekt veateatega. Võimalikud veateated:

- **Must supply Signature certificate! –** allkirjastaja sertifikaadi väärtus on tühi.

8.17 FinalizeSignature

Antud päring on allkirjastamise lõpetamiseks kiipkaardiga allkirjastamise korral. FinalizeSignature päringuga lõpetatakse PrepareSignature sammul ettevalmistatud allkiri. DigiDoc faili lisatakse allkirjastatud signatuur ja võetakse OCSP kehtivuskinnitus.

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator
- **SignatureId –** allkirja unikaalne tunnus. Allkirja identifikaator tagastati teenuse poolt PrepareSignature sammu tulemusena.
- **SignatureValue –** Signatuuri (allkirjastatud räsi) väärtus HEX stringi kujul. Antud väärtus tagastatakse signeerimiseks kasutatud signeerimisprogrammi (ActiveX või Applet) poolt.

Päringu vastus:

- **Status** – päringu õnnestumise korral „OK“
- **SignedDocInfo** – Sessioonis oleva DigiDoc-i info uue allkirja lisamise järgselt. SignedDocInfo struktuur on kirjeldatud käesolevas dokumendis peatükis 9.1.

8.18 GetSignatureModules

Päring kiipkaardiga allkirjastamiseks vajalike moodulite laadimiseks. Kui soovitakse kiipkaardiga allkirja anda, siis antud päringu tulemusena saadetakse teenust kasutavale rakendusele allkirjastamismoodulid, mis tuleks kasutajaliidesesse integreerida. Allkirjastamisfunktsionaalsust pakkuval lehel viiteid ka allkirjastamiseks vajalikele moodulitele nagu Java2 appleti või ActiveX moodul. Mooduleid on kahte tüüpi – FAIL (ohjurprogramm, applet, vms.) ja HTML (dünaamiline HTML/JavaScript). HTML moodulite kood sisaldab markereid, mis tuleb asendada vastava infoga (räsikood, sertifikaat jne.) Vajadusel korral võib teha HTML koodis teisendusi (näiteks väljanägemine/javascript funktsionaalsus),

kuid vajalik on garanteerida signeerimise appleti /ActiveX ja veebiteenuse vaheline parameetrite vahetamine.

Päringu parameetrid:

- **Sesscode** – aktiivse sessiooni identifikaator
- **Platform** – platvorm, mille tarbeks soovitakse allkirjastamismooduleid hankida. Võimalikud variandid on:
  - LINUX-MOZILLA - Signeerimisrakendusena tagastatakse Java Applet ja Linuxi jaoks vajalik PKCS#11 ohjurprogramm kiipkaardiga suhtlemiseks.
  - WIN32-MOZILLA – Signeerimisrakendusena tagastatakse Java Applet ja Windowsi jaoks vajalik PKCS#11 moodul kiipkaardiga suhtlemiseks.
  - WIN32-IE – signeerimisrakendusena tagastatakse ActiveX moodul.
- **Phase** – samm mille jaoks mooduleid laetakse: Võimalikud variandid on:
  - PREPARE – allkirjastamise moodulid kiipkaardilt sertifikaadi lugemiseks (vajalik enne PrepareSignature meetodi välja kutsumist).
  - FINALIZE – allkirjastamise moodulid signeerimistoimingu teostamiseks (vajalik enne FinalizeSignature meetodi välja kutsumist).
- **Type –** määrab mis osa moodulitest tagastatakse. Võimalikud variandid on:
  - FILE – tagastatakse ainult fail tüüpi allkirjastamismoodulid (ActiveX, Applet, PKCS#11 moodul)
  - HTML – tagastatakse ainult HTML moodulid
  - ALL – tagastatakse nii failed, kui HTML moodulid.

Päringu vastus:

- **Status** – päringu õnnestumise korral „OK“.
- **Modules** – päringu tulemusena saadetud moodulite loetelu, iga element sisaldab järgmisi atribuute:
  - Name – mooduli nimetus, FAIL tüübi moodulite puhul , tuleb moodul sama nimega faili salvestada.
  - Type - määrab, kas tegu on HTML või fail tüüpi mooduliga. HTML mooduli korral parameetri väärtuseks “HTML”, faili puhul “FAIL”.
  - Location – Määrab, kus kohta antud moodul tuleb veebilehel integreerida.
    Võimalikud variandid:
    - HTML-HEAD
    - HTML-FORM-BEGIN
    - HTML-FORM-END
    - HTML-BODY
    - HTML-SCRIPT
    - LIBDIR fail tuleb salvestada kataloogi, millele HTML lehel viidatakse, vaikimisi sama kataloog, kus script käivitati. Sõltuvalt HTML locationist tuleb moodul HTML lehel õigesse kohta paigutada.
  - ContentType – määrab mis kujul on kodeeritud content väljal olev sisu. Hetkel kasutatakse alati Base64 kodeeringut.
  - Content – mooduli sisu ContentType parameetris määratud kujul.

8.19 GetTSACertificate

Meetod ajatempliteenuse osutaja (TSA) sertifikaadi pärimiseks.
Antud meetod on vajalik vaid juhul, kui digitaalallkirjastatud dokument sisaldab RFC 3161 ajatempleid. (DigiDoc failiformaadid 1.0, 1.1, 1.2 ja 1.3 selliseid ajatempleid ei sisalda).

NB! Antud teenuse versioonis on realiseeritud ainult antud meetodi liides, funktsionaalsust implementeeritud ei ole.

8.20 GetTimestamp

Meetod ajatempli info pärimiseks. Antud meetod on vajalik vaid juhul, kui digitaalallkirjastatud dokument sisaldab RFC 3161 ajatempleid. (DigiDoc failiformaadid 1.0, 1.1, 1.2 ja 1.3 selliseid ajatempleid ei sisalda).

NB! Antud teenuse versioonis on realiseeritud ainult antud meetodi liides, funktsionaalsust implementeeritud ei ole.

8.21 GetCRL

Meetod allkirja koosseisus oleva tühisusnimekirja (CRL) pärimiseks. Antud meetod on vajalik juhul, kui allkirjastatava dokumendi koosseisus sertifikaatide kehtivusinfo on tühisusnimekirja kujul (DigiDoc failiformaatides 1.0, 1.1, 1.2 ja 1.3 on sertifikaadi kehtivusinfo alati OCSP kehtivuskinnituse näol ja tühisusnimekirju ei kasutata).

NB! Antud teenuse versioonis on realiseeritud ainult antud meetodi liides, funktsionaalsust implementeeritud ei ole.

8.22 MobileCreateSignature

Meetod Mobiil-ID-ga allkirjastamise protsessi käivitamiseks.

Meetodi kasutamise tulemusena tagastatakse DigiDoc-i <Signature> element ja teenust väljakutsuv rakendus peab ise hoolitsema selle lisamise eest DigiDoc faili koosseisu.

Meetod hoolitseb sisemiselt allkirjastaja sertifikaadi, kehtivuskinnituse ja vajadusel RFC3161 ajatemplite hankimise ning signeerimispäringu kasutaja telefonile saatmise eest.

Päringu kasutamiseks ei ole vaja luua StartSession meetodiga uut sessiooni. Kui soovitakse allkirjastada sessioonis olevat DigiDoc faili, tuleb antud meetodi asemel kasutada MobileSign meetodit.

Päring:

Parameeter	Tüüp	K	Kirjeldus
IDCode	String	+	Allkirjastava isiku isikukood
Country	String(2)	+	Allkirjastaja isikukoodi välja andnud riik, kasutatakse ISO 3166 2 tähelisi riigikoode (näiteks: EE).
PhoneNo	String	-	Allkirjastaja telefoninumber koos riigikoodiga kujul +xxxxxxxxx (näiteks +3706234566). Kui telefoninumber on määratud, ei pea IDCode ja Country parameetrid olema määratud. Kui on määratud nii PhoneNo kui ka IDCode parameetrid, kontrollitakse telefoninumbri vastavust isikukoodile ja mittevastavuse korral tagastatakse SOAP veakood 301.
Language	String(3)	+	Kasutaja telefonil kuvatavate teadete keel. Kasutatakse 3-tähelisi koode suurtähtedes. Võimalikud variandid: EST, ENG ja RUS.
ServiceName	String(20)	+	Allkirjastamisel telefonil kuvatav teenuse nimetus, maksimaalne pikkus 20 tähemärki. Eelnevalt on vajalik kasutatava teenuse nimetuse kokkuleppimine teenuse pakkujaga.
MessageToDisplay	String(40)	-	Täiendav tekst, mis allkirjastamise PIN-i küsimise eelselt lisaks teenuse nimetuse kasutaja telefonile kuvatakse. Maksimaalne pikkus 40 tähemärki
Role	String	-	Allkirjastaja poolt allkirjastamisel sisestatud rolli või resolutsiooni tekst
City	String	-	Allkirjastamise asukoha linna nimi
StateOrProvince	String	-	Allkirjastamise asukoha maakonna nimi
PostalCode	String	-	Allkirjastamise asukoha postiindeks
CountryName	String	-	Allkirjastamise asukoha riiginimi
SigningProfile	String	-	Parameeter määramaks allkirjastamisel tekitatava allkirja omadusi (näiteks, kas allkiri sisaldab lisaks OCSP kehtivuskinnitusele veel täiendavaid ajatempleid). Vaikemäärangute kasutamiseks tuleb parameeter väärtustada tühja stringiga. Antud teenuse versioonis parameetri väärtust ignoreeritakse.
Datafiles	List	+	Andmefailide list. Iga elemendil on järgmised atribuudid: - Id – faili sisemine unikaalne tunnus. Andmefailide tunnused algavad sümboliga 'D', millele järgneb faili järjekorranumber. - DigestType - algandmefaili räsikoodi tüüp, esialgu on toetatud vaid “sha1”. - DigestValue – algandmefaili räsikoodi väärtus Base64 kujul. Räsi arvutatakse üle vastava DigiDoc <Datafile> elemendi kanoniseeritud kuju.
Format	String	+	Allkirjastatud faili formaat, näiteks “DIGIDOC-XML”
Version	String	+	Allkirjastatud faili formaadi versioon, näiteks “1.3”
SignatureID	String	+	Loodava allkirja identifikaator. Väljakutsuv rakendus peab kontrollima milline on suurim eelnev allkirja ID

			ja kasutama sellest ühe võrra suuremat väärtust. Näiteks kui viimane allkiri on identifikaatoriga “S2”, peaks antud parameetri väärtus olema “S3”. Kui dokumendil ei ole ühtegi allkirja, tuleks väärtusena kasutada “S0”.
MessagingMode		+	Määrab,mis režiimis tagastatakse MobileCreateSignature päringu vastus. Võimalikud variandid on: - “asynchClientServer” – rakenduse pakkuja teeb pärast MobileCreateSignature päringut täiendavaid staatusepäringuid; - “asynchServerServer” – signeerimistoimingu lõppemisel või vea tekkimisel saadetakse vastus teenuse kasutajale asünkroonselt.
AsyncConfiguration	Integer	-	Määrab asünkroonselt vastuse tagasisaatmiseks kasutatava konfiguratsiooni. Antud parameetri väärtust kasutatakse ainult juhul, kui MessagingMode on “asynchServerServer”. Konfiguratsioon lepitakse kokku teenuse kasutaja ja teenuse pakkuja vahel. Hetkel on toetatud vastuse tagasi saatmine kasutades Java Message Services (JMS) liidest.

Vastus:

Välja nimetus	Tüüp	Kirjeldus
Sesscode	Integer	Loodud sessiooni identifikaator
ChallengeID	String	4 tähemärgiline kontrollkood, mis arvutatakse signeerimiseks saadetava räsi põhjal. Antud kontrollkood tuleb mobiilallkirjastamist võimaldaval rakendusel kuvada kasutajale ning selle kaudu on võimalik kasutajal veenduda päringu autentsuses (sama kontrollkood kuvatakse allkirjastamisel ka telefonile).
Status	String	Toimingu edukal täitmisel “OK”. Juhul kui meetodi väljakutsel juhtub viga tagastatakse SOAP veaobjekt. SOAP veaobjektide kirjeldus ja veakoodid on toodud peatükis 9.4.

Kui kasutatakse “asynchClientServer” režiimi tuleb pärast antud päringule positiivse vastuse saamise järgselt teenusele saata GetMobileCreateSignatureStatus päringuid.

NB! Enne esimese staatuse päringu saatmist on soovitatav oodata vähemalt 15 sekundit kuna autentimise protsess ei saa tehniliste ja inimlike piirangute tõttu kiiremini lõppeda.

Juhul, kui kasutatakse “asynchServerServer” režiimi, saadetakse mobiilallkirjastamise toimingu lõppemisel automaatselt teenuse kasutajale allolev vastus vastavalt kokku lepitud konfiguratsioonile.

Asünkroonselt tagasi saadetav vastus on XML kujul ja selle struktuur on:

Välja nimetus	Tüüp	Kirjeldus
Sesscode	Integer	Vastusega seotud sessiooni identifikaator
Status	String	Toimingu staatuskood. Toimingu õnnestumisel "SIGNATURE". Teised võimalikud olekud on kirjeldatud GetMobileCreateSignatureStatus meetodi vastuses.
Data	String	Mobiilallkirjastamise käigus tekkinud <Signature> blokk halja XML-ina.

8.23 GetMobileCreateSignatureStatus

Antud meetodit kasutatakse ClientServer režiimis mobiilallkirjastamise protsessi oleku teada saamiseks.

Päring:

Parameeter	Tüüp	K	Kirjeldus
Sesscode	Integer	+	Sessiooni identifikaator
WaitSignature	Boolean	+	Kui TRUE, siis päringule ei tagastata vastust enne, kui telefonilt on signatuuri väärtus saabunud või on juhtunud viga. FALSE korral tagastatakse kohe vastus ja teenuse kasutaja peab tegema mõne aja möödumisel (soovitavalt 2-10 sekundi pärast) korduva staatuse päringu.

Vastus:

Välja nimetus	Tüüp	Kirjeldus
Sesscode	Integer	Sessiooni identifikaator
Status	String	Mobiilallkirjastamise protsessi olek: - REQUEST_OK – käsklus vastu võetud; - EXPIRED_TRANSACTION – saabus timeout enne kui kasutaja jõudis allkirjastasda; - USER_CANCEL - kasutaja keeldus allkirjastamast või katkestas; - SIGNATURE - allkirjastamine edukalt tehtu; - OUTSTANDING_TRANSACTION – toiming kestab, staatuse päringut tuleb korrata; - MID_NOT_READY - telefoni Mobiil-ID funktsionaalsus ei ole veel kasutatav, proovida mõne aja pärast uuesti; - PHONE_ABSENT – telefon ei ole levis; - SENDING_ERROR – muu sõnumi saatmise viga (telefon ei suuda sõnumit vastu võtta, sõnumikeskus häiritud); - SIM_ERROR – SIM rakenduse viga; - INTERNAL_ERROR – teenuse tehniline viga
Signature	String	Tekitatud DigiDoc-i <Signature> element Base64 kujul

Kui vastuses on Status väärtus ei ole OUTSTANDING_TRANSACTION, siis meetodi välja kutsumise järgselt sessioon suletakse.

8.24 GetMobileCertificate

Meetod Mobiil-ID teenuse olemasolu ja sertifikaatide info pärimiseks.

Päring:

Parameeter	Tüüp	K	Kirjeldus
IDCode	String	+	Sertifikaadiomaniku isikukood
Country	String(2)	+	Isikukoodi välja andnud riik, kasutatakse ISO 3166 2 tähelisi riigikoode(näiteks: EE).
PhoneNo	String	-	Sertifikaadiomaniku telefoninumber koos riigikoodiga kujul +xxxxxxxxx (näiteks +3706234566), juhul kui telefoninumber on määratud, ei pea IDCode ja Country parameetrid olema määratud. Kui on määratud nii PhoneNo kui ka IDCode parameetrid, kontrollitakse telefoninumbri vastavust isikukoodile ja mittevastavuse korral tagastatakse SOAP veakood 301.
ReturnCertData	String	-	Väärtused: “auth” – autentimissertifikaadi päring, “sign” –allkirjastamissertifikaadi päring, “both” – mõlemad, “none” mitte kumbagi. Vaikeväärtuseks on “none”.

Vastus:

Parameeter	Tüüp	K	Kirjeldus
AuthCertStatus	String	+	OK – isikutuvastuse sertifikaat on teenindamiseks valmis; NOT_ACTIVATED – sertifikaat ei ole aktiveeritud; REVOKED – sertifikaat on tühistatud; SUSPENDED – sertifikaat on peatatud.
SignCertStatus	String	+	OK – allkirjastamise sertifikaat on teenindamiseks valmis; NOT_ACTIVATED – sertifikaat ei ole aktiveeritud; REVOKED – sertifikaat on tühistatud; SUSPENDED – sertifikaat on peatatud.
AuthCertData	String	-	Isikutuvastuse sertifikaat PEM kujul
SignCertData	String	-	Allkirjastamise sertifikaat PEM kujul

Kui kasutaja ei ole Mobiil-ID klient, antakse SOAP fault vastavalt 9.4 toodule.

9 Kasutatavad andmestruktuurid

9.1 SignedDocInfo

Esitab terviklikult allkirjastatud DigiDoc faili struktuuri

- **Format** – Allkirjastatud konteineri failiformaat (hetkel toetatud DIGIDOC-XML)
- **Version** - Allkirjastatud failiformaadi versioon (1.1, 1.2, 1.3)
- **DataFileInfo –** Konteineris sisalduvate andmefailide info. Andmestruktuur on kirjeldatud käesolevas dokumendis peatükis 9.3. Ühe SignedDocInfo plokis võib olla DataFileInfo plokk esineda 0..n korda sõltuvalt andmefailide arvust.
- **SignatureInfo** – Sisaldab allkirjastatud failis olevate allkirjade infot. Antud blokki võib olla 0..n arv korda sõltuvalt allkirjade arvust. Sisaldab järgmisi atribuute:
    - **Id –** Allkirja antud dokumendi/transaktsiooni piires unikaalne allkirjaidentifikaator. Allkirjade tunnused algavad sümboliga 'S', millele järgneb allkirja järjekorranumber.
    - **Status** – Allkirja olekuinfo. Kui antud atribuudi väärtuseks on **"OK"** on allkiri kehtiv. Kui allkiri ei kehti on antud elemendi väärtuseks **"Error"** ja täpsem veainfo on esitatud Error elemendis.
    - **Error** – Sisaldab allkirja kehtivuse kontrollil ilmnenud vea infot. Sisaldab järgmisi atribuute:
        - **code** – veakood
        - **category –** veakategooria, hetkel on 3 veakategooriat: TECHNICAL –tehniline probleem; USER - kasutaja poolt likvideeritav probleem; LIBRARY – DigiDoc teegi sisene viga.
        - **description –** vea tekstiline kirjeldus inglise keeles. Kasutatavad veakoodid ja kirjelduses on samad, mis DigiDoc C-teegis.

    - **SigningTime** – allkirja andmise lokaalne (nt. allkirjasta arvuti, allkirjastamise veebiserveri) aeg vastavalt "The W3C note Date and Time Formats" [5] esitatud kujul. NB! See ei ole allkirja „ametlik" aeg, allkirja andmise ametlik aeg on määratud käesoleva struktuuri *Confirmation-> ProducedAt* elemendis.
    - **SignerRole –** allkirjastaja poolt allkirjastamisel märgitud roll või resulolutsioon. Määratud järgmiste atribuutidega:
        - **Certified –** Määrab, kas roll on allkirjastaja poolt ise määratud või sertifitseerija poolt antud. Hetkel kasutatakse ainult kasutajapoolt määratavaid rolle, mille puhul antud parameetri väärtus on 0.
        - **Role –** Rolli või resolutsiooni tekst
    - **SignatureProductionPlace -** Allkirja atribuutide hulka kuuluv andmehulk, mis kirjeldab allkirjastamise kohta.Allkirja andmisel on antud bloki täitmine mittekohustuslik. Sisaldab järgmisi andmeid:
        - **City** – Allkirjastamise asukoha linna nimi
        - **StateOrProvince** – Allkirjastamise asukoha maakonna nimi
        - **PostalCode** – Allkirjastamise asukoha postiindeks
        - **CountryName** – Allkirjastamise asukoha riiginimi

    - **Signer** – info allkirjastaja kohta, sisaldab järgmisi atribuute:
        - **CommonName** – Allkirjastaja nimi, võetakse allkirjastaja sertifikaadi Subject väljalt CN parameetrist.

- **IDCode** – allkirjastaja isikukood, võetakse allkirjastaja sertifikaadi Subjecti Serial Number parameetrist.
- **Certificate** allkirjastamiseks kasutatud sertifikaadi põhiinfo vastavalt käesolevas dokumendis peatükis 9.2 esitatud kujul.

- **Confirmation –** OCSP kehtivuskinnituse andmete blokk. Iga korrektne kehtiv allkiri sisaldab ühte kehtivuskinnituse plokki. Confirmation plokk sisaldab järgnevaid atribuute:
  - **ResponderID** – OCSP kehtivuskinnituse serveri eraldusnimi (OCSP Responder ID)
  - **ProducedAt** – Kehivuskinnituse võtmise aeg vastavalt "The W3C note Date and Time Formats" [5] esitatud kujul. (näiteks "2005.09.14T21:00:00Z"). NB! Antud aega loetakse digitaalallkirja andmise ajaks.
  - **Responder Certificate –** Kehtivuskinnituse teenuse serveri (OCSP) sertifikaat vastavalt käesolevas dokumendis peatükis 9.2 esitatud kujul.
- **Timestamps –** Info allkirjaga seotud RFC3161 ajatemplite kohta. DigiDoc failiformaadid 1.0, 1.1, 1.2 ja 1.3 ei sisalda vastaid ajatempleid ja antud teenuse versioonis ei ole ajatemplite funktsionaalsus realiseeritud.
- **CRLInfo –** Info allkirjaga seotud tühisusnimekirja kohta. DigiDoc failiformaatides 1.0, 1.1, 1.2 ja 1.3 tühisusnimekirju ei kasutata ja antud teenuse versioonis ei ole tühisusnimekirjadega seotud funktsionaalsus veel realiseeritud.

Näidisandmete blokk:

```
<SignedDocInfo xsi:type="d:SignedDocInfo">
   <format xsi:type="xsd:string"></format>
   <version xsi:type="xsd:string"></version>
   <DataFileInfo xsi:type="d:DataFileInfo">
      <Id xsi:type="xsd:string"></Id>
      <Filename xsi:type="xsd:string"></Filename>
      <MimeType xsi:type="xsd:string"></MimeType>
      <ContentType xsi:type="xsd:string"></ContentType>
      <Size xsi:type="xsd:int">0</Size>
      <DigestType xsi:type="xsd:string"></DigestType>
      <DigestValue xsi:type="xsd:string"></DigestValue>
         <Attributes xsi:type="d:DataFileAttribute">
         <name xsi:type="xsd:string"></name>
         <value xsi:type="xsd:string"></value>
      </Attributes>
   </DataFileInfo>
<SignatureInfo xsi:type="d:SignatureInfo">
   <Id xsi:type="xsd:string"></Id>
   <Status xsi:type="xsd:string"></Status>
   <Error xsi:type="d:Error">
      <code xsi:type="xsd:int">0</code>
      <category xsi:type="xsd:string"></category>
      <description xsi:type="xsd:string"></description>
   </Error>
   <SigningTime xsi:type="xsd:string"></SigningTime>
```

```
      <SignerRole xsi:type="d:SignerRole">
            <certified xsi:type="xsd:int">0</certified>
            <Role xsi:type="xsd:string"></Role>
      </SignerRole>
      <SignatureProductionPlace
si:type="d:SignatureProductionPlace">
         <City xsi:type="xsd:string"></City>
         <StateOrProvince
      xsi:type="xsd:string"></StateOrProvince>
         <PostalCode xsi:type="xsd:string"></PostalCode>
         <CountryName xsi:type="xsd:string"></CountryName>
      </SignatureProductionPlace>
      <Signer xsi:type="d:SignerInfo">
         <CommonName xsi:type="xsd:string"></CommonName>
         <IDCode xsi:type="xsd:string"></IDCode>
         <Certificate xsi:type="d:CertificateInfo">
            <Issuer xsi:type="xsd:string"></Issuer>
            <Subject xsi:type="xsd:string"></Subject>
            <ValidFrom xsi:type="xsd:string"></ValidFrom>
            <ValidTo xsi:type="xsd:string"></ValidTo>
            <IssuerSerial
            xsi:type="xsd:string"></IssuerSerial>
            <Policies xsi:type="d:CertificatePolicy">
               <OID xsi:type="xsd:string"></OID>
               <URL xsi:type="xsd:string"></URL>
               <Description
                  xsi:type="xsd:string"></Description>
            </Policies>
         </Certificate>
      </Signer>
      <Confirmation xsi:type="d:ConfirmationInfo">
         <ResponderID xsi:type="xsd:string"></ResponderID>
         <ProducedAt xsi:type="xsd:string"></ProducedAt>
         <ResponderCertificate xsi:type="d:CertificateInfo">
            <Issuer xsi:type="xsd:string"></Issuer>
            <Subject xsi:type="xsd:string"></Subject>
            <ValidFrom xsi:type="xsd:string"></ValidFrom>
            <ValidTo xsi:type="xsd:string"></ValidTo>
            <IssuerSerial
            xsi:type="xsd:string"></IssuerSerial>
            <Policies xsi:type="d:CertificatePolicy">
               <OID xsi:type="xsd:string"></OID>
               <URL xsi:type="xsd:string"></URL>
               <Description
                  xsi:type="xsd:string"></Description>
            </Policies>
         </ResponderCertificate>
      </Confirmation>
    </SignatureInfo>
  </SignedDocInfo>
```

9.2 CertificateInfo

Sertifikaadi põhivälju sisaldav andmeblokk. Kasutatakse nii allkirjastaja sertifikaadi, kui ka kehtivuskinnituse sertifikaadi info edastamiseks.

Sisaldab järgmisi atribuute:

- **Issuer** – Sertifikaadi väljaandja eraldusnimi (distinguished name)
- **IssuerSerial** - Sertifikaadi seerianumber
- **Subject** – Sertifikaadi eraldusnimi (distinguished name)
- **ValidForm** – Sertifikaadi kehtivuse algusaeg vastavalt The W3C note Date and Time Formats *[5] esitatud kujul. (näiteks "*2005.09.14T21:00:00Z")
- **ValidTo** – Sertifikaadi kehtivuse lõppemise aeg vastavalt [5] esitatud kujul.
- **Policies** - Kinnituspõhimõtete plokk, seda võib esineda 0..n tükki
  - **OID** - Kinnituspõhimõtete unikaalne tunnus
  - **URL –** Viide kinnituspõhimõtetele (kasutatakse peamiselt asutuste digitaalkinnituste põhjal)
  - **Description –**Kinnituspõhimõtete lühikirjeldus

Näidisandmete blokk:

```
<Certificate xsi:type="d:CertificateInfo">
   <Issuer
xsi:type="xsd:string">/emailAddress=pki@sk.ee/C=EE/O=AS
Sertifitseerimiskeskus/OU=ESTEID/SN=1/CN=ESTEID-SK</Issuer>
   <Subject xsi:type="xsd:string">/C=EE/O=ESTEID/OU=digital
signature/CN=KESKEL,URMO,38002240232/SN=KESKEL/GN=URMO/seria
lNumber=38002240232</Subject>
   <ValidFrom
xsi:type="xsd:string">2005.03.18T22:00:00Z</ValidFrom>
   <ValidTo
xsi:type="xsd:string">2008.03.22T22:00:00Z</ValidTo>
   <IssuerSerial
xsi:type="xsd:string">1111128454</IssuerSerial>
   <Policies xsi:type="d:CertificatePolicy">
      <OID
      xsi:type="xsd:string">1.3.6.1.4.1.10015.1.1.1.1</OID>
      <URL xsi:type="xsd:string">http://www.sk.ee/cps/</URL>
      <Description xsi:type="xsd:string">none</Description>
   </Policies>
</Certificate>
```

9.3 DataFileInfo

Antud andmeblokk kirjeldab DigiDoc konteineri koosseisus oleva või selle koosseisu lisatava andmefaili andmeid. Antud blokis võib sisalduda andmefail Base64 kujul, kuid blokk võib sisaldada ka vaid andmefaili räsi* - sõltuvalt ContentType atribuudi väärtusest.

- **Id** – faili sisemine unikaalne tunnus. Andmefailide tunnused algavad sümboliga 'D', millele järgneb faili järjekorranumber. Startsession päringu käigus antud atribuuti ei väärtustata ja edastatakse tühistring.
- **Filename** – andmefaili nimi ilma teekonnata.
- **ContentType** – Andmefaili sisu tüüp (HASHCODE, EMBEDDED_Base64)
  - **HASHCODE** – teenusele ei saadeta tervet andmefaili sisu, vaid ainult üle andmete arvutatud räsikood*. Räsikoodi arvutamise algoritm on määratud atribuudis *DigestType* ja räsikoodi ennast hoitakse väljal *DigestValue.*
  - **EMBEDDED_BASE64 –** Faili sisu on Base64 kujul DfData alamelemendis.
- **MimeType** – algandmete andmetüüp.
- **Size** – tegeliku algandmefaili suurus baitides.
- **DigestType** - algandmefaili räsi algoritm. Hetkel toetatud vaid “sha1”. Nõutud vaid HASHCODE tüüpi faili puhul.
- **DigestValue** – algandmefaili räsikoodi* väärtus Base64 kujul. Nõutud vaid HASHCODE tüüpi faili puhul.
- **Attributes** - Suvaline hulk muid atribuute (metaandmed), mis lisatakse DigiDoc faili koosseisu <Datafile> plokki atribuutideks kujul <nimi>="<väärtus>".
- **DfData** - andmefaili sisu Base64 kujul.

* Vaata näidist, kuidas algandmefailist räsi arvutada ning teenusele saata, punktist 8.1

9.4 SOAP veakoodid

SOAP veaobjektis <faultstring> sisaldab veakoodi ja <detail><message> selgitavat teksti inglise keeles.

Veakoodid on grupeeritud järgmiselt:

100-199 - teenust kasutava kliendi põhjustatud vead
200-299 - teenusesisesed vead
300-399 - lõppkasutaja ja tema telefoniga seotud vead.

Veakoodide tähendused:

Veakood	Tähendus
100	Teenuse üldine veasituatsioon.
101	Sisendparameetrid mittekorrektsel kujul.
102	Mõni kohustuslik sisendparameeter on määramata
103	Ligipääs antud meetodile antud parameetritega piiratud (näiteks kasutatav *ServiceName* ei ole teenuse pakkuja juures registreeritud.
200	Teenuse üldine viga.
201	Kasutaja sertifikaat puudub.
202	Kasutaja sertifikaadi kehtivus ei ole võimalik kontrollida.
300	Kasutajaga telefoniga seotud üldine viga.
301	Kasutajal pole Mobiil-ID lepingut.

302	Kasutaja sertifikaat ei kehti (OCSP vastus REVOKED).
303	Kasutajal pole Mobiil-ID aktiveeritud. Aktiveerimiseks tuleks minna aadressile http://mobiil.id.ee

10 Teenuse muudatuste ajalugu

10.1 Erinevused teenuse versioonide 2.3.30 ja 2.3.5 vahel

- Lisatud meetod CheckCertificate
- Tehtud mitmeid teenuse sisemisi täiendusi

10.2 Erinevused teenuse versioonide 2.3.3 ja 2.3.5 vahel

- Lisatud meetod GetMobileCertificate.

10.3 Erinevused teenuse versioonide 1.100 ja 2.3.3 vahel

- Lisatud meetodid MobileAuthenticate, GetMobileAuthenticateStatus, MobileCreateSignature ja GetMobileCreateSignatureStatus;
- Muudetud MobileSign meetodit;
- Kõikide parameetrite nimed on suure algustähega (Sesscode, Datafile jne).
- Suurendatud teenuse jõudlust ja töökindlust

10.4 Erinevused teenuse versioonide 1.100 ja 1.101 vahel

- Meetoditele StartSession, MobileSign, PrepareSignature lisatud täiendav parameeter SigningProfile.
- Sessiooni identifikaator sesscode viidud sõnumi päisest kehasse esimeseks parameetriks.
- Lisatud meetodid RFC 3161 ajatemplite ja tühisusnimekirjade (CRL) käsitlemiseks.

10.5 Erinevused teenuse versioonide 1.000 ja 1.100 vahel

- Lisatud Mobiil-ID signeerimise meetodid: MobileSign ja GetStatusInfo.