

Tallinna Ülikool
Informaatika Instituut

Tarvo Arikas

DIGIALLKIRJASTAMINE VEEBIRAKENDUSENA

Seminaritöö

Juhendaja: Jaagup Kippar

Tallinna Ülikool, November 2008

Sisukord

SISUKORD	2
DIGIALLKIRJASTAMINE JA TEMA KASUTUSVÕIMALUSED	4
Allkiri. Mis see on	4
Digi ja paberdokumendi ning –allkirja erinevused	4
Digiallkirjastamise olemus ja protsess	4
ID-kaardist ja digiallkirjastamisest Eestis	4
Digiallkirjastamine	4
ID-kaart ja allkirjastamisvahend - isiklik võti	5
Sertifikaadid	5
Kehtivuskinnitused	5
Põhiline digiallkirjastamise meespea	5
OLEMASOLEVA BAASRAKENDUSE (AUTOMATWEB) TUTVUSTUS	6
AutomatWeb (AW) ja tema võimalused	6
Patendiamet ja tema vajadused	6
Patendiametist	6
Vajadused seoses AW'ga	6
LÕPPEESMÄRK	8
Töövoog	8
Kasutajalood	8
EELUURIMINE	10
Senised ID-kaarti ja digiallkirjastamist kasutavad veebirakendused	10
Sertifitseerimiskeskus (SK)	10
SK pakutavad abimaterjalid digiallkirja kasutavate rakenduste loomiseks	11
Veebiteenus ehk DigiDocService	11
REALISATSIOON	12
Rakenduse jaoks valitud serveri tarkvara valimine ja seadmistamine	12

Klienditeegi sisu ja selle kasutamine	13
Kaasasoleva näiterakenduse tööle seadmine	13
Protsess AW'ga integreerimiseks	14
AW koodipool	14
AW kasutajaliides	15
Alternatiivne lahendus	15
Ülevaade koodist	16
Kasutusjuhend	18
EKRAANIKUVAD VALMINUD VEEBIRAKENDUSEST	19
Kaubamärgitaotluse töölaud	19
DigiDoc objekti allkirjade vaade, uue allkirja lisamisega	19
Patendi objekti vaade	20
LÕPPSÕNA	21
KASUTATUD KIRJANDUS	22

Digiallkirjastamine ja tema kasutusvõimalused

Allkiri. Mis see on

Allkiri seob, dokumendi tema looja ja/või kinnitajaga ning tagab dokumendile tema nõu tõestusväärtused, olenemata allkirja vormist ehk siis kas tegu on omakäelise, digitaalse või mingit kolmandat tüüpi allkirjaga. Dokumendi tõestusväärtusteks loetakse järgmisi punkte:

- Dokumendi loojat ja/või kinnitajat ning loomise ja/või kinnitamise aega peab olema võimalik hiljem kindlaks teha.
- Peab olema võimalik veenduda et dokumenti ei ole peale selle loomist/kinnitamist muudetud.

Digi ja paberdokumendi ning –allkirja erinevused

Kui paberdokumendi ning tema allkirja ühendavad nende seotus ühe kindla andmekandjaga, ehk füüsilise paberilehega kuhu nad on kantud, siis digidokument ja tema allkiri on mingil suvalisel digitaalsel andmekandjal olev bitijada, ehk ta ei ole seotud mingi kindla andmekandjaga. Samas ei võimalda tavaline digidokument, ning tema juurde lisatud looja nimi, kuidagi kinnitada seda, kas dokumenti ennast või looja nime on peale loomist muudetud või mitte. Seega on rikutud dokumendi tõstusväärtuse mõlemat punkti. Siit tuleneb ka fakt, et digidokumendi puhul ei saa rakendada seni kehtinud allkirjastamise põhimõtteid, kus allkirjastaja lisas tekstikujul dokumendile allkirjastamise aja ning oma signatuuri.

Digiallkirjastamise olemus ja protsess

Digiallkirjastamine on üks asümmeetrilise krüptograafia rakendusi, mis võimaldab õigel rakendamisel kinnitada allkirjastatud sõnumi allkirjastaja õigsust. Digiallkirjastamise protsess kaasab endas alati vähemalt kolme põhilist algoritmi:

- Võtme genereerimise algoritm, mis tekitab väljundina privaatse ja temale vastava avaliku võtme.
- Allkirjastamise algoritm, mis tekitab temale allkirjastatava sõnumi ja privaatvõtme ette andmisel digiallkirja.
- Allkirja kontrollimise algoritm, mis kontrollib temale etteantud allkirjastatud sõnumi, allkirja ja avaliku võtme kokkulangevust. Ehk kas antud allkiri on antud vastavale sõnumile vastava avaliku võtme seotud privaatvõtmega.

ID-kaardist ja digiallkirjastamisest Eestis

Digiallkirjastamine

ID-kaardi abil antav digiallkiri on seaduse silmis võrdne omakäelise allkirjaga. Kõik Eesti avalikud asutused on kohustatud võtma vastu digiallkirjastatud dokumente.

ID-kaart ja allkirjastamisvahend - isiklik võti

ID-kaardil on salajane allkirjastamisvõti, mida saab kasutada PIN-koodi abil. Selle võtmega märgistatakse allkirjastatud dokument unikaalsel ja võltsimatul viisil, mis võimaldab hiljem tõestada, et just sina selle allkirjastasid.

Sertifikaadid

ID-kaartide väljastamisel väljastatakse igale kasutajale kaks sertifikaati, millest üks on isikutuvastuseks, teine digiallkirjastamiseks. Sertifikaati võib võrrelda sinu allkirjanäidisega - see on avalik ja selle abil saavad kõik kontrollida, kas sinu antud allkiri on tõepoolest ehtne. Sertifikaadis on kirjas ka sinu isikuandmed, sealhulgas nimi ja isikukood. Sertifikaadi abil saab kontrollida digitaalallkirju - kui sertifikaat ja allkiri omavahel matemaatiliselt klapiavad, võib olla kindel, et allkirja on andnud see isik, kes on sertifikaadis kirjas.

Kehtivuskinnitused

Vastavalt "Digitaalallkirja seadusele" on kehtetu või peatatud sertifikaadiga antud allkirjad kehtetud.

Peale allkirja andmist tuleb kontrollida, kas allkirja andja sertifikaat kehtib või ei ehk kas tal on õigus sel hetkel digitaalallkirja anda. Selleks võtab allkirja andmiseks kasutatud programm automaatselt ühendust Sertifitseerimiskeskuse serveriga ning kontrollib, kas sertifikaat on kehtiv - kui on, väljastab Sertifitseerimiskeskuse server talle spetsiaalse tõendi, mis lisatakse allkirjale.

Põhiline digiallkirjastamise meelespea

- Digiallkirjastamiseks on vaja ID-kaarti, Internetiühendusega arvutit, kaardilugejat ja digiallkirjastamiseks mõeldud ID-kaardi PIN-koodi
- Digiallkirju saab anda sertifikaadi kehtimise ajal
- Digiallkirja kontrollimisel vaata alati, kas allkirjaga on seotud kehtivuskinnitus

Olemaoleva baasrakenduse (AutomatWeb) tutvustus

AutomatWeb (AW) ja tema võimalused

AutomatWeb on Struktuur Meedia väljatöötatud üle interneti kasutatav tarkvaraplatvorm veebilahenduste jaoks. Kõik AW rakendused toetuvad samale baasosale. AW'd võib kujutleda puuna, mille võra ehk rakendusi toetab kindel tüvi ehk platvorm. AW on multifunktsionaalne veebivara: täna võib AW ühtses tarkvarakeskkonnas kasutada paarikümmend erinevat töölauda. Uute võimaluste hulk kasvab kiiresti tänu süsteemi paindlikkusele.

Hetkel kuuluvad AW tooteperekonda järgmised suuremad osad:

- Kliendihaldus CRM
- Broneeringute haldamise töölaud
- Tootmise planeerija
- Sisuhalduslahendused CMS
- E-kaubandus
- Otsimootorid
- Broneerimissüsteemid
- Statistiliste aruannete veebi-põhine esitamine
- Vastuvõtu infosüsteem koolidele
- Jne..

Patendiamet ja tema vajadused

Patendiametist

Eesti Patendiamet (ka Patendiamet) on Eesti Majandus- ja Kommunikatsiooniministeeriumi valitsemisalas tegutsev valitsusasutus tööstusomandi kaitseks ja sellest teavitamiseks. Tõstataks siinkohal üles Patendiameti ühe põhilisestest ülesannetest, mis on otseselt seotud antud töö ja valmiva rakenduse osaga.

“Tööstusomandi esemetele (leiutised, kaubamärgid, tööstusdisainilahendused, mikrolülituse topoloogiad, geograafilised tähised) õiguskaitse andmine riigi nimel ja avalikkuse teavitamine õiguskaitse andmisest ning selle kehtivusest ametlike väljaannete kaudu, mida levitab ka Eesti Patendiraamatukogu”

Valmiva rakendusosaga on siis täpsemalt tegemist kaubamärkide õiguskaaise puhul, täpsemalt nende registreerimisel ja haldamisel.

Vajadused seoses AW'ga

Vajadus lisafunktsionaaluse järele AW platvormis tekkis olukorras kus Patendiamet soovis kaubamärkide registreerimise viia üle internetipõhiseks. Kuna aga vastavad toimingud nõuavad

isiku korrektset ja turvalist tuvastamist ning esitatud avalduse allkirjastamist, oli vastava rakenduse arenduseks vaja kasutada selliseid võimalusi pakkuvat ID-kaarti ning tema isikutuvastus ja digiallkirjastmise teenuseid.

Lõppeesmärk

Töövoog

- ID-kaardi kasutusvõimaluste ja tausta uurimine
- Digiallkirjastamise kasutusvõimaluste uurimine
- Rakenduse serveri nõuete uurimine
- Serveri seadistamine
- Rakenduse realiseerimine

Kasutajalood

KL1 Kaubamärgi registreerimine

1. Kasutaja läheb patendiameti kaubamärgitaotluste elektroonilise esitamise portaali (<http://online.epa.ee>)
2. Kasutaja sisestab oma ID-kaardi kaardilugejasse
3. Kasutaja logib portaali sisse kinnitades oma isikut ID-kaardi ja sellele vastava PIN1 koodiga
4. Kasutaja valib uue taotluse esitamise vormi
5. Kasutaja alustab vormi täitmist
 - 5.1. Kasutaja täidab uue taotluse esitamise vormi täielikult. Kasutajalugu jätkub punktis 6.
 - 5.2. Kasutaja täidab vormi osaliselt ning lahkub enne taotluse allkirjastamist/esitamist portaalist
6. Kasutaja kinnitab digiallkirjaga täidetud vormi õigusust
7. Kasutaja esitab taotluse

KL2 Kinnitatud / esitatud kaubamärgi vaatamine

1. Kasutaja läheb patendiameti kaubamärgitaotluste elektroonilise esitamise portaali (<http://online.epa.ee>)
2. Kasutaja sisestab oma ID-kaardi kaardilugejasse
3. Kasutaja logib portaali sisse kinnitades oma isikut ID-kaardi ja sellele vastava PIN1 koodiga
4. Kasutaja valib saadetud taotluste lehekülje
5. Kasutajale kuvatakse tema eelnevalt kinnitatud ning saadetud taotlusi
6. Kasutaja valib soovitud taotluse
7. Kasutajale kuvatakse valitud taotluse andmed

KL3 Osaliselt täidetud või allkirjastamata/esitamata taotluste lõpetamine ja saatmine

1. Kasutaja läheb patendiameti kaubamärgitaotluste elektroonilise esitamise portaali (<http://online.epa.ee>)
2. Kasutaja sisestab oma ID-kaardi kaardilugejasse
3. Kasutaja logib portaali sisse kinnitades oma isikut ID-kaardi ja sellele vastava PIN1 koodiga
4. Kasutaja valib allkirjastamata/esitamata taotluste lehekülje
5. Kasutajale näidatakse esitamata taotlusi
6. Kasutaja valib soovitud taotluse

7. Kasutaja jätkab taotluse vormi tämist vastavalt KL1'le alatest punktist 5.

KL4 Taotluste patendiameti poolne kinnitamine

1. Patendiameti volinik läheb logib ennast sisse AW'i keskkonda kastades selleks kas traditsioonilist kasutaja/parool kombinatsiooni või ID-kaarti.
2. Volinik avab kaubamärgitaotluste halduse rakenduse
3. Volinik valib taotluste vaate
4. Volinik valib kinnitamata taotluste hulgast taotluse
5. Volinik kontrollib esitatud andmete õigsust ning sobivust vastava seadusandlustikuga
6. Volinik märgib taotluse kinnitatuks
7. Kasutuslugu jätkub punktis 4.

Eeluurimine

Senised ID-kaarti ja digiallkirjastamist kasutavad veebirakendused

Antud nimekiri on pidevalt muutuv ning selle ajakohane täielik väljatoomine ei oleks otstarbekas. Loetlen siiani tähtsamat rolli omavad ja riiklikud veebipõhised teenused mis kasutavad nõ ID-lähenemist.

- Praktiliselt kõikide pankade internetipangad (Swedbank, SEB, Krediidipank, Sampo pank, Nordea, MARFIN pank, BIG, Tallinna äripank, Parex pank)
- Riiklikult kordineeritud avalikud teenused (eKool, ID-pilet, DigiDoc portaal, eesti.ee, Hariduse infosüsteem, iPatsient, Pensionikeskus)
- Riigiasutused ja nende teenused (Maksu- ja tolliameti e-maksuamet, Vabariigi Valimiskomisjoni e-valimised, ARK'i Paberivaba ARK, Registrate ja Infosüsteemide Keskuse Äriregistri teabesüsteem, - Äriregistri ettevõtjaportaali ning Laevakinnistusraamat, Rahandusministeeriumi Riigihangete register ning E-riigikassa, Patendiameti Kaubamärgi taotlemise portaali, Keskkonnaministeeriumi Kalanduse Infosüsteem ning Põllunduse Registrate ja Informatsiooni Ameti e-PRIA).
- Suuremate ettevõtete nagu näiteks AS Sertifitseerimiskeskus, Elion, EMT, Tele2, Eesti Energia, Eesti Gaas, Tallinna Vesi jne e- ja iseteenindusbürood.

Sertifitseerimiskeskus (SK)

- Alates asutamisest 2001. aastal on SK tegelenud infotehnoloogiliste lahenduste pakkumisega, sealhulgas nii tarkvara kui riistvara tarnimise, projektijuhtimise koordineerimise, süsteemide paigaldamise, kasutajate koolitamise kui ka süsteemide hooldamisega.
- SK omanikud on võrdsetes osades Swedbank, SEB, Elion Ettevõtted ja EMT.
- SK korraldab Eesti ID-kaartidele sertifikaatide väljastamist, nende haldust ning uuendamist. Sertifikaadid on vajalikud ID-kaardi elektrooniliseks kasutamiseks, eeskätt isikutuvastamiseks (nt netipanka sisselogimine), digiallkirja andmiseks (nt lepingute, taotluste allkirjastamiseks) ning dokumentide krüpteerimiseks. SK on alates 2002. aastast väljastanud ca 900 000 sertifikaadipaari (igal ID-kaardil on üks paar sertifikaate).
- On loonud ID-kaardi kasutamiseks vajalikku baastarkvara, sh välja töötanud DigiDoc tarkvara, mis võimaldab anda digitaalallkirju, kontrollida digitaalallkirjade kehtivust ning salastada andmeid. SK tarkvara vastab rahvusvahelistele standarditele.
- Pakub ajatempli teenust ehk nt annab sõltumatu kolmanda osapoolena kella ja kuupäeva konkreetsele digiallkirjale.
- On loonud ja opereerib maailmas ainulaadset ID-pileti süsteemi. Iga päev kasutab ID-piletit üle 100 000 inimese, kokku on reisijad alates 2004. aasta algusest ostnud ligi 2 miljonit ID-piletit.
- Omab ja haldab ülalkirjeldatud teenuste pakkumiseks vajalikku riist- ja tarkvara.

SK pakutavad abimaterjalid digiallkirja kasutavate rakenduste loomiseks

DigiDoc on SK loodud terviklik arhitektuur digitaalallkirjade loomiseks, käsitlemiseks, edastamiseks ja kontrolliks. Lisaks allkirjastamise funktsionaalsusele toetab DigiDoc failide salastamist ehk krüpteerimist.

DigiDoc'i saab lihtsalt integreerida olemasolevatesse ja loodavatesse rakendustesse. DigiDoc'i suuremad osad on järgnevad: klientprogramm, portaal (<http://digidoc.sk.ee>), veebiteenus, tarkvarateegid ning failivormingud. Täpsemalt uurin ja kasutan edaspidi veebiteenuseid, kuna need on vajalikud loodavas veebirakenduses digiallkirjastamise kasutuselevõtuks.

Veebiteenus ehk DigiDocService

Veebiteenus on mõeldud DigiDoc integreerimiseks veebipõhiste infosüsteemidega. Veebiteenuse abil on olemasolevasse süsteemi lihtsalt integreeritav allkirjastamise ja DigiDoc failide kontrollimise funktsionaalsus. Veebiteenuse kasutamise lihtsustamiseks on loodud erinevatele platvormidele teenuse kasutamist lihtsustavad klienditeegid ja näidisrakendused.

DigiDocService on SOAP põhine veebiteenus võimaldamaks võimalikult lihtsalt digitaalallkirjastamise ja allkirjade verifitseerimise ja Mobiil-ID funktsionaalsust siduda teiste infosüsteemidega.

Teenust on võimalik kasutada erinevatelt arenduskeskkondadest/platvormidelt, millel on SOAP 1.0 RPC-encoded tugi. Teenuse poolt pakutav funktsionaalsus:

- Isikutuvastus Mobiil-ID'ga
- DigiDoc failide moodustamine
- Digitaalallkirjastamine Mobiil-ID'ga
- Digitaalallkirjastamine ID-kaardi (ja muu kiipkaardiga)
- Digitaalallkirjastatud failide (DigiDoc) sisu ja allkirjade kehtivuse kontroll.

Teenust on võimalik kasutada otseselt DigiDocService protokoll järgides (http://www.sk.ee/files/DigiDocService_spec_est.pdf). Teenusele ligipääsu võimaldatakse IP aadressi põhisel, teenuse kasutamiseks tuleb teenuse kasutajal sõlmida leping AS Sertifitseerimiskeskusega. Teenuse kasutamise maksumus teenuse kaudu tehtud autentimiste ja allkirjastamiste arvust (võetud kehtivuskinnitustest) ja ühelt rakenduselt tulevatest üheaegsete päringute arvust. Teenuse kasutamise lihtsustamiseks on loodud õhukesed klienditeegid PHP ja Java jaoks. Digiallkirjastamise võimaluste loomiseks AW platvormile kasutasin PHP klienditeeke, vajadusel neid veidi muutes ja AW'ga sobitades.

Realisatsioon

Rakenduse jaoks valitud serveri tarkvara valimine ja seadmistamine

Serveri tarkvara sai esmajoonel valitud lähtudes AW tavaelistusi, ehk millel AW platvormi siiani edukalt kõige rohkem jooksatud on. Selleks sai operatsioonisüsteemil Linux jooksvad veebiserver Apache ja MySQL andmebaasimootor. Apache'I veebiserveri valiku õigsus sai kinnitust ka veel lisaks AW'ga sobivusele ID-kaardiga autentimise tarbeks vajaliku konfiguratsiooni lihtsusega ning vajalike näpunäidete saadavusega.

Kuna AW funktsionaalne pool on seni täies mahus realiseeritud PHP programmeerimiskeeles, sai ka digiallkirjastamise implementeerimiseks kasutatud SK poolt ette valmistatud PHP klienditeeki. Antud teegi kasutamine nõuab veebiserverilt :

- PHP versiooni alates 4.3.0 kuid väiksem kui 5 (uuendatud PEAR'I pakettidega ka võimalik 5's versioon).
- Installeeritud PHP OpenSSL moodul
- Installeeritud PHP CURL moodul

Lisaks on vajalikud ka PHP Pear'i paketid SOAP ja XML Serializer, kuid need on kaasas ka PHP klienditeegiga, ning soovitatav on kasutada just neid vastavaid kaasas olevaid versioone.

Digiallkirjastamise jaoks eraldi spetsiifilisi konfiguratsioone veebiserverile vaja ei ole teha. Teatud direktiivid tuleb määrata ainult ID-kaardiga autentimiseks, ning sellest tulenevalt neid siin kirjeldama ka ei hakka.

Klienditeegi sisu ja selle kasutamine

PHP konfiguratsiooni ja koodifailid:

- `conf.php` – konfiguratsioonifail
- `wSDL.class.php` – põhimeetodid kasutamaks digiallkirjastamise funktsionaalsust. Saadakse vajadusel päringu tulemusena ka Sertifitseerimiskeskuse vastavalt teenuselt. Protsessi kiirendamiseks on mõttekas seda faili lokaalselt rakendusega ühes serveris hoida ja sealt kasutada, ning uuendada läbi teenuse ainult `wSDL` faili sisu muutumisel (sellest teavitatakse avalikult teenuse pakkuja poolt).
- `DigiDoc.class.php` – õhuke vaheliides `wSDL.class.php` ümber, mis lihtsustab, kuid samas natuke piirab digiallkirjastamise realiseerimist. Pakub põhilist allkirjastamise funktsionaalsust läbi lihtsustatud liidese.

Veateadete html vormid

- `error.html` – kuvatakse vea esinemisel allkirjastamisel

Erinevate brauserite jaoks mõeldud erinevad komponendid ja nende lisad, mis suhtlevad läbi brauseri otse kasutaja ID-kaardiga, lugedes sealt vajalikke andmeid.

Internet Exploreri tarbeks vajaminev ActiveX komponent:

- `EIDCard.cab` - Internet Explorer

Mozilla, Firefoxi ning Netscape'i tarbeks vajaminevad Java komponendid

- `kasutajatelesteid-pkcs11.dll`
- `iaikPkcs11Wrapper.jar`
- `iaikPkcs11Wrapper_sig.jar`
- `libesteid-pkcs11.so`
- `libpkcs11wrapper.so`
- `PKCS11Wrapper.dll`
- `SignApplet_sig.jar`

Lisaks veel kataloog "inc" vajalike PHP Pear'i pakettidega.

Kaasoleva näiterakenduse tööle seadmine

Lihtsaima näidisrakenduse saab näidisklienditeegi abil tööle panna üsnagi kergelt, lihtsalt liigutades kõigest klienditeegis mainitud failid mõnda veebiserveri poolt näidatavasse kataloogi ning märkides "data" kataloogile piisavalt õigusi, et veebiserver saaks sinna faile tekitada ja neid kustutada. Kui kõik läks korralikult peaks kasutajale brauserist vastu vaatama sarnane leht:



Antud pildil on siis tegemist PHP klienditeegile rajatud minimaalse funktsionaalse näiterakendusega, millega saab allkirjastada faile, vaadata allkirjastatud faile ning luua uusi tühju DigiDoc konteinereid kuhu saab lisada nii allkirjastatavaid faile kui ka allkirju.

Protsess AW'ga integreerimiseks

Kui üldise digiallkirjastamise funktsionaalsuse ja näiterakenduse töölesamine on klienditeekide loomisega veebiarendaja jaoks tehtud mugavaks ja kiireks, siis põhimure jääb arendaja jaoks see kuidas antud lahendus efektiivselt ja võimalikult valutult liita oma baasrakendusega. Eelnevate kogemuste puudumisega AW platvormile analoogse süsteemi implementeerimisel ning teatavate ajaliste kitsenduste tõttu oli võimalik lähtuda ainult konkreetse projekti vajadusi silmas pidades. Samas, tuleviku huvides, oli ka äärmiselt oluline eelnevalt vähemalt pinnapealselt mõelda läbi protsess selle teostamiseks ning igal võimalikult juhul erinevaid juhtumeid vastavast projekti skoobist välja üldistades.

AW koodipool

AW poolele sai lisaks loodud uus DigiDoc klass, asendamaks klienditeegi poolt kaasa pandud liidesklassi, saavutamaks AW jaoks võimalikult suurt paindlikkust. Omakorda lihtsustamaks AW sisest digiallkirjastamise paremat ja mugavamalt ära kasutamist.

Patendiameti rakenduse tarbeks sai loodud võimalus allkirjastada AW's "Patent" tüüpi objekte. Rakenduse sees tähendas see seda, et patendi objektist loodi XML väljund koos kõigi tema omaduste ja nende väärtustega. Sellest sai allkirjastatav dokument, mis omakorda peale allkirjastamist seoti DigiDoc objektiga. Kõik operatsioonid seoses allkirjastamisega toimuvad läbi DigiDoc objekti, nendeks on näiteks DigiDoc klassil meetodid:

- `is_signed()` - kontrollib kas on allkirjastatud
- `add_file()` - lisab konteinerisse faili/objekti, mida allkirjastada
- `remove_file()` - eemaldab konteinerist faili/objekti
- `get_file()` - tagastab soovitud faili/objekti
- `get_ddoc()` - tagastab kogu DigiDoc faili
- `set_ddoc()` - määrab uue DigiDoc faili sisu
- `remove_signature()` - eemaldab allkirja
- `sign()` - lisab uue allkirja (alustab allkirjastamise protsessi)
- `get_signatures()` - tagastab info allkirja kohta

Lisaks on veel hulk tehnilisemaid abimeetodeid ja –klasse kogu protsessi haldamiseks.

AW kasutajaliides

Rakenduse kasutaja jaoks on DigiDoc'I objekt sisuliselt ära peidetud, ehk kasutaja antud juhul käib ümber Patendi objektiga, seda allkirjastades. Samas võimaldab süsteem allkirjastada sama loogika alusel ükskõik millist AW's olemasolevat objekti (olgu see sisuhalduse dokument või ressursiplaneeri automaatselt genereeritud tellimuse arve).

Alternatiivne lahendus

Proovieesmärgil sai realiseeritud ka digiallkirjastamise funktsionaalsus teises programmeerimiskeeles, teisel platvormil. Valitud sai DigiDoc COM teek, mis on Digidoc C-teegil baseeruv lisakiht, mis võimaldab lihtsalt Windowsi platvormi rakendustesse DigiDoc funktsionaalsust integreerida. DigiDoc COM teeki kasutades on võimalik ise allkirjastamise, digitaalallkirjade verifitseerimise ja failide krüpteerimise funktsionaalsust realiseerida näiteks Visual Basicus (visual basicus sai realiseeritud ka kõneall olev proovirakendus). Sama teeki kasutab ühtlasi ka DigiDoc Client ise.

Huviatava lisana võib mainida et lisaks Eesti ID-kaardile töötab COM teek ka teiste kiipkaartidega, näiteks SK asutuse kaardiga, EID kaardiga ja Belgia ID-kaardiga.

Loodud rakenduse töötamise eelduseks on

- 2 faili olemasolu (allkiri.exe, ojsp_token_30_10_2008.p12d). Antud failid peavad asuma arvutis ühes ja samas kaustas.
- DigiDoc klientprogrammi olemasolu arvutis. Sellega paigaldatakse ja registreeritakse arvutisse ka vastavad COM teegid. Täpsed juhised DigiDoc kliendi paigaldamiseks leiab aadressilt <http://www.sk.ee/link.php/1821>

DigiDoc COM teegi põhjale vastava rakenduse arendamine on PHP'ga võrreldes natuke rohkem aega ning vaeva nõudev, seda just puuduliku dokumentatsiooni ning robustsema kasutajaliidese tõttu. Antud nähtus tuleneb ilmselgelt aga suuresti sellest, et tänapäeval on tendents kõikvõimalikel rakendustel veebipõhiseks kujuneda. Sellest tulenevalt on ka arengusuunad ja arendusressursid suunatud veebi poolele. Just puudulik ja osaliselt ebatäpne dokumentatsioon oli see mis viivitas allkirjastamise põhifunktsionaalsuse implemteerimist käesolevasse lihtsasse ning väikesesse utiliiti.

Põhiliselt aega viitnud ja segadust tekitanud probleem seisnes failis ojsp_token_30_10_2008.p12d, mis on rakenduse töötamiseks vajalik. Antud fail sisaldab õigel kujul allkirjastamiseks vajalikke sertifitseerimiskeskuse sertifikaate. Kuigi vastav fail on kaasas ka DigiDoc Client'iga, ei ole kuskil dokumentatsioonis eraldi märgitud et just seda faili on vaja kasutada ning kuidas seda kasutada.

Ülevaade koodist

<i>Dim i As Integer</i>	Abimuutuja silmuses
<i>Dim dataFile As New DIGIDOCLIBCOMLib.ComDataFile</i>	Muutuja allkirjastatava faili hoidmiseks
<i>Dim dummyVariant As Variant</i>	Baitide vektor räsi jaoks
<i>Dim signedDoc As New DIGIDOCLIBCOMLib.ComSignedDoc</i>	Muutuja digidoc konteineri jaoks
<i>Dim signatureInfo As New DIGIDOCLIBCOMLib.ComSignatureInfo</i>	Muutuja allkirja hoidmiseks

DigiDoc konteineri initsialiseerimine

Call signedDoc.Initialize(COM_DIGIDOC_XML_1_1_NAME, COM_DIGIDOC_XML_1_1_VER)

Allirjastatava Faili lisamine digidoc konteinerisse

<i>signedDoc.createDataFile _</i> <i> "C:\allkirjastatava\faili\asukoht.txt", _</i> <i> COM_CONTENT_EMBEDDED_BASE64, _</i> <i> "text/plain", _</i> <i> 0, _</i>	<i>Allkirjastatava faili asukoht</i> <i>Allkirjastatava faili MIME tüüp</i> Faili suurus baitides. Väärtus 0 tähendab et hiljem tuleb välja kutsuda meetod <i>calculateDataFileSizeAndDigest</i>
<i> dummyVariant, _</i>	Räsi baitide vektor. Kui seda eelnevalt ei täideta, tuleb hiljem kutsuda välja meetod <i>calculateDataFileSizeAndDigest</i>
<i> 0, _</i>	Räsi pikkus. Väärtus 0 tähendab et väärtus valitakse meetodi poolt.
<i> COM_DIGEST_SHA1_NAME, _</i> <i> COM_CHARSET_ISO_8859_1, _</i> <i> dataFile</i>	Räsi tüüp Tekstiandmete formaat Andmefaili muutuja

Andmefaili räsi ja suuruse välja arvutamine

signedDoc.calculateDataFileSizeAndDigest _
dataFile.szld, _
"C:\allkirjastatava\faili\asukoht.txt", _
COM_DIGEST_SHA1

Allkirja loomine

signedDoc.createSignatureInfo signatureInfo
signedDoc.addAllDocInfos signatureInfo

Järgnev rida kutsub realselt välja koodi, mis võtab ühendust kaardipesas oleva ID-kaardiga ning peale õige PIN2 koodi sisestamist arvutab välja reaalse allkirja.

signatureInfo.calculateSignatureWithCSPEstID signedDoc, 1

Antud allkirjale sertifitseerimiskeskuse serverist kehtivuskinnituse hankimine. Selleks käiakse tsükliga üle kõik DigiDoc konteineris olevad allkirjad, ning kinnitatakse nende kehtivust.


```
For i = 0 To (signedDoc.nSignatures - 1)
    signedDoc.getSignature i, signatureInfo
```

Küsime konteinerist allkirja ning talletame eraldi muutujasse

```
signedDoc.getConfirmation _
```

Küsime allkirja kehtivust sertifitseerimisekeskuse teenuse käest
Allkirja hoidev muutuja
Protsessiks vajalikke sertifikaate hoidev fail
Sertifikaatide faili parool
Kehtivuskinnituse teenuse aadress
Proxy aadress (võib jääda tühjaks)
Proxy port (võib jääda tühjaks)

```
signatureInfo, _
"ocsp_token_30_10_2008.p12d", _
"" , _
"http://ocsp.sk.ee", _
"" , _
""
```

```
Next i
```

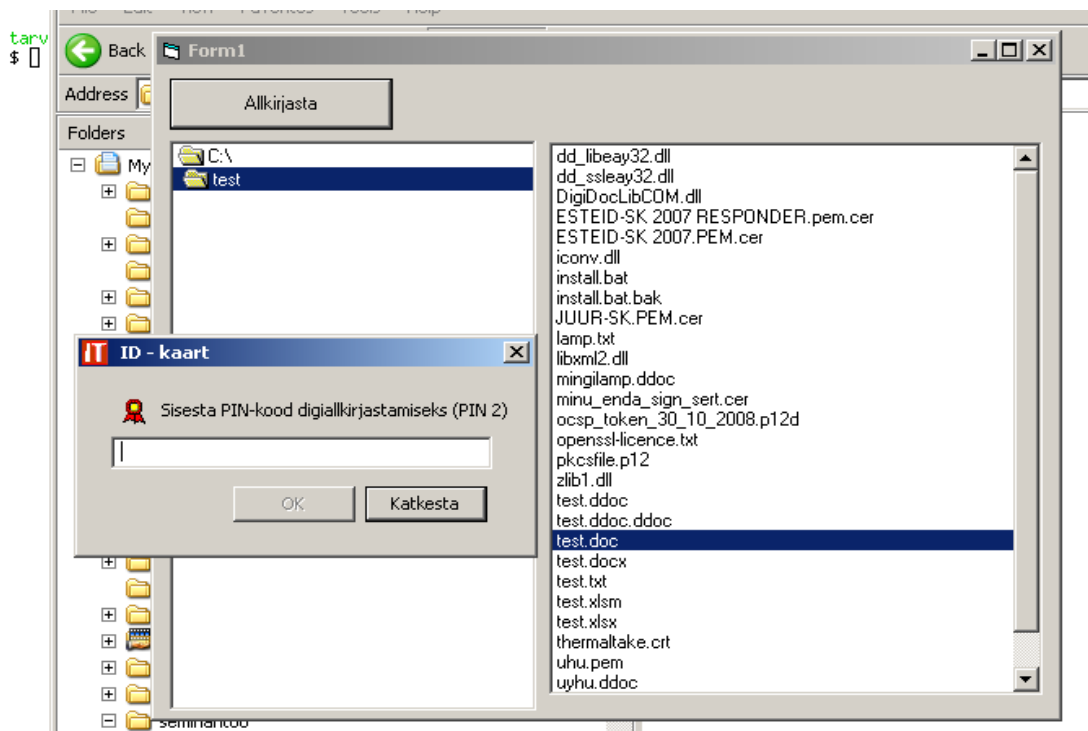
Andmefaili ja allkirjadega varustatud DigiDoc konteineri salvestamine arvutisse

```
signedDoc.createSignedDoc "C:\allkirjastatava\faili\asukoht.txt.ddoc", ""
```

Vastava allkirjastava koodijupi saab siis igaüks vastavalt vajadusele panna just endale sobiva kasutajaliidese külge. Olgu see “kellade ja viledega” varustatud ilus ja suur aplikatsioon, mis võimaldab teatud andmeid allkirjastada, või väike utiliit mis käimapanemisel allkirjastab kõik teatud kataloogis olevad failid. Kasutusvõimalusi piirab ainult tarkvaraarendaja või tellija kujutlusvõime.

Kasutusjuhend

Programmi kasutajaliides omab kahte põhilist paani, vasakul on kataloogipuu, ning paremal kataloogipuust valitud kataloogis asuvate failide nimekiri. Klõpsates parempoolsel failil asuval failil ning seejärel nupule allkirjasta, alustatakse allkirjastamise protsessi. Sama tulemini jõuab ka, tehes faili peal topeltklõps. Seejärel küsitakse kasutajalt ID-kaardi PIN2 koodi (eeldusel et ei tekkinud tõrkeid programmi töös –COM teegi või sertifikaatide faili puudumise näol). Järgmisena allkirjastatakse ning vastutatakse kehtivuskinnitusega uus, loodud DigiDoc konteiner mis salvestakse valitud failiga ühte kausta, lisades failinimele lõppu “.ddoc”. Saadav fail on korrektselt digiallkirjastatud ning omab juriidilist õigust.



Ekraanikuvad valminud veebirakendusest

Kaubamärgitaotluse töölaud

The screenshot shows the AutomatWeb.com interface for managing trademark applications. The top navigation bar includes the site logo, user information (Eesti, Seaded, Logi välja), and search options (Lisa kiiresti, Järgehoidja, Ajalugu, Otsi). The main menu has tabs for Üldine, Taotlused, Eksport, Volinikud, and Seostehaldur. The left sidebar contains a 'Taotluste puu' (Applications tree) with folders for Kinnitatud (Kaubamärk, Patent, Kasulik mudel, Tööstusdisain, EP patent, Arhiiv) and Kinnitamata. The main area displays a table of trademark applications with columns: Vali, Taotluse tüüp, Märgi tüüp, Taotluse number, Esitaja nimi, Esitaja kontaktandmed, Voliniku nimi, Esitamise kuupäev, Allkirjad, and Kinnita. Two rows are visible, both for Trademark applications with numbers 70749 and 70750. Below the table is an 'Objektide otsing' (Object search) form with fields for Esitaja nimi, Voliniku nimi, Alates (date), and Kuni (date), and an 'Otsi' button. The footer contains copyright information for Struktuur Meedia and AutomatWeb.

DigiDoc objekti allkirjade vaade, uue allkirja lisamisega

The screenshot shows the AutomatWeb.com interface for the DigiDoc object signature view. The top navigation bar includes the site logo, user information (Eesti, Seaded, Logi välja), and search options (Otsi). The main menu has tabs for Üldine, Failid, Allkirjad, and Seostehaldur. The main area displays a table with columns: Vali, Eesnimi, Perekonnanimi, Isikukood, and Allkirjad. A Mozilla Firefox dialog box is open over the table, titled 'Võti: "ARIKAS,TARVO,38505050028"'. The dialog box contains input fields for Linn, Maakond, Postiindeks, Riik, and Roll, and buttons for 'Allkirjasta' and 'Katkesta'. The footer contains copyright information for Struktuur Meedia and AutomatWeb.

Patendi objekti vaade



Struktuur Meedia | Trademark | Kinnitamata taotlus nr [37913] Eesti Seaded Logi välja

Asukoht: Tagasi

[Üldine](#) [Prioriteet](#) [Riigilõiv](#) [Kaubamärk](#) [Kaupade ja teenuste loetelu](#) [Seostehaldur](#) [Lisa kiiresti](#) [Järjehoidja](#) [Ajalugu](#) [Otsi](#)

[Tagasiside](#) [Kasutajatugi](#) [Abi](#)



Nimi

Taotleja  



Allkirja staatus [Lisa allkiri \(DigiDoc konteinerisse\)](#)

Allkirjastajad

Allkirjastaja amet

Volinik  

Volikiri

Volitatud isik  

Volitatud isikute isikukoodid

Lisainfo

Kinnitatud

Taotluse number

AutomatWeb® on Struktuur Meedia registreeritud kaubamärk. Kõik õigused kaitstud. © 1999-2008. Palun külasta meie kodulehekülgi: [Struktuur Meedia](#), [AutomatWeb](#).

Lõppsõna

Digiallkirjastamine tundub hakkavat tasapisi muutuma sama tavapäraseks kui pangakaardiga maksmine. Selleni on veel küll veidi aega, kuid suund sinnapoole on võetud. Ja seda suuresti tänu senisele ID-kaardi ja digiallkirjastamise infrastruktuuri arendusele. Olukord, kus iga üsnagi kogenumatu asjaarmastaja saab tunni-paariga kasvõi enda koduarvutis tööle panna digiallkirjastamise näiterakenduse, või kui kogunud arendaja saab väga lühikese ajakuluga liita põhilise digiallkirjastamise funktsionaalsuse mingi olemasoleva rakendusega liita, on ainult kiiduväärt. Ja antud juhul ei piirdu see ka ainult veebirakendustega, analoogsed teegid on valmistatud ka muude keskkondade jaoks. Nii saab iga soovija kergelt liita digiallkirjastamise eelised vastavalt oma soovidele, olgu see vana hea tava järgi DOS'I põhine programm, Visual Basicus kirjutatud mõne Microsofti Office tooteperekonna lisana kirjutatud lisafunktsionaalsus või platvormivaba Java's realiseeritud rakendus.

Konkreetne, teemaks olnud AW lisafunktsionaalsuseks arendamisele kulus küll veidi rohkem aega, kuid arvestada tuli ligi 9 aastat pidev-arenduses olnud väga mahuka veebivara võimalustepagasi ja funktsionaalsusega. Arvesse tuli võtta ja läbi mõelda digiallkirjastamise kasutuselevõtmisel AW mitmete teiste lahendustega, mitte ainult uue, loodava kaubamärgi taotluse ja halduse lahendusega.

Protsessi käigus Eesti Patendiametile valminud kaubamärgi taotluse ja halduse lahendus on nüüdseks aktiivses kasutuses olnud ligi 2 aastat. Oma tõusude ja möönadega, mis on suuremalt jaolt olnud seotud ID-kaardiga autentimise tarbeks vajalike serveritarkvara konfiguratsioonidega ning füüsilise serveri vahetamisega. Valminud tarkvara kliendiliidesega saab igaüks tutvuda vabalt Patendiameti Kaubamärgitaotluste elektroonilise esitamise portaalis aadressil <http://online.epa.ee>. Soovi korral näha lähemalt rakenduse administreerimisosa (AutomatWeb'i), kontakteeruda eelnevalt töö autoriga.

Tööga on lisaks kaasas ka PHP klienditeek, mida iga kasutaja saab kergelt üles seada omale sobivas arvutis. Selleks on samas teegis kaasas ka õpetussõnad, kuid toon eraldi siinkohal välja põhilised neist, mille abil sai ka edukalt klienditeeki proovitud:

- Installeeritud veebiserver Apache (võib olla nii versioon 1.x kui 2)
- Installeeritud PHP (versiooninumbriga võrdne või suurem kui 4.3.0 ja väiksem kui 5)
- Installeeritud PHP OpenSSL moodul
- Installeeritud PHP CURL moodul
- DigiDoc'i klienditeegi sisu kopeeritud Apache poolt näidatavasse kataloogi
- Kopeeritud DigiDoc'I klienditeegi kataloogis oleva "data" kataloogil peavad olema nii lugemis kui kirjutamisõigused veebiserverile.

NB! Taoliselt üles seatud näiterakenduse päringud sooritatakse kõik Sertifitseerimiskeskuse test-serverile, mis tähendab seda et sellega antud allkirjad ei oma juriidilist õigust.

Näidisenä sai üles seatud ka kõneall olev PHP klienditeegi näiterakendus. Mainima peab küll fakti et tegu on autori personaalses arendusserveris asuva rakendusega, mis tähendab et aegajalt võib lehekülg olla mitte kättesaadav. Pikema lehe kättesaadavusprobleemi korral võtta ühendust töö autoriga.

Näiterakenduse aadress - <http://89.235.206.86/digidoc/>

Kasutatud kirjandus

- Avalike suuremate E-teenuste loetelu <http://id.ee/?id=11456>
- AutomatWeb platvormi tutvustav veebileht <http://www.automatweb.com/>
- Patendiameti ametlik veebileht <http://www.epa.ee/>
- Kaubamärgi elektroonilise esitamise portaal <http://online.epa.ee/>
- Sertifitseerimiskeskuse üldinfo <http://www.sk.ee/pages.php/02020104>
- Sertifitseerimiskeskuse poolt veebirakenduste tarbeks kasutatav DigiDoc service teek
<http://www.sk.ee/pages.php/020207010701>
- Sertifitseerimiskeskuse poolt Windowsi rakenduste tarbeks kasutatad DigiDoc COM teek
<http://www.sk.ee/pages.php/020207010803>