

Riigi Infosüsteemide Arenduskeskus

**ID- KAARDI JA DIGITAALALLKIRJA BAASTARKVARA
ARENDUS JA TUGI NING TEHNILINE TUGI**

Riigihanke tehniline kirjeldus

Sisukord

1. Eesmärk.....	3
2. Mõistete seletus.....	3
3. Üldkirjeldus.....	4
4. ID kaardi baastarkvara funktsionaalsed nõuded	7
5. Täiendavad nõuded	8

1. Eesmärk

- 1.1 Hanke eesmärgid on:
 - 1.1.1 Uuendatakse ID kaardi olemasolevat baastarkvara
 - 1.1.2 Tagatakse ametliku ID kaardi baastarkvara olemasolu vähemlevinud operatsioonisüsteemidele
 - 1.1.3 Tagatakse ametliku ID kaardi baastarkvara olemasolu vähemlevinud brauseritele
 - 1.1.4 Sertifikaatide uuendamise võimalus lisatakse ID kaardi utiliiti
 - 1.1.5 Lihtsustatakse paigaldustarkvara, et suurendada ID kaardi tarkvara kasutatavust
 - 1.1.6 ID kaardi baastarkvara lisatakse enamlevinud Linuxi distributsioonide paigaldustarkvara pakettidesse
 - 1.1.7 Kasutajatele luuakse keskne veebiportaal (domeen lepitakse kokku Hankijaga) kogu ID kaardi kasutamist puudutava info levitamiseks.
 - 1.1.8 Tagatakse ID kaardi baastarkvara täielik toimimine operatsioonisüsteemide, brauserite vms. muudatuste korral.
 - 1.1.9 Tagatakse e-posti allkirjastamise ja krüpteerimise võimalus toetatavatel platvormidel.

2. Mõistete seletus

- 2.1 **ID kaardi utiliit** – rakendus, mis võimaldab ID-kaardilt lugeda selle omaniku isikuandmeid, registreerida sertifikaate süsteemi sertifikaadihoidlasse või salvestada faili, vahetada PIN ja PUK koode, lukustunud PIN koodi lahti blokeerida ning vaadata kaardi kasutamise statistika. Samuti peab saama antud rakendusega seadistada oma ametlikku e-posti aadressi.
- 2.2 **DigiDoc klient** - DigiDoc klient on rakendus, mis võimaldab anda digitaalallkirju, kontrollida digitaalallkirjade kehtivust ning avada ja salvestada DigiDoc konteineris sisalduvaid dokumente. Lisaks digitaalallkirjastamise funktsionaalsusele võimaldab programm andmeid krüpteerida ja krüpteeritud andmeid muuta loetavale kujule, kasutades ID kaardi PIN koodi
- 2.3 **ID kaardi draiverid** - ID-kaardi kasutamiseks arendatud draiverid, mis võimaldavad ID-kaarti kasutada Internet Exploreri, DigiDoc Cliendi, Outlooki ja teiste laiatarberakendustega.
- 2.4 **ID kaardi minidraiverid** - Windows Vista platvormil on erinevate kiipkaartide toe lisamise lihtsustamiseks loodud Smart Card Base CSP (Cryptographic Service provider), edaspidi SC Base CSP. Antud CSP-d on võimalik täiendada erinevate kiipkaardi minidraiveritega, mis pakuvad baasfunktsioone kiipkaardiga suhtlemiseks. Kogu CSP baasfunktsionaalsus on realiseeritud SmartCard Base CPS-s.
- 2.5 **Installatsioonipakett** – kasutaja poolt arvutisse laetav tarkvara installatsioon, mis võimaldab paigaldada kogu ID-kaardi baastarkvara kasutaja arvutisse läbi graafilise kasutajaliidese.
- 2.6 **ID kaardi baastarkvara** – baastarkvara hõlmab ID kaardi utiliiti, DigiDoc klienti, ID kaardi draivereid ning installatsioonipaketti. ID kaardi baastarkvara on vajalik ID kaardiga seotud funktsionaalsuse kasutamiseks.
- 2.7 **Kriitiline viga** – viga, mis ohustab kasutaja ja ta arvuti turvalisust või mille tõttu ei ole võimalik ID-kaardi baastarkvara põhifunktsionaalsuse (elektrooniline isikutuvastus, digitaalallkirjastamine, dekrüpteerimine) kasutamine. Kriitiliseks loetakse antud probleeme juhul kui see puudutab enam kui 1000 kasutajat.

3. Üldkirjeldus

- 3.1 **ID kaardi baastarkvara arendus Microsoft Windows operatsioonisüsteemides:** DigiDoc kliendi uuendamine, mis sisaldab kasutaja vajaduste täpsustamist ning analüüsi ning tarkvara uuele tehnoloogiale üleviimist (hetkel on kasutusel Visual Basic 6.0).
Ühtse installatsioonipaketi koostamine, mis võimaldab installeerida kogu vajamineva tarkvara (võimalusel ka kaardilugeja draiverid) ühe tegevusena. Installatsioonipakett peab sisaldama ID kaardi utiliiti, DigiDoc klienti ning ID kaardi draivereid.
Antud pakett peab suutma tuvastada olemasolevad brauserid koos nende versioonidega (Internet Explorer ning Firefox) ning vastavalt sellele võimaldama kasutajal valida, millistele brauseritele draivereid soovitakse või teavitama kasutajat vajaliku brauseri puudumisest.
Lisaks tuleb arendada minidraiver, mis oleks kasutatav Windows Vista SP1 ja uuemate operatsioonisüsteemidega ning kasutatav PIN padita PC/SC toega kiipkaardilugejatega millele on olemas vastava operatsioonisüsteemi draiver.
- 3.2 **ODF dokumentide allkirjastamine ja krüpteerimine:** kasutajal on ID kaardiga võimalik allkirjastada ja krüpteerida dokumente ODF toega kontoritarkvara pakettides. Samuti peab olema võimalik avada allkirjastatud ja krüpteeritud dokumente. Allkirjastamine ja krüpteerimine peab olema lihtne ning intuiitselt kasutatav. Vajalikud seadistused tehakse automaatselt.
- 3.3 **ID kaardi baastarkvara tugi Microsoft Windows operatsioonisüsteemides:** ID kaardi baastarkvara uuendamine vajadusel, tagamaks ID kaardi tõrgeteta töö järgmistes MS operatsioonisüsteemides:
MS Windows 98
MS Windows 2000
MS Windows ME
MS Windows XP
MS Windows Vista
- 3.4 **ID kaardi tugi Internet Explorer 6.0 ja uuemates versioonides:** Kõigis toetatavates MS Windows operatsioonisüsteemides, kus on olemas Internet Explorer 6.0 või uuem peab olema võimalik kasutada e-teenustesse sisenemiseks, veebirakendustes digitaalse allkirja andmiseks ning Digidoc portaalis dokumentide allkirjastamiseks ID kaarti. Juhul, kui Microsoft toob turule Internet Exploreri uusi versioone või olemasolevatele versioonidele uuendusi peab peale versiooni uuendusi olema võimalik kasutada ID kaardi kogu funktsionaalsust.
- 3.5 **ID kaardi tugi Mozilla Firefox 1.5 ja uuemates versioonides:** Kõigis toetatavates operatsioonisüsteemides, kus on olemas Mozilla Firefox 1.5 või uuem peab olema võimalik kasutada e-teenustesse sisenemiseks, veebirakendustes digitaalse allkirja andmiseks ning Digidoc portaalis dokumentide allkirjastamiseks ID kaarti. Juhul, kui tuleb turule Mozilla Firefox uusi versioone või olemasolevatele versioonidele uuendusi/muudatusi peab peale versiooni uuendusi olema võimalik kasutada ID kaardi kogu funktsionaalsust.
- 3.6 **ID kaardi tugi Mozilla Thunderbird 1.5 ja uuemates versioonides:** Kõigis toetatavates operatsioonisüsteemides, kus on olemas Mozilla Thunderbird 1.5 või uuem peab olema võimalik digitaalselt allkirjastada ning krüpteerida e-kirju kasutades ID kaardi sertifikaate. ID kaardi seadistamine allkirjastamiseks ning krüpteerimiseks peab toimuma automaatselt või minimaalsete kasutajapoolsete tegevustega. Juhul, kui tuleb turule Mozilla Thunderbird uusi versioone või olemasolevatele versioonidele uuendusi/muudatusi peab peale versiooni uuendusi olema võimalik kasutada ID kaardi kogu funktsionaalsust
- 3.7 **ID kaardi baastarkvara arendus Mac OS X operatsioonisüsteemides:** - Tuleb arendada graafilise kasutajaliidesega ID kaardi utiliid, graafilise kasutajaliidesega DigiDoc klient ning ühtne installatsiooni pakett, mille abil on kasutajal võimalik paigaldada kogu ID kaardi kasutamiseks vajalik baastarkvara.
- 3.8 **ID kaardi baastarkvara tugi Mac OS operatsioonisüsteemides:** - Vaja on tagada ID kaardi baastarkvara töö järgneva 3 aasta jooksul järgmistel operatsioonisüsteemidel:
Mac OS X 10.4 (Tiger)
Mac OS X 10.5 (Leopard)
Kuna Mac OS X platvormil on Safari brauser tihedalt seotud operatsioonisüsteemiga, hõlmab käesolev nõue ka Safari uuenduste korral ID kaardi töö tagamist.
- 3.9 **ID kaardi baastarkvara arendus Linux distributsioonides:** Tuleb arendada graafilise kasutajaliidesega ID kaardi utiliid ning graafilise kasutajaliidesega DigiDoc klient.

- 3.10 **ID kaardi baastarkvara tugi Linux distributsioonides:** Vaja on tagada ID kaardi baastarkvara töö järgneva 3 aasta jooksul viiel Eestis enim levinud distributsioonil. Distributsioonide nimekiri tuleb üle vaadata vähemalt kord aastas
- 3.11 **Tugi veebikeskkonnas:** Tuleb tagada ID kaardi tarkvara paigaldamiseks ning kasutamiseks vajaliku informatsiooni kättesaadavus veebikeskkonnas(domeen lepitakse kokku Hankijaga). Kasutajatele publitseeritav informatsioon peab minimaalselt sisaldama:
- Kasutusjuhendid ID kaardi tarkvara kasutamiseks
 - Kompileerimisjuhendeid Linux platvormidele
 - Korduma kippuvad küsimused (KKK) ja vastused ID kaardi baastarkvara paigaldamise ja kasutamise kohta
 - Probleemilahendajad (troubleshooter) ID kaardi baastarkvara probleemide määramiseks ja parandamiseks
- Kogu informatsioon veebi keskkonnas peab olema ajakohane.
- 3.12 **Teise astme kasutajatugi:** tugi asutuste IT osakondadele ja ID kaardi telefonitoe pakkujatele. Tugi toimib veebipõhise probleemihalduskeskkonnana. Teise astme toele esitatavad nõuded:
- i. Kasutajatugi peab olema kättesaadav tööpäeviti 08:00 – 18:00
 - ii. Probleemid tuleb lahendada ning selle kohta tagasiside anda kahe (2) tööpäeva jooksul peale probleemist teavitamist, kui lahendus on kasutajatoe pädevuses. Juhul, kui probleemi lahendamine eeldab tarkvara arendust, tuleb probleem suunata arendajatele ning edastada eeldatav lahenduse või tagasiside aeg probleemist teavitajale. Kriitilised vead tuleb parandada ning parandatud versioon avalikustada 5 tööpäeva jooksul.
 - iii. Probleemidest teavitamine (läbi probleemihaldus keskkonna) peab olema võimalik ööpäeva ringselt
 - iv. Kolmandatele osapooltele edastatud probleemi monitooringu kohustus on kasutajatoel
 - v. Probleem lõpetatakse ainult ja alati kliendipoolse positiivse tagasisidega
 - vi. Kasutajatoe kohustus on ennetada probleeme nendest teavitamisega ja protsesside korraldamisega. Väljaspool probleemide lahendamist on see kasutajatoe töö põhisisu.
 - vii. Pakkujal peab olema valmisolek pakkuda II taseme kasutajatuge arvestusega, et ID-kaardi elektrooniliste kasutajate arv kasvab aastaks 2009 kuni 400 000 kasutajani, tagades vastava hulga toeinimeste olemasolu
 - viii. ID-kaardi tehnilise toe pakkumisega on hõivatud vähemalt kaks inimest alates lepingu sõlmimisest
- 3.13 **.deb installatsiooni pakett:** deb pakihaldusega Linux distributsioonidele valmistatakse ID kaardi baastarkvara pakett, mida on võimalik lisada uutesse distributsioonidesse ning kasutajal on võimalik ID kaardi tarkvara installeerida süsteemselt. Juhul kui distributsioonides puuduvad vajalikud teigid, tuleb need paigaldada koos ID kaardi tarkvaraga
- 3.14 **.rpm installatsioonipakett:** rpm pakihaldusega Linux distributsioonidele valmistatakse ID kaardi baastarkvara pakett, mida on võimalik lisada uutesse distributsioonidesse ning kasutajal on võimalik ID kaardi tarkvara installeerida süsteemselt. Juhul kui distributsioonides puuduvad vajalikud teigid, tuleb need paigaldada koos ID kaardi tarkvaraga.
- 3.15 **ID kaardi baastarkvara tugi:** Baastarkvara täienduste avaldamine peab toimuma perioodiliselt vähemalt 2 korda aastas (sisaldavad viimase 6 kuu jooksul tuvastatud mittekriitiliste probleemide lahendusi). Kriitiliste vigade paranduste avaldamine nii kiiresti kui võimalik, kuid mitte hiljem kui 5 tööpäeva jooksul. Kõigil toetatavatel platvormidel hõlmad baastarkvara tugi tarkvara uuendusi vastavalt:
- a) tarkvaras tuvastatud vigadele
 - b) kasutajate ettepanekutele
 - c) operatsioonisüsteemide muudatustele
 - d) brauserite muudatustele
 - e) ID-kaardi muudatustele (kasutava kiibi platvorm, krüptoalgoritmid)
 - f) kiipkaardilugejate muudatustele
 - g) sertifitseerimisteenuse osutaja teenussertifikaatide või muude teenuse parameetrite muudatustele
 - h) Euroopa standardite ja soovitude muutmisele
 - i) seadusandluse muutumisele

- 3.16 **Baastarkvara repositoorium:** seadistatakse repositoorium ID kaardi baastarkvarale ning tarkvara lähtekoodile. Repositooriumis hoitavad failid peavad olema kätte saadavad läbi avaliku veebikeskkonna.
- 3.17 **DigiDoc portaali haldus:** Tuleb tagada DigiDoc portaali töö ID kaardi draiverite, sertifikaatide, brauserite vms uuenduste korral. DigiDoc portaalil peab kasutajal olema võimalik digitaalselt allkirjastada üles laetud dokumente. Samuti peab olema võimalik avada ja lugeda kasutaja poolt üles laetud digitaalselt allkirjastatud dokumente.

4. ID kaardi baastarkvara funktsionaalsed nõuded

- 4.1 **ID kaardilt kaardi omaniku andmete lugemine** – ID kaardi utiliit peab võimaldama lugeda ID kaardilt omaniku isikuandmeid, dokumendi numbrit ning isikuga seotud e-posti aadressi.
- 4.2 **ID kaardil olevate sertifikaatide registreerimine süsteemis** – operatsioonisüsteemis peab olema võimalik registreerida ID kaardil olevaid signeerimissertifikaati ja autentimissertifikaati
- 4.3 **ID kaardi sertifikaatide kontroll** – ID kaardi utiliidi abil peab kasutajal olema võimalus vaadata signeerimissertifikaati ning autentimissertifikaati.
- 4.4 **ID kaardi sertifikaatide salvestamine** – ID kaardi utiliidi abil peab kasutajal olema võimalus salvestada signeerimissertifikaati ja autentimissertifikaati arvuti kõvakettale.
- 4.5 **ID kaardi PIN ja PUK koodide muutmine** - ID kaardi utiliidi abil peab kasutajal olema võimalus muuta tema ID kaardiga seotud PIN ja PUK koode. PUK koodi muutmiseks peab kasutaja teadma vana PUK koodi. PIN koodi muutmiseks peab kasutaja teadma vastavat vana PIN koodi.
- 4.6 **ID kaardi lukustunud PIN koodide blokeeringu maha võtmine** - Juhul kui kasutaja on sisestanud PIN koodi 3 (kolm) korda valesti, PIN kood blokeeritakse. ID kaardi utiliit peab võimaldama PIN koodide blokeeringu maha võtmist, tuvastades kasutaja PUK koodi abil.
- 4.7 **ID kaardi kasutamise statistika vaatamine** – kasutajal on võimalik kontrollida tema ID kaardiga antud digitaalsete allkirjade ning kaardiga sooritatud autentimiste arvu kasutades ID kaardi utiliiti.
- 4.8 **Dokumendi digitaalne allkirjastamine** - kasutajal peab olema võimalik allkirjastada mistahes dokumente kasutades DigiDoc klienti. Kasutajal peab olema võimalus allkirjastada mitu dokumenti korraga, dokumentide lisamine toimub läbi DigiDoc kasutajaliidese. Allkirjastamisel saab kasutaja määrata allkirjastaja asukoha (Linn/Maakond/Riik/Indeks) ning allkirjastaja rolli/resolutsiooni. Kogu sisestatud informatsioon lisatakse digitaalsele allkirjale. Allkirjastamisel tuleb kasutajal sisestada PIN2 kood. Digitaalallkiri peab olema vastavuses Euroopa Liidu direktiivile „1999/93/EC On a Community framework for electronic signatures”
- 4.9 **Digitaalselt allkirjastatud dokumentide avamine** – kasutajal peab olema võimalus avada digitaalselt allkirjastatud dokumendi (.ddoc laiendiga) konteinerid kasutades selleks DigiDoc klienti. Avamisel kuvatakse kasutajale allkirjastatud failide nimekiri ning allkirjastajate andmed. Kasutajal on võimalik avada kõiki konteineris olevaid faile. Failide sisu muutmine ei ole võimalik
- 4.10 **Dokumendi ID kaardiga krüpteerimine** – kasutajal peab olema võimalus krüpteerida dokumente kasutades Digidoc klienti. Kõigepealt krüpteeritakse fail sümmeetrilise algoritmiga, mille jaoks genereeritakse juhuslik võti (edaspidi transpordivõti). Seejärel krüpteeritakse transpordi võti aadressaadi avaliku võtmega, kasutades asümmeetrilist algoritmi. Kui aadressaate on mitu, siis krüpteeritakse transpordivõti iga aadressaadi avaliku võtmega eraldi.
- 4.11 **Dokumendi ID kaardiga dekrüpteerimine** – kasutajal peab olema võimalik dekrüpteerida krüpteeritud faili (.cdoc laiendiga) DigiDoc kliendiga, kasutades ID kaardil asuvat autentimissertifikaadis olevale avalikule võtmele vastavat salajase võtit. Vajadusel peab olema võimalik kasutada ka eelmisi privaatvõtmeid, mis on ID kaardil säilitatud, et võimaldada eelmistele sertifikaatidele saadetud krüpteeritud info avamist.
- 4.12 **Dokumendi digitaalsete allkirjade kontrollimine** – kasutajal peab olema võimalus kontrollida digitaalselt allkirjastatud dokumendi allkirjastamise andmeid kasutades DigiDoc klienti. Kasutajal peab olema võimalus vaadata kõiki allkirjastamisega seotud andmeid vastavalt Euroopa Liidu direktiivile „1999/93/EC On a Community framework for electronic signatures”
- 4.13 **Dokumendi digitaalsete allkirjade eemaldamine** – kasutajal peab olema võimalus eemaldada dokumendile lisatud digitaalseid allkirju kasutades DigiDoc klienti. Allkirjade eemaldamine ei tohi mingil moel mõjutada DigiDoc konteinerisse lisatud dokumentide sisu. Allkirja kustutamise jõustumiseks tuleb kasutajal Digidoc konteiner salvestada. Juhul, kui konteiner suletakse ilma salvestamata, siis allkirja ei kustutata. Allkirja kustutamisel küsitakse kasutajalt kinnitust.

- 4.14 **Dokumendi digitaalsete allkirjade printimine ja kinnituslehe koostamine** – DigiDoc kliendiga peab kasutajal olema võimalus trükkida dokumendile lisatud digitaalsete allkirju ühtsele kinnituslehele. Kasutajal ei ole võimalik muuta kinnituslehel olevaid andmeid. Kinnitusleht sisaldab:
- Andmeid allkirjastatud failide kohta
 - Andmeid allkirjastajate kohta
 - Teadet, et kinnitusleht kehtib vaid koos allkirjastatud failide väljatrukkidega.
- 4.15 **ID kaardi sertifikaatide uuendamise tööriist** – kasutajal peab olema võimalus uuendada ID kaardi signeerimissertifikaati ning autentimissertifikaati juhul, kui sertifikaadid on aegunud, kasutades ID kaardi utiliiti
- 4.16 **E-teenustesse sisenemine**– kasutajal peab olema võimalik ennast autentida e-teenustesse sisenemisel kasutades brauserit. Autentimiseks tuleb kasutajal sisestada PIN1 kood.
- 4.17 **Veebirakendustes digitaalallkirja andmine**- kasutajal peab olema võimalus anda digitaalset allkirja dokumentidele läbi brauseri.
- 4.18 **E-kirjade signeerimine ja krüpteerimine** – kasutajal peab olema võimalus digitaalselt allkirjastada ning samuti krüpteerida ning dekrüpteerida e-kirju ID kaardi sertifikaatidega, kasutades Thunderbird e-posti klienti.
- 4.19 **Ametliku @eesti.ee e-posti aadressi seadistamine** – kasutajal peab olema võimalik seadistada tema ID kaardiga seotud @eesti.ee e-posti aadressi kasutades ID-kaardi utiliiti. Seadistamine ei pea toimuma utiliidis, piisab kui kasutaja suunatakse kodanikuportaali e-posti seadistamise lehele. (Vastav link antakse RIA poolt). ID kaardi utiliit peab kontrollima e-posti seadete olemasolu ning nende puudumisel soovutama seadistamist.

5. Täiendavad nõuded

- 5.1 Arendatav tarkvara peab olema avatud lähtekoodiga
- 5.2 Kogu tarkvara peab toimima 32- ja 64-bitistel platvormidel
- 5.3 ID kaardi utiliidi graafiline kasutajaliides peab olema kõigil arendatavatel platvormidel ühetaoline
- 5.4 DigiDoc kliendi graafiline kasutajaliides peab olema kõigil arendatavatel platvormidel ühetaoline
- 5.5 Firefox peab olema toetatud kõigil platvormidel samaselt
- 5.6 Arendatavad brauserite laiendused peavad olema ühilduvad vältimaks vajadust brauserite tuvastamiseks veebirakendustes.
- 5.7 Thunderbird peab olema toetatud kõigil platvormidel samaselt
- 5.8 Arendatav tarkvara ning paigalduspaketid peavad olema intuiitselt kasutatav
- 5.9 Arendatava tarkvara kasutajaliidesed peavad olema kõigil platvormidel minimaalselt kolmes keeles – Eesti, Vene ja Inglise keeles
- 5.10 Kogu kasutajale suunatud dokumentatsioon peab olema minimaalselt kolmes keeles - Eesti, Vene ja Inglise keeles
- 5.11 ID kaardi portaali peab olema minimaalselt kolmes keeles - Eesti, Vene ja Inglise keeles
- 5.12 Tarkvara testimise käigus viiakse vastavalt vajadusele kui mitte vähem kui kord aastas läbi tarkvara turvaaudit
- 5.13 DigiDoc klient peab käsitlema digitaaltempliit samal viisil kui digitaalallkirja.
- 5.14 Hankijale tuleb esitada järgnev aruandlus perioodiliselt üks kord kuus, kogu II astme toe teenuse pakkumise aja jooksul:
- a. Intsidendide ja kaebuste arv tarkvarakomponentide lõikes
 - b. Määr intsidendist, mida ei suudetud lahendada kahe tööpäeva jooksul
 - c. Keskmise intsidendi lahendamise aeg
 - d. Tarkvaras tuvastatud probleemide (tarkvaravigade) arv komponentide lõikes