

eRA SmartCardin järjestelmäkuvaus

Tietoturvasuunnitelman liitteeksi

Sisältö

1	Johdanto.....	3
1.1	Liitteen käyttö tietoturvasuunnitelmassa.....	3
2	eRA SmartCard ohjelmiston perustiedot	4
3	eRA SmartCard -ohjelmiston kuvaus	5
3.1	Tietoturvakäytännöt	5
3.1.1	Kanta-vaatimusten sertifiointi	Virhe. Kirjanmerkkiä ei ole määritetty.
3.1.2	eRA SmartCard -ohjelmiston tietoturallinen kehittäminen.....	5
3.1.3	Tietoturvan vastuiden rajausta	5
3.2	Tukipalvelu	6
3.3	Menettely virhe- ja ongelmatilanteissa	6
3.3.1	Toiminta virhe- ja ongelmatilanteissa	6
3.3.2	1st ja 2nd line support tasojen määritelmät	6
3.3.3	Vastuut virhe- ja poikkeustilanteissa	6
3.3.4	Vikasietoisuus ja virhetilanteet	Virhe. Kirjanmerkkiä ei ole määritetty.
3.4	Tekninen kuvaus eRA SmartCardin toiminnasta	6
3.4.1	Lokitus	7
3.4.2	Varmenteet	7
4	Ohjelmiston käyttö	9
4.1	eRA SmartCardin asennus ja käyttöönotto	9
4.1.1	Yhtäaikainen käyttö muiden kortinlukijaohjelmistojen kanssa.....	9
4.2	Käyttöohjeiden hallinnointi ja jakelu	10
5	Päivitykset ja muutostenhallinta	11
5.1	Julkaisuprosessi ja muutoksenhallinta	11
5.2	Päivityksistä tiedottaminen.....	11
5.3	Päivitysten tarve	11

1 Johdanto

Tämä dokumentti esittelee eRA SmartCard kortinlukijaohjelmiston niiltä osin, mitä sosiaali- ja terveydenhuollon organisaatio tarvitsee omavalvontasuunnitelmaansa varten. Tähän dokumenttiin on tarkoitus viitata organisaation omasta omavalvontasuunnitelmasta.

Ohjelmistoa käytetään toimikortilla kirjautumiseen ja sähköiseen allekirjoitukseen sen kanssa yhteensopivissa palveluissa. eRA SmartCard on ollut tuotantokäytössä vuodesta 2014 ja sen tuottaa Atostek Oy.

1.1 Liitteen käyttö tietoturvasuunnitelmassa

Jokaisella sosiaali- ja terveydenhuollon organisaatiolla tulee olla tietoturvasuunnitelma.

Tietoturvasuunnitelman käyttötarkoitus on täyttää uuden asiakastietolain¹ 784/2021 27 §:n ja THL:n määräyksen 3/2021² mukaiset velvoitteet. Suunnitelma kokoaa yhteen asiakastietolaissa vaaditut omavalvonnan kohteelta edellytettävät selvitykset ja vaatimukset.

Ennen uuden asiakastietolain 784/2021 voimaantuloa käytössä ollut vanhan asiakastietolain 159/2007 mukainen omavalvontasuunnitelma vastasi pääosin sisällöltään tietoturvasuunnitelmaa. Näin ollen kyse on THL:n määräyksen 3/2021 tultua voimaan omavalvonnan kohteen käytössä olevien omavalvontasuunnitelmien päivittämisestä uusiksi tietoturvasuunnitelmiksi.

Tämä liite esittää perustiedot eRA SmartCard-ohjelmistosta, joten olemassa olevaan tietoturvasuunnitelmaan riittää maininta ja viittaus tähän liitteeseen, sekä kuvaus organisaation omista toimintatavoista liittyen eRA SmartCard -ohjelmiston käyttöön. Näitä ovat mm. käyttäjien koulutusta, lokien katselua ja virhetilanteita koskevat toimintaohjeet.

Tietoturvasuunnitelman ylläpitäminen on aina sosiaali- ja terveydenhuollon organisaation omalla vastuulla.

¹ <https://www.finlex.fi/fi/laki/alkup/2021/20210784#Pidp447918064>

² <https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maanittelyt/maaraykset>

2 eRA SmartCard ohjelmiston perustiedot

Järjestelmä	eRA SmartCard
Versio	2.4
Toimittaja	Atostek Hermiankatu 3A, 33720 Tampere +35845 154 6103 erasupport@atostek.com
Käyttötarkoitus	Toimikorttiautentikaatio ja sähköinen allekirjoitus. eRA SmartCard itsessään sisältää toiminnallisuudet kortin aktivointiin, PIN-koodien vaihtoon sekä lukituksen avaamiseen. Pääasiallinen käyttötarkoitus on kuitenkin toimikorttiautentikointi ja sähköinen allekirjoitus, joita käytetään yhdessä eRA SmartCardia tukevan palvelun kanssa.
Käyttäjärühmät	Terveystieteiden ammattilaiset ja terveydenhuollon organisaation hallintohenkilökunta, sosiaalihuollon ammattilaiset, sosiaalihuollon organisaation hallintohenkilökunta, em. tahojen ylläpitohenkilökunta

eRA SmartCard -ohjelmistoa ei ole yksittäisenä ohjelmistona luokiteltu sosiaali- ja terveydenhuollon tietojärjestelmien luokittelun mukaisesti mihinkään luokkaan. eRA SmartCard -ohjelmistoa voidaan käyttää osana tietojärjestelmää, joka on luokiteltu em. luokituksen mukaisesti ja näin eRA SmartCard päätyy luokittelun piiriin. eRA SmartCard on luokiteltu osana eRA-palvelua luokkaan A3, eli eRA SmartCard on mahdollista luokitella korkeimpaan A3 luokkaan asti.

3 eRA SmartCard -ohjelmiston kuvaus

3.1 Tietoturvakäytännöt

Atostekilla on ISO 9001-sertifioitu laatujärjestelmä ja ISO 13485 sertifikaatti, jotka ohjaavat eRA SmartCardin kehitystä.

Atostek toimittaa eRA-palvelunsa mukana eRA SmartCard -ohjelmistoa, jonka myötä eRA SmartCardin tulee täyttää eRA-palvelulle asetetut vaatimukset. eRA on sertifioitu A3-luokan järjestelmä. Se tarkoittaa, että eRAn toiminnallisuudet, kehitysprosessi ja käyttöympäristö ovat ulkopuolisen viranomaisen auditoimia ja hyväksymiä.

3.1.1 Todistus tietoturvan arvioinnista

eRA SmartCard täyttää terveydenhuollon tietojärjestelmien A3-luokan viranomaisvaatimukset ja se on sertifioitu KPMG:n toimesta osana eRA-järjestelmää. eRA SmartCard -ohjelmistoa ei ole yksittäisenä ohjelmistona luokiteltu sosiaali- ja terveydenhuollon tietojärjestelmien luokittelun mukaisesti mihinkään luokkaan.

KPMG IT Sertifiointi Oy on sertifioinut Atostek Oy:n eRA järjestelmän THL:n määrittelemää ”Tietoturva-vaatimukset A-luokkaan kuuluville järjestelmille ja järjestelmien käyttöympäristöille” -vaatimuskriteeristöä (<https://www.kanta.fi/jarjestelmakehittajat/sertifiointi>) vasten. Järjestelmä on hyväksytty Kelan yhteistestauksessa sähköisen reseptin osalta 2.7.2015 sekä sähköisen arkiston osalta 24.5.2016.

Voimassaolo edellyttää vuosittaisiin seuranta-auditointeihin osallistumista sekä olennaisista tietojärjestelmään tai vaatimustenmukaisuustodistuksen tietoihin liittyvistä muutoksista ilmoittamista muutositilauksella. Uusin vaatimuksenmukaisuustodistus on aina ladattavissa eRA-palvelusta.

Auditoitaviin ominaisuuksiin kuuluvat eRA SmartCardin osalta mm.

- Käyttäjien tunnistaminen, todentaminen ja pääsynhallinta
- Istunnon hallinta ja lukittuminen
- Varmenneratkaisut
- Palvelin- ja tietoliikenneympäristöt
- Salattu tietoliikenne

3.1.2 eRA SmartCard -ohjelmiston tietoturallinen kehittäminen

eRA SmartCard -ohjelmiston kehittämisen korkea laatu ja turvallisuus varmistetaan hyvillä ohjelmistokehitysmenetelmillä. Tällaisia menetelmiä ovat mm. ohjelmiston kehityksen jäljitettävyyden (esim. vaatimustenhallinta ja versionhallinta), laadunvarmistus (esim. koodikatselmoinnit), testaus (esim. yhteistestaukset, regressiotestaukset) ja hyvät julkaisukäytännöt (julkaisujen hyväksyntäkriteerit).

3.1.3 Tietoturvan vastuiden rajaus

Atostek on vastuussa eRA SmartCardin tietoturvasta.

Kun eRA SmartCardia käytetään integroituna toiseen järjestelmään, on vastuu tämän järjestelmän tietoturvasta, päivityksistä ja muusta toiminnasta kyseisen järjestelmän toimittajan sopimuksen mukainen, eikä Atostek ota tähän kantaa.

Sosiaali- ja terveydenhuollon organisaatio tai heidän valtuuttamansa taho vastaa työasemien ja muun tietoliikenneympäristönsä tietoturvasta ja päivityksistä itse.

3.2 Tukipalvelu

Atostekin eRA-järjestelmän tuki päivystää sopimuksen mukaisena aikana.

erasupport@atostek.com, 045 1546103.

3.3 Menettely virhe- ja ongelmatilanteissa

3.3.1 Toiminta virhe- ja ongelmatilanteissa

Atostekin eRA SmartCard-järjestelmän virhetilanteiden eskalointiprosessi on seuraava:

1. **Käyttäjä** havaitsee järjestelmässä ongelman. Jos ongelma estää sovelluksen käytön, käyttäjä toimii organisaatiossa sovitun virhetilanneprotokollan mukaan. Käyttäjä raportoi ongelmasta **oman organisaation** ylläpitohenkilöstölle.

2. Mikäli **oman organisaation ylläpitohenkilöstö** ei osaa ratkaista ongelmaa, otetaan sieltä edelleen yhteys järjestelmätoimittajan tarjoamaan IT-tukeen (**1st line support**).

3. Mikäli **1st line support** ei osaa vastata, sieltä ollaan yhteydessä Atostekin tukeen (**2nd line support**). Atostekin eRA-järjestelmän tuki päivystää sopimuksen mukaisena aikana.

Atostek hoitaa ongelman jatkoselvityksen ja tiedottamisen eteenpäin olennaisille tahoille.

3.3.2 1st ja 2nd line support tasojen määritelmät

Sosiaali- ja terveydenhuollon organisaatiot ovat sopimussuhteessa joko eRAn jälleenmyyjään (yleisempi tilanne) tai suoraan Atostekiin. Siitä riippuu, kuka tarjoaa 1st ja 2nd line supportin.

	Sopimussuhde Atostekiin	Sopimussuhde eRA jälleenmyyjään
Oma organisaatio	Koulutetut ylläpitäjät	Koulutetut ylläpitäjät
1st line support	Atostek	Sopimuskumppani
2nd line support		Atostek

Voimassa oleva tieto käytönaikaisesta tuesta löytyy aina sopimuksesta.

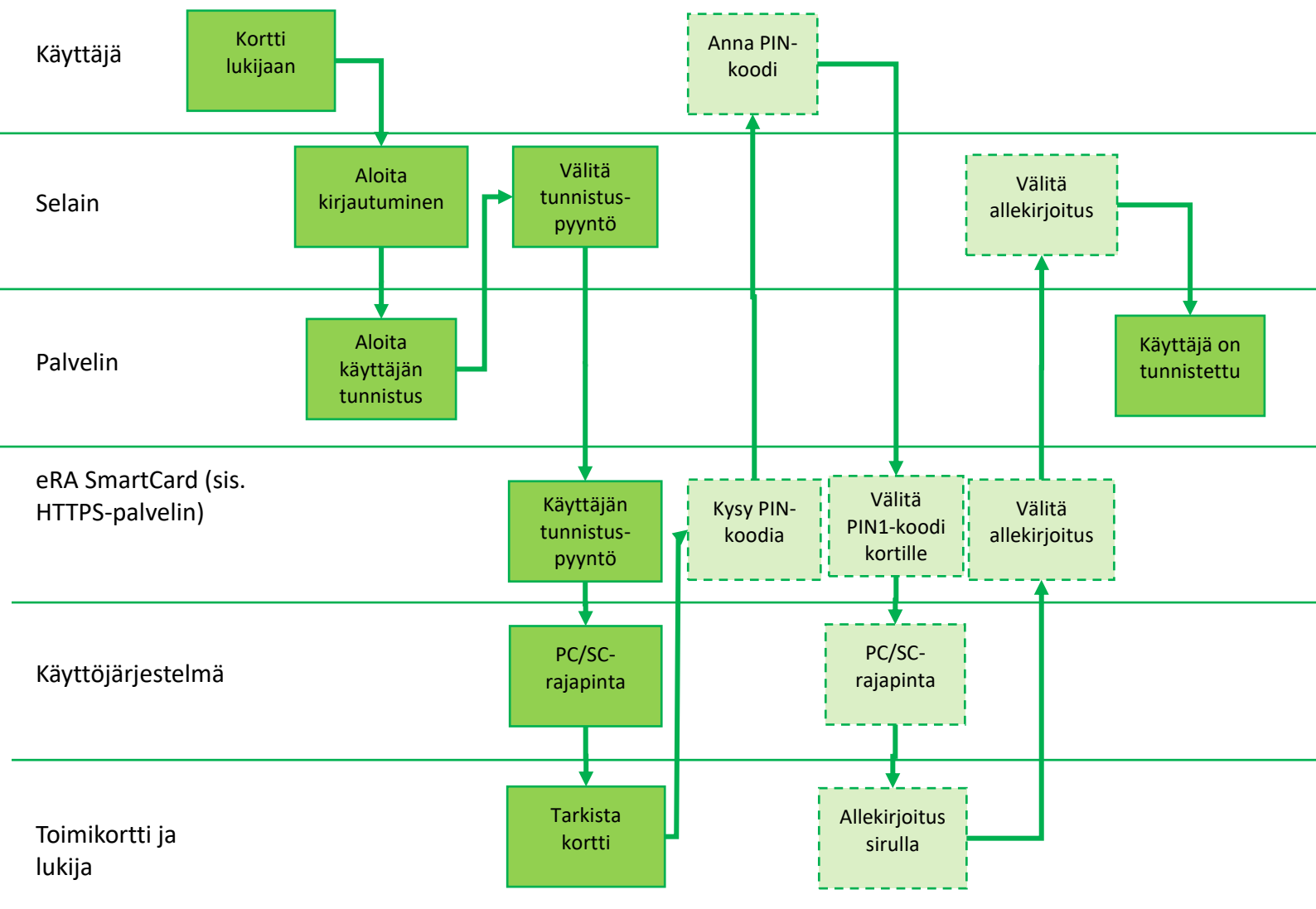
3.3.3 Vastuut virhe- ja poikkeustilaneissa

Vastuukysymykset ja palvelulupaukset on käsitelty sopimuksessa tai erillisessä SLA-dokumentaatiassa.

3.4 Tekninen kuvaus eRA SmartCardin toiminnasta

eRA SmartCard käynnistää paikallisen web-palvelimen joka kuuntelee vain paikallisia yhteyksiä, ja keskustele selaimen ja kortinlukijan kanssa käyttäen. Se käyttää tähän kirjautuneen käyttäjän oikeuksia. Portit ovat oletuksena 44304, 52984 ja 64007, mutta mikäli yksikään näistä ei ole vapaana, eRA SmartCard käyttää satunnaista porttia.

Kaikki yhteydet ovat TLS-salattuja. Tuettuna ovat kaikki TLS versiot versiosta 1.0 alkaen. TLS-protokollan käytetty versio riippuu käyttäjän selaimesta. Lähtökohtaisesti käytetään mahdollisimman uutta versiota, eli käytännössä versiota 1.3 tai 1.2.



Kuva 1: eRA SmartCard toiminnan prosessikuva

3.4.1 Lokitus

eRA SmartCard tuottaa vain teknistä lokia. Varsinainen käyttöloki muodostuu järjestelmiin, joiden kautta eRA SmartCardin autentikaatio- tai allekirjoitusominaisuuksia hyödynnetään.

eRA SmartCard-ohjelma ei itse tallenna mitään käyttäjätietoja tai sisällä tietokantaa, vaan se välittää vain kirjautumistietoja.

3.4.2 Varmenteet

eRA SmartCard vaatii toimiakseen https-varmenteen. eRA SmartCardin toimintaedellytys on, että selain pystyy ottamaan yhteyden eRA SmartCardiin. Kun käyttäjä on ladannut verkkosivun salatun yhteyden (https-yhteyden) kautta, selaimet edellyttävät muiden yhteyksien olevan salattua. Tämän takia yhteys eRA SmartCardiin on oltava salattu. Verkkoselaimiin on tulossa muutos, joka muuttaa näitä toimintaperiaatteita, mutta tuki ei ole vielä laajaa ja sen kehittymistä seurataan.

eRA SmartCard sallii yhteydenotot vain paikalliselta koneelta (eli ns. localhostista, 127.0.0.1). Käytännössä yhteydenotto eRA SmartCardiin on toteutettu siten, että on luotu verkko-osoite erasmartcard.ehoito.fi, joka viittaa paikalliseen koneeseen (ts. osoitteeseen 127.0.0.1) ja tälle osoitteelle on https-varmenne.

eRA SmartCard hakee käynnistyksen yhteydessä varmenteen eRA-järjestelmästä salatusti ja tallentaa sen muistiin myöhempää käyttöä varten. eRA SmartCard tarkistaa tasaisin väliajoin varmenteen voimassaolon ja mikäli varmenne ei ole enää voimassa, yrittää eRA SmartCard hakea uuden varmenteen eRA-järjestelmästä. eRA SmartCardin käyttämä varmenne voidaan tarvittaessa poistaa käytöstä eRA-järjestelmästä, jonka seurauksena kaikki kyseistä varmennetta käyttävät eRA SmartCardit noutavat uuden varmenteen. Mikäli varmenteen noutaminen ei onnistu jossakin vaiheessa, käytetään eRA SmartCardin sisältä löytyvää varmennetta. Näin voidaan taata, että eRA SmartCardin käyttö ei esty vaikka varmennetta ei saataisikaan noudettua. Asennuksen yhteydessä voidaan konfiguroida eRA SmartCard ns. suljettuun ympäristöön, jolloin eRA SmartCard ei yritä hakea varmennetta eRA-järjestelmästä, vaan käytetään aina eRA SmartCardin sisäistä varmennetta.

3.4.3 Vikasietoisuus ja virhetilanteet

eRA SmartCard on kehitetty lähtökohtaisesti vikasietoisaksi ohjelmaksi. Tämä tarkoittaa käytännössä mm. poikkeuksien turvallista käsittelyä ja kaikkien syötteiden validointia. Jos eRA SmartCard ei toimi tai se toimii väärin, vaikutukset ovat rajatut. Pahimmissa mahdollisissa skenaarioissa käyttäjän pääsy tietojärjestelmään estyy kokonaan tai käyttäjä ei voi käyttää tiettyjä tietojärjestelmän toimintoja (esim. reseptin kirjoitus).

4 Ohjelmiston käyttö

4.1 eRA SmartCardin asennus ja käyttöönotto

eRA SmartCard kortinlukijaohjelmiston uusimman version voi ladata eRAn sivuilta tai ohjelmiston automaattisella päivitystoiminnolla.

Käyttääkseen kortinlukijaohjelmistoa, käyttäjällä tulee olla kortinlukijalaite ja voimassa oleva toimikortti. Järjestelmä- ja selainvaatimukset on esitetty sopimuksessa ja käyttöönoton yhteydessä. Käyttöä varten ei tarvita muita kortinlukijaohjelmistoja (esim. mPollux Digisign Client), mutta niiden käyttö yhtäaikaista on mahdollista, kts. kohta 4.1.1.

Asennusohjelma voidaan käynnistää graafisen käyttöliittymän kanssa tai sitä voidaan käyttää komentoriviltä. Windowsilla asennus voidaan tehdä Group Policy Objectina MSI-paketin kautta. Asennuksen yhteydessä voidaan päättää esimerkiksi ohjelmiston ilmoituksista ja DVV Root -varmenteen asentamisesta. Usean käyttäjän komentoriviasennuksen yhteydessä parametreilla voidaan tehdä hieman enemmän valintoja, kuten määrittää polku, jolla selain käynnistetään työpöydän kuvakkeesta.

Asennuksen yksityiskohdat on esitetty tarkemmin asennusohjeessa.

4.1.1 Yhtäaikainen käyttö muiden kortinlukijaohjelmistojen kanssa

Käyttöä varten ei tarvita muita kortinlukijaohjelmistoja (esim. mPollux Digisign Client), mutta niiden käyttö yhtäaikaista on mahdollista. Yhtäaikaisen käytön aikana eri ohjelmistot lukevat samaa kortinlukijassa olevaa toimikorttia.

Yhtäaikaisen käytön toiminta on varmistettu seuraavin keinoin:

- Kahden toimikortinlukijaohjelmiston yhdenaikainen toiminta perustuu siihen, että molemmat ohjelmistot käyttävät toimikorttia Windowsin Smart Card Resource Managerin läpi. Komennot suoritetaan ainakin eRA SmartCardissa transaktion sisällä, mikä takaa sen, että toimikorttia käytetään vain yksi ohjelmisto kerrallaan eikä yksi ohjelmisto voi pitää korttia hallussaan loputtomiin.
- Dokumentaation mukaan mPollux Digisign Client ohjelmisto käyttää samaa rajapintaa (PC/SC) kuin eRA SmartCard.
- Kahden toimikortinlukijaohjelmiston yhdenaikainen toiminta on todettu toimivaksi käytännössä. Atostekin kehittäjillä on ollut eRA SmartCard ja mPollux Digisign Client samanaikaisesti käytössä eRA SmartCardin käyttöönotosta saakka. Lisäksi joissain potilastietojärjestelmissä on käytössä molemmat ohjelmistot ja niiden on todettu toimivan yhdessä asiakkaiden potilastietojärjestelmien, esimerkiksi Effican, kanssa.

Seuraavat asiat kannattaa kuitenkin huomioida:

- DVV:n sivuilla ja mPollux-käyttöohjeessa on maininta: "DigiSign Client -ohjelmiston asentaminen tai päivittäminen edellyttää, että tietokoneelle ei ole asennettu muita kortinlukijaohjelmistoja tai DigiSign Client -ohjelmiston aikaisempia versioita".
- Fujitsu mainitsee ohjeessaan muiden kortinlukijaohjelmistojen poistamista suositeltavaksi asennus-/päivitysvaiheessa, koska asiaa ei ole tutkittu. Fujitsu ei kuitenkaan kiellä muiden toimikortinlukijaohjelmistojen käyttöä ja usean vuoden kokemuksemme mukaan yhtäaikainen toiminta ei kuitenkaan ole aiheuttanut ongelmia.

Yhtäaikainen käyttö on siis testattu useaan otteeseen toimivaksi vaihtelevasta ohjeistuksesta huolimatta. Käyttöönottoon liittyvässä testauksessa on kuitenkin huomioitava rinnakkaisten kortinlukijaohjelmistojen toimivuus rinnakkain sekä asennuksessa/päivityksessä että yhtäaikaisessa käytössä.

4.2 Käyttöohjeiden hallinnointi ja jakelu

Atostekin eRA-järjestelmään on saatavilla erilaisia käyttöohjeita. Alla olevassa taulukossa on luetteloitu käyttöohjetyypit sekä niiden jakelukanavat.

Käyttöohjeen nimi	Kohderyhmä	Ensisijainen jakelutapa
eRA käyttöohje	Lääkärit, hoitajat, palveluntuottajat ja organisaation uusien henkilöiden kouluttajat	Saatavilla eRA-järjestelmästä
eRA ylläpitäjän käyttöohje	Järjestelmän pääkäyttäjät/ylläpitäjät	Saatavilla eRA-järjestelmästä
eRA SmartCard käyttöohje	Lääkärit, hoitajat, palveluntuottajat ja organisaation uusien henkilöiden kouluttajat	Avattavissa eRA SmartCard-ohjelmasta
eRA SmartCard asennusohje	Järjestelmää käyttävän organisaation IT-tuki	Levitetään eRA SmartCardin asennuspaketin yhteydessä

5 Päivitykset ja muutostenhallinta

5.1 Julkaisuprosessi ja muutoksenhallinta

eRA SmartCard ohjelmiston julkaisuprosessi noudattaa laatujärjestelmän mukaista prosessia. Ohjelmistolle suoritetaan ennalta suunnitellut julkaisutestaus testitapaukset. Suoritettujen testien tuloksien perusteella tehdään julkaisun hyväksyntä ja suoritetaan julkaisu esitestaajille. Laatujärjestelmän prosessin mukaisesti ennen julkaisun hyväksyntää hyväksytetään myös ajantasainen riskianalyysi, vaatimusmäärittely, käyttöohjeet ja koodikatselmointi raportti. Ohjelmisto julkaistaan esitestaukseen halukkaille tahoille, ennalta sovituksi ajaksi. Esitestauskierroksen havaintojen mukaan versio joko julkaistaan tuotantokäyttöön, tai versio jätetään julkaisematta. Esitestausryhmään liittymisestä sovitaan erikseen.

5.2 Päivityksistä tiedottaminen

eRA SmartCard ilmoittaa uusista päivityksistä, ja tarjoaa käyttäjälle omasta käyttöliittymästään mahdollisuuden päivittää ohjelmisto. Tämän voi kuitenkin ottaa pois päältä, mikäli käyttäjällä ei ole oikeutta tällaisiin toimenpiteisiin työasemallaan.

Esitestaustahot saavat tiedon uusista versioista etukäteen.

5.3 Päivitysten tarve

Lähtökohtaisesti asiakas itse päättää koska päivittää ohjelmiston uuteen versioon. Vanhojen versioiden tuen päättymisestä tai esimerkiksi pakollisista tietoturvapäivityksistä tiedotetaan kuitenkin erikseen, ja tällöin päivittäminen on toiminnan jatkumiseksi välttämätöntä. eRA SmartCardin varmenteet kuitenkin saattavat asettaa reunaehdoja päivitystarpeille. Suljettujen ympäristöjen tapauksessa tulee asiakkaan päivittää eRA SmartCard vähintään kerran vuodessa, jotta eRA SmartCardin sisäinen varmenne ei pääse vanhenemaan ja eRA SmartCardin käyttö ei esty. Varmenteiden vanhenemisesta käyttäjälle näytetään ilmoitus 2 kuukautta ennen varmenteen vanhenemista.