KANSALLISARKISTO
RIKSARKIVET

Kansallisarkisto

SÄHKE2-SERTIFIOINTIKRITEERIT

SÄILYTYSJÄRJESTELMÄ

v. 2.0 (23.4.2015)

VERSIOHISTORIA

Versio	Päivämäärä	Tekijä	Sisältö
1.0	15.3.2012	Mikko Eräkaski	yhteensä 37 vaatimusta
1.1	21.5.2013	Mikko Eräkaski	Täydennetty johdantotekstiä, ei muutoksia kriteereihin.
1.2	26.8.2014	Mikko Eräkaski	Poistettu metatieto ”versio”vaatimuksesta 2.2 Muokattu vaatimusten 2.1 ja 2.2 kirjoitusasua. Hävittämisen vaatimuksia 6.7, 6.8 ja 6.10 muokattu Vaatimuksen 6.5 lisätietoja muokattu.
2.0	23.4.2015	Nina Eerikäinen	Poistettu VAPA:a koskevat vaatimukset.

1. Yleistä säilytysjärjestelmän sertifiointikriteereistä

Säilytysjärjestelmällä tarkoitetaan tietojärjestelmää, jossa tietoa ei enää käsitellä tai muokata, vaan sinne tallennetun tiedon käsittely on päättynyt. SÄHKE2-vaatimusten mukaisesti säilytysjärjestelmässä tulee olla myös määräajan säilytettävien asiakirjatietojen hävittämistoiminnallisuus.

SÄHKE2-sertifioinnilla varmistetaan, että säilytysjärjestelmä täyttää ominaisuuksiltaan SÄHKE2-normin vaatimukset. Säilytysjärjestelmän sertifiointikriteereihin ei sisälly vaatimuksia tiedon pitkäaikaista tai pysyvää säilyttämistä varten, siten SÄHKE2-sertifioinnilla ei voida todentaa, että tietojärjestelmään sisältyy mainittuja ominaisuuksia.

2. Aineiston vastaanotto

Säilytysjärjestelmään voidaan siirtää aineistoa joko asiakirjallisen tiedon käsittelyprossin mukaisina kokonaisuuksina (yksi tai useampi kerralla) tai asiakirjan mukaisina kokonaisuuksina (yksi tai useampi kerralla) tai molempia tapoja käyttäen.

2.1

Vaatimus
Säilytysjärjestelmään tallennettavilla asiakirjallisen tiedon käsittelyprosesseilla tulee olla pakolliset metatiedot tallennettuna. Tämä voi tapahtua joko 1) siten, että metatiedot on saatu operatiivisesta järjestelmästä tai 2) että ne lisätään eAMS-ohjautuvasti tallennuksen yhteydessä tehtäväluokan mukaan.

Todentaminen
Säilytysjärjestelmästä tulee todentaa, että toiminto, jolla se liittää asiakirjallisen tiedon käsittelyprosessille eAMSista määräytyvän oletusmetatietoarvon siinä vaiheessa, kun se tallennetaan säilytysjärjestelmään, on olemassa. Todentaminen tehdään siten, että säilytysjärjestelmään tallennetaan asiakirjallisen tiedon käsittelyprosessi, jossa ei ole ko. metatietoja ja seurataan, että se saa oikeat, eAMSiin määritellyt metatietoarvot vastaanoton yhteydessä. Asiakirjallisen tiedon käsittelyprosessi saa eAMSin oletusmetatietoarvot tehtäväluokan perusteella
TAI
Säilytysjärjestelmässä tulee todentaa, että se tarkastaa vastaanoton yhteydessä, että jäljempänä määriteltävät metatiedot ovat vastaanotettavalla asiakirjallisen tiedon käsittelyprosessilla. Todentaminen tehdään siten, että säilytysjärjestelmään yritetään tallentaa asiakirjallisen tiedon käsittelyprosessi, jolta puuttuu metatieto, jolloin se ei tallennu säilytysjärjestelmään.

A	Säilytysjärjestelmä tarkastaa aineistoa vastaanottaessaan, että tallennettavalla asiakirjallisen tiedon käsittelyprosessilla on kyseinen metatietoarvo.	*Ohje: Sertifioija valitsee joko A, B tai X, sen mukaisesti miten vaatimus toteutuu ko. järjestelmässä.* *X-vaihtoehdossa vaatimus ei täyty.* *Taulukossa on harmaalla merkitty ne B-vaihtoehdot, jotka eivät ole hyväksyttyjä.*
B	Asiakirjallisen tiedon käsittelyprosessille liitetään vastaanoton yhteydessä tehtäväluokan mukaan eAMSiin määritelty metatietoarvo.	
X	Ei toteudu	

			Vastaus			
id	**Elementti**	**Sähke2 viite**	**A**	**B**	**X**	**Tarkenne**
1.	Julkisuusluokka	2.6.1				
2.	Salassapitoaika	2.6.2				
3.	Salassapitoperuste	2.6.4				
4	Salassapidon päättymisajankohta	2.6.3				

	5.	Turvallisuusluokka	2.6.6				
	6.	Henkilötietoja	2.6.7				
	7.	Säilytysajan pituus	2.11.1				
	8.	Säilytysajan peruste	2.11.2				
	9.	Säilytysajan päättymisajankohta	2.11.3				
	10.	Yksilöivä identifiointitunnus	2.3				

2.2

Vaatimus
Säilytysjärjestelmään tallennettavilla asiakirjoilla tulee olla pakolliset metatiedot tallennettuna. Tämä voi tapahtua joko 1) siten, että metatiedot on saatu operatiivisesta järjestelmästä tai 2) että ne lisätään eAMS-ohjautuneesti tallennuksen yhteydessä.

Todentaminen
Säilytysjärjestelmästä tulee todentaa, että toiminto, jolla se liittää asiakirjalle eAMSista määräytyvän oletusmetatietoarvon siinä vaiheessa, kun se tallennetaan säilytysjärjestelmään, on olemassa. Todentaminen tehdään siten, että säilytysjärjestelmään tallennetaan asiakirja, jossa ei ole jäljempänä määriteltyjä metatietoja ja seurataan, että se saa oikeat, eAMSiin määritellyt, metatietoarvot vastaanoton yhteydessä. Asiakirja saa oletusmetatietoarvot tehtäväluokan ja asiakirjatyypin perusteella.
TAI
Säilytysjärjestelmässä tulee todentaa, että se tarkastaa vastaanoton yhteydessä, että jäljempänä määriteltävät metatiedot ovat vastaanotettavalla asiakirjalla. Todentaminen tehdään siten, että säilytysjärjestelmään yritetään tallentaa asiakirja, jolta puuttuu kyseinen metatieto, jolloin se ei tallennu säilytysjärjestelmään.

A	Säilytysjärjestelmä tarkastaa aineistoa vastaanottaessaan, että asiakirjalla on kyseinen metatietoarvo	*Ohje: Sertifioija valitsee joko A, B tai X, sen mukaisesti miten vaatimus toteutuu ko. järjestelmässä.* *X-vaihtoehdossa vaatimus ei täyty.* *Taulukossa on harmaalla merkitty ne B-vaihtoehdot, jotka eivät ole hyväksyttyjä.*
B	Asiakirjalle liitetään vastaanoton yhteydessä tehtäväluokan ja asiakirjatyypin mukaan eAMSiin määritelty metatietoarvo.	
X	Ei toteudu	

			Vastaus			
id	**Elementti**	**Sähke2 viite**	**A**	**B**	**X**	**Tarkenne**
1.	Julkisuusluokka	2.6.1				
2.	Salassapitoaika	2.6.2				
3.	Salassapitoperuste	2.6.4				
4	Salassapidon päättymisajankohta	2.6.3				
5.	Turvallisuusluokka	2.6.6				
6.	Henkilötietoja	2.6.7				
7.	Säilytysajan pituus	2.11.1				
8.	Säilytysajan peruste	2.11.2				
9.	Säilytysajan päättymisajankohta	2.11.3				
10.	Yksilöivä identifiointitunnus	2.3				

3. Metatietoarvojen muokkaaminen ja hallinnointi

Metatietojen muokkaaminen ja hallinnointi koskee asiakirjallisen tiedon käsittelyprosessin, toimenpiteen ja asiakirjan metatietoja.

	Vaatimus		kyllä	ei	Miten vaatimus todennetaan?
3.1	Onko säilytysjärjestelmässä ominaisuus, jolla metatietokenttien näkyvyyttä voidaan hallita?				Järjestelmässä tulee olla mekanismit, joilla voidaan hallita sitä, että määrätyt metatietokentät näkyvät vain niille tahoille, joilla on niihin oikeus.
3.2	Onko säilytysjärjestelmässä ominaisuus, jolla on mahdollista muokata asiakirjallisen tiedon käsittelyprosessin (asian) seuraavia metatietoarvoja käyttäjäroolien mukaan? *(viittaus SÄHKE2-metatietomalliin):*				Muokkausoikeus tarkistetaan sekä sellaisella käyttäjätunnuksella, jolla on oikeus, että sellaisella, jolla ei ole oikeutta.
	Julkisuusluokka	2.6.1			
	Salassapitoaika	2.6.2			
	Salassapitoperuste	2.6.4			
	Turvallisuusluokka	2.6.6			
	Henkilötietoja	2.6.7			
3.3	Onko säilytysjärjestelmässä ominaisuus, jolla on mahdollista muokata asiakirjan seuraavia metatietoarvoja käyttäjäroolien mukaan? *(viittaus SÄHKE2-metatietomalliin):*				Muokkausoikeus tarkistetaan sekä sellaisella käyttäjätunnuksella, jolla on oikeus, että sellaisella, jolla ei ole oikeutta.
	Julkisuusluokka	2.6.1			
	Salassapitoaika	2.6.2			
	Salassapitoperuste	2.6.4			
	Turvallisuusluokka	2.6.6			
	Henkilötietoja	2.6.7			
	Säilytysajan pituus	2.11.1			
	Säilytysajan peruste	2.11.2			
3.4	Onko säilytysjärjestelmässä ominaisuus, jolla salassapitoajan muuttaminen muuttaa automaattisesti salassapidon päättymisajankohta kuvaavaa metatietoarvoa?				
3.5	Onko säilytysjärjestelmässä ominaisuus, jolla säilytysajan pituuden muuttaminen muuttaa automaattisesti säilytysajan päättymisajankohtaa kuvaavaa metatietoarvoa?				
3.6	Onko säilytysjärjestelmässä ominaisuus, jolla asiakirjallisen tiedon käsittelyprosessin tai asiakirjan tehtäväluokan muuttaminen on estetty?				

	Vaatimus	kyllä	ei	Miten vaatimus todennetaan?
3.7	Onko säilytysjärjestelmässä toiminnallisuus, jolla asiakirjallisen tiedon käsittelyprosessin ja asiakirjan muuttumista julkiseksi voidaan hallita siinä vaiheessa, kun salassapitoaika lakkaa eli salassapidon päättymisajankohta saavutetaan?			Säilytysjärjestelmässä on toiminnallisuus, jolla se säännöllisin eräajoin tai vastaavin mekanismein automaattisesti tarkistaa asiakirjallisen tiedon käsittelyprosessien ja asiakirjojen salassapidon voimassaolon ja muuttaa salassa pidettävät kohteet julkisiksi. **TAI** Säilytysjärjestelmä tulkitsee salassapitoajaltaan päättyneet asiat ja asiakirjat julkisiksi. **TAI** Tietyn roolin mukaisin käyttöoikeuksin on mahdollista käydä manuaalisesti muuttamassa metatietoarvoja**.**

4. Käyttövaltuushallinta

	Vaatimus	kyllä	ei	Miten vaatimus todennetaan?
4.1	Onko säilytysjärjestelmässä mekanismi, jolla voidaan määritellä oikeudet tallentaa asiakirjoja ja/tai asiakirjallisen tiedon käsittelyprosesseja? *ks. vaatimus nro.1*			Mahdollisuus määritellä käyttöoikeudet rooleittain. Mahdollisuus tallentaa asiakirja ja/tai asiakirjallisen tiedon käsittelyprosessi säilytysjärjestelmään testataan sellaisella käyttäjätunnuksella, jolla ei ole määritelty oikeuksia ja jolla on määritellyt oikeudet. **TAI** Asiakirjat / asiakirjallisen tiedon käsittelyprosessit siirtyvät järjestelmään automaattisena tiedonsiirtona toisesta tietojärjestelmästä, jolloin manuaalista tallentamista ei tapahdu.
4.2	Onko säilytysjärjestelmässä mekanismi, jolla voidaan estää pääsy salassapidettävän asiakirjallisen tiedon käsittelyprosessin asiakirjoihin muilta kuin niiltä käyttäjäryhmiltä, joille on määritelty oikeus nähdä salassapidettävää tietoa?			Pääsy salassa pidettävään tietoon testataan sellaisella käyttäjätunnuksella, jolle ei ole määritelty oikeuksia ko. asiakirjallisen tiedon käsittelyprosessiin.

5. Asiakirjan käsittelyvaatimukset

	Vaatimus	kyllä	ei	Miten vaatimus todennetaan?
5.1	Onko asiakirjojen tietosisällön muuttaminen estetty säilytysjärjestelmässä?			Yritetään muuttaa asiakirjan tietosisältöä.
5.2	Onko asiakirjan ylikirjoittaminen eli korvaaminen uudella asiakirjalla estetty säilytysjärjestelmässä?			Jos asiakirja yritetään korvata toisella asiakirjalla, tallentuu se aina uutena asiakirjana. *Uusi asiakirja voi tallentua esimerkiksi vanhan asiakirjan uutena versiona.*
5.3	Onko säilytysjärjestelmässä ominaisuus, jolla asiakirjallisen tiedon käsittelyprosessin (asian) säilytysaika automaattisesti asianomaiseen käsittelyprosessiin sisältyvän pisimpään säilytettävän asiakirjan säilytysajan mukaan.			Asiakirjallisen tiedon käsittelyprosessi (asia) voi sisältyä hävitysesitykseen vasta siinä vaiheessa, kun kaikki siihen tallennetut asiakirjat on hävitetty tai kun em. asiakirjat sisältyvät hävitysesitykseen. *Ohje: A, B ja C ovat vaihtoehtoisia tapoja. Järjestelmän on toteutettava jokin niistä.* **A.** Säilytysjärjestelmä laskee asiakirjallisen tiedon käsittelyprosessille säilytysajan siihen liittyvän pisimpään säilytettävän asiakirjan mukaan. **B.** Säilytysjärjestelmä tarkastaa asiakirjallisen tiedon käsittelyprosessia vastaanotettaessa, että sillä on mainittu metatietoarvo. **C.** Asiakirjallisen tiedon käsittelyprosessia ei tarvitse erikseen hävittää, vaan se häviää, kun viimeinen asiaan kuulunut asiakirja hävitetään.

	Vaatimus	kyllä	ei	Miten vaatimus todennetaan?
5.4	Onko säilytysjärjestelmässä ominaisuus, jolla varmistetaan, että salassa pidettävillä asiakirjallisen tiedon käsittelyprosesseilla ja asiakirjoilla on salassapidon päättymisajankohta?			Säilytysjärjestelmä laskee salassa pidettäville asiakirjallisen tiedon käsittelyprosesseille ja asiakirjoille salassapidon päättymisajankohdan salassapitoajan ja sen laskentaperusteen mukaan. **TAI** Säilytysjärjestelmä tarkastaa asiakirjallisen tiedon käsittelyprosessia ja asiakirjaa vastaanotettaessa, että sillä on mainittu metatietoarvo.
5.5	Onko säilytysjärjestelmässä toiminnallisuus, jolla asiakirjallisen tiedon käsittelyprosessin ja asiakirjan muuttumista julkiseksi voidaan hallita siinä vaiheessa, kun salassapitoaika lakkaa eli salassapidon päättymisajankohta saavutetaan?			Säilytysjärjestelmässä on toiminnallisuus, jolla se säännöllisin eräajoin tai vastaavin mekanismein automaattisesti tarkistaa asiakirjallisen tiedon käsittelyprosessien ja asiakirjojen salassapidon voimassaolon ja muuttaa salassa pidettävät kohteet julkisiksi. **TAI** Säilytysjärjestelmä tulkitsee salassapitoajaltaan päättyneet asiat ja asiakirjat julkisiksi. **TAI** Tietyn roolin mukaisin käyttöoikeuksin on mahdollista käydä manuaalisesti muuttamassa metatietoarvoja**.**

6. Määräajan säilytettävien asiakirjallisten tietojen hävittäminen

	Vaatimus	kyllä	ei	Miten vaatimus todennetaan?
6.1	Sisältyykö järjestelmään hävitystoiminnallisuus, joka tuottaa hävitysesityksen määriteltyjen hävittämiskriteerien mukaan ja mahdollistaa siten asiakirjatietojen keskitetyn hävittämisen järjestelmässä.			Järjestelmässä on hävitystoiminnallisuus, joka tuottaa automaattisesti etukäteen määritellyin väliajoin hävitysesityksen hävittämiskriteerien mukaan. **TAI** Järjestelmä tuottaa hävittämiskriteerien mukaisen hävitysesityksen, kun auktorisoidun roolin mukainen käyttäjä käynnistää hävitystoiminnallisuuden.

	Vaatimus	kyllä	ei	Miten vaatimus todennetaan?
6.2	Onko järjestelmässä toiminnallisuus, jolla hävitysesitys on mahdollista tuottaa siten, että siihen sisältyvät kaikki hävittämiskriteerit täyttävät asiakirjatiedot?			Järjestelmän tuottamaan hävitysesitykseen sisältyvät kaikki asiakirjatiedot, joiden säilytysaika on päättynyt hävitysesityksen laatijan oikeuksien mukaisesti. *HUOM! Hävittämisesityksen muodostamiseksi on myös sallittua asettaa lisäksi muita kriteereitä, jotka rajaavat hävitysesitykseen tulevien asiakirjojen joukkoa, esim. tehtäväluokka, jolloin hävittäminen voidaan tehdä erissä vaiheittain.*
6.3	Onko järjestelmässä toiminnallisuus, joka varmistaa, että hävitysesitykseen sisältyy ainoastaan asiakirjatietoja, joiden säilytysaika on päättynyt?			Laaditaan hävitysesitys aineistosta, jossa on sekä pysyvästi säilytettäviä asiakirjatietoja että sellaista, jonka säilytysaika ei ole vielä päättynyt. Tarkistetaan, että hävitysesitys ei sisällä asiakirjatietoja, joiden säilytysaika ei ole vielä päättynyt tai pysyvästi säilytettäviä asiakirjatietoja.
6.4	Onko järjestelmässä ominaisuus, jolla hävitysesityksen hyväksyntä voi tapahtua vain määritellyin käyttövaltuuksin.			Hävitysesityksen hyväksyminen on mahdollista vain määritellyin käyttövaltuuksin. Yritetään suorittaa järjestelmässä hävitysesityksen hyväksyntä ilman asianmukaisia oikeuksia.
6.5	Onko järjestelmässä ominaisuus, jolla hävitysesitys on mahdollista poistaa /peruuttaa kokonaisuudessaan ennen sen hyväksyntää.			Auktorisoidun roolin mukaisen käyttäjän on mahdollista poistaa tai peruuttaa hävitysesitys järjestelmästä ennen sen hyväksyntää. *Auktorisoidun roolin mukaisen käyttäjän on myös mahdollista poistaa hävitysesitykseen kuuluvia asiakirjoja joko yksittäin hävitysesityksestä tai tuottamalla uusi hävitysesitys uusien kriteerien mukaan.*
6.6	Onko järjestelmässä ominaisuus, jolla asiakirjan tietojen yhteydessä näkyy sen sisältyminen hävitysesitykseen.			Hävitysesityksestä on voitava luotettavasti yksilöidä kaikki siihen kuuluvat asiakirjatiedot. Käytännössä asiakirjan ID:n ja nimekkeen on käytävä ilmi hävitysesityksestä. Lisäksi asiakirjan metatietojen

	Vaatimus	kyllä	ei	Miten vaatimus todennetaan?
				yhteydestä on käytävä ilmi, että se sisältyy hävitysesitykseen.
6.7	Onko järjestelmässä toiminnallisuus, jolla tieto hävitetyistä asiakirjatiedoista jää talteen.			Järjestelmässä on toiminnallisuus, jolla tieto hävitetyistä asiakirjatiedoista voidaan tulostaa/ottaa talteen asiakirjana TAI Järjestelmässä on toiminnallisuus, jolla tieto hävitetyistä asiakirjatiedoista jää talteen erilliseen rekisteriin.
6.8	Onko järjestelmässä toiminnallisuus, jolla seuraavat SÄHKE2-metatietomallin mukaiset metatiedot hävitetyistä asiakirjoista jäävät talteen vaatimuksessa 6.7 esitetyllä tavalla.			Metatietojen *nimeke, tehtävä ja asiakirjatyyppi* tulee tallentua luettavassa muodossa, eikä esim. koodina.
	Identifiointitunnus (2.3)			
	Nimeke (2.7)			
	Tehtävä (2.13)			
	Asiakirjatyyppi (2.15)			
6.9	Onko järjestelmässä toiminto, jolla asiakirjallisen tiedon käsittelyprosessi ja toimenpiteet voivat sisältyä hävitysesitykseen vasta sitten, kun kaikki siihen liitetyt asiakirjat on joko hävitetty tai ne kuuluvat hävitysesitykseen?			Asiakirjallisen tiedon käsittelyprosessi ei sisälly hävitysesitykseen ennen kuin viimeinen siinä oleva asiakirja on hävitetty tai se sisältyy hävitysesitykseen.
6.10	Onko järjestelmässä toiminto, jolla määräajan säilytettävät asiakirjallisen tiedon käsittelyprosessit hävitetään saman määrämuotoisen hävittämismenettelyn mukaisesti kuin asiakirjat ja niistä jää talteen tieto samalla tavalla kuin asiakirjoista.			Asiakirjallisen tiedon käsittelyprosessi ohjautuu automaattisesti hävitysesitykseen, kun siihen kuulunut pisimpään säilytettävä asiakirja ohjautuu hävitysesitykseen, jolloin asiakirjallisen tiedon käsittelyprosessi hävitetään yhdessä asiakirjojen kanssa. **TAI** Hävitysesitys on mahdollista tuottaa säilytysjärjestelmästä siten, että siihen sisältyvät hävittämiskriteerit täyttävät asiakirjallisen tiedon käsittelyprosessit (eli käsittelyprosessit, joihin kuuluva pisimpään säilytettävä asiakirja on hävitetty). Asiakirjallisen tiedon käsittelyprosessien hävittäminen tapahtuu samalla tavalla kuin asiakirjan hävittäminen.