CGI

Experience the commitment®

CGI eSign

Sähköinen allekirjoitus
Kiistämättömyys ja eheyden tarkistaminen

Sisällysluettelo

1 eSign web pohjainen sähköinen allekirjoitus

eSign on digitaalinen allekirjoitusprosessi, jota voidaan käyttää organisaatioille räätälöityjen digitaalisten allekirjoitusten tekemiseen.

CGI:n sähköinen allekirjoituksen avulla luodaan digitaalinen allekirjoituspalvelu, jota käytetään erilaisten CGI:n myyntisopimusten sopimusten allekirjoittamiseen.

2 Allekirjoituksen kiistämättömyys ja eheys

eSign tukee monia erilaisia digitaalisen allekirjoituksen menetelmiä ja erilaisia prosesseja, joissa käyttäjiltä kerätään allekirjoituksia. Jokaiselle allekirjoitusprosessille luodaan XML-tiedosto ja loppukäyttäjän allekirjoitukset kootaan standardimuotoon (XML-allekirjoitus, XAdES). Tämä tiedosto yhdessä muiden tietojen kanssa, jotka vaaditaan todistamaan, että "tämä henkilö allekirjoitti nämä tiedot tällä hetkellä" tallennetaan sähköiseen arkistoon mahdollista myöhempää käyttöä varten. Tämä arkistoitu tietue ei ole tarkoitettu päivittäiseen käyttöön vaan se on tarkoitettu käytettäviksi, jos joku allekirjoittaja kiistää allekirjoittaneensa tai muun tarpeen todistaa, mitä allekirjoitettiin ja milloin. Teknisesti tämä arkistoitu kopio antaa tietojen kiistämättömyyden ja eheyden.

Päivittäiseen käyttöön luodaan dokumentin käyttökopio. Tämä on PDF-muotoinen kansilehti, joka näyttää allekirjoituksia koskevat tiedot luettavassa muodossa. Tämä kansilehti on liitetty alkuperäiseen allekirjoitettuun sopimukseen ja tämä yhdistetty PDF allekirjoitetaan digitaalisesti sähköiseen allekirjoituksen järjestävän organisaation puolesta. Kun osapuolet saavat tämän PDF-tiedoston, ne voivat validoida sähköisen allekirjoituksen aitouden (tämä tiedosto on CGI eSginissa allekirjoitettu) ja eheys (nämä tiedot eivät ole muuttuneet allekirjoituksen jälkeen).

PDF-tiedostoissa käytetyt sähköiset allekirjoitukset luodaan siten, että PDF-ohjelmasta riippumatta sähköisen allekirjoituksen voidaan tarkistaa. Teknisesti tämä tarkoittaa sitä, että CGI:lle on myönnetty Väestörekisterikeskuksen järjestelmäallekirjoitusvarmenne (CA), jonka salausavainta käytetään sähköisessä allekirjoituksessa. Varmenne on nimetty CGIesign systemsigner nimellä.

3 Miten tarkastaa allekirjoitettu dokumentti

PDF-ohjelmalla kautta tehtävä allekirjoitusvalidointi

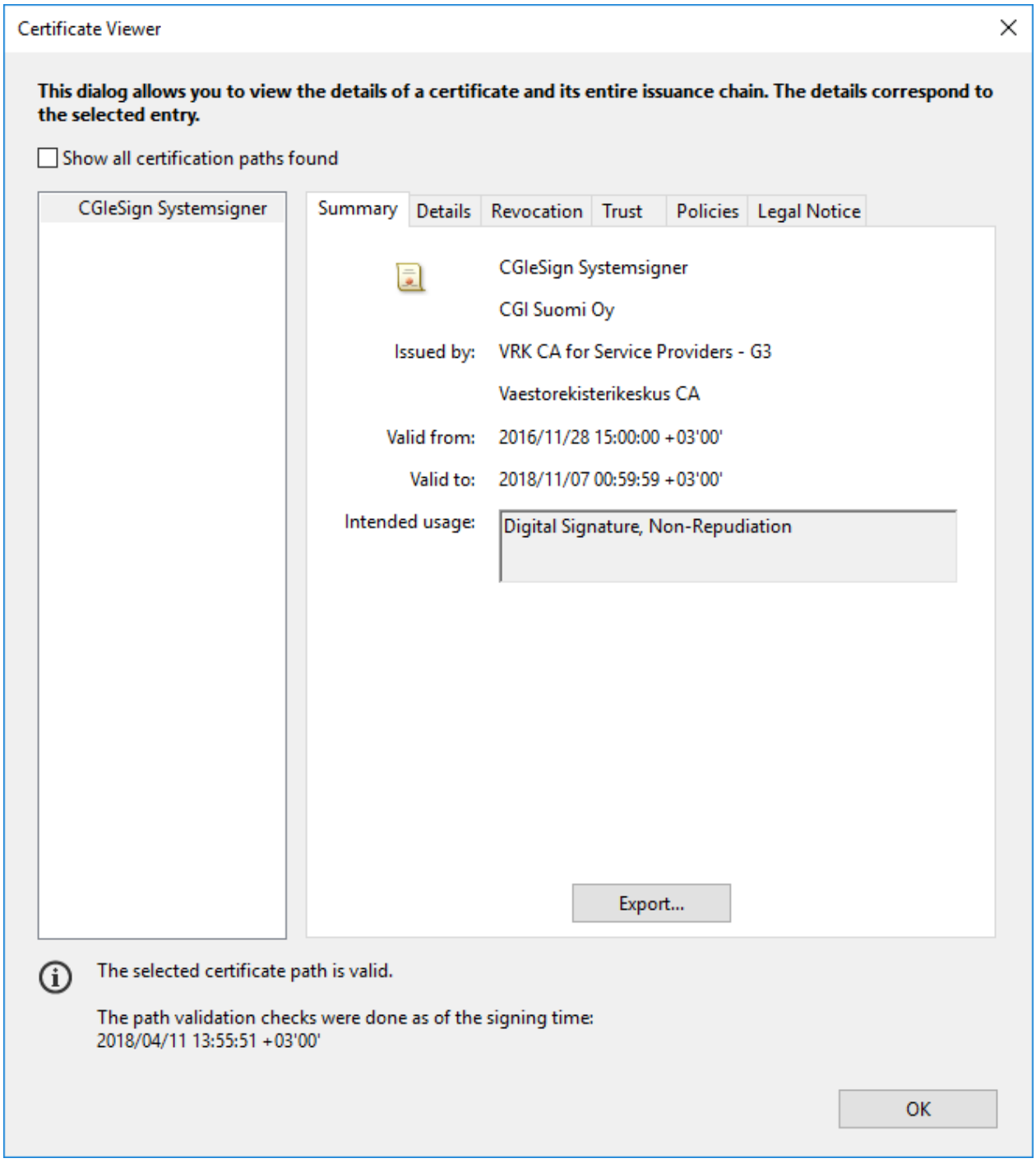
Kun digitaalisesti allekirjoitettu PDF-tiedosto avataan PDF-tiedostojen katseluun soveltuvalla ohjelmistolla, esimerkiksi Adobe Acrobat Readerilla, allekirjoituksen voimassaolo näkyy käyttäjälle jollakin seuraavista arvoista:

1. Digitaalinen allekirjoitus on voimassa, ja käytetyn varmenteen liikkeeseenlaskija on luotettu
2. Digitaalinen allekirjoitus on pätevä, liikkeeseenlaskijan käyttämä sertifikaatti ei ole tiedossa
3. Digitaalinen allekirjoitus ei ole kelvollinen

Jos osapuoli avaa PDF-tiedostot ja tulos on 1, allekirjoitus on luotu käyttämällä varmenteen myöntäjää, joka on Adoben ennakkoon hyväksymä, eli kuuluu Adoben hyväksytyt listaan (Trust List, AATL).

Jos PDF-tiedostot avataan ja tulos on 2, allekirjoitus on luotu varmenteen myöntäjällä, joka ei ole Adoben tuntema. Varmenteen voi hyväksyä itse tai keskitetyn työasemanhallinnan kautta, jonka jälkeen allekirjoitus näkyy tilanteessa 1. Väestörekisterikeskuksen myöntämä ei kuulu Adoben AATL:n vaan

käyttäjä voi itse todeta tiedostosta sähköisen allekirjoituksen voimassaolon. CGIeSign Systemsigner, Väestörekisterikeskus CA.



Tulos 3 tarkoittaa aina, että PDF-tiedosto on vioittunut allekirjoituksen jälkeen. Tämä voi tarkoittaa joko aktiivista väärentämistä tai teknisiä ongelmia (virhe kuljetuksessa tai varastoinnissa).

cgi.fi