LAB University of Applied Sciences

Digitaalinen allekirjoitus

LAB-ammattikorkeakoulu
Insinööri (AMK), Tieto- ja viestintätekniikka
2023
Jukka Natunen

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Jukka Natunen	Opinnäytetyö, AMK	2023
	Sivumäärä 26	

Työn nimi

Digitaalinen allekirjoitus

Tutkinto ja koulutusala

Insinööri (AMK), tieto- ja viestintätekniikan koulutus

Toimeksiantajaorganisaatio (jos opinnäytetyöllä on toimeksiantaja)

Evitec Oy

Tiivistelmä

Opinnäytetyössä keskityttiin digitaalisen allekirjoituksen prosessien laadunvarmistukseen ja tarkistuslistojen kehittämiseen Evitec Oy:lle. Työn tavoitteena oli tuottaa yleiskäyttöisiä tarkistuslistoja, jotka tukevat organisaatioita digitaalisen allekirjoituksen prosessien laadun ja toimivuuden varmistamisessa. Työssä hyödynnettiin sekä teoreettista tutkimusta että käytännön soveltamista.

Työssä analysoitiin digitaalisen allekirjoituksen historiallista kehitystä ja nykytilaa, mukaan lukien lainsäädäntöä ja standardeja. Keskeiset tulokset olivat tarkistuslistat, jotka käsittelivät teknisiä vaatimuksia, järjestelmän integraatiota, käyttäjähallintaa ja tietoturvaa. Tarkistuslistat on suunniteltu helpottamaan organisaatioiden digitaalisen allekirjoituksen prosessien hallintaa ja kehittämistä.

Työn päätelmissä korostetaan, että digitaalinen allekirjoitus on keskeinen osa liiketoimintaa ja sen käyttö vaatii jatkuvaa päivitystä ja kehitystä. Työn tulokset tarjoavat organisaatioille vankan perustan ja ohjeistuksen digitaalisen allekirjoituksen tehokkaaseen hyödyntämiseen ja haasteiden hallintaan.

Asiasanat

digitaalinen allekirjoitus, käyttöönotto, ylläpito

Abstract

Author(s)	Type of Publication	Published
Jukka Natunen	Thesis, UAS	2023
	Number of Pages	
	26	

Title of Publication

Digital signature

Degree, Field of Study

Engineer (UAS), information and communication engineering

Organisation of the client (if the thesis work is commissioned by another party)

Evitec Oy

Abstract

This thesis focused on quality assurance processes and the development of checklists for digital signature implementation for Evitec Oy. The primary objective was to create universally applicable checklists that support organizations in ensuring the quality and functionality of their digital signature processes. The study utilized both theoretical research and practical application.

The thesis analyzed the historical development and current state of digital signatures, including legislation and standards. Key outcomes included the development of checklists addressing technical requirements, system integration, user management, and cybersecurity. These checklists are designed to facilitate the management and improvement of digital signature processes within organizations.

The conclusions of the work emphasize the integral role of digital signatures in business operations, necessitating continuous updates and advancements. The results provide organizations with a solid foundation and guidance for the effective utilization and management of digital signatures.

Keywords

digital signature, implementation, maintenance

Sisällys

1 Johdanto

Opinnäytetyössä keskitytään digitaalisen allekirjoituksen prosessien laadunvarmistukseen ja tarkistuslistojen kehittämiseen. Digitaalinen allekirjoitus on nykyään keskeinen osa modernia liiketoimintaa tarjoten nopean, turvallisen ja tehokkaan tavan allekirjoittaa asiakirjoja sähköisesti. Työn tarkoituksena on tuottaa yleiskäyttöisiä tarkistuslistoja, jotka auttavat organisaatioita varmistamaan digitaalisen allekirjoituksen prosessien laadukkuuden ja toimivuuden erilaisissa toimintaympäristöissä.

Työ tehdään Evitec Oy:lle, joka on kokenut teknologiayritys Pohjoismaissa. Yritys on perustettu vuonna 1992 ja yli 300 asiantuntijan voimin toimiva yritys on erikoistunut liiketoiminnan modernisointiin tarjoten ohjelmistoratkaisuja, konsultointipalveluita sekä analytiikka- ja tiedonhallintapalveluita. Evitecin asiakaskunta keskittyy pääasiassa finanssialalle. (Evitec 2023.)

Digitaalisten allekirjoitusten käyttöönotto, hallinta ja ylläpito ovat keskeisiä teemoja työssä. Kehitettävät tarkistuslistat tulevat olemaan olennainen työkalu organisaatioille digitaalisen allekirjoituksen tehokkaaseen ja turvalliseen käyttöön. Lisäksi työssä käsitellään mahdollisia mukautuksia ja muutoksia digitaalisen allekirjoitusjärjestelmän prosesseihin, jotka ovat välttämättömiä sen joustavuuden ja toimivuuden varmistamiseksi. Työn tulokset auttavat organisaatioita ymmärtämään ja hallitsemaan digitaalisen allekirjoituksen monimutkaisia haasteita, mikä on olennaista erityisesti nopeasti muuttuvalla finanssialalla.

2 Digitaalisen allekirjoituksen teoria

2.1 Historia ja kehitys

Kryptoanalyytikot Whitfield Diffie ja Martin Hellman esittelivät ensimmäisen kerran digitaalisen allekirjoitusten idean vuonna 1976. Heidän työnsä oli keskeinen askel julkisen avaimen kryptografian alalla, mikä puolestaan loi perustan digitaalisille allekirjoituksille. Diffie ja Hellman julkaisivat merkittävän paperin "New Directions in Cryptography", jossa he esittelivät uusia ideoita ja suuntia kryptografian alalla, mukaan lukien digitaaliset allekirjoitukset. (Lake 2019.)

Ronald Rivest, Adi Shamir ja Len Adleman keksivät vuonna 1977 RSA-algoritmin, mikä oli ensimmäisiä digitaalisen allekirjoituksen järjestelmiä. RSA-algoritmi perustuu kahden suuren alkuluvun tuloon ja se mahdollisti salauksen sekä digitaalisen allekirjoituksen. Algoritmin avulla oli mahdollista luoda digitaalisia allekirjoituksia, jotka osoittivat, kuinka digitaalisia allekirjoituksia voitaisiin käyttää viestien ja dokumenttien aitouden ja eheyden varmistamiseen. (Hovorka 2020; GetAccept 2021.)

Modernin ajan murrokset ja innovaatiot digitaalisissa allekirjoituksissa alkavat oikeudellisista puitteista, jotka mahdollistavat digitaalisten allekirjoitusten laillisen käytön. Vuonna 1999 hyväksytty Uniform Electronic Transactions Act (UETA) ja vuonna 2000 hyväksytty Electronic Signatures in Global and National Commerce Act (ESIGN Act) olivat keskeisiä tekijöitä digitaalisten allekirjoitusten oikeudellisen aseman vahvistamisessa Yhdysvalloissa . (Signix 2023.)

Digitaalisten allekirjoitusten historia ja kehitys heijastavat laajempaa digitaalista evoluutiota ja osoittavat, kuinka teknologiset innovaatiot ja oikeudelliset puitteet ovat yhdessä muovanneet digitaalisen allekirjoituksen kenttää, mikä mahdollistaa luotettavien ja turvallisten digitaalisten transaktioiden toteuttamisen nykypäivänä. (Signix 2023.)

2.2 Digitaalinen allekirjoitus

Digitaalinen allekirjoitus on keskeinen teknologia nykyaikaisessa kryptografiassa tarjoten vahvan mekanismin digitaalisten viestien ja asiakirjojen aitouden sekä eheyden varmistamiseen. Monimutkaisia matemaattisia algoritmeja käyttämällä digitaalinen allekirjoitus luo yksilöllisen tunnisteen, joka on erottamattomasti liitetty kyseiseen viestiin tai asiakirjaan. Tämä prosessi ei ainoastaan varmista tiedon koskemattomuutta sen lähetyksen aikana, vaan myös todentaa allekirjoittajan identiteetin tarjoten näin kaksitahoisen turvallisuuden tason. (Goldwasser & Bellare 2018, 168.)

Digitaalinen allekirjoitus on osa laajempaa Public Key Infrastructure (PKI) -järjestelmää, joka käyttää digitaalisia sertifikaatteja. Nämä sertifikaatit sisältävät julkisen avaimen ja muita tietoja, ja ne ovat digitaalisesti allekirjoitettuja luotettavan tahon, kuten sertifikaatin myöntäjän, toimesta. Tämä järjestelmä mahdollistaa sen, että digitaalisen allekirjoituksen avulla voidaan varmistaa sekä viestin että sen lähettäjän aitous. (Goldwasser & Bellare 2018, 168.)

Käytännössä digitaalinen allekirjoitus syntyy, kun viestin lähettäjä käyttää omaa yksityistä avaintaan viestin allekirjoittamiseen. Tämä allekirjoitus voidaan myöhemmin varmentaa käyttämällä lähettäjän julkista avainta, mikä takaa, että viesti on peräisin todelliselta lähettäjältä ja että viesti ei ole muuttunut allekirjoituksen jälkeen. Tämä ominaisuus on erityisen tärkeä sähköisessä viestinnässä ja digitaalisissa transaktioissa, missä tiedon eheys ja alkuperä ovat kriittisiä. (Goldwasser & Bellare 2018, 168.)

Digitaalisten allekirjoitusten käyttö PKI-järjestelmässä mahdollistaa sen, että käyttäjät voivat vahvistaa toistensa julkiset avaimet käyttämällä luotettujen tahojen, kuten sertifikaatin myöntäjien, allekirjoittamia sertifikaatteja. Tämä lisää merkittävästi järjestelmän luotettavuutta ja turvallisuutta, sillä se minimoi riskin, että käyttäjät luottaisivat väärennettyihin tai muutoin epäluotettaviin julkisiinavaimiin. (Goldwasser & Bellare 2018, 168.)

2.2.1 Ero perinteiseen allekirjoitukseen

Digitaaliset ja perinteiset allekirjoitukset eroavat toisistaan monin tavoin. Perinteinen allekirjoitus on fyysinen allekirjoitus paperilla, kun taas digitaalinen allekirjoitus on elektroninen ja perustuu kryptografisiin algoritmeihin. Digitaalisilla allekirjoituksilla on useita etuja perinteisiin allekirjoituksiin nähden:

- Nopeus ja helppous: Digitaaliset allekirjoitukset voidaan luoda ja jakaa nopeasti ja helposti missä tahansa ja milloin tahansa, kun taas perinteiset allekirjoitukset vaativat fyysisen läsnäolon ja manuaalisen prosessin. (Certifaction 2023.)
- Turvallisuus: Digitaaliset allekirjoitukset luovat dokumentille ainutlaatuisen digitaalisen sormenjäljen kryptografisen teknologian avulla tarjoten parannetun turvallisuuden ja eheyden. Ne ovat myös paljon vaikeampia väärentää verrattuna käsin kirjoitettuihin allekirjoituksiin. (Certifaction 2023.)
- Kustannussäästöt: Digitaaliset allekirjoitukset vähentävät paperin, tulostuksen ja postituksen kustannuksia sekä matkustamis- ja kokoustilaisuuksien kustannuksia, joita perinteiset allekirjoitukset usein vaativat. (Certifaction 2023.)

- Tallennus ja arkistointi: Digitaaliset allekirjoitukset mahdollistavat helpon sähköisen tallennuksen ja arkistoinnin, mikä parantaa dokumenttien arkistointia ja hakuominaisuuksia verrattuna perinteisiin paperipohjaisiin arkistointijärjestelmiin. (LuxTrust 2020.)

Digitaaliset allekirjoitukset tuovat merkittäviä etuja, jotka voivat parantaa organisaatioiden tehokkuutta, tietoturvaa ja yhteistyötä, samalla kun ne vastaavat modernin digitaalisen ympäristön haasteisiin ja vaatimuksiin.

2.2.2 Digitaalisen allekirjoituksen keskeiset osat

Digitaalinen allekirjoitus on nykyaikaisen digitaalisen infrastruktuurin kulmakivi, joka mahdollistaa turvalliset ja luotettavat digitaaliset transaktiot sekä viestinnän. Tämän teknologian ydin koostuu useista keskeisistä osista, jotka yhdessä muodostavat luotettavan järjestelmän digitaalisen luottamuksen ja tietoturvan varmistamiseksi. Seuraavassa tarkastellaan digitaalisen allekirjoituksen neljää keskeistä osaa ja niiden merkitystä. (Cybersecurity & infrastructure security agency 2021.)

- Julkisen ja yksityisen avaimen pari: Digitaalisen allekirjoituksen perustana on julkisen ja yksityisen avaimen pari. Yksityinen avain on allekirjoituksen tekijän hallussa, kun taas julkinen avain on julkisesti saatavilla. Tämä avainpari mahdollistaa viestien tai dokumenttien allekirjoittamisen ja varmentamisen turvallisesti, ja se on kriittinen osa digitaalisen allekirjoituksen mekanismia. (Cybersecurity & infrastructure security agency 2021.)

- Algoritmi: Kryptografiset algoritmit ovat digitaalisen allekirjoituksen ytimessä, ja ne luovat yksilöllisen allekirjoituksen jokaiselle viestille tai dokumentille. Nämä algoritmit käyttävät matemaattisia menetelmiä viestin tiivistämiseen ja allekirjoituksen luomiseen, mikä takaa viestin eheyden ja alkuperän. (Cybersecurity & infrastructure security agency 2021.)

- Sertifikaatti: Digitaaliset sertifikaatit ovat olennainen osa digitaalisen allekirjoituksen ekosysteemiä. Sertifikaatit myöntävät luotettu kolmas osapuoli ja ne vahvistavat allekirjoittajan identiteetin sekä avainten omistajuuden. Sertifikaatit ovat digitaalisen allekirjoituksen luotettavuuden ja oikeellisuuden tae, ja ne ovat välttämättömiä digitaalisen allekirjoituksen toimivuuden kannalta. (Cybersecurity & infrastructure security agency 2021.)

- Tarkistusprosessi: Digitaalisten allekirjoitusten tarkistusprosessi on kriittinen vaihe, joka varmistaa allekirjoituksen ja viestin eheyden sekä allekirjoittajan identiteetin.

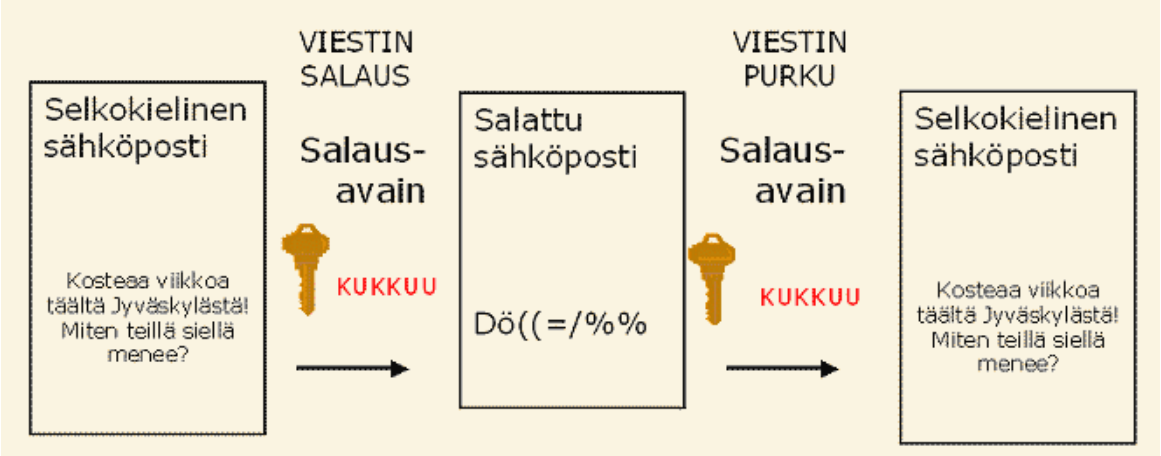
Tämä prosessi käyttää julkista avainta allekirjoituksen varmentamiseen ja tarkistaa, että viesti ei ole muuttunut allekirjoituksen tekemisen jälkeen. (Cybersecurity & infrastructure security agency 2021.)

Näiden osien yhdistelmä muodostaa digitaalisen allekirjoituksen perusrakenteen, joka on keskeinen tekniikka digitaalisen luottamuksen ja tietoturvan alalla. Digitaalinen allekirjoitus on olennainen osa nykyaikaista digitaalista infrastruktuuria, joka mahdollistaa turvalliset ja luotettavat digitaaliset transaktiot ja viestinnän. Se on myös kriittinen tekijä monissa sovelluksissa ja palveluissa, jotka ovat osa digitaalista yhteiskuntaamme. (Cybersecurity & infrastructure security agency 2021.)

2.3 Symmetrinen ja epäsymmetrinen salaus

Salaustekniikat ovat keskeisiä tietoturvan varmistamisessa digitaalisissa ympäristöissä. Salausmenetelmät voidaan jaotella kahteen pääluokkaan: symmetriseen ja epäsymmetriseen salaukseen, joista molemmilla on omat etunsa ja haasteensa.

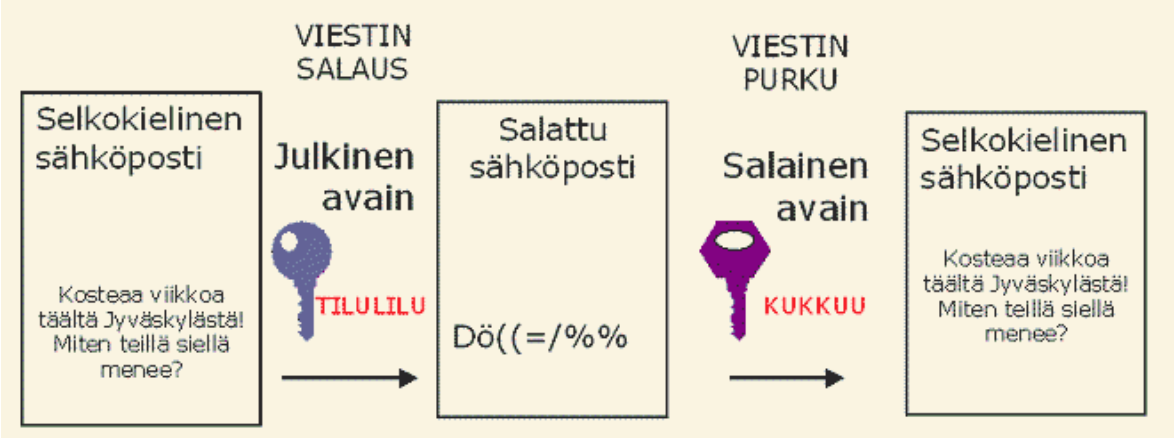
Symmetrisessä salauksessa käytetään samaa salausavainta sekä tiedon salaamiseen että purkamiseen. Tämän salausmenetelmän etuna on sen nopeus ja tehokkuus, mutta samalla se tuo mukanaan haasteita avaimen jakamisessa ja hallinnassa. Jos symmetrinen avain paljastuu, tiedon eheys ja luottamuksellisuus vaarantuvat. Suosittuja symmetrisen salauksen algoritmeja ovat esimerkiksi Advanced Encryption Standard (AES) ja Data Encryption Standard (DES). (Järvinen 2003, 77–78.) Kuviossa 1 havainnollistetaan, miten symmetrinen salaus toimii.



Kuvio 1. Symmetrinen salaus (Heinonen)

Toisin kuin symmetrisessä salauksessa, epäsymmetrisessä salauksessa käytetään kahta erillistä avainta: julkista avainta tiedon salaamiseen ja yksityistä avainta tiedon purkamiseen. Julkinen avain on julkisesti saatavilla, kun taas yksityinen avain pidetään salaisena.

Epäsymmetrinen salaus mahdollistaa turvallisen tiedonvaihdon avoimissa verkoissa, kuten internetissä, ilman, että osapuolten on jaettava salaisia avaimia etukäteen. Epäsymmetrisen salauksen etuna on myös se, että se mahdollistaa digitaalisten allekirjoitusten käytön, jotka varmistavat viestien alkuperän ja eheyden. Suosittuja epäsymmetrisen salauksen algoritmeja ovat esimerkiksi RSA ja Elliptic Curve Cryptography (ECC). (Järvinen 2003, 131–132.) Kuviossa 2 havainnollistetaan, miten epäsymmetrinen salaus toimii.



Kuvio 2. Epäsymmetrinen salaus (Heinonen)

Yhteenvetona, symmetrinen ja epäsymmetrinen salaus ovat molemmat kriittisiä komponentteja digitaalisen tietoturvan ja digitaalisten allekirjoitusten maailmassa. Niiden ymmärtäminen on ensiarvoisen tärkeää, kun tarkastellaan digitaalisia allekirjoituksia ja niiden käyttöä turvallisten digitaalisten järjestelmien rakentamisessa.

2.4 Julkisen avaimen infrastruktuuri (PKI)

Julkisen avaimen infrastruktuuri (PKI) on digitaalisen tietoturvan rakenteellinen perusta, joka mahdollistaa digitaalisten sertifikaattien myöntämisen ja hallinnoinnin, tunnistautumisen ja viestinnän salaamisen internetissä. PKI:n perusajatuksena on epäsymmetrinen salaus, jossa käytetään kahta toisiinsa liittyvää avainta: julkista ja yksityistä avainta. (Järvinen 2003, 165.)

Tämän infrastruktuurin keskiössä ovat seuraavat komponentit ja toimijat:

- Sertifikaatin myöntäjät (Certificate Authorities, CA): Ne ovat luotettuja tahoja, jotka myöntävät ja hallinnoivat digitaalisia sertifikaatteja. CA vahvistaa sertifikaatin hakijan identiteetin ja linkittää julkisen avaimen sertifikaatin haltijaan. (Keyfactor 2023.)
- Rekisteröintiviranomaiset (Registration Authorities, RA): RA:t toimivat CA:n ja sertifikaatin hakijan välillä varmistaen, että hakijalla on oikeus saada sertifikaatti. (Keyfactor 2023.)

- Digitaaliset sertifikaatit: Nämä sertifikaatit sisältävät sertifikaatin haltijan julkisen avaimen ja muita tietoja, kuten sertifikaatin voimassaoloajan ja CA:n digitaalisen allekirjoituksen. (Keyfactor 2023.)
- Avainparit: Jokainen sertifikaatin haltija saa avainparin, joka koostuu julkisesta ja yksityisestä avaimesta. Julkinen avain jaetaan vapaasti, kun taas yksityinen avain pidetään salaisena. (Keyfactor 2023.)
- Sertifikaatin peruutuslistat (Certificate Revocation Lists, CRL): CA ylläpitää listaa peruutetuista sertifikaateista, jotta voidaan varmistaa, että vanhentuneita tai kompromisoituja sertifikaatteja ei käytetä väärin. (Keyfactor 2023.)
- Sertifikaatin varastot: Sertifikaatin varastot ovat tietokantoja, joissa säilytetään ja hallinnoidaan digitaalisia sertifikaatteja ja muita tietoturvaan liittyviä tietoja. (Keyfactor 2023.)

PKI on elintärkeä digitaalisten allekirjoitusten ja monien muiden tietoturvasovellusten kannalta. Se mahdollistaa turvalliset verkkomaksut, salatun sähköpostiviestinnän ja monia muita digitaalisen maailman perustoimintoja. PKI:n ymmärtäminen on välttämätöntä, kun käsitellään digitaalisia allekirjoituksia ja niiden roolia nykyaikaisessa tietoturvassa. (Keyfactor 2023.)

2.5 Allekirjoituksen varmennus ja todentaminen

Digitaalisen allekirjoituksen varmennus ja todentaminen ovat olennaisia toimintoja, joilla varmistetaan allekirjoitettujen digitaalisten dokumenttien eheys ja aitous. Varmennusprosessi keskittyy allekirjoituksen aitouden tarkistamiseen, kun taas todentamisprosessi keskittyy allekirjoittajan henkilöllisyyden varmistamiseen.

Digitaalisen allekirjoituksen varmennuksessa tarkastetaan, että allekirjoituksen mukana tulevat tiedot, kuten aikaleimat ja avaintiedot, ovat oikein ja että allekirjoitus on voimassa. Tämä prosessi käsittää usein monimutkaista laskentaa, jolla varmistetaan, ettei allekirjoitettua dataa ole muokattu allekirjoituksen jälkeen. Varmennus on kriittistä digitaalisten sopimusten ja oikeudellisten dokumenttien käsittelyssä, missä allekirjoituksen aitouden todentaminen on välttämätöntä. (Järvinen 2003, 155.)

Todentamisessa keskitytään allekirjoittajan henkilöllisyyden varmistamiseen. Tämä sisältää usein sähköisen identiteetin, kuten sähköpostiosoitteen tai puhelinnumeron tarkastamisen. Järjestelmät voivat myös hyödyntää lisävarmennusmenetelmiä, kuten kaksivaiheista todennusta, henkilöllisyyden vahvistamiseen. Todentaminen on erityisen tärkeää liiketoimissa, joissa henkilöllisyyden varmistaminen on olennaista. (Järvinen 2003, 33–38.)

Turvallisuus on kriittinen näkökohta varmennus- ja todentamisprosesseissa. Väärinkäytösten ja väärentämisen estämiseksi on tärkeää, että käytetyt järjestelmät ovat luotettavia ja että ne päivitetään säännöllisesti uusimpien tietoturvariskien varalta. Lisäksi organisaatioiden on varmistettava, että käyttämänsä digitaalisen allekirjoituksen ratkaisut noudattavat alueellisia ja kansainvälisiä standardeja. (Järvinen 2003, 110–112.)

Yhteenvetona voidaan todeta, että allekirjoituksen varmennus ja todentaminen ovat kriittisiä toimintoja digitaalisten allekirjoitusten luotettavuuden ja oikeudellisen pätevyyden kannalta. Nämä prosessit auttavat varmistamaan, että digitaaliset sopimukset ja asiakirjat ovat sekä ehtoja että alkuperäänsä koskien aitoja ja luotettavia.

2.6 Digitaalisen allekirjoituksen lainsäädäntö ja standardit

DSS (Digital Signature Standard) on merkittävä standardi, jonka Yhdysvaltain Kansallinen Turvallisuusvirasto kehitti ja Kansallinen Standardien ja Teknologian Instituutti hyväksyi vuonna 1994. DSS käyttää Digitaalisen allekirjoituksen algoritmia (DSA) digitaalisten allekirjoitusten luomiseen, jotka liittyvät yksityisiin ja julkisiin avaimiin. Tämä standardi on ollut keskeinen osa digitaalisten allekirjoitusten teknologista ja lainsäädännöllistä kehitystä, ja se määrittää, miten digitaalisia allekirjoituksia voidaan luoda ja varmentaa teknisesti. (U.S. Department of Commerce 2023.)

eIDAS (Electronic Identification, Authentication, and Trust Services) on Euroopan komission vuonna 2015 hyväksymä säädös, joka pyrkii edistämään elektronisten transaktioiden luottamusta yksilöiden, yritysten ja hallituksen välillä EU:n jäsenvaltioissa. eIDAS-standardi yhdenmukaistaa elektroniset tunnistamisjärjestelmät ja luottamusta lisäävät palvelut, mukaan lukien elektroniset allekirjoitukset, aikaleimat, elektroniset sinetit ja verkkosivuston autentikointi. Tämä on merkittävä askel kohti digitaalisten palveluiden ja sopimusten yhdenmukaistamista Euroopan laajuisesti, ja se edistää rajat ylittävien digitaalisten transaktioiden sujuvuutta ja luotettavuutta. (Euroopan parlamentti ja neuvosto 2014.)

ISO/IEC 20248 on kansainvälinen standardi, joka on suunniteltu digitaalisten allekirjoitusten ja automaattisen tunnistuksen ja tiedonkeruutekniikoiden parissa. Standardi määrittää digitaalisen allekirjoituksen datarakennekaavion ja on sovellusspesifikaatio julkisen avaimen infrastruktuuriin (PKI) digitaalisille allekirjoituksille ja sertifikaateille. Aiemmin vuoden 2018 versio oli vallitseva, mutta se on päivitetty vuoden 2022 versioon, joka jatkaa saman teknisen rakenteen ja sovellusspesifikaation tarjoamista automatisoiduille tunnistuspalveluille. (Iso.)

Euroopan unionissa elektronisten allekirjoitusten lainsäädäntö on yhdenmukaistettu eIDAS-säädöksen kautta. Tämä säädös on ollut voimassa vuodesta 2016 lähtien, ja se

mahdollistaa elektronisten allekirjoitusten käytön rajat ylittävissä sopimuksissa ja transaktioissa ilman laajoja validointiprosesseja. eIDAS-säädös säästää aikaa ja resursseja poistamalla tarpeen resurssi-intensiiviselle validointiprosessille, ja se on edistänyt digitaalisten sopimusten ja transaktioiden sujuvuutta Euroopassa. (Yau 2020.)

Suomessa elektronisten allekirjoitusten käyttö on sallittu ja niiden laillinen asema on tunnustettu. Kuten muissakin EU-maissa, Suomi noudattaa eIDAS-säädöstä, mikä takaa elektronisten allekirjoitusten laillisen aseman ja niiden käytön rajat ylittävissä sopimuksissa ja transaktioissa. Suomen lainsäädäntö ja käytännöt elektronisten allekirjoitusten osalta ovat linjassa EU:n yleisten säädösten ja standardien kanssa. (kyberturvallisuuskeskus 2023.)

2.7 Digitaalisen allekirjoituksen hyödyt ja haasteet

Digitaalisen allekirjoituksen teknologia on merkittävä kehitysaskel sähköisessä viestinnässä ja dokumenttien hallinnassa. Tämän teknologian ansiosta on mahdollista varmistaa dokumentin alkuperä ja eheys digitaalisesti, mikä mahdollistaa paperittoman työskentelyn ja tuo mukanaan useita muita etuja. Samalla digitaalisen allekirjoituksen käyttöönotto tuo mukanaan myös haasteita, jotka liittyvät muun muassa teknologiaan, tietoturvaan ja lainsäädäntöön.

Digitaalinen allekirjoitus tarjoaa turvallisen ja autentikoidun viestin lähetyksen, mikä mahdollistaa lähettäjän tunnistamisen sekä varmistaa, että viestiä ei ole muutettu lähetyksen jälkeen. Tämä on erityisen tärkeää liiketoimintaprosesseissa ja oikeudellisissa yhteyksissä, joissa dokumentin alkuperän ja eheyden varmistaminen on kriittistä. Lisäksi digitaalinen allekirjoitus voi nopeuttaa prosesseja ja vähentää paperityön tarvetta, mikä voi johtaa merkittäviin kustannussäästöihin. Kryptografisen teknologian avulla digitaalinen allekirjoitus varmistaa lähettäjän identiteetin ja suojaa dokumenttia muutoksilta, mikä tarjoaa korkean turvallisuustason. (Hart 2022.)

Toisaalta digitaalisten allekirjoitusten käyttöön liittyy myös haasteita. Teknologian monimutkaisuus voi olla esteenä joillekin käyttäjille, ja se vaatii koulutusta ja tukea laajalle käyttöönotolle. Tietoturva on myös keskeinen huolenaihe, ja digitaalisten allekirjoitusten asianmukainen suojaus on välttämätöntä tietoturvauhkien, kuten haittaohjelmien ja identiteettivarkauksien, estämiseksi. Teknologian nopea kehitys voi myös johtaa siihen, että digitaaliset allekirjoitukset vanhenevat nopeasti, mikä voi vaatia säännöllisiä päivityksiä ja investointeja uuteen teknologiaan. Lainsäädännölliset haasteet ovat myös merkittäviä, sillä digitaalisten allekirjoitusten laillinen asema ja hyväksyntä voivat vaihdella maittain ja alueittain, mikä voi aiheuttaa haasteita erityisesti kansainvälisissä yhteyksissä. (Järvinen 2003, 376–378.)

Yhteenvetona voidaan todeta, että digitaalisten allekirjoitusten hyödyntäminen voi tuoda merkittäviä etuja, mutta samalla se edellyttää huolellista suunnittelua ja valmistautumista teknologisiin, tietoturvaan ja lainsäädännöllisiin haasteisiin. Tämän teknologian ymmärrys ja sen asianmukainen käyttöönotto ovat avainasemassa hyötyjen maksimoinnissa ja riskien minimoimisessa.

2.8 Tulevaisuuden näkymät

Vuonna 2023 digitaalisten allekirjoitusten tulevaisuus näyttää erittäin lupaavalta, sillä alalla odotetaan monia uusia ja innovatiivisia kehitysaskelia. Yksi merkittävä edistysaskel on lohkoketjuteknologian yhdistäminen digitaalisiin allekirjoituksiin. Tämä yhdistelmä tuo mukanaan lisääntyvää luotettavuutta ja varmuutta digitaalisiin allekirjoituksiin, mikä tekee niistä entistä vaikeampia väärentää. Kun dokumentti allekirjoitetaan käyttäen lohkoketjuun perustuvaa digitaalista allekirjoitusta, dokumentin ainutlaatuinen kryptografinen tiiviste tallennetaan lohkoketjuun. Tämä menetelmä varmistaa, että allekirjoitettua dokumenttia ei voi muuttaa tai väärentää ilman, että se huomataan. Tällainen turvallisuuden taso on erityisen arvokas aloilla, kuten oikeudellisessa ja terveydenhuollon sektorilla, joissa dokumenttien eheys on ensiarvoisen tärkeää. (WeSignature 2023.)

Salasanaan perustuvan tunnistautumisen sijaan tulevaisuudessa siirrytään yhä enemmän biometrisiin tunnistautumismenetelmiin. Teknologiat kuten kasvontunnistus, sormenjälkien skannaus ja jopa äänentunnistus tulevat yleisemmiksi allekirjoittajien identiteetin varmistamisessa. Biometrinen tunnistautuminen ei ainoastaan paranna turvallisuutta, vaan myös yksinkertaistaa allekirjoitusprosessia käyttäjille. Nopealla vilkaisulla tai kosketuksella allekirjoittajat voivat vahvistaa identiteettinsä, mikä tekee digitaalisista allekirjoituksista helpommin saavutettavia ja käyttäjäystävällisempiä. (WeSignature 2023.)

Digitaalisten allekirjoitusten markkinan odotetaan kasvavan merkittävästi seuraavan vuosikymmenen aikana. Markkinoiden arvon ennustetaan kasvavan 5,25 miljardista dollarista vuonna 2023 43,14 miljardiin dollariin vuoteen 2030 mennessä, mikä osoittaa alan kasvun voimakkuuden ja laajentumisen mahdollisuudet. (Fortune Business Insights 2023.)

3 Digitaalisen allekirjoituksen käyttöönotto

3.1 Käyttöönoton tarkistuslista

Digitaalisen allekirjoituksen käyttöönotto on monivaiheinen prosessi, joka vaatii huolellista suunnittelua ja tarkkaa toteutusta. Tässä kontekstissa on laadittu tarkistuslista (Liite 1), joka toimii kattavana ohjeistuksena ja tarkistuspisteenä koko käyttöönoton ajan. Tämä tarkistuslista sisältää kriittiset askeleet ja huomioitavat tekijät, jotka varmistavat järjestelmän sujuvan käyttöönoton ja toiminnan eri organisaation toimintaympäristöissä. Alla kuvassa 1 on kuva osasta liitteessä 1 olevasta tarkistuslistasta.

Kuva 1. Digitaalisen allekirjoituksen käyttöönotto tarkistuslista (Liite 1)

Tarkistuslista kattaa eri osa-alueita, kuten sopivan allekirjoitustyypin valinnan, salauksen ja tietoturvan toteutuksen, lainsäädännön noudattamisen sekä käyttäjähallinnan ja tunnistautumisprosessien järjestämisen. Nämä ovat välttämättömiä komponentteja, jotka takaavat digitaalisen allekirjoituksen luotettavuuden, turvallisuuden ja lainmukaisuuden. Lisäksi tarkistuslista sisältää ohjeita järjestelmän integroinnista olemassa oleviin IT-järjestelmiin, testausstrategioita ja koulutuksen suunnittelua käyttäjille.

3.2 Tekniset vaatimukset

Digitaalisen allekirjoitusjärjestelmän tekniset vaatimukset ovat ratkaisevassa asemassa sen onnistuneessa käyttöönotossa. Teknisten vaatimusten huolellinen määrittäminen takaa, että järjestelmä ei ainoastaan vastaa operatiivisia tarpeita, vaan täyttää myös kaikki lainsäädännölliset vaatimukset. Lainsäädännön noudattaminen on erityisen tärkeää digitaalisen tiedon luotettavuuden ja turvallisuuden kannalta. Ensimmäisenä askeleena on valita sopiva allekirjoitustyyppi, jossa yksinkertaisen ja vahvistetun elektronisen allekirjoituksen

välillä punnitaan turvallisuustasoja. Erityisesti yritysympäristöissä korostetaan usein vahvistetun allekirjoituksen merkitystä, sillä se tarjoaa korkeamman turvallisuustason.

Salaus ja tietoturva muodostavat toisen kriittisen teknisen vaatimuksen. Järjestelmän on käytettävä vahvoja salausmenetelmiä tiedon eheyden ja suojauksen varmistamiseksi. Tähän sisältyvät avainten hallinta, sertifikaattien turvallinen säilytys ja tietoliikenteen suojauksen takaaminen. Avainten hallinnan tarkoituksena on varmistaa, että yksityiset avaimet ovat vain asianomaisen henkilön käytössä ja suojattu luvattomalta pääsyltä, kun taas julkiset avaimet ovat laajasti saatavilla. Sertifikaattien säilytys ja hallinta vaativat järjestelmältä luotettavaa infrastruktuuria, joka mahdollistaa sertifikaattien aitouden ja voimassaolon seurannan.

Digitaalisen allekirjoituksen lainsäädännöllinen noudattaminen on olennainen osa teknisten vaatimusten määrittelyä. Digitaalisen allekirjoituksen järjestelmän on vastattava kansallisia ja kansainvälisiä lainsäädännöllisiä vaatimuksia, kuten EU:n eIDAS-asetusta. Tämä asetus määrittelee sähköisten allekirjoitusten laillisuuden ja tunnustamisen EU:n jäsenvaltioissa, mikä on tärkeää erityisesti rajat ylittävissä toiminnoissa. Lainsäädännön noudattaminen varmistaa, että digitaaliset allekirjoitukset hyväksytään oikeudellisesti päteviksi, mikä on olennaista digitaalisten transaktioiden ja viestinnän luotettavuuden kannalta.

Käyttäjähallinnan merkitys teknisissä vaatimuksissa korostuu, kun otetaan huomioon tarve varmistaa, että vain valtuutetut henkilöt voivat luoda allekirjoituksia. Tämä edellyttää kehittyneitä mekanismeja käyttäjien tunnistamiseen ja valtuutusten hallintaan. Organisaation sisäiset käytännöt määrittelevät, kuka voi allekirjoittaa tietyntyyppisiä dokumentteja tai viestejä, ja järjestelmän on pystyttävä tukemaan näitä käytäntöjä luotettavasti. Käyttäjähallinta voi sisältää monivaiheisen tunnistautumisprosessin ja yksilöllisten käyttäjäprofiilien luomisen, jotka sisältävät tarvittavat valtuutukset ja käyttöoikeudet.

Järjestelmän yhteensopivuuden ja integroinnin varmistaminen on viimeinen tärkeä tekninen vaatimus. Digitaalisen allekirjoitusjärjestelmän tulee integroitua saumattomasti olemassa olevaan IT-infrastruktuuriin ja muihin sovelluksiin. API-rajapintojen kehittäminen ja datan siirron protokollien määrittely ovat keskeisiä elementtejä, jotka mahdollistavat tietojen sujuvan siirron ja käytön. Yhteensopivuuden ja integroinnin onnistuminen on ratkaisevaa, jotta digitaalinen allekirjoitusjärjestelmä voi toimia osana laajempaa tietojärjestelmää ja tukea organisaation prosesseja.

3.3 Järjestelmän integraatio ja yhteensopivuus

Kun otetaan käyttöön digitaalinen allekirjoitusjärjestelmä, on ensiarvoisen tärkeää kiinnittää huomiota järjestelmän integrointiin ja yhteensopivuuteen. Tämän prosessin onnistuminen

varmistaa, että uusi teknologia toimii saumattomasti yhdessä olemassa olevien järjestelmien ja prosessien kanssa, mikä on välttämätöntä käyttöönoton sujuvuuden ja tehokkuuden kannalta.

Integraatiomekanismien määrittely ja toteutus muodostavat prosessin perustan. Tämä tarkoittaa käytännössä uuden järjestelmän yhdistämistä olemassa oleviin järjestelmiin siten, että tiedonkulku on esteetöntä ja luotettavaa. Keskeistä on API-rajapintojen kehittäminen, jotka mahdollistavat eri ohjelmistojen ja järjestelmien välisten tietojen vaihdon. Lisäksi on varmistettava ohjelmistoalustojen yhteensopivuus ja määriteltävä datan siirtoon liittyvät protokollat, jotta tiedonsiirto on turvallista ja tehokasta.

Perusteellinen testaus ja mahdollinen pilotointivaihe ovat olennaisia ennen järjestelmän laajamittaista käyttöönottoa. Testausvaiheen aikana arvioidaan järjestelmän toimivuutta ja varmistetaan, että se integroituu oikein muihin järjestelmiin. Pilotointi antaa arvokasta tietoa järjestelmän käytännön toimivuudesta ja mahdollistaa mahdollisten ongelmien tunnistamisen ja korjaamisen ennen täysimittaista käyttöönottoa.

Lisäksi on varmistettava, että uuden järjestelmän integroiminen ei heikennä organisaation tietoturvaa. Tämä tarkoittaa tietoturvan huomioimista sekä teknisellä että hallinnollisella tasolla, mukaan lukien salauksen, käyttäjien todentamisen ja tietoturvakäytäntöjen noudattamisen. Tietoturvan varmistaminen kattaa sekä tekniset että hallinnolliset toimet, kuten salauksen, käyttäjien todentamisen ja tietoturvakäytäntöjen noudattamisen. Tämä on kriittinen vaihe, sillä tietoturvaongelmat voivat aiheuttaa merkittäviä riskejä organisaation toiminnalle ja maineelle.

3.4 Koulutus ja käyttäjien ohjeistus

Käyttäjien koulutus ja ohjeistus ovat olennainen osa uuden teknologian, kuten digitaalisen allekirjoituksen, onnistunutta käyttöönottoa. Tämän vaiheen merkitys korostuu, sillä käyttäjien osaaminen ja ymmärrys ovat avainasemassa järjestelmän tehokkaassa ja turvallisessa hyödyntämisessä. Koulutusprosessin tulee olla kattava ja räätälöity vastaamaan käyttäjien tarpeita ja organisaation vaatimuksia.

Koulutusohjelmien suunnittelu ja toteutus ovat prosessin ydin. Tavoitteena on tarjota käyttäjille perusteellinen käsitys digitaalisen allekirjoituksen periaatteista, käyttötavoista ja parhaista käytänteistä. Tämä sisältää monipuoliset koulutusmuodot, kuten työpajat, webinaarit ja interaktiiviset oppimismateriaalit. Näiden avulla varmistetaan, että käyttäjät saavat tarvittavat tiedot ja taidot järjestelmän tehokkaaseen käyttöön. Koulutuksen tulisi kattaa niin tekniset yksityiskohdat kuin käytännön soveltamiset, ja sen tulisi olla joustavasti saatavilla eri käyttäjäryhmille. Tärkeässä roolissa on myös ohjeistusmateriaalien kehittäminen. On

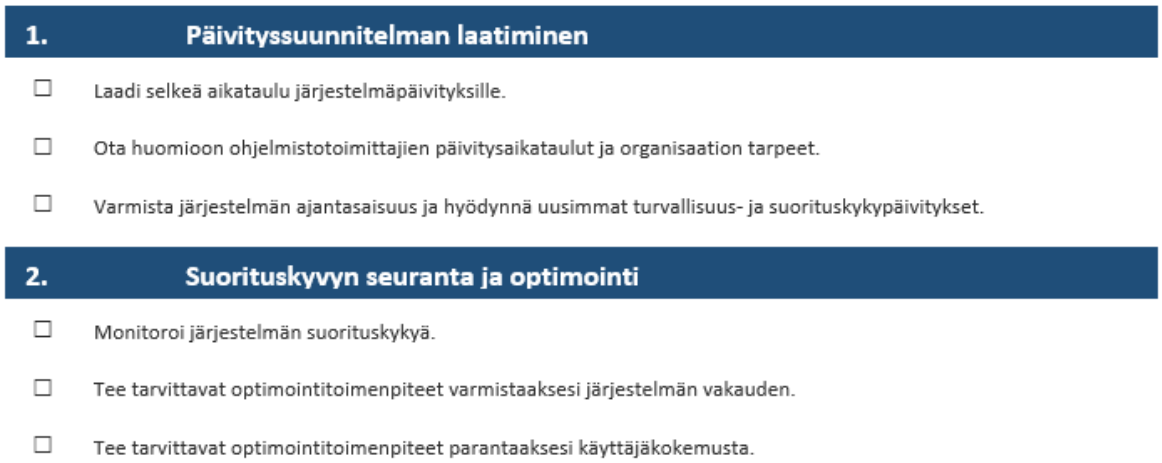
tärkeää luoda selkeitä ja ymmärrettäviä ohjeistuksia, käyttöoppaita ja usein kysyttyjen kysymysten kokoelmia, jotka tukevat käyttäjiä järjestelmän käyttöönoton eri vaiheissa ja tarjoavat nopean viitteen ongelmatilanteiden ratkaisemiseksi. Selkeät ohjeistukset ja dokumentaatio auttavat vähentämään virheitä ja parantamaan käyttäjäkokemusta.

Jatkuva tuki ja koulutuksen päivittäminen ovat välttämättömiä järjestelmän pitkäaikaisen onnistumisen kannalta. Tämä sisältää teknisen tuen ja neuvonnan tarjoamisen käyttäjille, sekä säännöllisen palautteen keräämisen ja analysoinnin. Palautteen perusteella järjestelmää voidaan jatkuvasti parantaa ja koulutusmateriaaleja päivittää vastaamaan muuttuvia tarpeita ja haasteita. Jatkuva tuki ja koulutus varmistavat, että käyttäjät pysyvät ajan tasalla järjestelmän kehityksestä ja muutoksista, mikä edistää sujuvaa ja tehokasta käyttöä. Tämä kokonaisvaltainen lähestymistapa koulutukseen ja ohjeistukseen varmistaa, että digitaalisen allekirjoituksen käyttöönotto onnistuu ja että käyttäjät ovat valmiita hyödyntämään järjestelmää tehokkaasti ja turvallisesti.

4 Digitaalisen allekirjoituksen hallinta ja ylläpito

4.1 Hallinnan ja ylläpidon tarkistuslista

Digitaalisen allekirjoituksen hallinnan ja ylläpidon prosessissa korostuu tarkistuslistan merkitys, jonka avulla varmistetaan järjestelmän kattava ja systemaattinen hallinta. Liitteessä 2 esitelty tarkistuslista kokoaa yhteen kaikki kriittiset toimenpiteet, jotka ovat tarpeen järjestelmän tehokkaan hallinnan ja ylläpidon varmistamiseksi. Tämä lista muodostaa perustan organisaatioiden toiminnalle, tarjoten selkeän ja johdonmukaisen ohjeistuksen järjestelmän seurantaan ja ylläpitoon liittyvissä toimissa. Tarkistuslistan käyttö on olennainen osa strategista lähestymistapaa, jossa painotetaan järjestelmän pitkäaikaista toimintakykyä ja käyttäjien tarpeiden täyttämistä. Alla kuvassa 2 on kuva osasta liitteessä 2 olevasta tarkistuslistasta.



Kuva 2. Digitaalisen allekirjoituksen hallinnan ja ylläpidon tarkistuslista (Liite 2)

Tarkistuslistan hyödyntäminen mahdollistaa hallitun ja johdonmukaisen prosessin, joka takaa järjestelmän luotettavuuden ja turvallisuuden säilymisen. Tämän avulla organisaatio voi varmistaa, että kaikki tarvittavat toimet, kuten suorituskyvyn seuranta, tietoturvan ylläpito ja käyttäjätietojen hallinta, toteutetaan systemaattisesti ja standardien mukaisesti. Tarkistuslistan avulla myös havaitaan ajoissa mahdolliset puutteet ja tarve päivityksille varmistaen järjestelmän joustavuuden ja sopeutumiskyvyn jatkuvasti muuttuvassa teknologisessa ympäristössä.

4.2 Järjestelmän päivitykset ja ylläpito

Hallinnan ja ylläpidon prosessit digitaalisen allekirjoituksen järjestelmässä ovat olennaisia sen pitkäaikaiselle toimivuudelle ja luotettavuudelle. Keskeinen elementti tässä on järjestelmän päivitysten huolellinen suunnittelu ja toteutus. Selkeän päivityssuunnitelman

laatiminen, joka määrittelee järjestelmäpäivitysten säännölliset aikataulut ottaa huomioon ohjelmistotoimittajien tarjoamat päivitysaikataulut ja organisaation omat tarpeet. Päivitysten säännöllinen implementointi varmistaa, että järjestelmä säilyy ajan tasalla, hyödyntäen viimeisimpiä turvallisuus- ja suorituskykypäivityksiä.

Järjestelmän suorituskyvyn aktiivinen seuranta ja tarvittaessa tapahtuva optimointi ovat välttämättömiä järjestelmän tehokkaan toiminnan kannalta. Järjestelmän suorituskykyä monitoroidaan jatkuvasti ja mahdolliset ongelmat ratkaistaan pikaisesti. Tämä ei ainoastaan paranna käyttäjäkokemusta, vaan myös varmistaa järjestelmän luotettavuuden ja vakauden.

Ohjelmistopäivitysten huolellinen testaus ennen niiden käyttöönottoa on myös kriittistä. Tämä prosessi takaa, että uudet päivitykset ovat yhteensopivia olemassa olevan infrastruktuurin kanssa ja ne eivät tuo mukanaan tietoturvariskejä. Päivitysten testaus sisältää yleensä sekä automatisoidut että manuaaliset testit, jotka kattavat laajan kirjon erilaisia käyttötilanteita ja varmistavat päivitysten toimivuuden.

Varmuuskopiointi ja palautusprosessien huolellinen suunnittelu ja toteutus ovat välttämättömiä järjestelmän pitkäaikaisen turvallisuuden kannalta. Säännölliset varmuuskopiot ja tehokkaat palautusprosessit takaavat, että kriittiset tiedot ovat turvassa ja että järjestelmä voidaan palauttaa nopeasti mahdollisissa ongelmatilanteissa. Varmuuskopiointi ja palautus ovat ratkaisevia järjestelmän häiriöttömän toiminnan ja datan eheyden varmistamisessa.

Kokonaisuudessaan nämä hallinnan ja ylläpidon toimenpiteet ovat ratkaisevia digitaalisen allekirjoituksen järjestelmän tehokkaassa toiminnassa. Järjestelmän jatkuva päivitys ja huolellinen ylläpito varmistavat sen ajantasaisuuden, turvallisuuden ja toimivuuden, mikä on keskeistä organisaation digitaalisen allekirjoituksen strategian onnistumisen kannalta.

4.3 Tietoturvan hallinta ja valvonta

Tietoturvan hallinta ja valvonta ovat keskeisiä tekijöitä digitaalisen allekirjoituksen järjestelmän onnistuneessa ylläpidossa. Tietoturvan ylläpito kattaa useita olennaisia toimenpiteitä, jotka varmistavat järjestelmän turvallisen käytön ja sen suojan potentiaalisia uhkia vastaan. Tietoturvariskien säännöllinen arviointi on välttämätön prosessi, jossa tunnistetaan ja arvioidaan mahdolliset turvallisuushaasteet. Tämän perusteella kehitetään toimintasuunnitelmat riskien hallintaan ja niiden vaikutusten minimoimiseen. Tämä sisältää uhkien ennakoinnin, haavoittuvuuksien tunnistamisen ja tarvittavien toimenpiteiden suunnittelun.

Tietoturvakäytänteiden jatkuva päivitys on myös kriittinen osa tietoturvan ylläpitoa. Tämä tarkoittaa, että tietoturvakäytänteet pysyvät jatkuvasti ajan tasalla, ottaen huomioon

uusimmat teknologiset muutokset ja mahdolliset uudet uhkat. Päivitettyjen käytänteiden avulla varmistetaan, että organisaation tietoturvastandardit ovat johdonmukaisia ja että ne noudattavat sekä kansallisia että kansainvälisiä sääntöjä ja määräyksiä.

Tietoturvakoulutuksen tarjoaminen käyttäjille on olennainen osa kokonaisvaltaista tietoturvastrategiaa. Säännöllinen koulutus auttaa käyttäjiä ymmärtämään mahdolliset tietoturvariskit ja opastaa heitä toimimaan turvallisesti digitaalisessa ympäristössä. Koulutuksen tulisi kattaa tietoturvan parhaat käytänteet, käyttäjien vastuut ja ohjeet, kuinka toimia turvallisesti eri tilanteissa. Tällainen jatkuva koulutus ja tietoisuuden ylläpito ovat avainasemassa tietoturvariskien minimoimisessa.

Lisäksi järjestelmän valvonta ja häiriöiden hallinta reaaliajassa ovat olennaisia tietoturvan ylläpidossa. Järjestelmän jatkuva valvonta mahdollistaa häiriöiden nopean havaitsemisen ja niiden korjaamisen, mikä on välttämätöntä, mikäli tietoturvaloukkauksia tai muita ongelmia ilmenee. Reaaliaikainen valvonta yhdistettynä tehokkaaseen häiriöiden hallintaan takaa, että tietoturvaloukkaukset ja muut ongelmat voidaan ratkaista nopeasti minimoiden niiden mahdolliset negatiiviset vaikutukset.

Tehokas tietoturvan hallinta ja valvonta ovat välttämättömiä digitaalisen allekirjoituksen järjestelmän luotettavuuden ja turvallisuuden takaamiseksi. Nämä toimenpiteet varmistavat, että järjestelmä on suojattu nykyisiä ja tulevia uhkia vastaan tarjoten luotettavan ja turvallisen alustan digitaalisen allekirjoituksen prosesseille.

4.4 Käyttöoikeuksien ja käyttäjätietojen hallinta

Digitaalisen allekirjoituksen järjestelmän hallinnassa ja ylläpidossa käyttöoikeuksien ja käyttäjätietojen huolellinen hallinta on keskeistä. Järjestelmän tehokkuus ja turvallisuus riippuvat suurelta osin siitä, miten käyttöoikeudet määritellään ja käyttäjätietoja hallinnoidaan. Selkeiden käytänteiden luominen käyttöoikeuksien määrittelyyn ja hallintaan on tärkeää, varmistaen, että käyttäjät pääsevät käsiksi vain heille tarpeellisiin ja sallittuihin tietoihin. Tämä vähentää väärinkäytön riskiä ja parantaa tietoturvaa. Käyttöoikeuksien hallinta edellyttää myös, että käyttäjäkohtaiset oikeudet ovat johdonmukaisia ja niitä päivitetään säännöllisesti organisaation tarpeiden ja käyttäjien roolien muuttuessa.

Käyttäjätietojen suojaaminen on toinen merkittävä osa-alue, joka sisältää kaikkien käyttäjätietojen suojaamisen ja käsittelyn tietosuojalakien ja -standardien mukaisesti. Tietojen turvaaminen on välttämätöntä, sillä se suojaa sekä yksilöiden yksityisyyttä että organisaation tietovarantoja. Tämä vaatii jatkuvaa valppautta ja päivityksiä tietoturvan käytänteisiin, jotta voidaan varmistaa, että tietojen käsittely on lainmukaista ja turvallista.

Pääsynvalvonta ja auditointi ovat myös olennainen osa käyttöoikeuksien ja käyttäjätietojen hallintaa. Järjestelmän seuranta ja käyttäjien toiminnan auditointi takaavat, että kaikki järjestelmän toiminnot ovat luvallisia ja käytänteiden mukaisia. Tämä prosessi auttaa tunnistamaan mahdolliset poikkeamat tai turvallisuusuhkat nopeasti, mahdollistaen ripeät toimenpiteet niiden ratkaisemiseksi.

Käyttäjätietokannan ajantasaisuuden ylläpitäminen on olennaista digitaalisen allekirjoituksen järjestelmän hallinnassa. Tämä sisältää käyttäjätietojen säännöllisen päivityksen ja tarpeettomien tai vanhentuneiden tietojen poistamisen. Käyttäjätietojen ajantasaisuus varmistaa, että järjestelmä toimii tehokkaasti ja että käyttöoikeudet ovat aina ajan tasalla, mikä on tärkeää sekä käytettävyyden että turvallisuuden kannalta.

Näiden toimenpiteiden yhdistelmä luo vankan perustan digitaalisen allekirjoituksen järjestelmän hallinnalle ja ylläpidolle varmistaen sen turvallisuuden, luotettavuuden ja käyttäjäystävällisyyden. Jatkuva seuranta, päivitykset ja koulutus sekä proaktiivinen lähestymistapa tietoturvaan ja käyttöoikeuksien hallintaan ovat avainasemassa tässä prosessissa.

5 Muutokset ja mukautukset digitaalisessa allekirjoituksessa

5.1 Muutosten ja mukautusten tarkistuslista

Mukautusten prosessissa digitaalisessa allekirjoitusjärjestelmässä keskeinen rooli on Liitteessä 3 esitetyllä tarkistuslistalla. Tämä lista toimii ohjenuorana, joka auttaa organisaatioita tunnistamaan tarvittavat muutokset ja mukautukset järjestelmässään. Tarkistuslistan avulla organisaatiot voivat arvioida ja priorisoida erilaisia muutostarpeita varmistaen, että jokainen toteutettava mukautus on linjassa sekä teknisten mahdollisuuksien että käyttäjien odotusten kanssa. Tarkistuslistan käyttö edistää järjestelmällistä lähestymistapaa muutosten suunnitteluun, mahdollistaen tehokkaan resurssien ja aikataulujen hallinnan. Alla kuvassa 3 on kuva osasta liitteessä 3 olevasta tarkistuslistasta.

1. Mukautettavien ominaisuuksien tunnistaminen

- ☐ Analysoi käyttäjätarpeita ja eri osastojen erityisvaatimuksia.
- ☐ Tunnista ominaisuudet, jotka parantavat järjestelmän käyttäjäystävällisyyttä ja toiminnallisuutta.

2. Lainsäädännön vaatimusten tarkastelu

- ☐ Arvioi mukautusten tarve lainsäädännön, kuten eIDAS-asetuksen ja kansallisten säännösten, näkökulmasta.
- ☐ Varmista, että mukautukset ovat laillisesti päteviä ja täyttävät lainsäädännölliset vaatimukset.

Kuva 3. Digitaalisen allekirjoituksen muutosten ja mukautusten hallinnan tarkistuslista (Liite 3)

Tarkistuslista sisältää muun muassa vaiheet mukautettavien ominaisuuksien tunnistamiseen, lainsäädännön vaatimusten tarkasteluun, teknologian rajoitusten huomioimiseen ja tietoturvan varmistamiseen. Tämän systemaattisen lähestymistavan avulla varmistetaan, että kaikki mukautukset ovat tarpeellisia, toteutettavissa ja turvallisia. Tarkistuslistan käyttö on keskeistä, jotta voidaan varmistaa, että järjestelmän muutokset ja mukautukset tukevat tehokkaasti organisaation tavoitteita ja parantavat sen operatiivista suorituskykyä pitkällä aikavälillä.

5.2 Mukautettavien ominaisuuksien tunnistaminen

Digitaalisessa allekirjoitusjärjestelmässä muutosten ja mukautusten toteuttaminen on tärkeä prosessi, joka varmistaa järjestelmän tehokkuuden ja käyttäjien tarpeiden täyttymisen. Tunnistamalla mukautettavat ominaisuudet, voidaan varmistaa, että järjestelmä palvelee organisaation erityistarpeita mahdollisimman hyvin. Tämä prosessi alkaa käyttäjätarpeiden syvällisellä analysoinnilla. Ymmärtämällä käyttäjäkunnan tarpeet, mukaan lukien eri

osastojen erityisvaatimukset, voidaan suunnitella mukautuksia, jotka tekevät järjestelmästä sekä käyttäjäystävällisen että toiminnallisesti tehokkaan.

Lainsäädännön vaatimusten huomioon ottaminen on myös olennainen osa mukautusprosessia. Arvioimalla, mitkä mukautukset ovat tarpeen lainsäädännön, kuten eIDAS-asetuksen tai kansallisten säännösten, täyttämiseksi, voidaan varmistaa, että järjestelmä ei ainoastaan vastaa organisaation sisäisiä tarpeita, vaan on myös laillisesti pätevä. Tämä on erityisen tärkeää digitaalisten allekirjoitusten kaltaisissa järjestelmissä, joilla on merkittävä rooli laillisissa transaktioissa ja viestinnässä.

Teknologian rajoitusten huomioiminen on olennainen osa mukautusprosessia. Tarkastelemalla olemassa olevan IT-infrastruktuurin ja ohjelmistojen rajoitukset, voidaan suunnitella mukautuksia, jotka ovat toteutettavissa ja yhteensopivia nykyisen teknologisen ympäristön kanssa. Tämä takaa, että mukautukset ovat paitsi teknisesti toteutettavissa, myös taloudellisesti järkeviä ja pitkällä aikavälillä kestäviä.

Tietoturvan varmistaminen kaikissa mukautuksissa on keskeistä digitaalisen allekirjoitusjärjestelmän turvallisuuden ja luotettavuuden kannalta. Kaikkien mukautusten tulee noudattaa korkeimpia tietoturvan standardeja, jotta voidaan varmistaa sekä järjestelmän että sen käyttäjien tietojen turvallisuus. Tietoturvan huomioon ottaminen kaikissa mukautuksissa on välttämätöntä, jotta voidaan säilyttää järjestelmän luotettavuus ja käyttäjien luottamus.

Näiden vaiheiden kautta voidaan varmistaa, että digitaalisen allekirjoitusjärjestelmän muutokset ja mukautukset ovat sekä tehokkaita että turvallisia, ja ne tukevat organisaation tavoitteita ja prosesseja. Mukautettavien ominaisuuksien tunnistaminen ja huolellinen suunnittelu ovat avainasemassa järjestelmän kehityksessä ja sen varmistamisessa, että se vastaa jatkuvasti muuttuvia tarpeita ja ympäristöjä.

5.3 Muutosten suunnittelu ja toteutus

Muutosten suunnittelu ja toteutus digitaalisen allekirjoitusjärjestelmässä ovat monivaiheinen prosessi, joka vaatii tarkkaa suunnittelua ja yhteistyötä eri sidosryhmien kanssa. Aluksi on tärkeää dokumentoida tarkasti muutosvaatimukset. Tämä sisältää mukautusten teknisten yksityiskohtien määrittelyn sekä käyttöönottoaikataulun. Selkeä suunnitelma auttaa varmistamaan, että kaikki muutokset toteutetaan johdonmukaisesti ja aikataulun mukaisesti, mikä on erityisen tärkeää digitaalisten järjestelmien päivittämisessä.

Sidosryhmien sitouttaminen muutosten suunnitteluprosessiin on myös ratkaisevan tärkeää. Tämä tarkoittaa, että IT-tiimin, johdon ja loppukäyttäjien tulee olla mukana suunnittelussa

alusta alkaen. Heidän osallistumisensa takaa, että muutokset vastaavat käyttäjien tarpeita ja organisaation tavoitteita, ja että niiden toteuttamiseen on tarvittava tuki ja resurssit.

Ratkaisujen kehittäminen tunnistettuihin muutostarpeisiin on prosessin seuraava vaihe. Teknisten ratkaisujen kehittäminen vaatii asiantuntemusta ja innovatiivisuutta, jotta voidaan varmistaa, että muutokset eivät ainoastaan vastaa nykyisiä tarpeita, vaan ovat myös kestäviä pitkällä aikavälillä. Tämä vaihe edellyttää tiivistä yhteistyötä teknisten asiantuntijoiden ja järjestelmän käyttäjien välillä, jotta varmistetaan, että ratkaisut ovat käytännöllisiä ja toteuttamiskelpoisia.

Integroinnin ja yhteensopivuuden varmistaminen on viimeinen kriittinen vaihe muutosten suunnittelussa ja toteutuksessa. Tämä tarkoittaa, että muutosten on sovittava sujuvasti yhteen nykyisten järjestelmien ja prosessien kanssa. Integrointiprosessin onnistuminen on elintärkeää, jotta varmistetaan, että muutokset eivät aiheuta häiriöitä organisaation toimintaan. Tämä vaatii huolellista suunnittelua ja testausta, jotta voidaan varmistaa, että uudet ominaisuudet ja toiminnallisuudet toimivat moitteettomasti olemassa olevien järjestelmien kanssa.

Voidaan todeta, että muutosten suunnittelu ja toteutus digitaalisen allekirjoitusjärjestelmässä ovat monimutkaisia, mutta välttämättömiä tehtäviä. Tämä prosessi edellyttää selkeää suunnittelua, sidosryhmien sitoutumista, innovatiivisten ratkaisujen kehittämistä ja huolellista integraatiota, jotta varmistetaan muutosten onnistuminen ja järjestelmän jatkuva tehokkuus ja käytettävyys.

5.4 Testaus ja laadunvarmistus

Digitaalisen allekirjoitusjärjestelmän muutosten ja mukautusten testaus ja laadunvarmistus ovat prosessin kriittisiä vaiheita. Ensimmäinen askel on testaussuunnitelman laatiminen, joka on perusteellinen ja kattava. Tämä suunnitelma kattaa kaikki mukautetut ominaisuudet ja skenaariot, varmistaen, että testausprosessi on kattava ja järjestelmällinen. Tällainen suunnitelma auttaa organisaatiota tunnistamaan ja käsittelemään mahdollisia ongelmia aikaisessa vaiheessa, mikä on elintärkeää järjestelmän luotettavuuden ja suorituskyvyn kannalta.

Testiympäristön luominen on seuraava vaihe, jossa luodaan erillinen, todellisia käyttöolosuhteita mallintava ympäristö. Tämä mahdollistaa uusien ominaisuuksien ja toimintojen testaamisen turvallisessa ympäristössä ilman riskiä olemassa olevan järjestelmän häiriintymisestä. Testiympäristön käyttö tarjoaa mahdollisuuden simuloida erilaisia käyttäjäryhmiä ja käyttötarkoituksia, mikä on ratkaisevan tärkeää järjestelmän kattavuuden ja monipuolisuuden varmistamiseksi.

Testausten suorittaminen on prosessin keskeinen osa, jossa uusia ominaisuuksia testataan eri käyttäjäryhmien ja käyttötapojen mukaisesti. Tämä vaihe takaa, että järjestelmä toimii suunnitellusti eri skenaarioissa ja käyttäjäprofiileissa. Testauksen aikana havaittujen virheiden ja puutteiden korjaaminen on välttämätöntä, ja se vaatii järjestelmällistä lähestymistapaa testitulosten analysointiin ja ongelmien ratkaisemiseen. Tämä varmistaa, että järjestelmä on virheetön ja toimii odotetulla tavalla ennen sen käyttöönottoa.

Laadunvarmistusprosessit ovat ratkaisevan tärkeitä varmistettaessa, että mukautukset täyttävät sekä sisäiset että ulkoiset laatuvaatimukset ja standardit. Laadunvarmistusprosessit takaavat, että järjestelmä ei ainoastaan toimi teknisesti, vaan myös vastaa käyttäjien ja sidosryhmien odotuksia ja vaatimuksia. Tämä vaihe sisältää myös jatkuvan arvioinnin ja seurannan, jotta varmistetaan järjestelmän jatkuva tehokkuus ja luotettavuus sen käyttöönoton jälkeen.

Voidaan todeta, että testaus ja laadunvarmistus ovat elintärkeitä varmistettaessa, että digitaalisen allekirjoituksen järjestelmän muutokset ja mukautukset ovat tehokkaita, turvallisia ja vastaavat organisaation tavoitteita ja prosesseja. Tämä prosessi edellyttää huolellista suunnittelua, perusteellista testausta ja jatkuvaa laadunvarmistusta, jotta voidaan varmistaa järjestelmän korkea laatu ja luotettavuus.

6 Yhteenveto ja johtopäätökset

Opinnäytetyössä keskityttiin digitaalisen allekirjoituksen prosessien laadunvarmistukseen ja tarkistuslistojen kehittämiseen. Työn keskeisenä tavoitteena oli tuottaa yleiskäyttöisiä tarkistuslistoja, jotka auttavat organisaatioita varmistamaan digitaalisen allekirjoituksen prosessien laadukkuuden ja toimivuuden erilaisissa toimintaympäristöissä.

Työn tuloksena syntyi kattava tietopohja digitaalisen allekirjoituksen historiasta, kehityksestä ja teoreettisesta viitekehyksestä. Kryptoanalyytikoiden Whitfield Diffien ja Martin Hellmanin työ sekä RSA-algoritmin kehittäminen muodostivat tärkeän perustan digitaalisten allekirjoitusten ymmärtämiselle. Lisäksi työssä käsiteltiin laajasti digitaalisen allekirjoituksen lainsäädäntöä ja standardeja, kuten DSS, eIDAS ja ISO/IEC 20248, jotka ovat keskeisiä digitaalisten allekirjoitusten käytössä ja hyväksynnässä.

Digitaalisten allekirjoitusten käyttöönottoon ja hallintaan liittyen työssä kehitettiin erityisiä tarkistuslistoja, jotka kattavat tekniset vaatimukset, järjestelmän integraation, käyttäjähallinnan ja tietoturvan hallinnan. Nämä tarkistuslistat tarjoavat organisaatioille konkreettisia työkaluja digitaalisen allekirjoituksen prosessien systemaattiseen arviointiin ja kehittämiseen.

Tulevaisuuden näkymissä korostui digitaalisten allekirjoitusten nopea kehitys, jossa uudet teknologiat kuten lohkoketjut ja biometriset tunnistautumismenetelmät luovat uusia mahdollisuuksia. Tämä kehitys edistää digitaalisten allekirjoitusten luotettavuutta ja käyttäjäystävällisyyttä.

Opinnäytetyössä korostuu, että digitaalinen allekirjoitus on keskeinen osa modernia liiketoimintaa, ja sen tehokas käyttö vaatii jatkuvaa kehitystä ja päivitystä vastaamaan nopeasti muuttuvan teknologisen ympäristön vaatimuksia. Työn tuloksena syntyneet tarkistuslistat tukevat organisaatioita digitaalisen allekirjoituksen prosessien hallinnassa, varmistaen niiden laadun, turvallisuuden ja tehokkuuden.

Opinnäytetyössä kehitetyt digitaalisen allekirjoituksen tarkistuslistat tarjoavat kattavan pohjan organisaatioiden käyttöön, on tärkeää huomata, että nämä järjestelmät eivät ole vielä olleet käytössä. Tämä antaa mahdollisuuden tulevaisuuden kehitykselle, jossa tarkistuslistoja testataan ja mukautetaan todellisissa työympäristöissä, keräten tärkeää palautetta ja kokemuksia sen käytettävyydestä ja toimivuudesta. Tulevissa kehityskohteissa keskitytään erityisesti järjestelmän käytännön implementointiin, käyttäjäkokemuksen parantamiseen ja teknologisen kehityksen mukanaan tuomiin uusiin mahdollisuuksiin. Jatkuvaa kehitystä ja päivitystä tarvitaan varmistamaan, että digitaalisen allekirjoituksen järjestelmät pysyvät ajan tasalla ja pystyvät vastaamaan nykyisiin ja tuleviin haasteisiin tehokkaasti ja turvallisesti.

Johtopäätöksenä voidaan todeta, että organisaatioiden on tärkeää olla perillä digitaalisen allekirjoituksen teknisistä ja lainsäädännöllisistä näkökohdista, ja ottaa käyttöön järjestelmällisiä prosesseja digitaalisen allekirjoituksen tehokkaaksi ja turvalliseksi hyödyntämiseksi. Työn tulokset tarjoavat tähän kattavan perustan ja suuntaviivat, jotka tukevat organisaatioita digitaalisen allekirjoituksen haasteiden kohtaamisessa ja mahdollisuuksien hyödyntämisessä.

Lähteet

Certifaction. 2023. Comparison: eSignature vs. traditional signature. Viitattu 14.10.2023. Saatavissa https://certifaction.com/comparison-esignature-vs-traditional/

Cybersecurity & infrastructure security agency. Understanding Digital Signatures. Viitattu 14.10.2023. Saatavissa https://www.cisa.gov/news-events/news/understanding-digital-signatures

Euroopan parlamentti ja neuvosto. 2014. Electronic Identification, Authentication, and Trust Services. Viitattu 22.10.2023. Saatavissa https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32014R0910

Evitec Oy. 2023. Me olemme evitec. Viitattu 23.11.2023. Saatavissa https://evitec.com/fi/yritys/me-olemme-evitec/

Fortune Business Insights. 2023. Digital signature market. Viitattu 29.10.2023. Saatavissa https://www.fortunebusinessinsights.com/industry-reports/digital-signature-market-10035

GetAccept. 2021. What is the difference between an electronic signature and digital signatures? Viitattu 7.10.2023. Saatavissa https://www.getaccept.com/story-of-esignatures

Goldwasser, S & Bellare, M. 2018. Lecture Notes on Cryptography. Viitattu 14.10.2023. Saatavissa https://cseweb.ucsd.edu/~mihir/papers/gb.pdf

Hart, L. 2022. What are the pros and cons of electronic signatures? Viitattu 27.10.2023. Saatavissa https://www.techtarget.com/searchcontentmanagement/answer/252523027/What-are-the-pros-and-cons-of-electronic-signatures

Heinonen, P. Tiedonsalaaminen. Viitattu 26.11.2023. Saatavissa https://appro.mit.jyu.fi/doc/tiedonsalaus/

Hovorka, D. 2020. 102: The History Of Digital Signatures [Infographic]. Viitattu 7.10.2023. Saatavissa https://www.skillzme.com/102-history-of-digital-signatures-infographic/

Iso. ISO/IEC 20248:2022. Viitattu 29.11.2023. Saatavissa https://www.iso.org/standard/81314.html

Järvinen, P. 2003. Salausmenetelmät. Porvoo: Docendo Finland Oy.

Keyfactor. 2023. What is PKI?. Viitattu 16.10.2023. Saatavissa https://www.keyfactor.com/education-center/what-is-pki/

Kyberturvallisuuskeskus. 2023. Sähköinen allekirjoitus ja muut eIDAS-palvelut. Viitattu 22.10.2023. Saatavissa https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-allekirjoitus-ja-muut-eidas-palvelut

Lake, J. 2019. What are digital signatures and how do they work?. Viitattu 7.10.2023. Saatavissa https://www.comparitech.com/blog/information-security/digital-signatures/

LuxTrust. 2020. Digital archiving vs long-term preservation of e-signatures. Viitattu 14.10.2023. Saatavissa https://www.luxtrust.com/en/news/digital-archiving-vs-long-term-preservation-e-signatures

Maxie, E. 2023. The History of Digital Signatures. Viitattu 7.10.2023. Saatavissa https://visual.ly/community/Infographics/technology/history-digital-signatures

Signix. 2023. The Evolution of Signatures: From Seals to Digital Signatures. Viitattu 7.10.2023. Saatavissa https://www.signix.com/blog/the-evolution-of-signatures-from-seals-to-digital-signatures

Turner, D. 2016. Digital Signature Standards & Compliance - A Global View. Viitattu 20.10.2023. Saatavissa https://www.cryptomathic.com/news-events/blog/major-standards-and-compliance-of-digital-signatures-a-world-wide-consideration

U.S. Department of Commerce. 2023. Digital Signature Standard (DSS). Viitattu 22.10.2023. Saatavissa https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

WeSignature. 2023. The Future of Digital Signatures: Trends and Innovations in 2023. Viitattu 29.10.2023. Saatavissa https://wesignature.com/blog/the-future-of-digital-signatures-trends-and-innovations/

Yau, J. 2020. Electronic Signature Laws Around the World: A Look at eSignature Laws and Requirements by Country. Viitattu 22.10.2023. Saatavissa https://sign.dropbox.com/blog/electronic-signature-laws-around-the-world-a-look-at-esignature-laws-by-country

Liite 1. Digitaalisen allekirjoituksen käyttöönotto tarkistuslista

Digitaalisen allekirjoituksen käyttöönotto tarkistuslista

1. Tekniset vaatimukset

- ☐ Valitse sopiva allekirjoitustyyppi.
- ☐ Varmista salauksen ja tietoturvan toteutus (avainten hallinta, sertifikaattien turvallinen säilytys).
- ☐ Tarkista lainsäädännön noudattaminen.

2. Käyttäjähallinnan järjestäminen

- ☐ Kehitä mekanismeja käyttäjien tunnistamiseen ja valtuutusten hallintaan.
- ☐ Määritä selkeät käytännöt allekirjoitusoikeuksille.
- ☐ Luo monivaiheinen tunnistautumisprosessi ja käyttäjäprofiilit tarvittavine valtuutuksineen.

3. Järjestelmän yhteensopivuuden ja integroinnin varmistaminen

- ☐ Suunnittele ja toteuta integraatiomekanismit olemassa oleviin järjestelmiin.
- ☐ Kehitä API-rajapintoja ja määritä datan siirron protokollat.
- ☐ Varmista ohjelmistoalustojen yhteensopivuus.

4. Järjestelmän testaus ja pilotointi

- ☐ Suorita kattava testaus uudelle järjestelmälle.
- ☐ Organisoi mahdollinen pilotointivaihe.
- ☐ Arvioi järjestelmän toimivuus ja yhteensopivuus.

5. Tietoturvan integroiminen ja varmistaminen

- ☐ Tarkista, että integraatio ei heikennä tietoturvaa.
- ☐ Huomioi salaus, käyttäjien todentaminen ja tietoturvakäytännöt.

6. Koulutusohjelman suunnittelu ja toteutus

- ☐ Suunnittele kattavat koulutusohjelmat.
- ☐ Järjestä työpajoja, webinaareja ja luo interaktiivisia oppimismateriaaleja.

7. Ohjeistusmateriaalien luominen

- ☐ Kehitä selkeitä ohjeistuksia, käyttöoppaita ja usein kysyttyjä kysymyksiä.
- ☐ Päivitä ohjeistusmateriaalit säännöllisesti.

8. Jatkuva tuki ja koulutuksen päivittäminen

- ☐ Tarjoa tekninen tuki ja neuvoja käyttäjille.
- ☐ Kerää ja analysoi palautetta järjestelmän kehittämisen tueksi.

Liite 2. Digitaalisen Allekirjoituksen hallinta ja ylläpidon tarkistuslista

Digitaalisen allekirjoituksen hallinnan ja ylläpidon tarkistuslista

1. Päivityssuunnitelman laatiminen

- ☐ Laadi selkeä aikataulu järjestelmäpäivityksille.
- ☐ Ota huomioon ohjelmistotoimittajien päivitysaikataulut ja organisaation tarpeet.
- ☐ Varmista järjestelmän ajantasaisuus ja hyödynnä uusimmat turvallisuus- ja suorituskykypäivitykset.

2. Suorituskyvyn seuranta ja optimointi

- ☐ Monitoroi järjestelmän suorituskykyä.
- ☐ Tee tarvittavat optimointitoimenpiteet varmistaaksesi järjestelmän vakauden.
- ☐ Tee tarvittavat optimointitoimenpiteet parantaaksesi käyttäjäkokemusta.

3. Ohjelmistopäivitysten testaus

- ☐ Testaa uudet päivitykset huolellisesti ennen niiden käyttöönottoa.
- ☐ Varmista päivitysten yhteensopivuus ja tietoturva.

4. Varmuuskopiointi ja palautusprosessit

- ☐ Laadi varmuuskopiointi- ja palautussuunnitelma.
- ☐ Tee säännöllisiä varmuuskopioita kriittisistä tiedoista.
- ☐ Varmista nopea palautuminen mahdollisissa ongelmatilanteissa.

5. Tietoturvariskien arviointi

- ☐ Arvioi säännöllisesti mahdolliset tietoturvariskit.
- ☐ Kehitä toimintasuunnitelmat riskien hallintaan.

6. Tietoturvakäytänteiden päivittäminen

- ☐ Pidä tietoturvakäytänteet ajan tasalla uusimpien uhkien ja teknologian muutosten suhteen.
- ☐ Varmista, että käytänteet noudattavat kansallisia ja kansainvälisiä sääntöjä.

7. Tietoturvakoulutus käyttäjille

- ☐ Tarjoa säännöllistä koulutusta tietoturvan parhaista käytännöistä.
- ☐ Opasta käyttäjiä toimimaan turvallisesti digitaalisessa ympäristössä.

8. Valvonta ja häiriöiden hallinta

- ☐ Valvo järjestelmää reaaliajassa häiriöiden havaitsemiseksi.
- ☐ Hallitse tehokkaasti tietoturvaloukkauksia ja muita ongelmia.

9. Käyttöoikeuksien määrittämine

- ☐ Laadi selkeät käytännöt käyttöoikeuksien määrittelyyn.
- ☐ Varmista, että käyttäjillä on pääsy vain tarpeellisiin tietoihin.

10. Käyttäjätietojen suojaaminen

- ☐ Suojaa kaikki käyttäjätiedot tietosuojalakien ja -standardien mukaisesti.
- ☐ Pidä tietoturvakäytännöt ajan tasalla.

11. Pääsynvalvonta ja auditointi

- ☐ Valvo ja auditoi käyttäjien toimintaa järjestelmässä.
- ☐ Varmista, että kaikki toiminnot ovat luvallisia ja käytänteiden mukaisia.

12. Käyttäjätietojen päivittäminen ja poistaminen

- ☐ Pidä käyttäjätietokanta ajantasaisena.
- ☐ Poista vanhentuneet tai tarpeettomat käyttäjätiedot asianmukaisesti.

Liite 3. Digitaalisen allekirjoituksen muutosten ja mukautusten hallinnan tarkistuslista

Digitaalisen allekirjoituksen muutosten ja mukautusten hallinnan tarkistuslista

1. Mukautettavien ominaisuuksien tunnistaminen

- ☐ Analysoi käyttäjätarpeita ja eri osastojen erityisvaatimuksia.
- ☐ Tunnista ominaisuudet, jotka parantavat järjestelmän käyttäjäystävällisyyttä ja toiminnallisuutta.

2. Lainsäädännön vaatimusten tarkastelu

- ☐ Arvioi mukautusten tarve lainsäädännön, kuten eIDAS-asetuksen ja kansallisten säännösten, näkökulmasta.
- ☐ Varmista, että mukautukset ovat laillisesti päteviä ja täyttävät lainsäädännölliset vaatimukset.

3. Teknologian rajoitusten huomioiminen

- ☐ Arvioi olemassa olevan IT-infrastruktuurin ja ohjelmistojen rajoitukset.
- ☐ Suunnittele mukautukset, jotka ovat teknisesti toteutettavissa ja taloudellisesti järkeviä.

4. Tietoturvan varmistaminen

- ☐ Varmista, että kaikki mukautukset noudattavat korkeimpia tietoturvan standardeja.
- ☐ Ylläpidä järjestelmän ja käyttäjien tietojen turvallisuutta kaikissa mukautuksissa.

5. Muutosvaatimusten dokumentointi

- ☐ Laadi yksityiskohtainen suunnitelma mukautuksista, sisältäen tekniset yksityiskohdat ja käyttöönottoa-ikataulun.

6. Sidosryhmien sitouttaminen

- ☐ Varmista, että IT-tiimi, johto ja loppukäyttäjät ovat mukana suunnitteluprosessissa.
- ☐ Rakenna yhteistyötä ja kommunikaatiota kaikkien sidosryhmien kesken.

7. Ratkaisujen Kehittäminen

- ☐ Kehitä teknisiä ratkaisuja, jotka vastaavat tunnistettuihin muutostarpeisiin.
- ☐ Varmista ratkaisujen pitkäaikainen kestävyys ja käytännöllisyys.

8. Integroinnin ja Yhteensopivuuden Varmistaminen

- ☐ Huolehdi, että muutokset integroituvat sujuvasti nykyisiin järjestelmiin.

- ☐ Testaa uudet ominaisuudet ja toiminnot varmistaaksesi niiden yhteensopivuuden.

9. Testaussuunnitelman laatiminen

- ☐ Laadi kattava testaussuunnitelma, joka kattaa kaikki mukautetut ominaisuudet ja skenaariot.

10. Testiympäristön luominen

- ☐ Luo erillinen testiympäristö, joka mallintaa todellisia käyttöolosuhteita.
- ☐ Varmista, että testaus tapahtuu turvallisessa ja kontrolloidussa ympäristössä.

11. Testausten suorittaminen

- ☐ Testaa uudet ominaisuudet eri käyttäjäryhmien ja käyttötapojen mukaisesti.
- ☐ Tunnista ja korjaa havaitut virheet ja puutteet.

12. Laadunvarmistusprosessit

- ☐ Varmista, että mukautukset täyttävät sekä sisäiset että ulkoiset laatuvaatimukset.
- ☐ Suorita jatkuva arviointi ja seuranta varmistaaksesi järjestelmän laadun ja luotettavuuden.