Laki julkisen hallinnon tiedonhallinnasta, luonnos 13.10.2020 Suosituskortti	B
14 § 1 mom Vastaanottajan tunnistaminen	versio 0.9

	14 § 1 mom kohta 2 Vastaanottajan tunnistaminen Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja.
	Perustelumuistio https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx
	Laki digitaalisten palvelujen tarjoamisesta 306/2019
	Vastaanottajan tunnistaminen riittävän tietoturvallisella tavalla määrittyy käyttötapausten mukaan. (Viranomais-) organisaatioiden sisäinen ja välinen tietojensiirto Lähtökohtaisesti tiedon vastaanottaja (ja pääsääntöisesti myös lähettäjä) tulisi tunnistaa vahvasti. Mikäli kyseessä on tietojärjestelmien välinen tietojen siirto, tapahtuu tämä tyypillisesti varmenteiden (sertifikaattien) avulla. Ihmisen ja tietojärjestelmän välillä vahva tunnistautuminen tapahtuu tyypillisesti monivaiheisella tunnistautumisella (*Multi-Factor Authentication, MFA*), jossa heikon käyttäjätunnus-salasana-parin lisäksi on yksi tai useampia tunnistavia tekijöitä, kuten fyysinen laite, (verkko)sijainti tai PIN-koodi matkapuhelinliittymään. Vastaavalla logiikalla heikkoja tietojärjestelmien välisiä tunnistamisratkaisuja (esimerkiksi API Key) voidaan vahvistaa yhdistämällä ne esimerkiksi tietoliikenteen HTTPS-salaukseen sekä IP-osoiterajoituksiin. Heikkoa tunnistamista, kuten pelkkää käyttäjätunnus-salasana-paria tai pelkkää palomuurin IP-osoiterajoitusta ei tulisi käyttää yleisissä tietoverkoissa ollenkaan. Yleisölle tarjottavat digitaaliset palvelut Laissa digitaalisten palvelujen tarjoamisesta (306/2019) todetaan, että salassa pidettäviä tietosisältöjä käsitelläkseen käyttäjän tulee tunnistautua vahvasti, mutta perustelluista syistä voidaan riskiperusteisesti käyttää myös muuta tunnistustapaa, kuten käyttäjätunnus-salasana-paria. Lähtökohtaisesti salassa pidettäviä tietoja käsiteltäessä kansalaisten vahva tunnistautuminen kannattaa toteuttaa Suomi.fi-tunnistuspalvelun avulla. Heikkoa tunnistautumista käytettäessä tulee ymmärtää, että sillä ei saavuteta sähköisen allekirjoituksen vaatimuksia, että käsiteltäväksi annettu tieto ei saa olla salaista ja että palvelulla ei saa olla merkittäviä oikeudellisia vaikutuksia käyttäjän etuihin, oikeuksiin tai velvollisuuksiin. Heikkoja tunnistautumistapoja ovat esimerkiksi käyttäjätunnus-salasana-pariin tai sosiaalisen median alustojen (esimerkiksi Facebook) tunnistautumiseen perustuvat.
	[Työkaluja ei suunnitella vielä tässä vaiheessa, mutta jos tällaisia sattuu suoraan olemaan, niin voidaan mainita] • https://azure.microsoft.com/en-us/resources/security-best-practices-for-azure-solutions/