Kuntasektorin arkkitehtuuriryhmä

Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri

Versio 1.0

Pääsynhallinta, provisiointi, tunnistautuminen ja kertakirjautuminen esimerkkiskenaarioita

Helsinki 2013

Kuntaliitto
Kommunförbundet

Sisältö

Johdanto

Tämä kuvaus on tarkoitettu käytettäväksi ohjeena mietittäessä kunnan toimintaan sopivia toimintamalleja kertakirjautumisen ja pääsynhallinnan sekä federoinnin ratkaisua tunnistettaessa.
Tavoitteena on tyyppitapauskuvausten avulla auttaa kuntaa tunnistamaan omaan ympäristöönsä sopivat vaihtoehtoiset toimintamallit.
Kuvaus on toteutettu liitteeksi kuntasektorin käyttövaltuushallinnan viitearkkitehtuuriin.

Taustaa

2.1 Lähtökohdat

Käyttövaltuushallinnan- KVH (IAM) -palvelun avulla kunnat voivat hallita käyttäjä- ja käyttövaltuustohallinnon prosesseja ja pienentää merkittävästi näihin käytettävää työmäärää organisaation eri osissa
Palvelun avulla:

- voidaan jakaa ja monistaa käyttäjähallinnan pääprosesseja ja roolimalleja
- voidaan toteuttaa korkean käytettävyyden käyttäjähakemisto jaetuin kustannuksin
- mahdollistetaan kustannustehokkaasti myös pienille kunnille 24/7-palvelu käyttäjähallinnan keskeisille komponenteille yhteisestä valvontapisteestä
- saadaan kuntatoimialalle yhtenäinen käyttäjävaltuuksien jakelutapa, mikä tehostaa uusien sovellusten hankintaa ja liittämistä

Käyttövaltuushallinta- (IAM) muodostuu osakokonaisuuksista (erillisistä järjestelmäpalveluista):
eSSO- – kertakirjautuminen, enterprice Single Sign On

- kertakirjautuminen sovelluksiin hallitaan palvelun avulla
- ei muutoksia käyttäjähallintaan

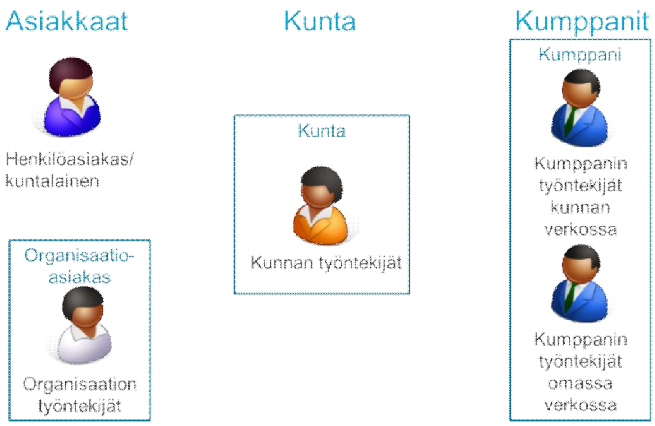
IdM– identiteetinhallinta, Identity Management

- tietojen synkronointi järjestelmien välillä
- käyttäjien aktivointi ja liittäminen palveluun
- hyväksymisprosessit ja valtuutus
- liittyminen ulkoisiin hakemistoihin

2.2 Käyttäjät /Roolit ylätasolla

Karkealla tasolla kunta ja sen ympärillä toimivat tahot ja käyttäjät (kuva alla) voidaan jakaa seuraaviin ryhmiin:

1. Asiakkaat:
    - henkilöasiakkaat,
    - Organisatioasiakkaisiin / sen työntekijöihin
2. Kunta
    - kunnan sisäiset työntekijät
3. Kumppanit
    - kumppanin työntekijät kunnan verkossa
    - kumppanin työntekijät omassa verkossaan



Kuva x: Kunnan ympärillä toimivat käyttäjät karkeasti ryhmiteltynä.

Ryhmä	Käyttäjä	Kuvaus
Asiakkaat	henkilöasiakas	Kunnan kanssa asioiva tai asioita hoitava/puolesta asioiva henkilö: • kuntalainen • ei-kuntalainen • jne.
	Organisaatioasiakas	Kunnan kanssa asioiva/asioita hoitavan organisaation työntekijä/jäsen. Organisaatioita voivat olla esimerkiksi • urheiluseurat • rakennusliikkeet, • mikä tahansa yritys tai yhdistys jne.
Kunta	Kunnan työntekijä	kunnan työntekijä: • kunnan virkamies • työsuhteinen työtekijä jne.)
	Muu kunnan toimija	Kunnan muu edustaja: • luottamushenkilö jne. kunnan käyttöoikeusverkkoa hyödyntävän organisaation työntekijät/jäsenet: • oppilas • tytäryhtiön työntekijä jne.
Kumppanit	Kumppanin työnteki-	Kunnalle tai kunnan puolesta palveluita tarjoavan/tuottavan organisaation työntekijä/jäsen, joka käyttää näiden tehtävien hoitamiseen kun-

	jä kunnan verkossa	nan käyttöoikeusverkkoa. Esimerkiksi: • vuokratyövoima • keikkalääkäri • räätälisovelluksen kehittäjä jne. Tällainen kumppanin työntekijä hyödyntää usein runsaasti kunnan tarjoamia tietojärjestelmäpalveluita.
	Kumppanin työnteki- jä omassa verkos- saan	Kunnalle tai kunnan puolesta palveluita tarjoavan/tuottavan organisaation työntekijä/jäsen, joka käyttää näiden tehtävien hoitamiseen pääasiassa oman organisaationsa käyttöoikeusverkkoa. Tällaisia kumppaneita voivat olla esimerkiksi • yksityinen päiväkoti • yleishyödyllisen organisaation hoitokoti • ruokapalveluita tuotava yritys • tietojärjestelmätoimittajan pääkäyttäjä jne. Tällainen kumppanin työntekijä hyödyntää yleensä kunnan tarjoamia tietojärjestelmäpalveluita vain vähäisissä määrin.

Toimintamalliskenaariot

Tässä luvussa on kuvattu tärkeimpiä käyttövaltuushallintaan kuuluvia tyyppitapauksia sekä erilaisia toimintamalleja, joilla tyyppitapauksen tavoitteisiin päästään. Kuvaukset selventävät tietojärjestelmäpalveluiden välisiä vastuita kuvaamalla niiden välillä kulkevat tietovirrat. Tyyppitapausten ja erilaisten toimintatapojen luettelot eivät ole kumpikaan tyhjentävän kattavia, mutta ne pyrkivät tuomaan esille ainakin keskeisimpiä vaihtoehtoja jatkokeskusteluiden ja -työn pohjaksi.
Tyyppitapauksissa esiintyvät tietojärjestelmäpalvelut voivat olla millä tahansa tavalla toteutettu. Esimerkiksi ”kunnan käytössä oleva käyttövaltuuksien ja identiteetinhallinta” voi olla kunnan omistama ja ylläpitämä tietojärjestelmäpalvelu tai kunnan palveluna ostama tietojärjestelmäpalvelu.

Kunnan työntekijät ja Kumppanin työtekijät kunnan verkossa
Tässä luvussa termillä työntekijä tarkoitetaan kahta käyttäjäryhmää:
- kunnan työntekijöitä
- kumppanin työntekijöitä kunnan verkossa.

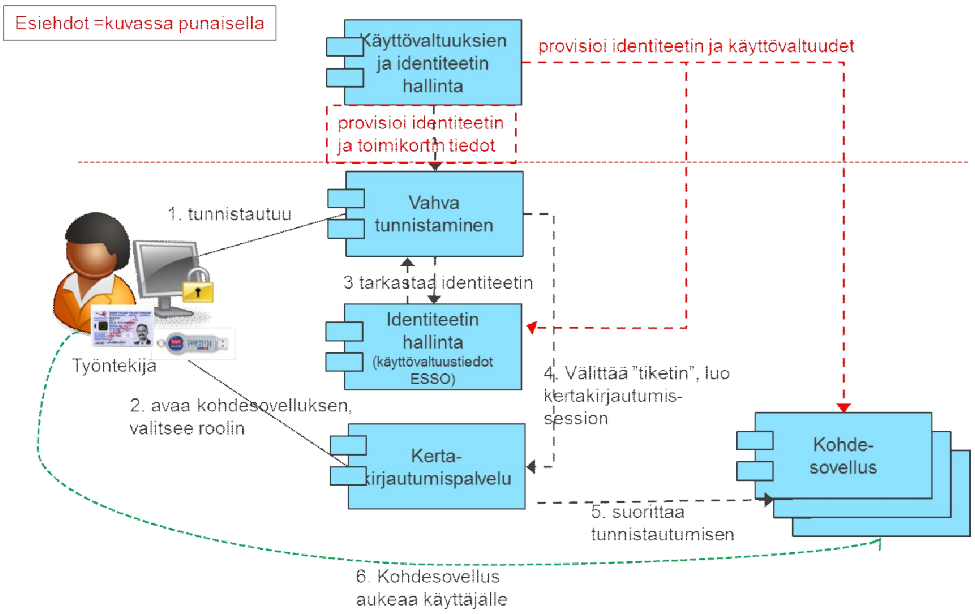
Federoiduissa toimintamalleissa Identity providerit, Service Providerit on esitetty selvyyden vuoksi yksinkertaisimman mallin mukaisina eli ne ovat kaikki kunnan käyttöönsä hankkimia (ostamalla tai palveluna).
Kun ryhdytään käyttämään ulkopuolisia Identity ja Service providereita toimintamallit muuttuvat samanlaisiksi kuin asiakaskäyttäjien tyyppitapauksissa on kuvattu.

3.1 Kunnan työntekijät ja kumppanit kunnan verkossa

Työntekijä kertakirjautuu sovellukseen

Tavoitteena kertakirjautuminen. Kertakirjautuminen edellyttää puolestaan vahvaa tunnistusta. Vahvan tunnistuksen tavoista toimikortit ovat ensisijainen ratkaisu. Toimikortilla tunnistetaan käyttäjä. Käyttäjälle on annettu oikeudet. Käyttäjälle voidaan myöntää myös väliaikainen toimikortti, jolloin käyttäjän tunnistus voidaan tehdä väliaikaisella toimikortilla. Juuri väliaikaisten toimikorttien takia käyttäjä pitää pystyä tunnistamaan usealla eri tavalla ja käyttövaltuuksien tulee olla ripustettuna käyttäjään – ei toimikorttiin.

3.1.1 Kertakirjautuminen kertakirjautumistietojärjestelmäpalvelun (ESSO) avulla



Kuva x: Työntekijä kertakirjautuu sovellukseen kertakirjautumisjärjestelmäpalvelun kautta (eSSO)

Esiehdot:

Työntekijän käyttövaltuudet ja identiteetti on provisioitu käyttövaltuuksien hallinnasta (luvitusprosessi) kertakirjautumistietojärjestelmäpalveluun sekä kohdejärjestelmiin. Käyttäjän identiteetti ja toimikortin tiedot on provisioitu vahvan tunnistuksen tietojärjestelmäpalveluun.

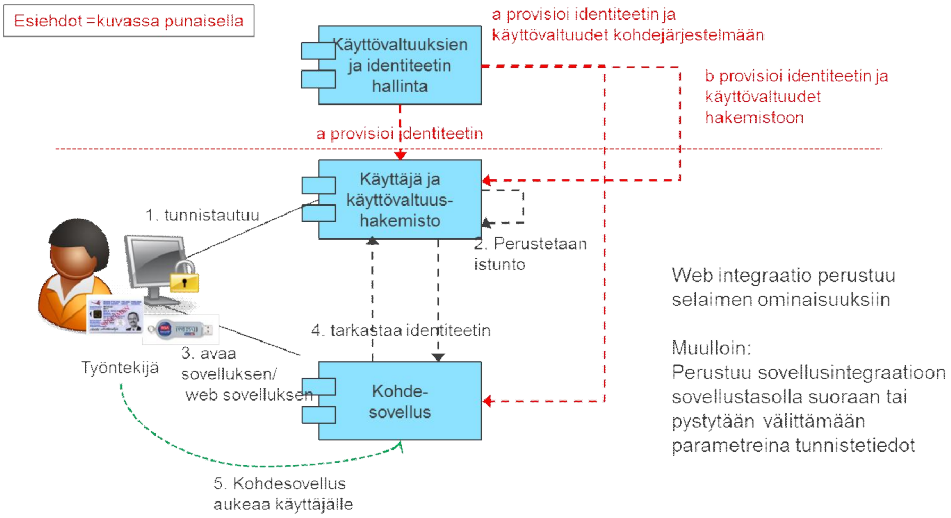
1. Käyttäjä tunnistautuu vahvasti ja vahva tunnistus tarkastaa käyttäjän tunnistautumisen valittua tunnistautumistapaa vasten ja välittää käyttäjän tiedot identifiointipalvelulle.
2. Käyttäjä avaa kohdesovelluksen kertakirjautumispalvelun avulla ja valitsee työroolin
3. Identifiointipalvelu (identiteetinhallinta) tarkastaa tunnistustietoja vasten käyttäjän identiteetin käyttövaltuushakemistosta. Käyttövaltuushakemistosta palautuvat tarvittavat identiteetti- ja valtuustiedot (tunnistusseloste).
4. Kertakirjautumisen sessio luodaan

5. Kertakirjautumispalvelu suorittaa tunnistautumisen kohdesovellukseen käyttäjän puolesta (usein syöttää käyttäjän käyttäjätunnuksen ja salasanan).
6. Kohdesovellus aukeaa käyttäjälle

Hyvät ja huonot puolet:

+ ei vaadi muutoksia kohdesovelluksiin
+ toimii useiden sovellusteknologioiden kanssa (Windows, Java, web, pääte-emulaattorit jne.)
+ mahdollistaa ns. kioski-moodin yhteiskäyttöisillä työasemilla
- Edellyttää kertakirjautumissovelluksen hankintaa ja käyttöönottoa

3.1.2 (Web) Kertakirjautuminen hakemistointegraation (esim paikallinen hakemisto) avulla



Kuva x: Kertakirjautuminen (myös Web) hakemistointegraation (esim.paikallinen hakemisto) avulla. Työntekijä kirjautuu sovellukseen

Esiehdot:

Työntekijän käyttövaltuudet ja identiteetti on provisioitu käyttövaltuuksien hallinnasta (luvitusprosessi) käyttäjä- ja käyttövaltuushakemistoon. Käyttövaltuuksien suhteen on tehty toinen seuraavista

- (a) identiteetti- ja käyttövaltuustiedot on provisioitu kohdesovellukseen.
- (b) käyttövaltuudet on provisioitu hakemistoon.

1. Käyttäjän työasematunnistautuminen tehdään käyttäjä- ja käyttöoikeushakemistoa vasten.
2. Käyttäjälle perustetaan istunto hakemistoon.
   - hakemisto pitää kirjaa, ketkä ovat kirjautuneet ja mitä oikeuksia heillä on
   - hakemistolta voidaan kysyä käyttäjän oikeuksia, tiketin voimassaoloa
3. Käyttäjä avaa kohdesovelluksen/ Web sovelluksen.
4. a. Työasema antaa käyttäjän identiteetin kohdesovellukselle. Kohdesovellus tarkastaa käyttäjän identiteetin hakemiston istuntoa vasten. Käyttövaltuudet sovellus

saa omasta kannastaan.
b. Työasema välittää käyttäjän identiteetin kohdesovellukselle, joka tarkastaa käyttäjän identiteetin hakemiston istuntoa vasten sekä hakee käyttövaltuudet hakemistosta.

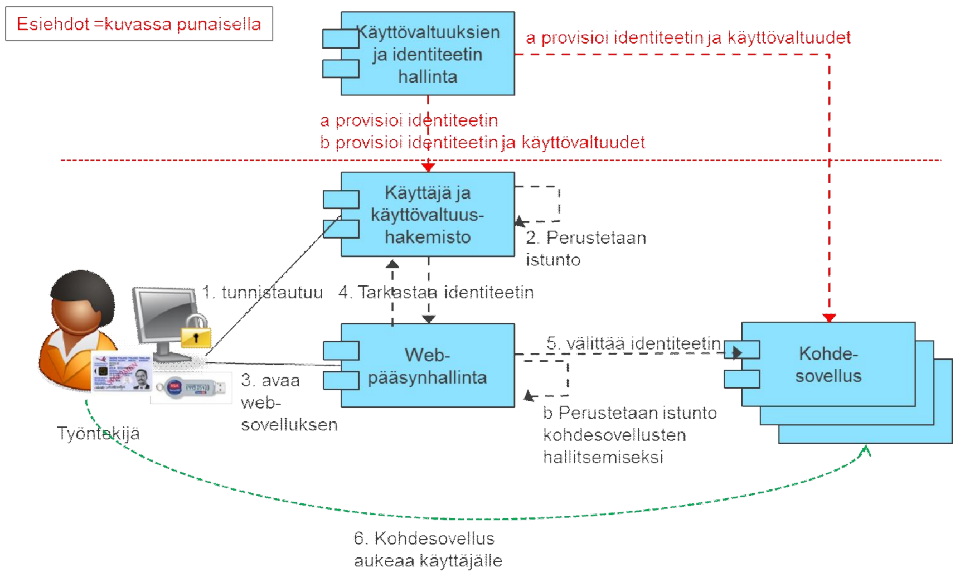
5. Kohdesovellus avautuu käyttäjälle.

Hyvät ja huonot puolet:
+ ei vaadi yleensä uusien tietojärjestelmäpalveluiden hankkimista
- kohdesovellus on integroitava käyttövaltuushakemistoon (sovelluksessa on oltava tämä ominaisuus valmiina tai se on rakennettava sovellukseen)
- hakemiston hallinta ja lähtötilanteen analysointi pitää hoitaa ulkoisella menettelyllä (tikettijärjestelmä, sähköposti) jolloin raportointi ja valvonta ei välttämättä järjestelmällistä tai tehokasta.

Kertakirjautuminen suoraan:
- toimii suppeamman sovellusteknologiajoukon kanssa (Windows verkko, web palvelut rajatusti -oman hakemiston ulottuvissa)
- kioski-moodi ei välttämättä toimi näin toteutetun kirjautumisen kanssa tai vaatii erillistä sovitustyötä (riippuu kioski-moodin toteutuksesta)

Web kertakirjautuminen:
- toimii vain käyttäjä- ja käyttövaltuushakemiston tunnistautumiseen nojaavissa päätelaitteissa
- toimintatapaa ei ole standardi ja tuki löytyy vain tietyissä selaimissa ja palvelinohjelmistoissa
- jokaiseen sovellukseen joudutaan rakentamaan kertakirjautuminen erikseen
- muut kirjautumistavat joudutaan rakentamaan jokaiseen sovellukseen erikseen

3.1.3 Kertakirjautuminen web-pääsynhallinnan avulla



Web pääsynhallinta:
1. Web pääsynhallinta pitää listaa kohdesovelluksista, session perustaminen ja purkaminen
2. Sisäänrakennettu pääsynhallinta, domainkohtaiset setup:t

Kuva x: Kertakirjautuminen web-pääsynhallinnan avulla. Kertakirjautuminen federoidussa pääsynhallinnassa

Esiehdot:
Käyttäjän käyttövaltuudet ja identiteetti on provisioitu käyttövaltuuksien hallinnasta (luvitusprosessi) käyttäjä- ja käyttövaltuushakemistoon. Käyttövaltuuksien suhteen on tehty toinen seuraavista

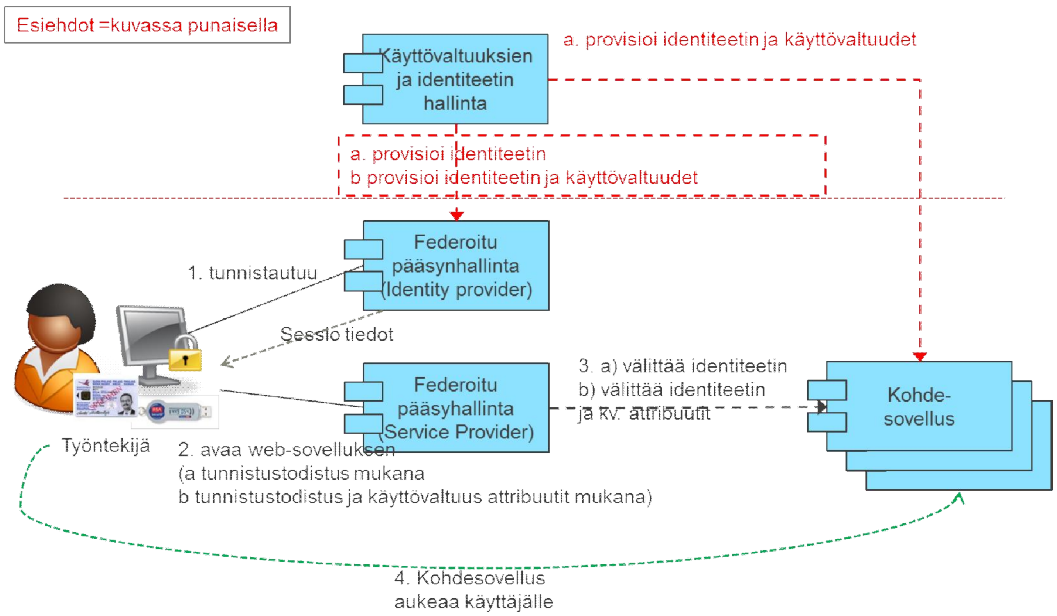
- (a) käyttäjä- ja käyttövaltuustiedot on provisioitu kohdesovellukseen.
- (b) käyttövaltuudet on provisioitu hakemistoon.

1. Käyttäjän työasematunnistautuminen tehdään käyttäjä- ja käyttöoikeushakemistoa vasten.
2. Käyttäjälle perustetaan istunto hakemistoon.
    - hakemisto pitää kirjaa, ketkä ovat kirjautuneet ja mitä oikeuksia heillä on
    - hakemistolta voidaan kysyä käyttäjän oikeuksia, tiketin voimassaoloa
3. Käyttäjä avaa web-sovelluksen.
4. Työasema välittää käyttäjän identiteetin web-pääsynhallinnalle, joka tarkastaa käyttäjän identiteetin hakemiston istuntoa vasten.
5. a) web-pääsynhallinta välittää käyttäjän tarkastetun identiteetin kohdesovellukselle. Kohdesovellus saa käyttövaltuudet omasta kannastaan.
   b) web-pääsynhallinta välittää käyttäjän tarkastetun identiteetin ja käyttövaltuudet kohdesovellukselle, luo sekä ylläpitää sessiota kohdesovellusten hallitsemiseksi. (Huom sessi pitää purkaa hallitusti hakemistosession purkamisen yhteydessä)
   Myös vaihtoehto c) on mahdollinen: web-pääsynhallinta voi toimia myös pelkän identiteetin tarkastajan roolissa, jolloin kohdesovellus hakee käyttäjän käyttövaltuudet hakemistosta

6. Kohdesovellus avautuu käyttäjälle.

Hyvät ja huonot puolet:
+ ei vaadi federointi - tietojärjestelmäpalveluiden hankkimista
+ web-pääsynhallinta pystyy tarjoamaan kertakirjautumisen myös muille tunnistustavoille (esim. kt+ss)
+ voidaan tallentaa muiden web-palveluiden käyttäjätunnuksia ja salasanoja varastoon (toimii kuten ESSO, mutta vain web-ympäristössä; kaikki WAM tuotteet eivät tue tätä toimintatapaa)
- web-pääsynhallinta on integroitava käyttövaltuushakemistoon (tuotteen on tuettava tätä ominaisuutta)
- toimii vain käyttäjä- ja käyttövaltuushakemiston tunnistautumiseen nojaavissa päätelaitteissa
- toimintatapaa ei ole standardi ja tuki löytyy vain tietyissä selaimissa ja palvelinohjelmistoissa
- Jokaiseen sovellukseen joudutaan rakentamaan kertakirjautuminen erikseen

3.1.4 Kertakirjautuminen federoidussa pääsynhallinnassa



Kuva x: Kertakirjautuminen federoidussa pääsynhallinnassa, jossa -a) identiteetit ja käyttövaltuudet provisioidaan erikseen tai b) käyttövaltuudet välitetään attribuutteina

Esiehdot:

- a) Käyttäjän identiteetti on provisioitu Identity providerille. Käyttövaltuudet ja identiteetti on provisioitu kohdesovellukseen.
- b) Käyttäjän identiteetti ja käyttövaltuudet on provisioitu Identity Providerille

1. Käyttäjän tunnistautuu Federoidun käyttäjähallinnan Identity Provideriin. Käyttäjälle perustetaan istunto federoinnin lähdehakemistoon. Federoinnin kohdehakemistoon perustetaan vastaava istunto, johon tuodaan tiedot lähdehakemistosta.
2. a) Käyttäjä avaa web-sovelluksen. Mukana siirtyy Identity Provideriltä saatu todistus identiteetin tunnistuksesta (tunnistusseloste eli ” tiketti”).

   b) Käyttäjä avaa web-sovelluksen. Mukana siirtyy Identity Provideriltä saatu todistus identiteetin tunnistuksesta sekä käyttövaltuudet sisältävät attribuutit
3. a) Federoidun pääsynhallinnan Service Provider tarkastaa todistuksen aitouden ja sen että Identity Provider kuuluu luotettuihin tunnistajiin. Federoitu pääsynhallinta välittää käyttäjän identiteetin kohdesovellukselle.
   Kohdesovellus saa käyttövaltuudet omasta kannastaan, istunto perustetaan.

   b) Federoidun pääsynhallinnan Service Provider tarkastaa todistuksen aitouden ja sen että Identity Provider kuuluu luotettuihin tunnistajiin. Federoitu pääsynhallinta välittää käyttäjän identiteetin sekä käyttövaltuudet sisältävät attribuutit kohdesovellukselle.
   Kohdesovellus saa käyttövaltuudet attribuuttien arvoista, istunto perustetaan
4. Kohdesovellus avautuu käyttäjälle.

Muita vaihtoehtoja:
Vaihtoehto, kohta:1 Työntekijä yrittää avata suoraan web-sovellusta

- Federoidun pääsyhallinnan Service Provider tietojärjestelmäpalvelu tarkastaa, onko käyttäjällä voimassa oleva istunto.
- Jos käyttäjällä on voimassa oleva istunto, hänen ei tarvitse tunnistautua uudestaan.
- Jos voimassa olevaa istuntoa ei ole, käyttäjä ohjataan tunnistautumaan Identity Providerille.

Vaihtoehto b) käyttövaltuudet välitetään attribuutteina

Kohdesovellus voi myös perustaa käyttäjälle identiteetin ja käyttövaltuustiedot omaan käyttäjäkantaansa. Ongelmana tässä toimintatavassa on se, että kohdesovelluksen yläpuolella oleva identiteetinhallinta ei tiedä tällä tavalla perustettuja käyttäjiä.

Hyvät ja huonot puolet:
+ standardoidut tavat toteuttaa federointi
+ useimmat yleisesti käytetyt selaimet, päätelaitteet ja käyttöjärjestelmät tukevat toimintatapaa
+ pystyy tarjoamaan kertakirjautumisen luottamusverkoston sisällä
- käyttäjät ja käyttövaltuudet pitää toimittaa erikseen kohdesovellukselle (jos omassa organisaatiossa) tai mahdollisesti toisen organisaation identiteetinhallinnalle (jos kohdesovellus toisessa organisaatiossa)
- vaatii federointiteknologian käyttöönoton kummassakin päässä
- luottamusverkosto pitää konfiguroida etukäteen
<u>a) identiteetit ja käyttövaltuudet provisioidaan erikseen</u>

- + kohdesovelluksen käyttäjät ovat ennalta tiedossa

b) käyttövaltuudet välitetään attribuutteina

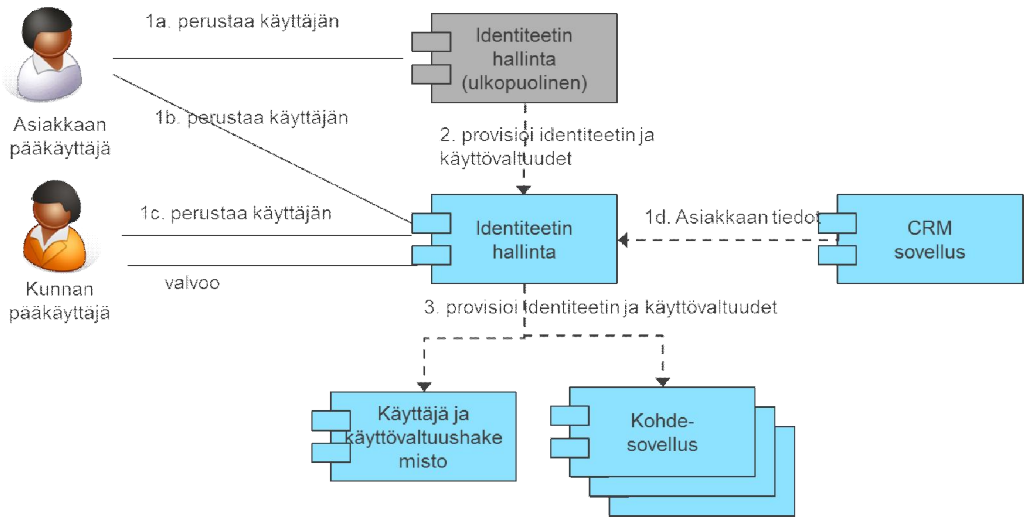
- + kohdesovelluksen käyttäjien ei tarvitse olla etukäteen kohdesovelluksen tiedossa. Tieto saattaa löytyä vain käyttölokeilta
- - Idenity providerin pitää olla ketterä, uusia attribuutteja saatetaan joutua lisäämään uusien kohdesovellusten myötä

3.2 Käyttövaltuuksien ja identiteetin hallinta ja valvonta- Asiakaskäyttäjät

Erilaiset tunnistautumis- ja valtuutuskäytönnöt johtavat myös erilaisiin ylläpitokäytäntöihin. Erilaisille asiakaita koskeville kertakirjautumistavoille on tässä esitetty seuraavat hallinta- ja valvontatavat (kunnan työntekijät hallitaan prosessien mukaisesti):

- **Kertakirjautuminen web-pääsynhallinnan avulla (ks. Asiakaskäyttäjät)**
  - Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)
  - Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)
- **Web-kertakirjautuminen federoidussa tunnistuksessa (identiteettien ja käyttövaltuuksien provisiointi erikseen) (ks. Asiakaskäyttäjät)**
  - Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (federoitu identiteetti ja käyttövaltuudet provisioidaan)
- **Web-kertakirjautuminen federoidussa tunnistuksessa (käyttövaltuudet attribuutteina) (ks. Asiakaskäyttäjät)**
  - Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi)
  - Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi)
  - Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)

3.2.1 Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)



Kuva x: Organisaatioasiakkaiden käyttövaltuuksien luonti ja provisiointi ilman federointia. Kertakirjautuminen hallitaan Web-pääsynhallinnan avulla (ks. asiakaskäyttäjät - kertakirjautuminen)

a) Asiakaskäyttäjät perustetaan kotiorganisaatiossaan:

1. Asiakkaan pääkäyttäjä perustaa organisaation käyttäjän ja antaa hänelle käyttövaltuudet oman organisaationsa identiteetinhallintajärjestelmässä.
2. Asiakasorganisaation identiteetinhallinta provisioi käyttäjän identiteetti- ja käyttövaltuustiedot kunnan käyttämään käyttövaltuus ja identiteetinhallintajärjestelmään
3. Kunnan käyttövaltuushallinta provisioi identiteetin ja käyttövaltuudet hakemistoihin ja kohdesovelluksiin.

b) asiakaskäyttäjät perustetaan kunnan käyttövaltuus ja identiteetin hallintajärjestelmään

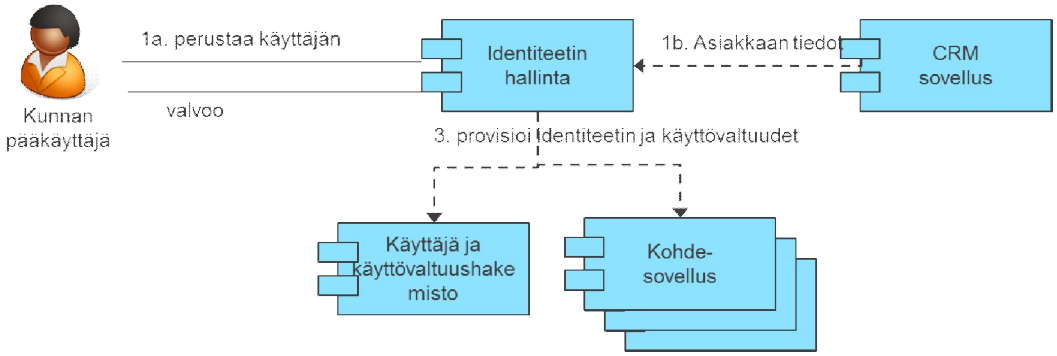
1. a) Asiakkaan pääkäyttäjä perustaa (organisaation) käyttäjän ja käyttövaltuudet kunnan käyttämään identiteetinhallintajärjestelmään.
   b) Kunnan pääkäyttäjä perustaa asiakaskäyttäjän ja käyttövaltuudet kunnan käyttämään identiteetinhallintaan.
2. -
3. Kunnan identiteetinhallinta provisioi identiteetin ja käyttövaltuudet hakemistoihin ja kohdesovelluksiin.

Muut vaihtoehdot menevät samalla tavalla kuin vaihtoehto (b), mutta niissä asiakastiedot ja käyttövaltuudet perustetaan seuraavilla eri mekanismeillä:

- (1d) CRM-sovellus toimittaa asiakkaan identiteetin ja käyttövaltuustiedot kunnan käyttämään identiteetinhallintaan.
- CRM-sovelluksen sijaan tiedot voivat tulla myös ydintiedon hallinnasta (MDM).

Kun käyttäjän identiteetti- ja käyttövaltuustiedot perustetaan tai välitetään kunnan identiteetinhallinnan kautta, voi kunnan pääkäyttäjä myös valvoa niitä (kenellä käyttäjällä on millaiset oikeudet).

3.2.2 Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)



Kuva x: Henkilöasiakkaiden käyttövaltuuksien luonti ja provisiointi ilman federointia. Kertakirjautuminen hallitaan Web-pääsynhallinnan avulla (ks. asiakaskäyttäjät - kerta-kirjautuminen)

Henkilöasiakkaat perustetaan ja aktivoidaan käyttäjiksi

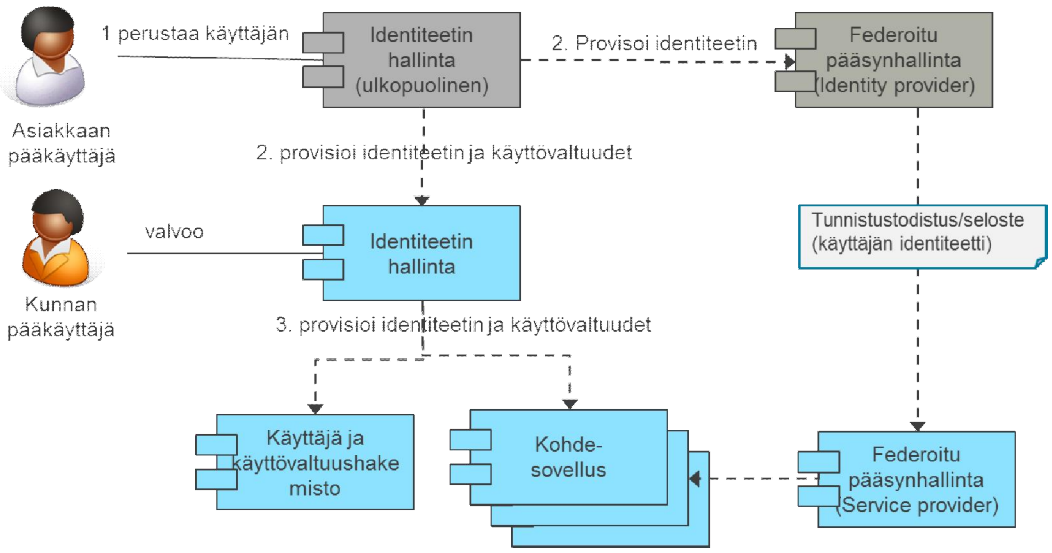
a) Kunnan pääkäyttäjä perustaa henkilöasiakaskäyttäjän ja antaa hänelle käyttövaltuudet kunnan käyttämässä identiteetinhallintajärjestelmässä

b) CRM-sovellus toimittaa asiakkaan identiteetin ja käyttövaltuustiedot kunnan käyttämään identiteetinhallintaan.

Kunnan identiteetinhallinta provisioi identiteetin ja käyttövaltuudet hakemistoihin ja kohdesovelluksiin.

Kun käyttäjän identiteetti- ja käyttövaltuustiedot perustetaan tai välitetään kunnan identiteetinhallinnan kautta, voi kunnan pääkäyttäjä myös valvoa niitä (kenellä käyttäjällä on millaiset oikeudet).

3.2.3 Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (identiteetti ja käyttövaltuudet provisioidaan)



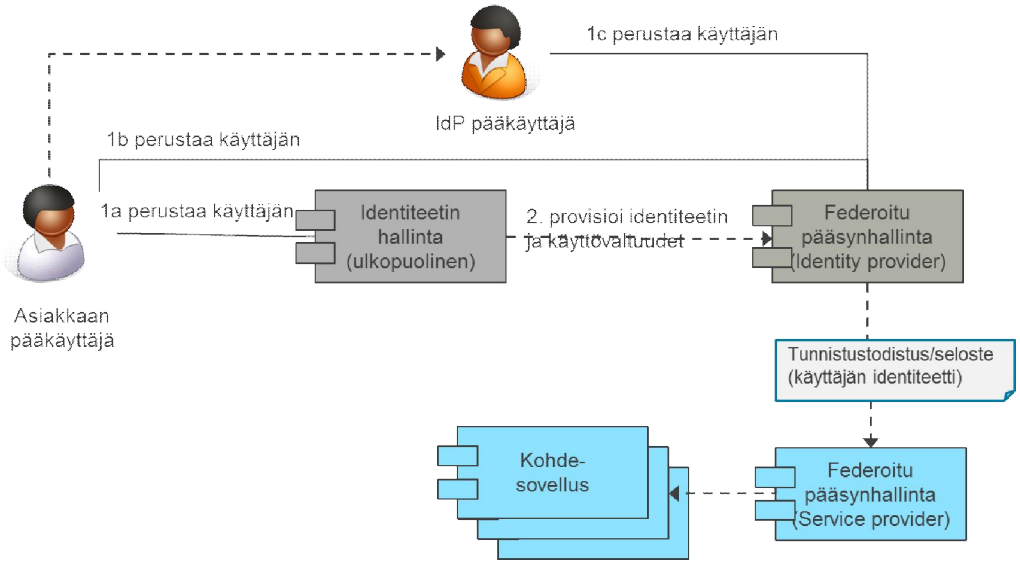
Kuva x: Organisaatioasiakkaiden käyttövaltuuksien luonti ja provisiointi federoidussa pääsynhallinnassa. Kertakirjautuminen hallitaan federoidun tunnistuksen mukaisesti (ks. asiakaskäyttäjät - kertakirjautuminen)

Tapahtumien kulku:

1. Asiakkaan pääkäyttäjä perustaa organisaation käyttäjän ja antaa hänelle käyttövaltuudet oman organisaationsa identiteetinhallintajärjestelmässä.
2. Asiakasorganisaation identiteetinhallinta provisioi käyttäjän identiteetti- ja käyttövaltuustiedot kunnan käyttämään identiteetinhallintajärjestelmään sekä asiakkaan käyttämälle Identity providerille.
3. Kunnan identiteetinhallinta provisioi identiteetin ja käyttövaltuudet hakemistoihin ja kohdesovelluksiin.

Kun käyttäjän identiteetti- ja käyttövaltuustiedot välitetään kunnan identiteetinhallinnan kautta, voi kunnan pääkäyttäjä myös valvoa niitä (kenellä käyttäjällä on millaiset oikeudet).

3.2.4 Organisaatioasiakkaiden identiteetin ja käyttöoikeuksien hallinta ja valvonta (pelkkä federointi)



Kuva x: Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta- pelkkä federointi. Kertakirjautumisen hallinta: Web-kertakirjautuminen federoidussa tunnistuksessa -käyttövaltuudet attribuutteina (ks. asiakaskäyttäjät – kertakirjautuminen)

Käyttäjä perustetaan kotiorganisaationsa identiteetinhallintaan

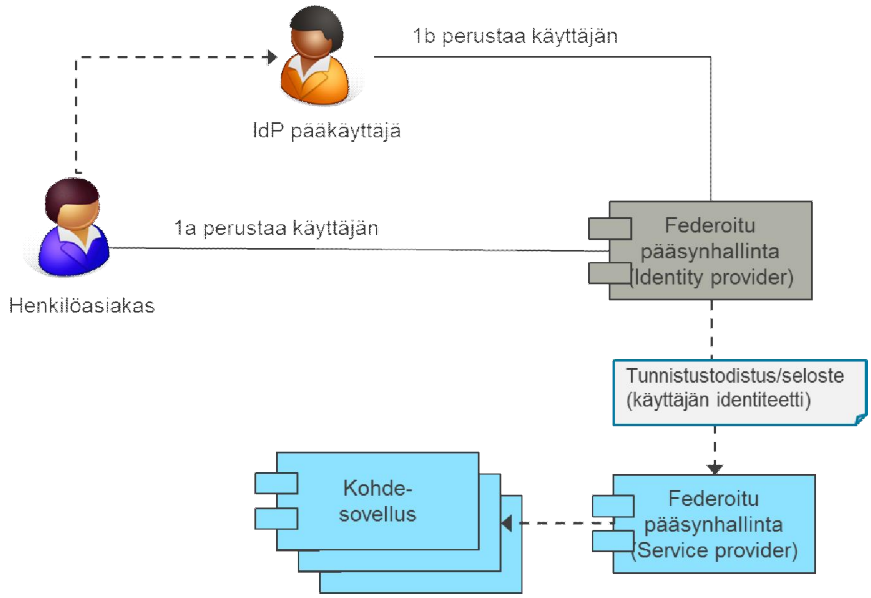
1. Asiakkaan pääkäyttäjä perustaa organisaation käyttäjän ja antaa hänelle käyttövaltuudet oman organisaationsa identiteetinhallintajärjestelmässä (a)
2. Asiakasorganisaation identiteetinhallinta provisioi käyttäjän identiteetti- ja käyttövaltuustiedot asiakkaan käyttämälle Identity providerille. Identiteetti ja käyttövaltuudet välittyvät tunnistustodistuksen mukana Idenitty providerilta kunnan Service providerille.

Muut mahdolliset tavat käyttäjän ja käyttövaltuuksien perustamiseksi:

1. Asiakkaan pääkäyttäjä perustaa organisaation käyttäjän ja antaa hänelle käyttövaltuudet suoraan Identity provideriin (b)
2. Asiakkaan pääkäyttäjä pyytää Identity providerin pääkäyttäjää perustamaan käyttäjän ja käyttöoikeudet (c)

Kun identiteetti- ja käyttövaltuustiedot eivät välity kunnan identiteetinhallinnan kautta, niitä voidaan seurata vain jälkikäteen lokeilta. Etukäteen ei voida tietää, keille kukin asiakasorganisaatio on antanut millaisiakin käyttöoikeuksia. Näissä tapauksissa tuleekin sopimuksellisesti siirtää kaikki käyttäjäidentiteetteihin ja käyttövaltuuksiin liittyvät ongelmatilanteet siirtää asiakkaan vastuulle, sillä kunnan on hyvin hankalaa tai mahdotonta tietää ja vaikuttaa käyttäjiin ja käyttövaltuuksiin.

3.2.5 Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi)



Kuva x: Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta- pelkkä federointi. Kertakirjautumisen hallinta: Web-kertakirjautuminen federoidussa tunnistuksessa käyttövaltuudet attribuutteina (ks. asiakaskäyttäjät - kertakirjautuminen)

Itsepalvelu:

- a) Henkilöasiakas perustaa itse itsensä Identity provideriin (ja antaa tarvittava oikeudet). Identiteetti- ja käyttövaltuudet välittyvät tunnistustodistuksen mukana Idenitty providerilta kunnan Service providerille.

Delegointi

- (b) Henkilöasiakas pyytää Identity providerin pääkäyttäjää perustamaan hänelle identiteetin ja käyttövaltuudet.

Kun identiteetti- ja käyttövaltuustiedot eivät välity kunnan identiteetinhallinnan kautta, niitä voidaan seurata vain jälkikäteen lokeilta. Etukäteen ei voida tietää, ketkä ovat mahdollisia käyttäjiä (ja millaisia käyttövaltuuksia heillä on). Näissä tapauksissa tuleekin sopimuksellisesti siirtää kaikki käyttäjäidentiteetteihin ja käyttövaltuuksiin liittyvät ongelmatilanteet asiakkaan vastuulle, sillä kunnan on hyvin hankalaa tai mahdotonta tietää ja vaikuttaa käyttäjiin ja käyttövaltuuksiin.

Huom. Perustaminen voi olla myös ”puoliautomaattista/välillistä”. Esim. VETUMA-tunnistus (Identity provider) nojaa pankkien TUPAS-tunnistukseen, jonka käyttäjätunnus luodaan nettipankin käyttöönoton yhteydessä.

3.3 Asiakaskäyttäjät

Asiakaskäyttäjille käytetty käyttövaltuuksien ja identiteetinhallintajärjestelmä ei tarvitse olla sama kuin työntekijöille, sillä asiakaskäyttäjien kohdalla esimerkiksi hyväksyn-

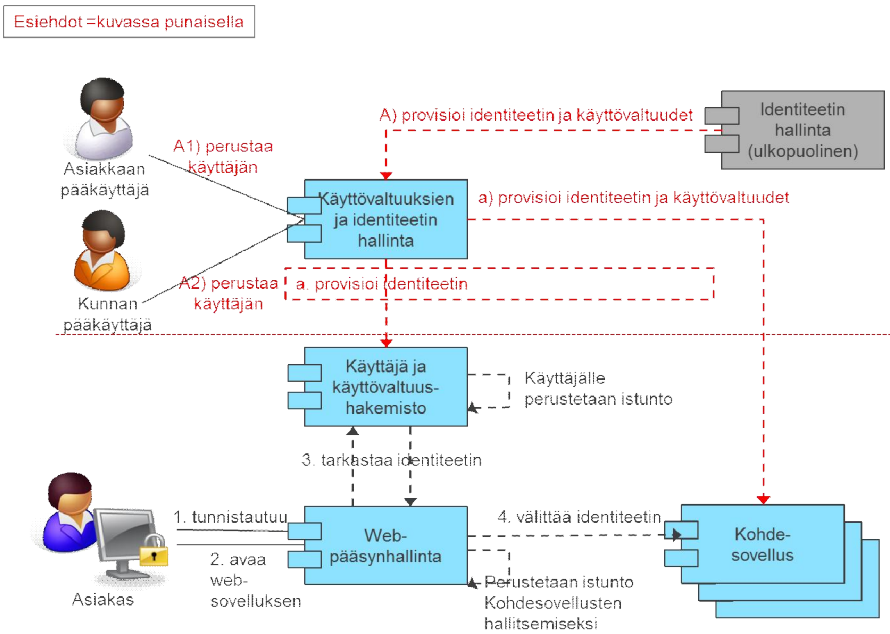
töihin liittyvälle kierrätykselle ei ole yleensä tarvetta. Asiakaskäyttöliittymät toimivat joskus teknisten tunnusten varassa, jolloin heitä ei välttämättä identifioida tai perusteta samalla tavalla käyttäjiksi kuin kunnan työntekijöitä, joten provisioinnit ovat erilaisia. Teknisten tunnusten käyttämisestä tulee pyrkiä eroon tavoitetilassa ja kaikkia käyttäjäryhmiä tulisi kohdella samalla tavalla.

Asiakaskäyttäjä kertakirjautuu sovellukseen
Toistaiseksi tällaiselle tyyppitapaukselle ei ole tunnistettu tarvetta, vaan asiakaskäyttäjät käyttävät aina web-sovelluksia/käyttöliittymiä.

Asiakaskäyttäjä kertakirjautuu web-sovellukseen
Asiakaskäyttäjien kohdalla ratkaisuvaihtoehdot ovat periaatteessa samat kuin kunnan työntekijöiden kohdalla lukuun ottamatta hakemistointegraatioon perustuvaa toimintamallia, joka ei ole käytännön realiteetit huomioon ottaen mahdollinen.
Mahdollisia ratkaisuehdokkaita ovat siis aiempana esitetyt (pienin muutoksin):

- Kertakirjautuminen web-pääsynhallinnan avulla
- web-kertakirjautuminen federoidussa tunnistuksessa
    - **a**) identiteettien ja käyttövaltuuksien provisiointi erikseen
    - **b**) käyttövaltuudet attribuutteina

3.3.1 Kertakirjautuminen web-pääsynhallinnan avulla



Kuva x: Kertakirjautuminen web-pääsynhallinnan avulla. Asiakas kirjautuu sovellukseen Web:n kautta
Esiehdot:

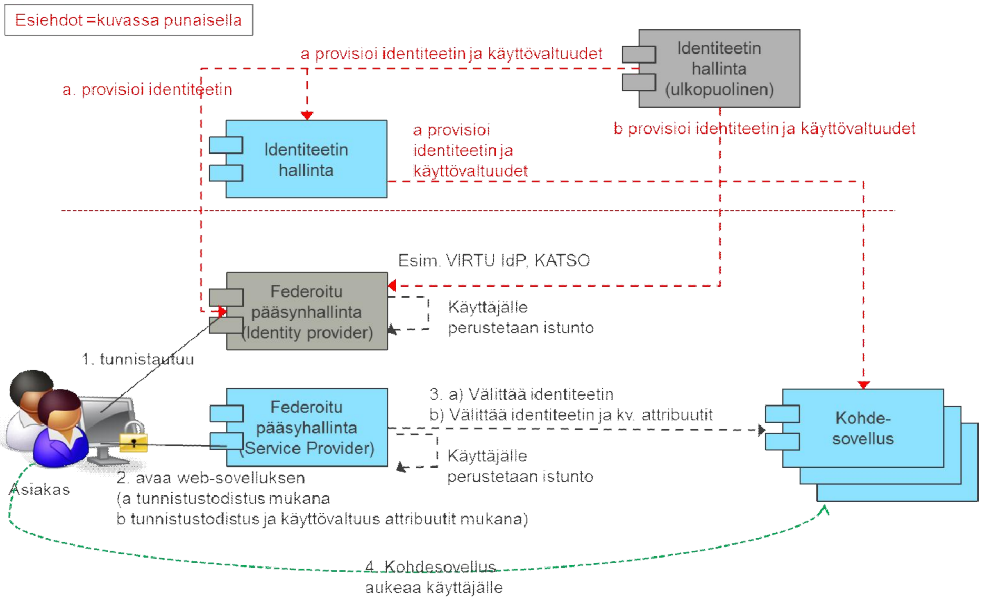
- (A) Asiakkaan käyttämä ulkoinen identiteetin hallinta provisioi identiteetin käyttövaltuuksien ja identiteetin hallintaan.

  - A1 Asiakkaan pääkäyttäjä ylläpitää niitä suoraan kunnan käyttämään identiteetin hallintaan
  - A2. Kunnan pääkäyttäjä ylläpitää niitä suoraan kunnan käyttämään identiteetin hallintaan
- Käyttäjän käyttövaltuudet ja identiteetti on provisioitu käyttövaltuuksien hallinnasta (luvitusprosessi) käyttäjä- ja käyttövaltuushakemistoon ja lisäksi
  - (a) käyttäjä- ja käyttövaltuustiedot on provisioitu kohdesovellukseen.

1. Asiakas tunnistautuu web pääsynhallintaan ja tunnistaminen tehdään käyttäjä- ja käyttöoikeushakemistoa vasten. Käyttäjälle perustetaan istunto käyttövaltuushakemistoon.
2. Asiakas avaa web-sovelluksen.
3. Työasema välittää käyttäjän identiteetin web-pääsynhallinnalle, joka tarkastaa käyttäjän identiteetin hakemiston istuntoa vasten.
4. web-pääsynhallinta välittää käyttäjän tarkastetun identiteetin kohdesovellukselle. Kohdesovellus saa käyttövaltuudet omasta kannastaan, luo session kohdesovellusten hallitsemiseksi.
5. Kohdesovellus avautuu käyttäjälle.

Asiakas on aktivoitu ja valtuudet luotu kohtien 3.2.1 Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia) ja
ja 3.2.2 Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia) mukaisesti

3.3.2 Web-kertakirjautuminen federoidussa tunnistuksessa



Kuva x: Kertakirjautuminen federoidussa pääsynhallinnassa, jossa -a) identiteetit ja käyttövaltuudet provisioidaan erikseen tai b) käyttövaltuudet välitetään attribuutteina

Esiehdot:

a) Identiteetti ja käyttövaltuustiedot on välitetty asiakkaan käyttämästä identiteetin hallinnasta kunnan käyttämään identiteetinhallintaa.
Identiteetti on provisioitu federoidun pääsynhallinnan identity provideriin (joka on usein eri kuin kunnan käyttämä).
Käyttövaltuudet ja identiteetti on provisioitu kohdesovellukseen.
b) Käyttäjän identiteetti ja käyttövaltuudet on provisioitu Identity Providerille.
Käyttövaltuudet välitetään kohdesovelluksille.

1. Käyttäjän tunnistautuu Federoidun käyttäjähallinnan Identity Provideriin. Käyttäjälle perustetaan istunto identity provideriin ja service provideriin.
2. a) Käyttäjä avaa web-sovelluksen. Mukana siirtyy Identity Provideriltä saatu todistus identiteetin tunnistuksesta (tunnistustodistus eli ” tiketti”).

   b) Käyttäjä avaa web-sovelluksen. Mukana siirtyy Identity Provideriltä saatu todistus identiteetin tunnistuksesta sekä käyttövaltuudet sisältävät attribuutit
3. a) Federoidun pääsynhallinnan Service Provider tarkastaa todistuksen aitouden ja sen että Identity Provider kuuluu luotettuihin tunnistajiin. Federoitu pääsynhallinta välittää käyttäjän identiteetin kohdesovellukselle.
   Kohdesovellus saa käyttövaltuudet omasta kannastaan.

   b) Federoidun pääsynhallinnan Service Provider tarkastaa todistuksen aitouden ja sen että Identity Provider kuuluu luotettuihin tunnistajiin. Federoitu pääsynhallinta välittää käyttäjän identiteetin sekä käyttövaltuudet sisältävät attribuutit kohdesovellukselle.
   Kohdesovellus saa käyttövaltuudet attribuuttien arvoista.
4. Kohdesovellus avautuu käyttäjälle.

HUOM. Erona lähinnä se työntekijän kertakirjautumiseen federoidussa tunnistuksessa:

a) identiteetti- ja käyttövaltuustiedot välitetään asiakkaan käyttämästä identiteetinhallinnasta kunnan käyttämään identiteetinhallintaan. Identiteetti provisioidaan federoidun pääsynhallinnan identity provideriin, joka on usein eri kuin kunnan käyttämä.
b)identiteetti- ja käyttövaltuustiedot välitetään asiakkaan käyttämästä identiteetinhallinnasta federoidun pääsynhallinnan identity provideriin, joka on usein eri kuin kunnan käyttämä. Huom! Käyttäjän identiteetti voi olla identity providerin käytössä ilman provisiointia tai perustamista. (esim. VETUMA hyödyntää pankkien TUPAS-tunnistusta, joten käyttäjää ei tarvitse erikseen perustaa VETUMA:an).

Asiakas on aktivoitu ja valtuudet luotu kohtien 3.2.3 Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (identiteetti ja käyttövaltuudet provisioidaan) vaihtoehdolle a, 3.2.4 Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi) ja 3.2.5 Henkilöasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi) vaihtoehdolle b mukaisesti

Hyvät ja huonot puolet:

+ Käyttäjien hallinta vastuutettu selkeästi kumppaneille
+ mahdollistaa kertakirjautumiskokemuksen kumppanin verkosta
+ Käyttöoikeus voidaan purkaa heti myös kumppanin taholta
+ saadaan ajantasainen tieto kumppanin käyttäjien tilasta (ryhmät, attribuutit jne)
- verkoston hajauttaminen lisää valvottavien ja auditoitavien kohteiden määrää
- Kumppanin alihankintaketju tai muut kumppanin IDP:n luvittamat käyttäjät voivat muodostaa ennakoimattomia tilanteita mikäli sopimusrakenteet ja/tai prosessit eivät ole kunnossa kumppanin kanssa.

3.4 Kumppanityöntekijä omassa verkossa

Kumppanien työntekijöille tarjottavat etäyhteydet kunnan sovelluksiin - muut kuin web-sovellukset - toteutetaan pääasiassa virtualisoitujen työasema-asiakasohjelmien kautta (esim. Citrix client). Tällöin kumppanien käyttäjille annetaan AD-käyttäjätunnus, jolla he kirjautuvat kunnan käyttöoikeusverkkoon. Näin olleen vaikka kumppanin työntekijä istuukin omalla toimistollaan, hän on kirjautunut kunnan käyttö oikeusverkkoon. Tämän takia tämä tapaus on sama kuin 3.1 Kunnan työntekijät ja kumppanit kunnan verkossa eikä kuulu tämän otsikon alle (Kumppanin työntekijä omassa verkossa).

3.4.1 Kumppanikäyttäjä kertakirjautuu web-sovellukseen

Omassa käyttöoikeusverkossaan toimivien kumppanikäyttäjien web-kertakirjautumiseen liittyvät toimintamallit ovat samat kuin organisaatioasiakkailla luvussa 3.3 Asiakaskäyttäjät eli

- Kertakirjautuminen web-pääsynhallinnan avulla
- web-kertakirjautuminen federoidussa tunnistuksessa (identiteettien ja käyttövaltuuksien provisiointi erikseen)
- web-kertakirjautuminen federoidussa tunnistuksessa (käyttövaltuudet attribuutteina)

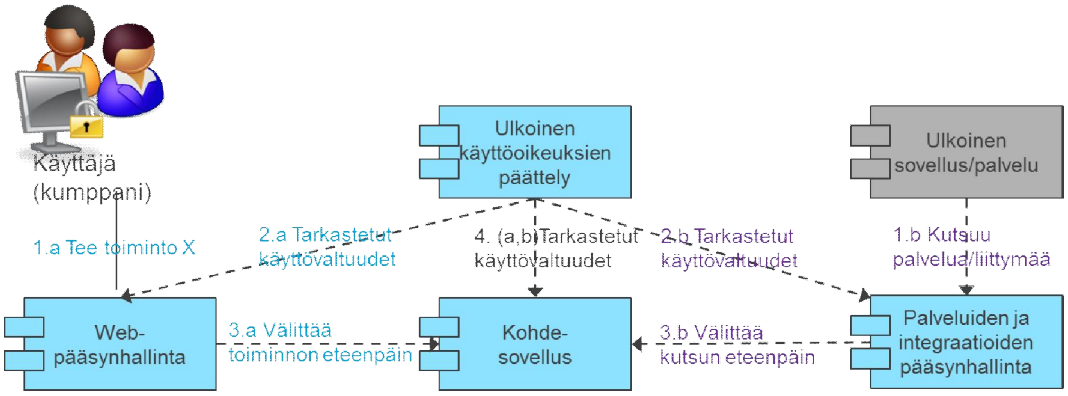
3.4.2 Kumppanikäyttäjän identiteetin ja käyttövaltuuksien hallinta ja valvonta

Omassa käyttöoikeusverkossaan toimivien kumppanikäyttäjien hallintaan ja valvontaan liittyvät toimintamallit ovat samat kuin organisaatioasiakkailla luvussa 3.2 Käyttövaltuuksien ja identiteetin hallinta ja valvonta- Asiakaskäyttäjät eli

- Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (ilman federointia)
- Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (identiteetti ja käyttövaltuudet provisioidaan)
- Organisaatioasiakkaiden identiteetin ja käyttövaltuuksien hallinta ja valvonta (pelkkä federointi)

3.5 Muita toimintamalleja

3.5.1 Ulkoinen käyttöoikeuksien päättely (EXT)



Kuva x: Ulkoinen käyttöoikeuksien päättely

Tapahtumien kulku (a) eli käyttäjä käyttää web-sovellusta

- Käyttäjä tekee toiminnon X
- web-pääsynhallinta tarkastuttaa ulkoisella käyttöoikeuksien päättelyllä käyttövaltuudet - karkea käyttövaltuuksien tarkastus (coarse grained), esimerkiksi tunnistetaan lähde, josta käyttäjä saapuu
- web-pääsynhallinta välittää toiminnon eteenpäin kohdesovellukselle.
- Kohdesovellus tarkastuttaa ulkoisella käyttöoikeuksien päättelyllä käyttäjän hienojakoiset käyttöoikeudet (fine grained), tunnistetaan ulkoisen päättelyn vlitäämien tietojen avulla käyttäjän oikeutus kohdejärjestelmään ja sen sisäisiin ryhmiin.

Toinen vaihtoehto (b) eli ulkoinen sovellus/palvelu kutsuu kohdesovelluksen tarjoamaa palvelua tai integraatiota

- Ulkoinen sovellus/palvelu kutsuu kohdesovelluksen tarjoamaa palvelua tai liittymää
- Palveluiden ja integraatioiden pääsynhallinta tarkastuttaa ulkoisella käyttöoikeuksien päättelyllä käyttövaltuudet - karkea käyttövaltuuksien tarkastus (coarse grained)
- Palveluiden ja integraatioiden pääsynhallinta välittää kutsun eteenpäin kohdesovellukselle.
- Kohdesovellus tarkastuttaa ulkoisella käyttöoikeuksien päättelyllä hienojakoiset käyttöoikeudet (fine grained)

Karkean tason (kohta 2.) tai hienonjakoisen tason (kohta 4): käyttövaltuuksien tarkastukset voidaan tehdä joko kummatkin tai vain toinen tai ei kumpikaan ulkoisen käyttöoikeuksien päättelyn tietojärjestelmäpalvelun avulla.

Esimerkki ulkoisesta päättelystä on palveluntuottaja, joka hankkii kolmannelta osapuolelta tunnistuspalvelun, jota vasten liitetään tuottajan asiakkaat. Kunta asiakkaana kirjautuu palveluntuottajan järjestelmään, jossa tunnistetaan oikeutus kohdesovelluksen käyttöön ja mahdolliset kohdesovelluksen oikeutustasot ja attribuutit. Tämän jälkeen sessio siirretään tunnistetietoineen palveluntuottajan kohdesovellukselle.

Ulkoinen käyttöoikeuksien päättelylle lähetetään usein mm. seuraavat tiedot käyttäjä, toiminto joka aiotaan tehdä tai objekti, jonka tietoja haetaan/muutetaan/jne. Ulkoinen käyttöoikeuksien päättely vastaa, onko käyttäjällä oikeudet kyseiseen toimintoon.