Lauri Penttinen

PK-yrityksen kertakirjautumisen toteuttaminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Ohjelmistotekniikka

Insinöörityö

22.9.2016

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Lauri Penttinen PK-yrityksen kertakirjautumisen toteutus 39 sivua + 1 liite 22.9.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Ohjelmistotekniikka
Ohjaaja(t)	Chief IAMist, Tapani Tanskanen Yliopettaja, Auvo Häkkinen

Työ käsittelee kertakirjautumista ja sen toteuttamiseen yleisesti käytettyjä menetelmiä ja standardeja. Kertakirjautuminen (Single Sign-on) on menetelmä, jossa käyttäjä pääsee yhden tunnistautumisen jälkeen useaan erilliseen järjestelmään tai palveluun kirjautumatta uudestaan. Sen tarkoituksena on tarjota käyttäjälle mahdollisimman laaja pääsy niihin palveluihin (esim. tuntikirjaus-, projektinhallinta- ja toiminnanohjausjärjestelmään), joihin hän on oikeutettu pääsemään yhdellä kirjautumisella.

Ensimmäinen osa keskittyy teoriaan ja jälkimmäisessä osassa esitetään työssä tehty kertakirjautumistoteutus. Insinöörityön teoriaosuus (luvut 1-2) käsittelee kertakirjautumista yleisesti. Kertakirjautuminen voidaan jakaa kahteen eri ryhmään: selainkertakirjautuminen (Web SSO) ja kertakirjautuminen työasemapohjaisiin sovelluksiin (ESSO, Enterprise Single sign-on). Tässä työssä keskitytään pääasiassa selainkertakirjautumiseen. Kertakirjautumisen hyötyihin lukeutuvat esimerkiksi salasanojen määrän vähentyminen, käyttökokemuksen paraneminen, järjestelmänylläpitäjien työmäärän pienentyminen ja käyttäjähallinnan kustannusten laskeminen. Kertakirjautumisen toteuttamiseen yleisesti käytettyjä menetelmiä ja standardeja ovat esimerkiksi SAML (Security Assertion Markup Language), Kerberos ja luottamusliitäntäpohjainen kertakirjautuminen. Tunnistautumisen osalta työ keskittyy tunnistusmenetelmiin ja vahvaan tunnistamiseen.

Jälkimmäinen osa (luvut 3-4) esittelee työssä tehdyn kertakirjautumisen suunnitelman ja teknisen toteutuksen. Työssä toteutettu kertakirjautumisjärjestelmä on suunniteltu niin, että se on sopiva PK-yritysten käyttöön. Se on pyritty suunnittelemaan myös niin, että se pystyy mukautumaan yrityksen sisäisen arkkitehtuurin muutoksiin mahdollisimman vähin muutoksin. Järjestelmien riippuvuuksia toisistaan on pyritty minimoimaan. Kertakirjautumisen toteuttamiseen käytettiin erillistä pääsynhallintatuotetta (NetIQ Access Manager).

Työ on tehty Spellpoint Oy:lle. Spellpoint on identiteetin- ja pääsynhallintaan (IAM, Identity and Access Management) erikoistunut IT-palveluyritys, joka työllistää noin 25 henkilöä. Spellpoint on toiminut identiteetin- ja pääsynhallinnan parissa jo 16 vuotta.

Avainsanat	Kertakirjautuminen, NetIQ

Author(s) Title Number of Pages Date	Lauri Penttinen Single Sign-on implementation for SMEs 39 pages + 1 appendix 22 September 2016
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Software Engineering
Instructor(s)	Tapani Tanskanen, Chief IAMist Auvo Häkkinen, Principal Lecturer

This thesis focuses on the field of SSO (single sign-on). SSO is a method for accessing multiple services with just a one login and one credentials.

The first part of this thesis focuses on the theory of SSO and the second part introduces the design and implementation of an SSO system suitable for small and medium sized companies. SSO can be divided in two different groups: Web SSO and ESSO (Enterprise single sign-on). This thesis focuses on Web SSO. The benefits of Single sign-on includes reduction in the number of credentials, improvement of user experience, reduction of administrative tasks and costs related to user accounts. Commonly used standards and methods to implement SSO are also presented in the study. These standards and methods include SAML (Security Assertion Markup Language), Kerberos and federation based SSO.

The study also introduces the design and implementation of the SSO implementation created in this project. The SSO implementation is designed so that it is suitable for use by small and medium sized companies. It has also been designed to be as adaptive as possible to the architectural changes of the company's internal architecture. Dependencies between systems have been minimized. The implementation was made with a separate Access Manager product (NetIQ Access Manager).

The study was done for Spellpoint Oy. Spellpoint is an IT services company specialized in the field of IAM (Identity and Access Management). Currently Spellpoint employs 25 employees. The company has been in the field of IAM for a 16 years.

Keywords	Single Sign-On, NetIQ

Sisällys

Lyhenteet

AD	Microsoft Active Directory. Microsoftin hakemisto mm. käyttäjätiedoille.
AD Domain	Microsoft Active Directory Domain. Active Directoryn toimialue.
AD FS	Active Directory Federation Services. Microsoftin toteutus luottamusliitäntäpohjaisen kertakirjautumisen mahdollistamisesta.
AS	Authentication Server. Kerberos-tunnistuspalvelin.
DC	Domain Controller. Active Direcoryn tunnistautumispalvelin.
ESSO	Enterprise Single Sign-On. Kertakirjautuminen työasemapohjaisiin sovelluksiin.
IAM	Identity and Access Management. Identiteetin- ja pääsynhallinta.
IdP	Identity Provider. Taho, joka tarjoaa käyttäjän tunnistautumisen.
Istunto	Istunto. Varmennetun käyttäjän todiste hyväksytystä tunnistautumisesta.
KDC	Key Distribution Center. Kerberos-tunnistuksessa käytetty avaintenjakopalvelin.
LDAP	Lightweight Directory Access Protocol. Hakemistojen kommunikaatioprotokolla.
SAML	Security Assertion Markup Language. Kertakirjautumisessa käytetty XML-pohjainen standardi
SP	Service Provider. Taho, joka tarjoaa kertakirjautumisen palveluun.
SSO	Single Sign-On. Kertakirjautuminen, kuuluu pääsynhallinnan piiriin.
TGS	Ticket Granting Service. Kerberoksessa käytetty KDC:n osa, joka myöntää pääsyoikeuksia käyttäjille.

TGT	Ticket Granting Ticket. Kerberos-tunnistuksen käyttämä tunnistetieto.
Web SSO	Web Single Sign-On. Selainpohjainen kertakirjautuminen.

1 Johdanto

Työssä suunniteltiin Spellpointin kertakirjautumisratkaisu ja toteutettiin siitä ensimmäinen vaihe. Osana toteutusta oli nykyisen ympäristön kartoitus ja arkkitehtuurin selvittäminen.

Tavoitteet pähkinänkuoressa:

1. kertakirjautumisen toteuttaminen Jira- ja Confluence-palveluihin sekä mahdollistaminen muihin Spellpointin käyttämiin palveluihin

2. nykyisen hakemistoarkkitehtuurin yksinkertaistaminen

3. kertakirjautumisen arkkitehtuurin suunnittelu siten, että yksikään komponentti ei ole korvaamaton

Työ on tehty Spellpoint Oy:lle. Spellpoint on identiteetin- ja pääsynhallintaan (IAM, Identity and Access Management) erikoistunut IT-palveluyritys, joka työllistää noin 25 henkilöä. Spellpoint on toiminut identiteetin- ja pääsynhallinnan parissa jo 16 vuotta. Omaan käyttöön pääsynhallintaratkaisuita ei ole aiemmin tarvittu, koska työntekijämäärä on ollut hallittavissa helposti manuaalisesti ja kohdejärjestelmien määrä on ollut kohtuullisen alhainen. Työntekijämäärän ja kohdejärjestelmien määrän tulevan kasvun kannalta kertakirjautumisen toteuttaminen oli ajankohtaista. Näin kertakirjautumisen toteuttaminen valikoitui insinöörityön aiheeksi. Työssä esitellään ratkaisu PK-yritykselle sopivan kertakirjautumisratkaisun toteutukseksi. Insinöörityön mahdolliset hyödyt Spellpointille on esitetty luvussa 2.2: Kertakirjautumisen hyödyt.

Työn teoriaosuudessa (luvut 1-2) esitellään kertakirjautumisteknologioita ja -standardeja. Työn toteutus tehtiin käyttäen pääsynhallintaan suunniteltua NetIQ Access Manager -tuotetta. Luvusta 3 eteenpäin käsitellään PK-yrityksen kertakirjautumisen toteuttamista tämän projektin näkökulmasta. NetIQ Access Managerin arkkitehtuuri ja käyttöön otetut ominaisuudet käydään läpi työn jälkimmäisessä osuudessa luvussa 4, jossa esitetään myös Spellpointille tehty tekninen toteutus.

Työn alkaessa asetetut tavoitteet saavutettiin ja aikataulu piti loppuun saakka. Työssä esiteltävä kertakirjautumisjärjestelmän toteutus asennettiin ja testattiin testiympäristössä. Toteutettu järjestelmä siirretään tuotantoon tämän insinöörityön ulkopuolisessa jatkokehitysprojektissa.

2 Kertakirjautuminen

Kertakirjautuminen (Single Sign-on) on menetelmä, jossa käyttäjä pääsee yhden tunnistautumisen jälkeen useaan erilliseen järjestelmään tai palveluun kirjautumatta uudestaan. Sen tarkoituksena on tarjota käyttäjälle mahdollisimman laaja pääsy niihin palveluihin (esim. tuntikirjaus-, projektinhallinta- ja toiminnanohjausjärjestelmään), joihin hän on oikeutettu pääsemään yhdellä kirjautumisella. [1.]

Kertakirjautumisen toteuttamiseen on olemassa lukuisia eri menetelmiä. Usein kertakirjautumisen toteutuksessa on käytetty useampia näistä yhdessä. Kertakirjautuminen voi olla mikä tahansa menetelmä, joka tarjoaa loppukäyttäjälle kirjautumisen moneen järjestelmään syöttämällä tunnuksensa vain kerran. [2.]

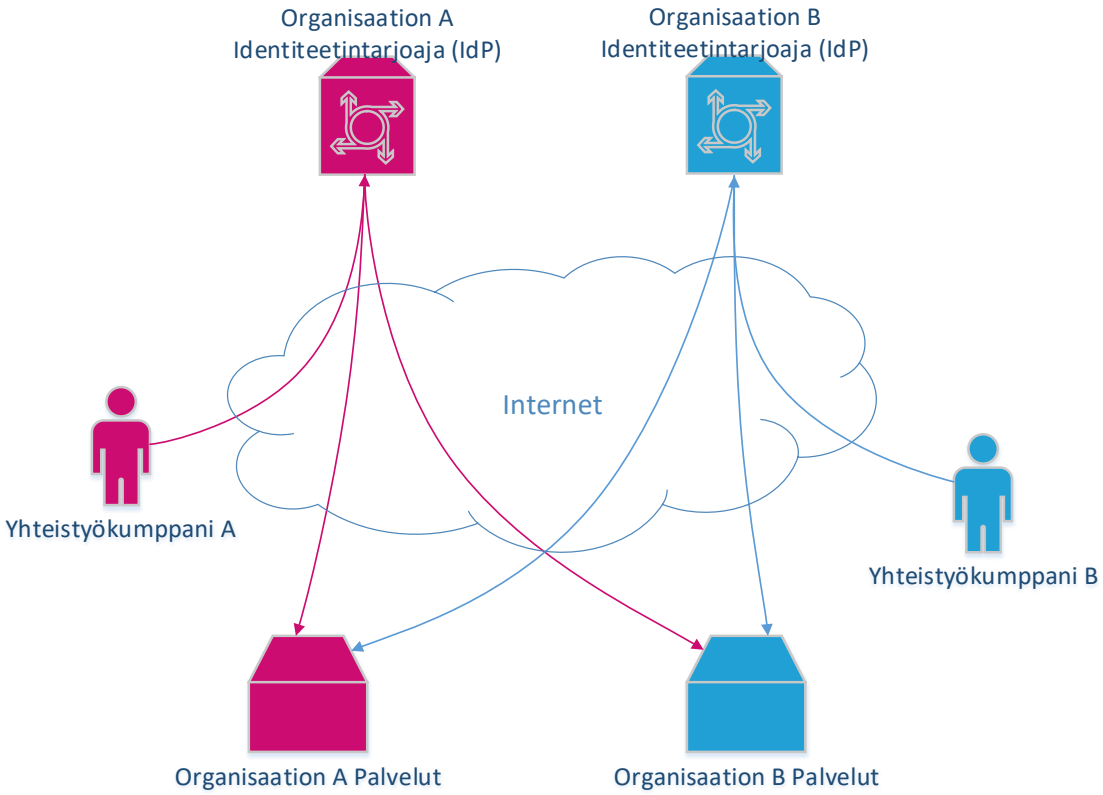
2.1 Kertakirjautumisen hyödyt

Kertakirjautumisratkaisu vähentää käyttäjien tunnus-salasana-pareja. Ilman kertakirjautumista käyttäjillä on jokaiseen tunnistusta vaativaan järjestelmään erilliset tunnus-salasana-parinsa, mutta keskitetyn tunnistuksen ansiosta käyttäjät pystyvät kirjautumaan palveluihin käyttäen vain yhtä tunnusyhdistelmää. Tämä tehostaa työskentelyä, koska käyttäjältä ei mene aikaa tunnusten kirjoittamiseen tai unohtuneiden tunnusten palauttamiseen. Yhden salasanan palauttaminen voi maksaa noin 70 dollaria [4]. Centrifyn rahoittaman ja WildMeyerin tekemän tutkimuksen mukaan yrityksen voivat menettää salasanojen unohduksien takia 420 dollaria/työntekijä/vuosi tehokkuuden laskun vuoksi. Suuremmissa yrityksissä tästä koituu jo suurempi menoerä, koska jo 500 työntekijän yrityksessä vuosittaiseksi menetykseksi koituisi noin 200 000 dollaria [5].

Kertakirjautuminen pienentää järjestelmäylläpitäjien työmäärää, koska käyttäjähallinnan toimet vähenevät. Esimerkiksi unohtuneiden salasanojen palautuspyynnöt vähenevät ja käyttäjien pääsynhallinta helpottuu. Ylläpitäjät voivat hoitaa pääsynhallinnan toimia yhdestä keskitetystä järjestelmästä kaikkiin kertakirjautumiseen liitettyihin kohdejärjestelmiin ja kaikille sisäisille ja ulkoisille käyttäjille. [4.]

Loppukäyttäjän käyttökokemus paranee, koska tarkoituksena on, ettei käyttäjä huomaa kertakirjautumisen toimia työskentelyn taustalla [4]. Käyttäjä voi käyttää suojattuja resursseja ja siirtyä kertakirjautumisen alaisen palvelun piiriin huomaamattaan. Ilman kertakirjautumista tulisi näissä tapauksissa syöttää kirjautumistiedot uudelleen.

Kertakirjautumisella pystytään myös helpottamaan eri sidosryhmien pääsyä toistensa suojattuihin palveluihin turvallisesti. Ulkoisten sidosryhmien käyttäjille voidaan tarjota pääsy oman organisaation suojattuihin resursseihin ja palveluihin ilman, että pitäisi pitää kirjaa ulkoisista käyttäjistä oman organisaation käyttäjähakemistossa [4]. Korkean tason arkkitehtuuri sidosryhmien yhteistyön helpottumisesta kertakirjautumisjärjestelmän ansiosta on esitetty kuvassa 1.



Kuva 1: Yhteistyö ulkoisten sidosryhmien välillä [4].

Kuva 1 on korkean tason arkkitehtuurikuvaus luottamusliitäntäpohjaisesta kertakirjautumisesta. Luottamusliitäntäpohjainen kertakirjautuminen esitetään tarkemmin luvussa 2.3: Kertakirjautumiseen soveltuvia teknologioita.

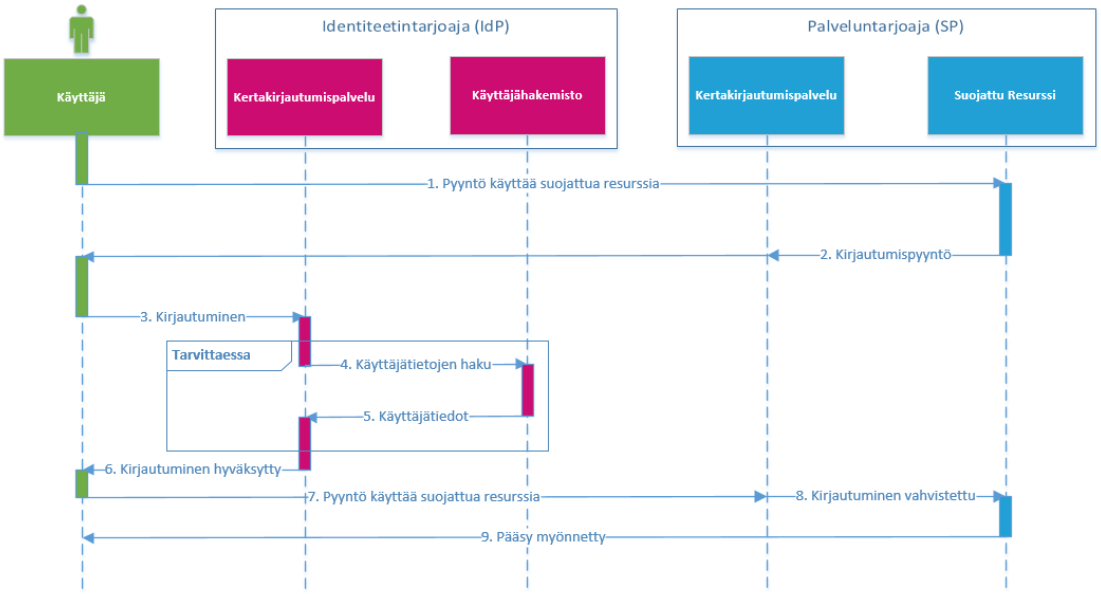
2.2 Kertakirjautumisen muodot

Kertakirjautumisen eri muotoihin kuuluu selainpohjainen kertakirjautuminen (Web SSO). Selainpohjaisella kertakirjautumisella tarkoitetaan kertakirjautumista, jossa käyttäjälle tarjotaan kertakirjautuminen selainpohjaisiin järjestelmiin ja palveluihin, mutta ei työasemapohjaisiin sovelluksiin.

Selainpohjaisen kertakirjautumisen pääkomponentit ovat internetselain, jonka avulla käyttäjä pyrkii saamaan pääsyn suojattuun resurssiin, identiteetin ja tunnistuksen tarjoava taho, suojattu resurssi, joka voi olla esimerkiksi verkkopalvelu ja palveluntarjoaja. Palveluntarjoaja on usein resurssin kanssa samalle palvelimelle asennettu palvelu, joka tarkistaa käyttäjän oikeudet käyttää kyseistä resurssia. Palveluntarjoaja ei ole käytössä, jokaisessa kertakirjautumistoteutuksessa, mutta sitä käytetään esimerkiksi luottamusliitäntäpohjaisessa kertakirjautumisessa. Joissain tapauksissa (esim. form fill) ei ole erillistä palveluntarjoajaa ja suojattua resurssia, vaan kertakirjautuminen tehdään suoraan suojattuun resurssiin [3].

Selainpohjainen kertakirjautuminen luokitellaan tavallisesti kahteen eri kirjautumistyyppiin. Toinen on palvelulähtöinen (SP-initiated) kertakirjautumisprosessi, jonka palveluntarjoaja käynnistää. Toinen on tunnistuslähtöinen (IdP-initiated) kertakirjautumisprosessi, jonka identiteetintarjoaja käynnistää.

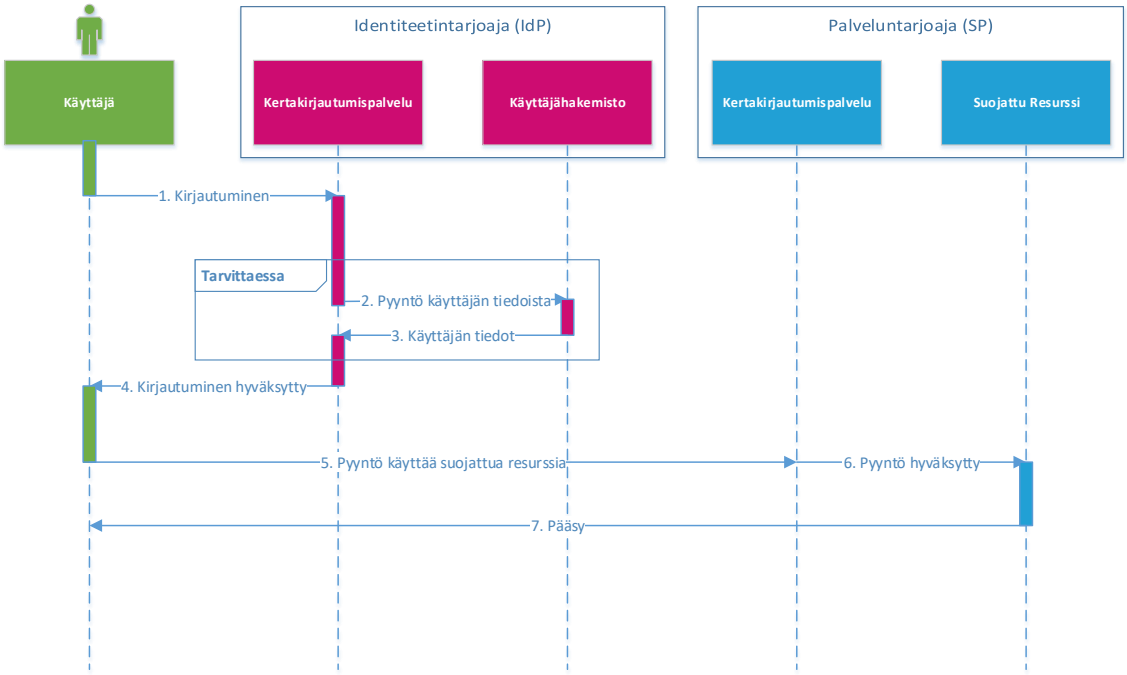
Palvelulähtöinen kertakirjautumisprosessi alkaa palveluntarjoajalta, jonka suojattuun resurssiin käyttäjä pyytää pääsyä. Siitä käynnistyy kertakirjautumisprosessi, jossa käyttäjä tunnistetaan. Kuvassa 2 on sekvenssikaavio palvelulähtöisestä kertakirjautumisprosessista.



Kuva 2: Palvelulähtöinen kertakirjautumisprosessi selainpohjaisessa kertakirjautumisessa

1. Käyttäjä pyytää pääsyä suojattuun resurssiin internetselaimella.
2. Palveluntarjoaja pyytää käyttäjää tunnistautumaan.
3. Kertakirjautumispalvelun tunnistuspyyntö ohjautuu Identiteetintarjoajalle.
4. Identiteetintarjoajan kertakirjautumispalvelu pyytää tarvittaessa käyttäjätiedot käyttäjähakemistolta.
5. Käyttäjähakemisto tarjoaa käyttäjätiedot kertakirjautumispalvelulle pyydettäessä.
6. Identiteetintarjoa tunnistaa käyttäjän ja ohjaa tämän takaisin palveluntarjoajalle.
7. Tunnistauduttuaan pyyntö ohjataan takaisin palveluntarjojalle.
8. Palveluntarjoajan kertakirjautumispalvelu tarkastaa käyttäjän tunnistautumisen. Hyväksytyn tunnistautumisen jälkeen käyttäjä saa pääsyn suojattuun resurssiin.

Tunnistuslähtöinen kertakirjautumisprosessi alkaa identiteetintarjoajalta, jonka kautta käyttäjä pyytää pääsyä suojattuun resurssiin. Siitä käynnistyy kertakirjautumisprosessi, jossa käyttäjä tunnistetaan. Kuvassa 3 on sekvenssikaavio tunnistuslähtöisestä kertakirjautumisprosessista.



Kuva 3: Tunnistuslähtöinen kertakirjautumisprosessi selainpohjaisessa kertakirjautumisessa

1. Käyttäjä kirjautuu identiteetintarjoajan käyttäjätietoja vasten.
2. Identiteetintarjoajan kertakirjautumispalvelu pyytää tarvittaessa käyttäjätiedot käyttäjähakemistolta.
3. Käyttäjähakemisto tarjoaa käyttäjätiedot kertakirjautumispalvelulle pyydettäessä.
4. Identiteetintarjoaja tunnistaa käyttäjän ja käyttäjällä on nyt avoin istunto, jonka avulla voi pyytää pääsyä kertakirjautumisen piirissä oleviin palveluihin.
5. Käyttäjä lähettää pyynnön palveluntarjoajalle.
6. Palveluntarjoajan kertakirjautumispalvelu tarkastaa käyttäjän tunnistautumisen. Hyväksytyn tunnistautumisen jälkeen käyttäjä saa pääsyn suojattuun resurssiin.

Toinen kertakirjautumisen muoto on ESSO (Enterprise Single Sign-on). ESSO-teknologiaa käytetään silloin, kun kertakirjautuminen toteutetaan työasemapohjaisiin sovelluksiin, jotka eivät toimi selaimessa. Useissa yrityksissä on vanhoja ns. legacy-järjestelmiä, jotka vaativat kirjautumisen työasemapohjaiseen sovellukseen. Yleensä ESSO-kertakirjautumistuotteet sisältävät keskitetyn palvelimen yrityksen sisäverkossa, jonne tallennetaan kaikkien käyttäjien profiilit ja salasanat. Käyttäjien työasemille lisätään ns. agentti, joka tallentaa käyttäjän kirjautumistiedot lompakkoon keskitetylle palvelimelle käyttäjän

kirjautuessa ensimmäistä kertaa johonkin sovellukseen. Se myös hakee tallennetut kirjautumistiedot työasemalle ja syöttää kirjautumistiedot kirjautumisikkunaan käyttäjän huomaamatta.

2.3 Kertakirjautumiseen soveltuvia teknologioita

Kertakirjautumisen toteuttamiseen on suuri määrä erilaisia ratkaisuja. Tässä luvussa esitetään standardeja ja menetelmiä, joilla pystytään mahdollistamaan kertakirjautuminen loppukäyttäjälle.

Tässä luvussa puhutaan myös luottamusliitäntäpohjaisesta kertakirjautumisesta (federation). Termistö on sekavaa luottamusliitäntäpohjaisessa kertakirjautumisessa, koska Active Directory Federation Services (AD FS) ja Security Assertion Markup Language (SAML) käyttävät samoista asioista eri termejä. Taulukossa 1 on selitetty, miten termit liittyvät toisiinsa ja tässä työssä käytettyihin termeihin.

Taulukko 1: Käsitteiden erot eri teknologioissa ja tässä työssä liittyen luottamusliitäntäpohjaiseen kertakirjautumiseen (Federation)

Käsite	Microsoft-termi	SAML 2.0 -termi	Tässä työssä käytetty termi
Luottamusliitäntäpohjainen kertakirjautuminen	Federation	Federation	Luottamusliitäntäpohjainen kertakirjautuminen
Identiteettejä ylläpitävän federointiosapuolen käyttäjää kuvaavan XML-dokumentti, jonka taho lähettää sovellusta hallitsevalla osapuolelle käyttöpyynnön aikana	Security Token	Assertion	Tunnistusväittämä
Federointiosapuoli, joka luo käyttäjälle Security Tokeneita	Claims Provider	Identity Provider	Identiteetintarjoaja

Federointiosapuoli, joka hyödyntää Security Tokeneita sovelluksen valtuutuksessa	Relying Party	Service Provider	Palveluntarjoaja
Käyttäjää kuvaavaa dataa, joka lähetetään Security Tokenissa	Claim	Assertion Statement	Tunnistusväittämä

Luottamusliitäntäpohjaisella kertakirjautumisella tarkoitetaan kertakirjautumista, jossa käyttäjän tunnistamiseen käytetään tunnistusväittämäpohjaista tunnistusteknologiaa. Luottamusliitäntäpohjaisessa kertakirjautumisessa identiteetin- ja palveluntarjoajien välille tehdään luottamusliitoksia. Luottamusliitoksien ansiosta kaikkien identiteetintarjoajien ei tarvitse pitää kirjaa kaikista luottamusliitäntäpohjaiseen kertakirjautumiseen kuuluvista käyttäjistä. Sen avulla voidaan mahdollistaa ulkoisten sidosryhmien pääsy oman yrityksen suojattuihin palveluihin ja omien käyttäjien pääsy ulkoisten sidosryhmien suojattuihin palveluihin. Tämä johtuu siitä, että palveluntarjoajat luottavat moneen eri identiteetintarjoajaan, eikä palveluntarjoajan näkökulmasta ole merkitystä, kuka on varmistanut käyttäjän henkilöllisyyden. Tunnistuksen tarjoava taho tarjoaa käyttäjälle tunnistusväittämät siitä, kuka hän on ja miten hänet tunnistaa. Palveluntarjoaja tunnistaa käyttäjän perustuen näihin tunnistusväittämiin.

Luottamusliitäntäpohjainen kertakirjautuminen on yleistä esimerkiksi suomalaisille korkeakouluille. Useat opiskelijat ja opettajat käyttävät ulkoisten sidosryhmien suojattuja palveluita, joihin pääsy mahdollistetaan luottamusliitäntäpohjaisen kertakirjautumisen avulla. Tästä hyvä esimerkki on Haka-tunnistautuminen. Haka on luottamusliitäntäpohjainen verkosto, jonka piiriin kuuluu 290 000 käyttäjää ja 160 eri suojattua palvelua. Haka-verkoston avulla tapahtuu 11 miljoonaa kirjautumista vuosittain. [15.] Esimerkiksi Metropolian MetCat-kirjastopalveluun on mahdollista tunnistautua Haka-verkostoa vasten. Kuvassa 4 on esitetty Haka-kirjautumisikkuna.

Kuva 4: Haka-kirjautumisikkuna

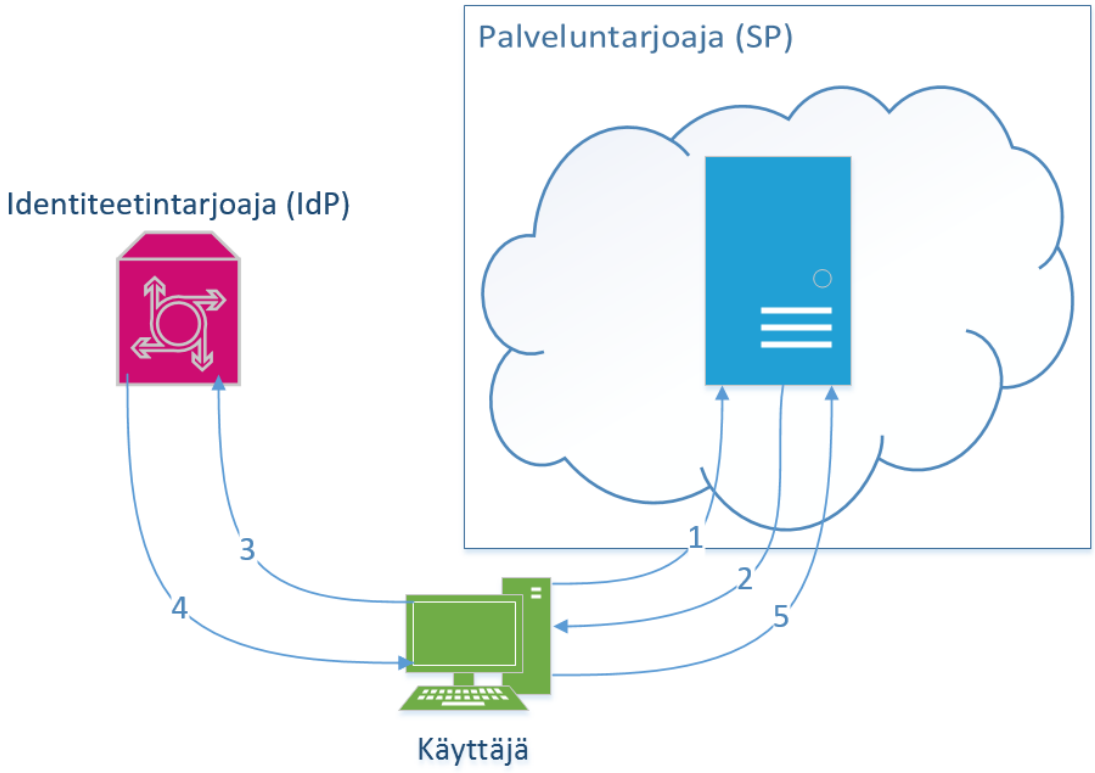
Luottamusliitäntäpohjaisen kertakirjautumisen esimerkkinä voidaan käyttää matkustavaa ihmistä. Passi on matkustajalle ”tunnistusväittämät”, jotka sisältävät todisteita kyseisestä henkilöstä ja siitä, miten hänet tulisi tunnistaa. Tunnistusväittämissä kerrotaan, miltä hän näyttää, mikä on hänen henkilötunnuksensa ja muuta tietoa väittämien omistavasta henkilöstä. Passissa on myös merkintöjä, joista se voidaan todeta aidoksi: mm. vesileima, hologrammi ja passin numero. Myös luottamusliitäntäpohjaisessa kertakirjautumisessa tunnistusväittämät tunnistetaan aidoksi ja tarkastetaan, jottei tunnistusväittämiä pystyttäisi väärentämään. Tunnistusväittämien alkuperä on tärkeää tarkastaa, koska muuten jokin taho voisi generoida tunnistusväittämät saadakseen pääsyn suojattuun resurssiin. Valtio on tässä esimerkissä identiteetintarjoaja, joka tarjoaa tunnistusväittämät käyttäjille. Matkustajan passin tarkastava tullivirkailija toimii samoin kuin digitaalisessa maailmassa toimisi palveluntarjoaja, jonka suojattuun resurssiin käyttäjä pyytää pääsyä. Käyttäjä on tunnistautunut valtiolle saadakseen passin, ja passi takaa sen, että käyttäjä on tunnistautunut valtion hyväksymästi. Täten henkilö on se, joka hän väittää olevansa. Passin avulla tullivirkailija pystyy tunnistamaan käyttäjän ja hänen pääsyoikeutensa kyseiseen valtioon. Tullivirkailija siis tarkastaa, onko matkustaja oikeutettu tulemaan valtioon ja mihin hän on siellä oikeutettu. Esimerkiksi Suomeen saapuva suomalainen on oikeutettu sosiaaliturvaan, mutta ulkomaalainen turisti ei. Luottamusliitäntäpohjaisen

kertakirjautumisen käyttäjien tunnistus ja valtuutus toimii samalla tavalla digitaalisessa ympäristössä. Tällä esimerkillä kuvattiin identiteetintarjoajalähtöinen kertakirjautumisprosessi tunnistusväittämäpohjaisessa kertakirjautumisessa. Esimerkki löytyy kuvasta 2 luvussa 2.2: Kertakirjautumisen eri muodot.

2.3.1 Security Assertion Markup Language (SAML)

SAML (Security Assertion Markup Language) on XML-pohjainen standardi, joka määrittelee tavan kirjautumistiedon siirtämiseen turvallisesti [6]. Se on tapa, jota käytetään laajalti selainkertakirjautumisen toteuttamiseen.

SAML-kirjautumisprosessi toimii lähes samoin tavoin kuten kaikissa luottamusliitäntäpohjaisissa kertakirjautumisteknologioissa. Suuri osa luottamusliitäntäpohjaisista teknologioista perustuukin SAML-standardiin. SAML-standardia hyödyntävän kertakirjautumisjärjestelmän kirjautumisprosessin kuvaus löytyy kuvasta 5.



Kuva 5: SAML-kertakirjautumisprosessi [6].

1. Käyttäjä pyytää pääsyä suojattuun resurssiin.

2. Palveluntarjoaja luo käyttäjälle SAML-pyynnön.
3. Palveluntarjoaja ohjaa pyynnön identiteetintarjoajalle.
4. Identiteetintarjoaja varmistaa käyttäjän henkilöllisyyden ja luo SAML-vastauksen palveluntarjoajalle ja lähettää pyynnön takaisin.
5. Palveluntarjoaja vahvistaa käyttäjän hyväksytyn tunnistuksen ja tarjoaa pääsyn suojattuun resurssiin. [6.]

SAML-viestien suojaaminen hyödyntää olemassaolevaa luottamussuhdetta. Tyypillisesti siihen kuuluu PKI-teknologia (Public Key Infrastructure) [6]. Sen avulla käyttäjät ja tietokoneet voivat vaihtaa tietoja turvallisesti verkossa ja todentaa toisen osapuolen [16].

2.3.2 Active Directory Federation Services (AD FS)

AD FS (Active Directory Federation Services) on Microsoftin palvelu, joka mahdollistaa luottamusliitäntäpohjaisen kertakirjautumisen. AD FS pohjautuu SAML- ja WS-Federation -standardeihin. WS-federation-standardi määrittelee metodit luottamusliitäntäpohjaisen kertakirjautumisen toteuttamiseen.

AD FS:n ja muiden luottamusliitäntäpohjaisten kertakirjautumisjärjestelmien hyötyihin lukeutuu [8]:

1. Mahdollistaa kertakirjautumisen kaikkien sidosryhmien välillä.

2. Ei tarvitse ylläpitää ulkoisten työntekijöiden kirjautumistietoja. Kumppanin identiteetin tarjoava taho lähettää tiedot sen omista käyttäjistään aina tarvittaessa.

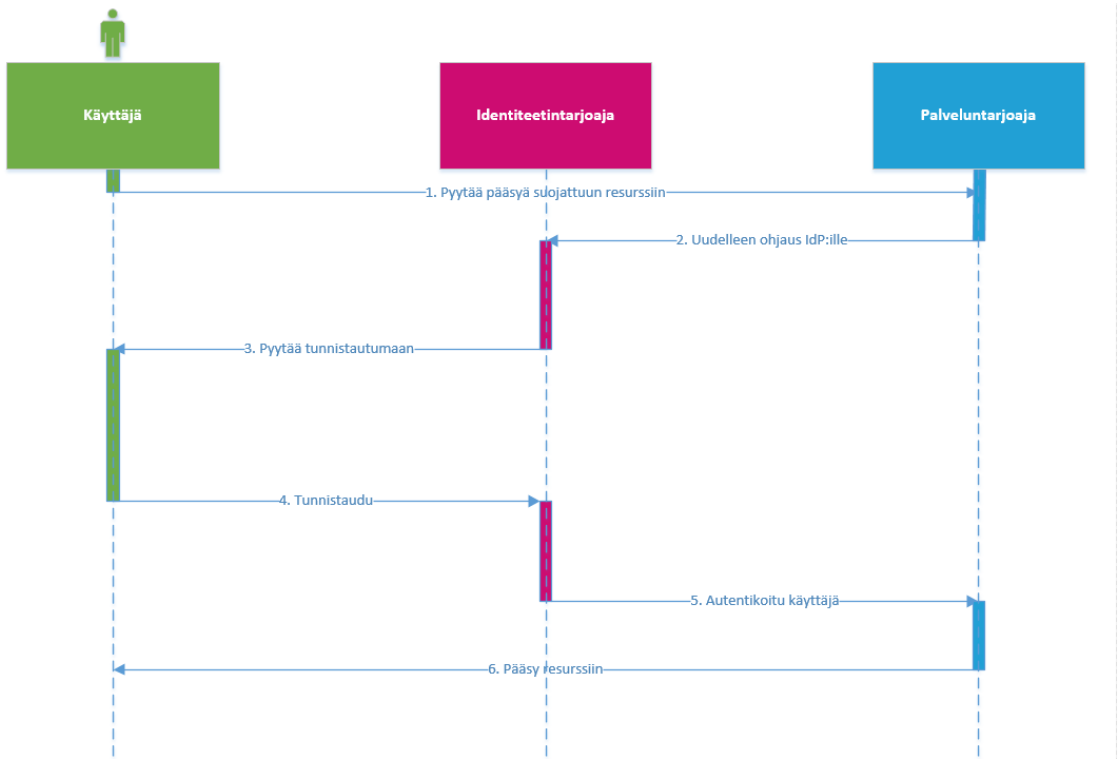
3. Ylläpitäjät pystyvät hallitsemaan kaikkien pääsyä palveluihin yhdestä työkalusta.

4. AD FS mahdollistaa luottamusliitäntäpohjaisen kertakirjautumisen myös muille järjestelmille riippumatta käyttöjärjestelmästä.

2.3.3 Shibboleth

Shibboleth on avoimen lähdekoodin ohjelmistopaketti, joka mahdollistaa luottamusliitäntäpohjaisen kertakirjautumisen. Sen avulla palveluntarjoajat voivat tehdä valtuutuspäätöksiä käyttäjän oikeuksista suojattuun resurssiin. Shibboleth-toteutus soveltaa laajasti luottamusliitäntäpohjaisia standardeja. Pääosin se on toteutettu käyttäen SAML:a käyttäjän ja sen oikeuksien tunnistamiseen. [3.]

Shibboleth lähettää käyttäjistä mahdollisimman vähän tunnistamiseen tarvittavaa tietoa kohdejärjestelmille. Käyttäjän on mahdollista määritellä omalta Shibboleth-sivultaan, mitä tietoja hänen sähköisestä identiteetistä lähetetään kullekin kohdejärjestelmälle. [3.]. Shibboleth ja AD FS ovat molemmat kertakirjautumismenetelmiä, jotka perustuvat luottamusliitäntäpohjaiseen kertakirjautumiseen. Täten molempien kirjautumisprosessi on korkealla tasolla samanlainen. Kuvassa 6 on esitetty palvelulähtöinen kertakirjautumisprosessi.



Kuva 6:Yleiskuvaus luottamusliitäntäpohjaisesta kertakirjautumisprosessista (SP-initiated)

Luottamusliitäntäpohjainen kertakirjautumisprosessi:

1. Pyyntö päästä suojattuun resurssiin. Resurssimonitori tarkistaa, onko käyttäjällä aktiivista istuntoa kyseiseen palveluun. Kun aktiivista istuntoa ei ole saatavilla, käyttäjä ohjataan palveluntarjoajalle.

2. Pyyntö saapuu palveluntarjoajalle ja palveluntarjoaja valmistelee tunnistuspyynnön ja ohjaa pyynnön identiteetintarjoajalle.

3. Identiteetintarjoaja tarkastaa, onko käyttäjällä aktiivista istuntoa kyseiseen kohdejärjestelmään. Kun aktiivista istuntoa ei ole saatavilla, se tunnistaa käyttäjän pyytämällä käyttäjää syöttämään tunnuksensa.

4. Tunnistamisen jälkeen identiteetintarjoaja valmistelee tunnistustodistuksen ja lähettää pyynnön edelleen palveluntarjoajalle.

5. Kun pyyntö saapuu takaisin palveluntarjoajalle se vahvistaa tunnistustodistuksen ja luo aktiivisen istunnon. Palveluntarjoaja valmistelee osan tunnistustodistuksessa olevista tiedoista suojattua resurssia varten ja ohjaa käyttäjän takaisin resurssin luo.

6. Käyttäjä pyytää pääsyä suojattuun resurssiin. Tällä kertaa käyttäjällä on aktiivinen istunto, ja resurssi tunnistaa käyttäjän. Käyttäjä saa pääsyn suojattuun resurssiin.

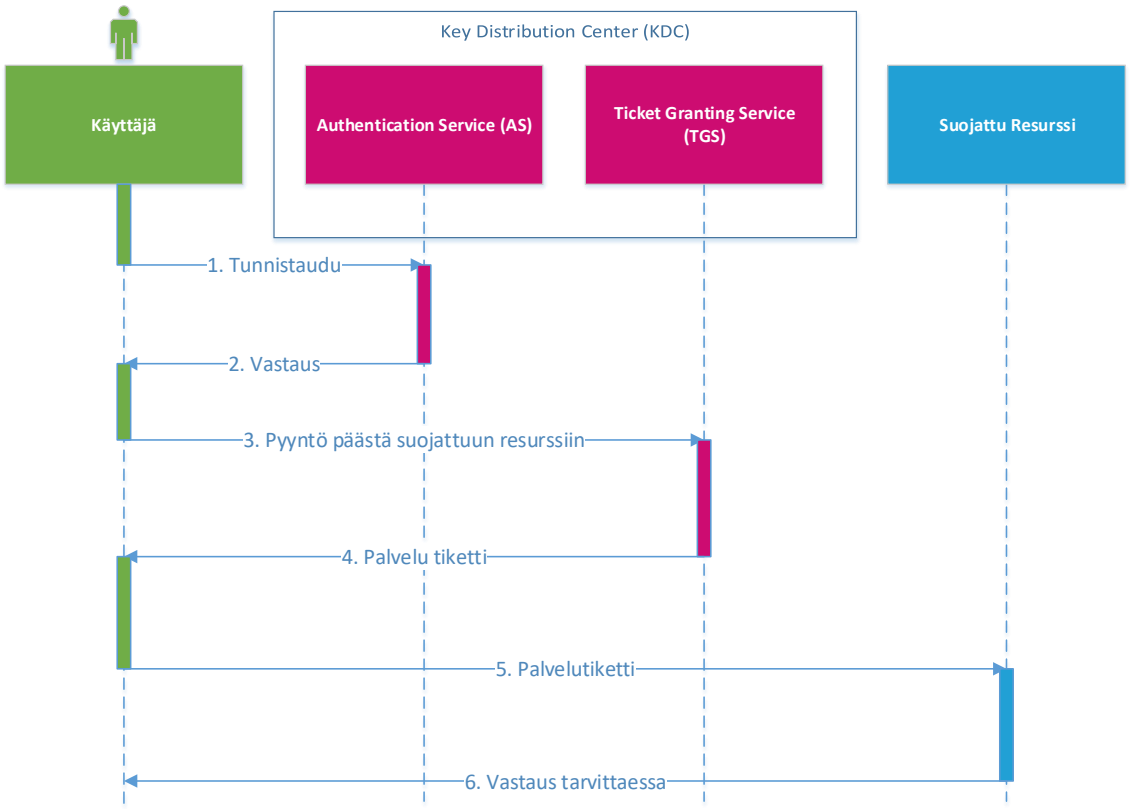
2.3.4 Kerberos

Kerberos-tunnistusprotokolla tarjoaa luotettavan tunnistamisen suojaamattomissa ja avoimissa tietoverkoissa. Kerberos-tunnistamisessa salasanat eivät ikinä liiku palvelinten ja asiakkaiden välillä. Kerberoksessa käytetään käyttäjien tunnistamiseen ns. jaettua salaisuutta eli tunnistautumispyynnöt salataan avaimella, joka on molempien tiedossa [1, s 67-71.]

Palveluntarjoajan ja avaimenhaltijan (Key Distribution Center, KDC) välille ei synny Kerberos-tunnistamisessa tietoliikennettä. Kaikki kommunikointi tapahtuu avaimenhaltijan ja käyttäjän työaseman tai palveluntarjoajan ja käyttäjän työaseman välillä. Käyttäjän työ-

asema säilöö Kerberos-tunnistamiseen tarvittavat tiedot, jottei kohdejärjestelmien muistia kuormiteta. [9.] Kuvassa 7 on esitetty sekvenssikaavio Kerberos-kirjautumisprosessista.

.



Kuva 7: Sekvenssikaavio Kerberos-kirjautumisprosessista

Kuvassa on esitetty sekvenssikaavio tapauksesta, jossa käyttäjä kirjautuu tietokoneelleen ja pyytää pääsyä suojattuun resurssiin, joka on tässä tapauksessa tiedostopalvelin. Sekä käyttäjän tietokone että tiedostopalvelin on lisätty AD (Active Directory) -toimialueeseen. AD Domain Controller toimii tässä tapauksessa avaintenhaltijana. Avaintenhaltijalla on kaksi eri palvelua: AS ja TGS. AS-palvelu (Authentication Server) on käyttäjän ja sen oikeuksien tunnistamiseen käytetty palvelu. TGS-palvelu (Ticket Granting Service) myöntää palvelutikettejä salattuihin resursseihin. Palvelutiketeillä tarkoitetaan ns. pääsylippuja suojattuihin resursseihin

Tunnistautuminen Kerberos-rajapinnan avulla toimii seuraavalla tavalla:

1. Käyttäjä kirjautuu työasemalleen. Työasema luo ja lähettää tunnistautumispyynnön avaintenhaltijan AS-palvelulle.

2. Avaintenhaltija lähettää käyttäjälle tunnistuksen onnistuessa vastauksen, jonka avulla se voi pyytää palvelutikettejä.
3. Käyttäjä pyytää pääsyä tiedostopalvelimeen.
4. Avaintenhaltija tunnistaa käyttäjän pyynnöstä, että se on jo tunnistautunut hyväksyttävästi, joten kirjautumistietoja ei tarvitse syöttää uudelleen. Vastauksena se lähettää käyttäjälle palvelutiketin pyydettyyn palveluun.
5. Käyttäjä lähettää palvelutiketin suojattuun resurssiin ja saa pääsyn kyseiseen palveluun.
6. Tarvittaessa palvelu lähettää vastauksen käyttäjälle esimerkiksi, jos palvelua vaaditaan tunnistautumaan.

Kerberos nojaa turvallisuudessa vahvasti aikaleimoihin. Kerberos-palvelutiketeissä on aikaleima myöntö- ja vanhenemishetkestä. Kun palvelutiketti vanhentuu, käyttäjä ohjataan avaintenhaltijalle. Järjestelmänylläpitäjät voivat määritellä Kerberos-viestin maksimivoimassaoloajan. Tämän työn toteutuksessa käytetty pääsynhallintajärjestelmä pystyy luottamaan Kerberos-tunnistautumisesta saatuun tikettiin ja sallimaan näin pääsyn suojattuun palveluun.

2.3.5 HTTP-otsake

Usein vanhat järjestelmät eivät tue SAML- tai WS-federation-standardeja. Tällöin kertakirjautuminen voidaan toteuttaa käyttäen HTTP-otsaketta. Esimerkiksi tässä työssä toteutettavassa kertakirjautumisjärjestelmässä kirjautumislomake täytetään HTTP-otsakkeen avulla.

HTTP-otsake sisältää kenttiä, joilla tarjotaan tarvittava tieto HTTP-pyyntöön tai vastaukseen. HTTP tukee monia tapoja käyttäjien tunnistautumiseen. Useimmin näistä käytetyt mekanismit voidaan jakaa kolmeen ryhmään.

1. Tunnusten lähettäminen suojataan haastekysymyksillä, joka estää hyökkäyksen HTTP:n kautta. Tämä tapa ei ole tuettu HTTP/1.1-yhteyksissä. [10.]

2. Käyttäjän salasanasta lähetetään tiiviste eli salasana on tiivistetty käyttäen hajautusfunktiota.

3. Käyttäjätunnus ja salasana lähetetään salaamattomana base64-muodossa kohdejärjestelmälle. Tämä tapa on altis salasanan kaappauksiin.

2.4 Tunnistautuminen

Tunnistautumisessa käyttäjä antaa tiedon siitä, kuka hän väittää olevansa. Yleensä tämä tieto annetaan esimerkiksi käyttäjätunnuksen muodossa. Tähän tunnistautumiseen ei voida luottaa, koska käyttäjää ei ole vielä varmennettu. Käyttäjän varmentamiseen vaaditaan vielä varmistus. Näitä varmistustapoja kutsutaan tunnistusmenetelmiksi ja ne voidaan jakaa yleisesti kolmeen eri ryhmään. [1, s 40.]

1. Jotain, mitä käyttäjä tietää. Useimmiten tämä on salasana. Tässä tapauksessa käyttäjää pyydetään syöttämään tieto, joka on liitetty hänen tunnukseensa. [1, s 53-59.]

2. Jotain, mitä käyttäjällä on. Tämä voi olla esimerkiksi pankkitunnukset, pankkikortti tai matkapuhelin. Tällöin käyttäjän tunnistautuessa pyydetään käyttäjää tunnistautumaan käyttäen jotakin, mitä hän omistaa. [1, s 61-66.]

3. Jotain, mitä käyttäjä on. Tämä on jokin biometrinen tunniste käyttäjästä. Käyttäjä tunnistautuu esimerkiksi sormenjäljen tai silmän iiriksen avulla. [1, s 53-66.]

Vahvaksi tunnistamiseksi kutsutaan tunnistamista, jossa käyttäjä tunnistetaan kahden eri yllämainitun tunnistamistavan avulla [11]. Vahva tunnistaminen on käytössä laajasti eri sovelluksissa. Päivittäisessä elämässä vahvaa tunnistamista käytetään esimerkiksi maksettaessa ostoksia pankkikortilla. Pankkikortin tunnusluku kuuluu ryhmään 1 ja itse pankkikortti ryhmään 2. Vahvaksi tunnistautumiseksi ei riitä esimerkiksi pin-koodin vaatiminen salasanan lisäksi.

2.5 Kertakirjautumisratkaisut

Tässä luvussa esitetään valmiita järjestelmiä, joilla on mahdollista toteuttaa kertakirjautuminen.

Azure AD on Microsoftin pilvipohjainen hakemisto- ja identiteetinhallinta-palvelu. Se helpottaa kertakirjautumisen tarjoamista pilvipalveluihin. Azure AD mahdollistaa käyttäjien kirjautumisen sisäisiin ja ulkoisiin palveluihin käyttäen organisaation sisäisiä tunnuksia. [12.]

Kertakirjautuminen on mahdollista toteuttaa Azure AD:lla kolmella eri tavalla:

1. Luottamusliitäntäpohjaisella tunnistustavalla palveluntarjoajien on mahdollista ohjata käyttäjä tunnistautumaan Azure AD:hen. Tässä tapauksessa käyttäjä syöttää omat sisäiset tunnuksensa Azure AD:hen ja pääsee näin käyttämään suojattua resurssia. Jos käyttäjällä on jo valmis istunto, niin hänen ei tarvitse syöttää tunnuksiaan uudestaan vaan hän pääsee suoraan käyttämään resurssia.

2. Salasanojen lähettäminen on mahdollista Azure AD:n avulla. Jos tämä madollisuus otetaan käyttöön, se säilöö käyttäjän tunnukset salattuna ja pystyy tarvittaessa tarjoamaan kirjautumistiedot palveluntarjoajille.

3. Käyttäen ulkopuolista kertakirjautumisen mahdollistavaa tuotetta tai järjestelmää. Nämä voidaan ottaa Azure AD:ssä käyttöön linkittämällä kertakirjautumispalvelu sen tai Office 365:n portaaliin, jonka avulla kyseisen kertakirjautumisjärjestelmän kattaviin tuotteisiin pääsee. Tässä tavassa käyttäjä tunnistautuu sen mukaisesti, miten kyseisen järjestelmän oma kertakirjautuminen on määritelty.

Kertakirjautuminen ja pääsynhallinta voidaan toteuttaa erillisellä pääsynhallintatuotteella. Tuotteita löytyy laaja valikoima. Ne mahdollistavat kertakirjautumisen usealla eri tavalla ja useaan eri järjestelmään ja palveluun. Ne tukevat kattavasti eri kirjautumistapoja sekä kertakirjautumisstandardeja. Usein nämä tuotteet ovat monipuolisesti muokattavissa vaihteleviin asiakasvaatimuksiin. Erillisestä pääsynhallintatuotteesta koituu lisäkustannuksia yritykselle, mutta sen hyödyt ovat niin suuret, että se on useimmissa tapauksissa kannattava hankinta.

Pääsynhallinta pystytään toteuttamaan näiden tuotteiden avulla tehokkaasti siten, että käyttäjillä on tarvittavat oikeudet juuri niihin järjestelmiin, joita he työssään tarvitsevat. Useimpien suoraan pääsynhallintaan tarkoitettujen tuotteiden hyödyiksi luetellaan [13]:

1. Hallittu pääsy palveluihin. Tämän ansiosta yritykset pystyvät hallitsemaan tarkemmin arkaluontoisen tiedon luottamuksellisuutta, koska pääsynhallinta valvoo kyseisten tietojen käyttöä ja niiden käyttöoikeuksien saamista.

2. Työn tehokkuus paranee, koska käyttäjillä on juuri ne oikeudet juuri niihin järjestelmiin, joita he tarvitsevat työnsä tekemiseen tehokkaasti.

3. Järjestelmien valvominen helpottuu. Järjestelmän valvojat pystyvät seuraamaan keskitetystä pääsynhallinnasta palveluiden käyttöä. Väärinkäyttötapaukset pystytään jäljittämään helpommin suoraan sen tehneeseen käyttäjään. Pääsyoikeudet voidaan poistaa käyttäjiltä todella nopeasti ja helposti. Esimerkiksi tunnusten katoamisen jälkeen voidaan käyttäjän pääsy kaikkiin järjestelmiin sulkea keskitetystä pääsynhallintajärjestelmästä.

3 Kertakirjautuminen Spellpointissa

Tässä luvussa esitetään suunnitelma Spellpoint Oy:n kertakirjautumisen toteuttamiseksi. Spellpoint työllistää tällä hetkellä noin 25 henkilöä, joten se kuuluu selvästi pienten yritysten ryhmään [14].

Kertakirjautuminen on toivottu ominaisuus työntekijöiden keskuudessa. Tämän päivän suuntauksena on laitteiden lisääntyminen työkäytössä. Työn tekemiseen ei käytetä enää pelkästään tietokonetta, vaan työntekijöillä on usein käytössä myös mobiililaitteita. Kertakirjautumisen tulisikin toimia yhtä hyvin sekä matkapuhelimella että tietokoneella.

PK-yrityksen pääsynhallinta kannattaa suunnitella hyvin, vaikka yritys työllistääkin vain murto-osan suuryrityksen henkilökunnan määrästä. Budjetti ja vaatimukset eroavat usein laajalti pääsynhallintaprojekteissa, jopa saman kokoluokan yrityksissä. Tästä syystä ratkaisut räätälöidään usein vastaamaan asiakasyrityksen tarkkaa määritelmää. Yritykset pystyvät harvoin turvautumaan samanlaiseen ratkaisuun, joka on toteutettu toisessa yrityksessä. PK-yritysten kertakirjautumisratkaisun budjetti henkeä kohden on usein suurempi kuin suuryrityksissä. PK-yritys tarvitseekin kustannuksiltaan pienemmän, mutta turvallisuudeltaan riittävän pääsynhallinnan ja kertakirjautumisen omaan ympäristöönsä.

Kertakirjautuminen on toteutettavissa ilman siihen tarkoitettua pääsynhallintajärjestelmää. Pääsynhallintajärjestelmän käyttäminen on kuitenkin suositeltavaa. Pitkällä aikavälillä myös implementoinnista johtuvat kustannukset maksavat itsensä takaisin, koska pääsynhallintatuote helpottaa kohdejärjestelmien lisäämistä valmiiseen kertakirjautumisjärjestelmään. Sen avulla kertakirjautumisen laajentaminen uusiin järjestelmiin on mahdollista suhteellisen pienellä työmäärällä. Kertakirjautumisjärjestelmät tukevat laajasti eri ominaisuuksia, joten useimmiten sen valikoimasta löytyy sopiva tapa kertakirjautumisen toteuttamiseen eri kohdejärjestelmille. Sen avulla voidaan myös hallita käyttäjien pääsyä keskitetystä järjestelmistä, eikä käyttäjien hallinta vaikeudu suunnattomasti, vaikka yritys laajenisikin voimakkaasti tulevaisuudessa.

3.1 Spellpointin vaatimukset kertakirjautumiselle

Tässä projektissa Spellpointilla oli kolme päätavoitetta. Niistä ensimmäinen oli toteuttaa Spellpoint Oy:n sisäinen kertakirjautuminen kahteen kohdejärjestelmään ja mahdollistaa kertakirjautumisen lisääminen myös muihin Spellpointin käyttämiin palveluihin. Tulevaisuudessa kertakirjautuminen olisi tarkoitus toteuttaa kaikkiin käytössä oleviin kohdejärjestelmiin. Tämän työn puitteissa kohdejärjestelmiksi valittiin Atlassianin Jira- ja Confluence-palvelut, jotka Spellpoint ostaa palveluna Ambientialta. Toinen vaatimus oli hakemistoarkkitehtuurin yksinkertaistaminen, jolla tarkoitetaan AD:n korvaamista nykyisessä muodossaan. Se tultaisiin korvaamaan toisella käyttäjähakemistolla tai paikallisen hakemiston kahdentamisella sopivaan pilvihakemistoon. Tämä mahdollistaa ketterämmän tavan toimia tulevaisuuden ympäristömuutoksissa. Kolmas vaatimus oli kertakirjautumisen suunnittelu niin, että mikään komponentti ei olisi korvaamaton. Esimerkiksi, jos käyttäjähakemisto halutaan vaihtaa toiseen, se olisi mahdollista tehdä siirtämällä käyttäjätiedot toiseen hakemistoon ja määrittelemällä kertakirjautumistuotteen käyttäjähakemisto uudelleen.

3.2 Vahva tunnistautuminen

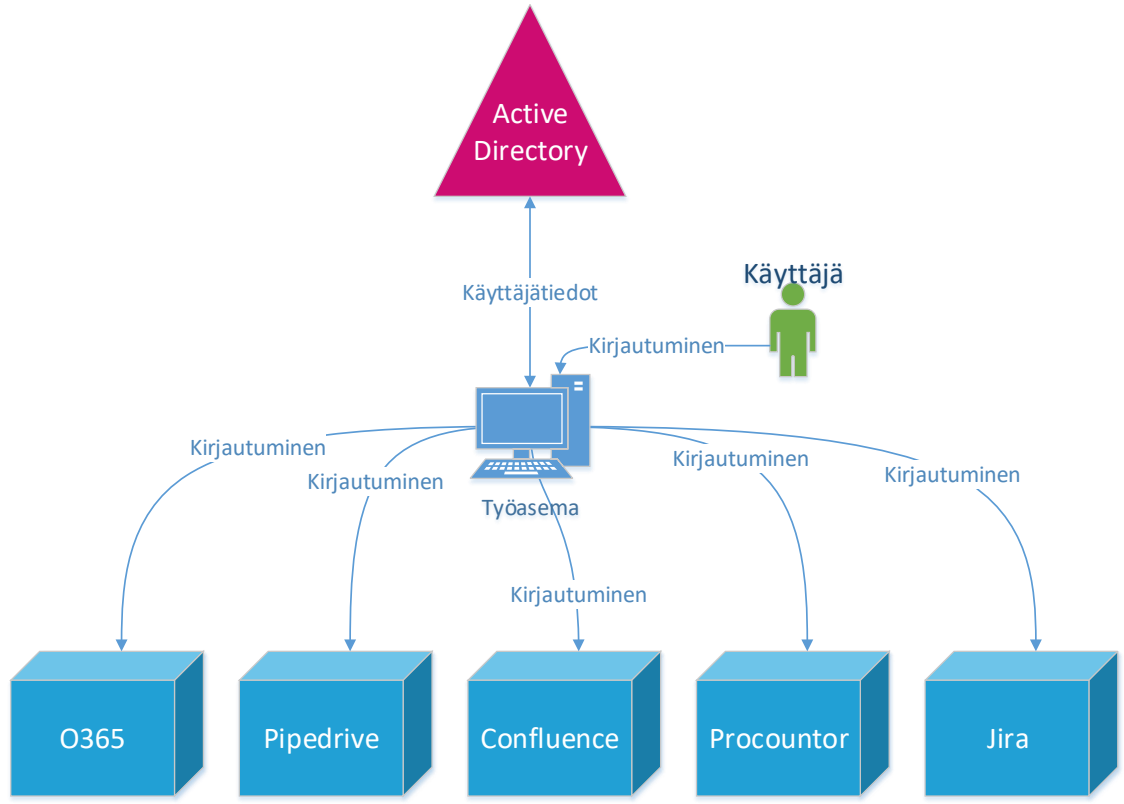
Vahvan tunnistautumisen haluttiin olevan mahdollista myös Spellpointin kertakirjautumisratkaisussa. Eri tunnistusmenetelmistä päätettiin tukea mobiilitunnistusta ja Google Authenticator -tunnistusta.

Mobiilitunnistuksessa käyttäjä syöttää tunnuksensa ja salasanansa kirjautumisikkunaan. Tämän jälkeen hän vastaanottaa esimerkiksi tekstiviestillä tunnistusavaimen, jonka hän syöttää palveluun.

Google Authenticator -tunnistuksessa käyttäjän kirjautuminen toimii käytännössä samalla tavalla kuin mobiilitunnistuksessa. Tämä eroaa vain siten, että tunnistusavaimen tarjoaa Google Authentication -palvelu. Se luo myös 6-8 merkkiä pitkän avaimen kirjautumista varten. Käyttäjällä on asennettuna matkapuhelimeensa Google Authenticator -sovellus, joka tarjoaa kirjautumisen yhteydessä tunnistusavaimen. Kirjautuessaan hän syöttää avaimen ja saa pääsyn kohdejärjestelmään.

3.3 Visio Spellpointin kertakirjautumisesta

Työn alkaessa Spellpointin ympäristö oli kuvan 8 mukainen.

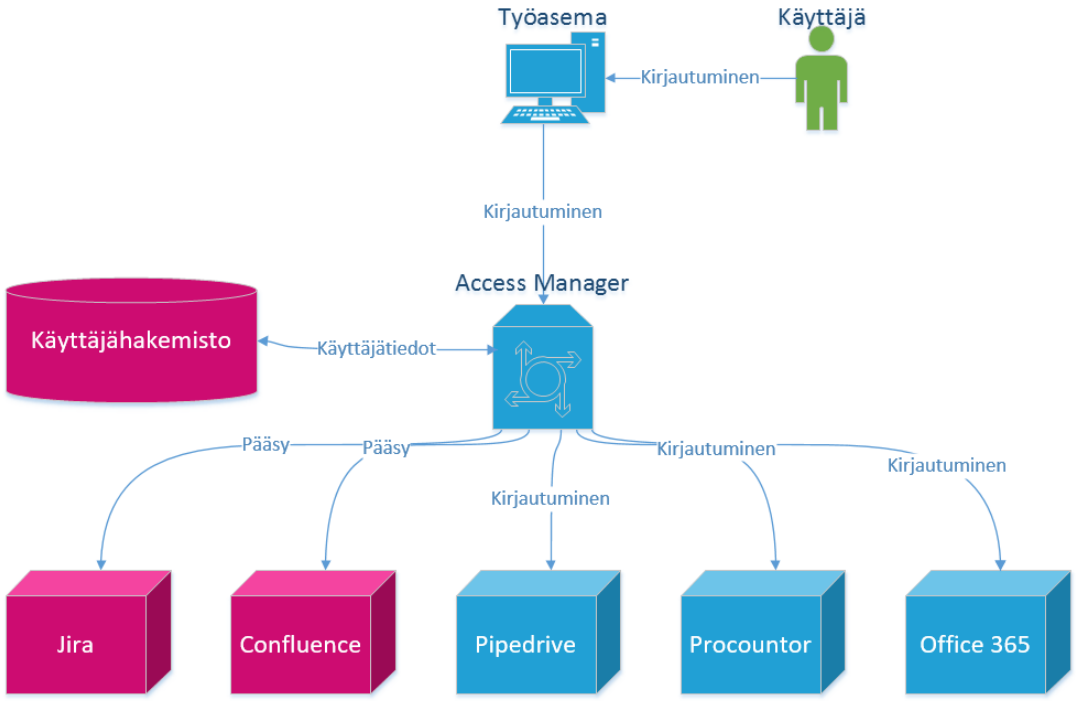


Kuva 8:Spellpointin nykytilanne

Päivittäisen työn tekemiseen vaadittiin päivittäin n. 5 – 10 kirjautumista eri järjestelmiin, joihin jokaiseen oli omat tunnuksensa. Salasanojen ylläpito oli järjestelmäkohtaista. Tämä tarkoittaa sitä, että salasanat kuhunkin järjestelmään vaihdettiin eri aikaan ja kaikki vaati eritasoista salasanaa. Nykytilanteessa työntekijöiden on kirjauduttava erillisillä tunnuksilla, kuhunkin kohdejärjestelmään. Kuvassa on esitetty työntekijöiden useimmiten käyttämät kohdejärjestelmät.

Tämän projektin alkaessa Spellpointissa ei ollut määritelty oman ympäristön henkilötiedoista vastaavaa lähdettä, ja se oli yksi tärkeä asia päättää ennen, kun toteutus aloitettiin. Henkilötietolähteeksi valittiin Procountor-järjestelmä, koska siellä Spellpoint pitää ajantasaista tietoa omista työntekijöistään ja tällöin voidaan olettaa sen olevan luotettava lähde henkilötiedoille. Henkilötiedot ylläpidetään henkilötietolähteessä ja sieltä siirretään tarvittavat käyttäjätiedot käyttäjähakemistoon.

Tässä insinöörityössä toteutettavan kertakirjautumisen ensimmäisen vaiheen puitteissa tavoitetilanne on seuraavanlainen. Käyttäjän jo ollessa kirjautuneena koneelleen ei hänen tulisi syöttää kirjautumistietojaan enää ollenkaan Jira- ja Confluence-palveluun. Tunnistautuminen tehdään pääsynhallintajärjestelmään. Tämän jälkeen käyttäjä saa pääsyn Jiraan ja Confluenceen syöttämättä kirjautumistietojaan uudelleen. Kirjautumistietoja ei tarvitse syöttää uudelleen, koska pääsynhallintajärjestelmä hoitaa kertakirjautumisen taustalla. Kuvassa 9 on esitetty kertakirjautumisen tavoitetilanne.



Kuva 9: Spellpointin tavoitetilanne

Tavoitetilanteessa käyttäjä saa pääsyn Jira- ja Confluence-palveluihin kirjauduttuaan kertakirjautumisjärjestelmään. Tällöin kertakirjautumisen piirin olisi liitetty nämä kaksi palvelua. Muiden palveluiden kertakirjautuminen tullaan toteuttamaan tämän insinöörityön ulkopuolella.

3.3.1 Käyttötapaukset

Tässä luvussa on esitetty käyttötapauksia, jotka toteutettiin tämän insinöörityön aikana sekä tullaan toteuttamaan projektin seuraavissa vaiheissa.

Käyttötapauksen nimi	Käyttäjän kirjautuminen tietokoneelta suojattuun palveluun
Toimijat	Kertakirjautumisjärjestelmä

Esiehdot	Käyttäjällä on käytössään tietokone.
Peruspolku	1. Käyttäjä kirjautuu tietokoneelleen. 2. Käyttäjä pyytää selaimella pääsyä suojattuun resurssiin. 3. Kertakirjautumisjärjestelmä ohjaa käyttäjän tunnistautumaan identiteetintarjoajalle. 4. Onnistuneen tunnistautumisen jälkeen kertakirjautumisjärjestelmä ohjaa pyynnön suojattuun palveluun. 5. Käyttäjä saa pääsyn suojattuun palveluun.
Vaihtoehtoinen polku	1. Käyttäjä kirjautuu tietokoneelleen. 2. Käyttäjä pyytää selaimella pääsyä suojattuun resurssiin. 3. Kertakirjautumisjärjestelmä tunnistaa, että käyttäjä on jo kirjautunut ja ohjaa pyynnön suojattuun palveluun 4. Käyttäjä saa pääsyn suojattuun palveluun.
Jälkiehdot	Käyttäjä on saanut pääsyn suojattuun palveluun.

Käyttötapauksen nimi	Käyttäjän kirjautuminen suojattuun palveluun matkapuhelimesta
Toimijat	Kertakirjautumisjärjestelmä
Esiehdot	Käyttäjällä on käytössä matkapuhelin, jossa on IOS- tai Android-käyttöliittymä ja siihen on ladattu NetIQ-matkapuhelinsovellus. Mobiilisovellusta ei ole lisätty yhdenkään käyttäjän tiliin.
Peruspolku	1. Käyttäjä pyytää pääsyä suojattuun resurssiin käyttäen NetIQ-matkapuhelinsovellusta. 2. Kertakirjautumisjärjestelmä tunnistaa, että matkapuhelinsovellusta ei ole rekisteröity yhdenkään käyttäjän tiliin. 3. Kertakirjautumisjärjestelmä estää pääsyn suojattuun palveluun 4. Kertakirjautumisjärjestelmä pyytää käyttäjää lisäämään selaimella matkapuhelinsovelluksen omiin tietoihinsa kertakirjautumisjärjestelmän käyttöliittymästä.
Vaihtoehtoinen polku	1. Käyttäjä pyytää pääsyä suojattuun palveluun käyttäen NetIQ-matkapuhelinsovellusta. 2. Kertakirjautumisjärjestelmä tunnistaa, että matkapuhelinsovellusta on rekisteröity käyttäjän tiliin.

	3. Kertakirjautumisjärjestelmä ohjaa käyttäjän suojattuun palveluun.
Jälkiehdot	Käyttäjä pääsee kirjautumaan tai hänet ohjataan lisäämään sovellus omiin tietoihinsa.

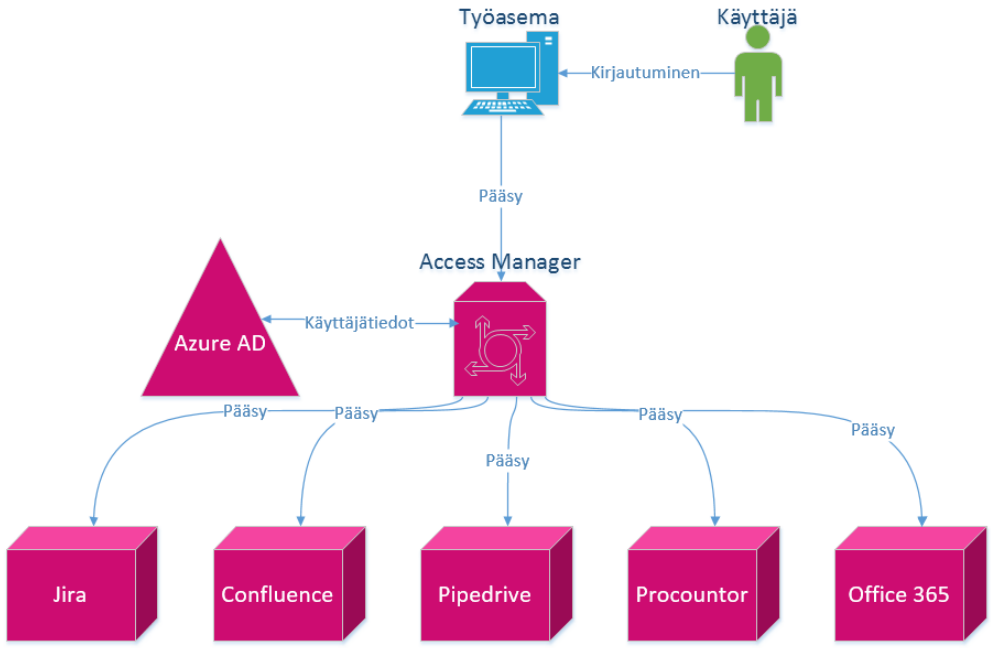
Käyttötapauksen nimi	Käyttäjän pääsy suojattuun palveluun estetään
Toimijat	Kertakirjautumisjärjestelmä
Esiehdot	Käyttäjällä on käytössään tietokone tai matkapuhelin.
Peruspolku	1. Käyttäjä pyytää pääsyä suojattuun palveluun. 2. Kertakirjautumisjärjestelmä ohjaa käyttäjän tunnistautumaan. 3. Käyttäjän syöttämiä kirjautumistietoja ei hyväksytä. 4. Kertakirjautumisjärjestelmä estää pääsyn suojattuun palveluun. 5. Kertakirjautumisjärjestelmä pyytää käyttäjää ottamaan yhteyttä järjestelmänylläpitäjään.
Vaihtoehtoinen polku	
Jälkiehdot	Käyttäjä ei saanut pääsyä suojattuun palveluun.

3.3.2 Pitkän tähtäimen kehityssuunnitelma

Spellpointin tavoitteena on vaihtaa nykyinen AD-käyttäjähakemisto kokonaan Azure AD -käyttäjähakemistoon. Tällöin Azure AD voitaisiin määrittää pääsynhallintatuotteen käyttäjähakemistoksi. Käyttäjähakemisto tullaan kahdentamaan juuri Azure AD:hen, koska Office 365 tilaukseen kuuluu Azure AD:n ilmaisversio. Azure AD:n ilmaisversio mahdollistaa sen käyttämiseen NAM:n käyttäjähakemistona. Nykyinen AD voidaan kahdentaa Azure AD:hen Azure AD connect -palvelun avulla, jolla hakemistot voidaan kahdentaa helposti toistensa kopioiksi. Azure AD sopii erinomaisesti Spellpointin ympäristöön, koska käytössä on muitakin Microsoftin tuotteita, kuten Office 365, Yammer ja Sharepoint.

Tavoitteena on myös vaihtaa järjestelmien integraatiotapa SAML-standardiin, kun kaikkiin käytössä oleviin palveluihin tulee SAML-tuki. Tällöin arkkitehtuurista tulee kuvan 10

mukainen. Tämä parantaisi käyttökokemusta huomattavasti, koska tällöin ei tarvitse huomioida pääsynhallintatuotteen käyttöliittymää muuten kuin valvonta- ja ylläpitotehtävien yhteydessä.



Kuva 10: Luottamusliitäntäpohjainen kertakirjautumisarkkitehtuuri käyttäen pääsynhallintatuotetta

SAML-tuen ansiosta olisi mahdollista siirtyä luottamusliitäntäpohjaiseen kertakirjautumiseen. Luottamusliitäntäpohjainen kertakirjautuminen mahdollistaisi myös sen, että käyttäjät syöttävät kirjautumistietonsa vain yhden kerran. Kaikkien työkoneet lisättäisiin käyttäjähakemistoon, joka määritettäisiin pääsynhallintatuotteen identiteetintarjoajaksi. Tämä tarkoittaa sitä, että pääsynhallintatuote luottaa suoraan käyttäjän kirjautumiseen, eikä tämän tarvitse tunnistautua uudelleen.

4 Kertakirjautumisratkaisun toteuttaminen Spellpoint Oy:lle

Tässä luvussa kuvataan kertakirjautumisen toteutus. Suurin osa kertakirjautumistuotteista kykenee toteuttamaan kertakirjautumisratkaisun monella eri tavalla. Spellpointin vaatimuksiin kuuluneet Jira- ja Confluence-integraatiot tulevaan kertakirjautumisjärjestelmään olivat tuotteen valinnassa suuressa roolissa.

Atlassianin Confluence ja Jira tarvitsevat lisäosan tukeakseen SAML-rajapintaa. SAML-integraatio on kyseisiin työkaluihin mahdollinen, mutta Spellpointille palveluna Atlassianin työkaluja tarjoava Ambientia ei voinut taata heidän järjestelmän yhteensopivuutta SAML-tuen mahdollistavan lisäosan kanssa. Tämän vuoksi kertakirjautuminen näihin palveluihin päätettiin toteuttaa lomakkeentäyttömetelmällä (form fill), jossa kertakirjautumisjärjestelmä täyttää ja lähettää kirjautumislomakkeen käyttäjän puolesta.

Vaatimus siitä, että pääsynhallintatuotteen olisi tuettava lomakkeentäyttömenetelmää rajasi vaihtoehtoja. Valinta tehtiin kahden todella kattavan ja monipuolisen pääsynhallintatuotteen välillä, jotka olivat CAM (Dell One Identity Cloud Access Manager) ja NAM (NetIQ Access Manager). Molemmilla tuotteilla voidaan tehdä Spellpointin vaatimukset täyttävä kertakirjautumisratkaisu. Molemmat tuotteet ovat hyvin muokattavissa ja räätälöitävissä niin, että kertakirjautumisjärjestelmä tulisi olemaan mahdollisimman muutoskykyinen.

NAM:n tuoteominaisuudet ovat erinomaiset. Sitä pystyy muokkaamaan monipuolisesti erilaisiin vaatimuksiin sopivaksi. Spellpointilta löytyy suuri määrä osaamista ja kokemusta kyseisestä tuotteesta, joten sen ylläpitäminen olisi helppoa. CAM on ominaisuuksiltaan myös erittäin hyvä tuote. Sillä pystyy toteuttamaan monipuolisesti erilaisia kertakirjautumisratkaisuja, mutta jotkin ominaisuudet eivät ole yhtä monipuolisia kuin NAM:lla. CAM:in hyviin ominaisuuksiin kuuluu helppo konfigurointi. Kaikki konfiguraatio tehdään graafisesta käyttöliittymästä ja kaikki yleisimmät integraatiot esim. Office 365, Active Directory ja SharePoint ovat tehtävissä helposti valmiilla ominaisuuksilla.

Yhtenä vaihtoehtona harkittiin myös pelkän Azure AD:n avulla toteutettavaa luottamusliitäntäpohjaista kertakirjautumista. Valittiin kuitenkin ratkaisu, jossa kertakirjautumisen hoitaa pääsynhallintatuote, jotta liitäntä- ja hallintamahdollisuudet ovat mahdollisimman monipuoliset.

Näistä vaihtoehdoista parhaimmaksi katsottiin NAM. Siitä on tarjolla kolme eri kaupallista versiota. Sisäiseen käyttöön valittiin ns. täyden pääsynhallintatuotteen, joka sisältää kaikki mahdolliset ominaisuudet.

4.1 NetIQ Access Manager

NAM on kertakirjautumiseen erikoistunut tuote, joka kuuluu NetIQ IAM -tuoteperheeseen. NAM:in tärkein tarkoitus on suojata yrityksen resurssit päästämällä vain oikeutetut käyttäjät käyttämään niitä.

NAM koostuu viidestä pääkomponentista:

1. Hallintapaneelista tehdään kaikki tuotteeseen liittyvät hallintatoimet.
2. Identiteetintarjoaja on vastuussa käyttäjätietojen hallinnasta, tunnistamisesta ja valtuuttamisesta.
3. Access Gateway avustaa identiteetintarjoajaa toteuttamaan kertakirjautumisen.
4. MobileAccess mahdollistaa kertakirjautumisen matkapuhelimella.
5. Käyttöliittymästä loppukäyttäjät pääsevät käyttämään tuotetta.

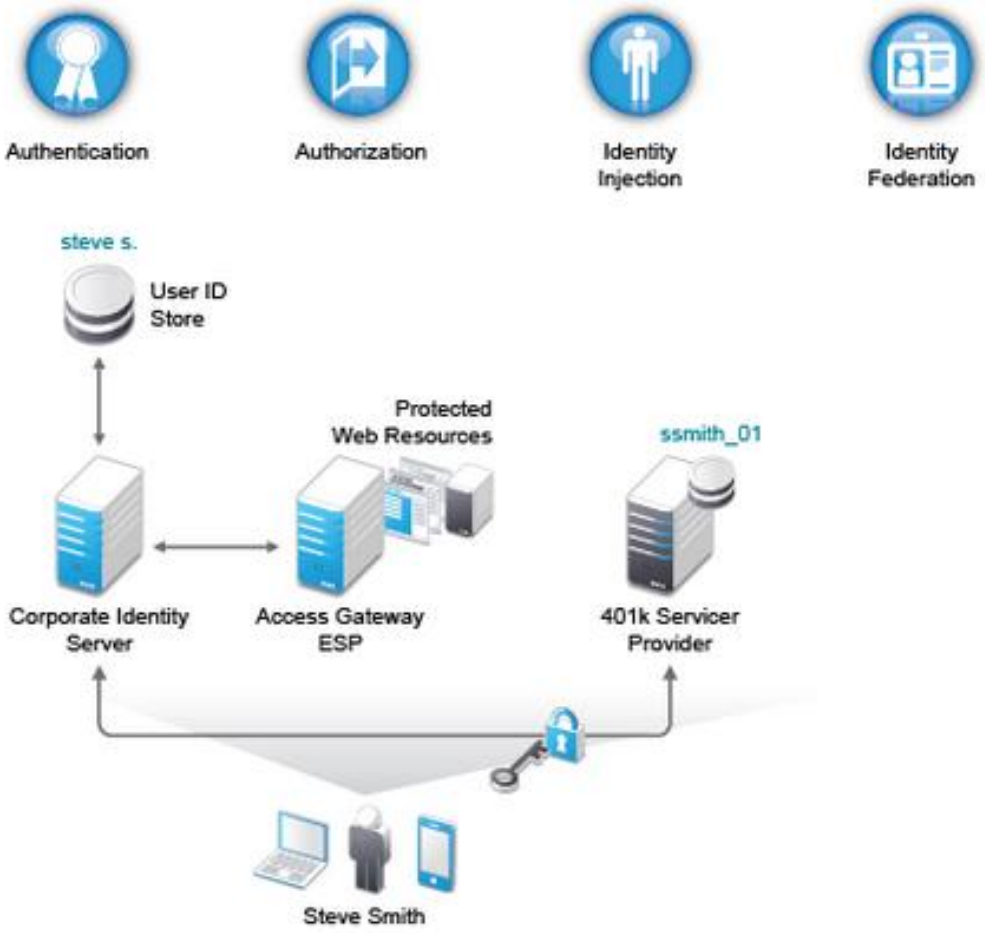
NAM:in ominaisuuksiin kuuluu neljä pääominaisuutta. Niistä ensimmäinen on tunnistaminen. Nam tukee monia tunnistustapoja, kuten tunnus/salasana, Radius token -pohjainen tunnistaminen, X.509 digitaaliset sertifikaatit, Kerberos, riskipohjainen tunnistaminen, aikapohjainen kertasalasana (TOTP), sosiaalinen tunnistautuminen ja OpenID Connect. Nämä tunnistamistavat on selitetty tarkemmin liitteessä 1: Tunnistamisteknologiat. Käyttäjätiedot säilytetään LDAP-hakemistossa, jossa käyttäjät tunnistautuvat. Toinen pääominaisuus on valtuuttaminen. Valtuuttamisprosessilla tunnistetaan mihin käyttäjä on oikeutettu kohdejärjestelmässä. NAM:n avulla voidaan määritellä rooleja ja sääntöjä, joiden avulla voidaan määritellä käyttäjien oikeudet kohdejärjestelmissä. Valtuutuspäätökset tehdään perustuen sääntöihin. NAM mahdollistaa lukuisien eri sääntöjen määrittelemisen. Kolmas pääominaisuus on Identiteetin injektointi. NAM:in Access Gateway -komponentti mahdollistaa käyttäjätietojen haun identiteetintarjoajalta ja niiden injektoinnin kirjautumisprosessissa. Identiteettitiedot voidaan injektoida HTML-otsakkeessa, tietokantakyselyssä tai käyttää tunnistautumisotsaketta. Tätä ominaisuutta voidaan käyttää sekä tunnistautumiseen että valtuuttamiseen. Neljäs pääominaisuus on luottamusliitäntäpohjainen kertakirjautuminen.

NAM suojaa verkkoresurssit salaamalla niiden oikean URL-osoitteen sisäisessä ja ulkoisessa verkossa. Resurssien käyttö ei ole riippuvainen siitä, missä käyttäjä on. Se tarjoaa pääsyn suojattuihin resursseihin sekä kotoa että toimistolta. Suojattuihin resursseihin pääsy ei ole laiteriippuvainen, koska NAM tarjoaa saman kokemuksen kertakirjautumi-

sesta sekä tietokoneella että matkapuhelimella. Tämä on loistava ominaisuus, koska nykyaikana työnteko ei ole sidottu tiettyyn paikkaan tai aikaan. Lähes kaikilla on työkäytössään matkapuhelin, joka on useimmiten mukana, vaikka ei olisikaan tietokoneensa ääressä.

NAM automatisoi roolien ja sääntöjen avulla käyttäjien oikeuksien poiston ja lisäyksen kohdejärjestelmiin. Tämän ansiosta pääsy voidaan tarjota nopeasti käyttäjille, eikä ylläpitäjien tarvitse etsiä esimerkiksi tiettyä ryhmäjäsenyyttä, jotta käyttäjät saavat pääsyn resurssiin. Esimerkiksi SAML-tuetussa kohdejärjestelmässä tällä tavoin voidaan myös varmistua siitä, että pääsy on yrityksen määrittelemien sääntöjen mukainen, koska NAM ei anna lisätä kiellettyjä oikeusyhdistelmiä (SoD, Segregation of Duties).

NAM:in avulla voidaan jakaa vain ne käyttäjätiedot, joita palveluntarjoajat tarvitsevat käyttäjän tunnistamiseen. Se suojelee käyttäjien yksityisyyttä, koska vain vähäisin mahdollinen määrä käyttäjän tietoja siirretään suojatun yhteyden kautta. Sen avulla voidaan pysyä helposti ajan tasalla yksityisyyttä määrittelevien lakien ja säännösten kanssa [17]. Arkkitehtuurikuvaus NAM:ista on esitetty kuvassa 11.



Kuva 11: NAM-arkkitehtuuri [17].

Kuvassa 11 on nähtävissä NAM:in pääkomponentit. Käyttäjätiedot säilytetään käyttäjähakemistossa. Palveluihin pääsy voidaan toteuttaa, joko Access Gatewayn tai suoraan identiteetintarjoajan avulla.

4.2 Tekninen toteutus

Tässä luvussa kuvaillaan Spellpointille tehty kertakirjautumisprojektin ensimmäinen vaihe. Esitetyt kuvat on otettu toteutuksen kehitysympäristöstä.

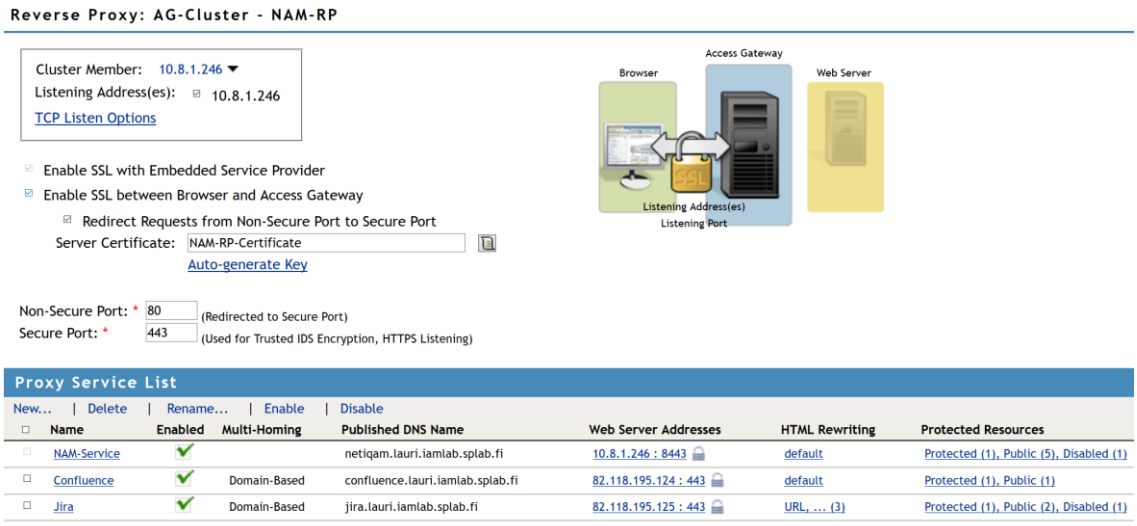
Spellpointin kertakirjautumisratkaisun keskiössä on siis NetIQ Access Manager. Käyttäjähakemistona toimii eDirectory, joka on kahdennettu manuaalisesti paikallisen AD:n kanssa. Käyttäjähakemistoksi valittiin eDirectory, koska se on hakemisto, joka tulee oletuksena NAM:in mukana ja tällöin yhteensopivuus pääsynhallintajärjestelmän kanssa on

paras mahdollinen. Kun käyttäjät kirjautuvat kertakirjautumisjärjestelmään ja sen suojaamiin palveluihin, he käyttävät eDirectory-tunnuksiaan. Nämä tunnukset ovat samat kuin heidän tähän asti käyttämät AD-tunnuksensa, koska jokainen käyttäjä on kahdennettu manuaalisesti NAM:in käyttämään eDirectoryyn.

NAM:n asennus on erittäin nopeasti tehtävissä, jos käytetään NAM Appliance -asennusta. Appliancella tarkoitetaan sitä, että NAM ja palvelimenkäyttöjärjestelmä tulevat samasta asennusmediasta. Asennus erosi normaalin SUSE Linux Enterprise Serverin asennuksesta vain siten, että asennuksen aikana täytyi täyttää muutama kohta tietoa NAM-alustusta varten. Asennus asentaa kaikki tuotteen arkkitehtuurin kannalta merkittävät komponentit. Näihin komponentteihin kuuluu Access Gateway, Identity Server ja Administration Console. Kaikki näistä asennettiin samalle palvelimelle.

Asennus määritteli tuotteen mukana tulleen eDirectoryn automaattisesti käytettäväksi käyttäjähakemistoksi. Asennuksen aikana käyttäjähakemistoon määriteltiin myös adminkäyttäjä, jolla on kaikki käyttöoikeudet pääsynhallintajärjestelmään. Tällä käyttäjällä tehtiin kaikki konfiguraatio teknistä toteutusta varten.

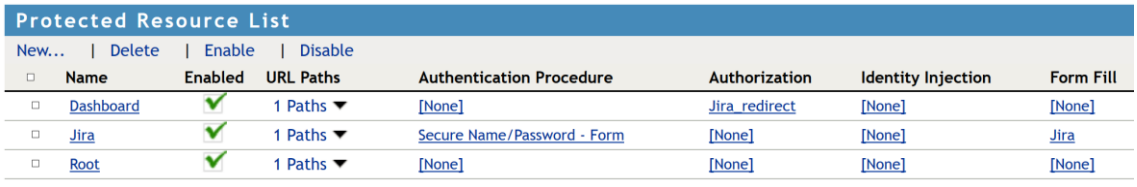
Kun asennus oli tehty, tuli kertakirjautumisen toteuttamiseksi määrittää uusi välityspalvelin (reverse proxy) NAM:in Access Gateway:hyn. Välityspalvelin välittää viestit käyttäjän ja palvelimen välillä. Näin käyttäjä ja palvelin eivät ikinä lähetä suoraan viestejä toisilleen, vaan välityspalvelin välittää ne niiden puolesta. Se suojelee käyttäjien henkilötietoja ja suojaa käyttäjiä ja palveluita verkkohyökkäyksiä vastaan. Sen avulla voidaan julkaista monia palveluja saman URL-osoitteen alla, vaikka ne eivät fyysisesti olisikaan samassa palvelimessa. Kuvassa 12 on esitetty NAM:in Access Gatewayn asetukset.



Kuva 12: Välityspalvelimet

Välityspalvelimeen tehtiin kaksi uutta palvelua (Proxy Service) oletuksena olevan NetIQ Access Manager (NAM-Service) -palvelun lisäksi. Palvelut määritettiin suojaamaan eri verkkopalveluita. NAM:issa välityspalvelimeen määritettyihin palveluihin voidaan määrittää suojattuja resursseja. NAM suojaa kaikki ne palvelun osat, joita ei ole julkaistu suojattuina resursseina. Tässä projektissa luotiin siis kaksi välityspalvelua ja niihin molempiin omat suojatut resurssit Jira- ja Confluence-palveluille.

Kuvassa 13 on esitetty kaikki toteutuksen vaatimat suojatut resurssit Jiralle. Suojatulle resurssille voidaan määrittää tunnistustapa, valtuutustapa, identiteetin injektointi ja lomakkeentäyttötapa. Kaikkia ei ole kuitenkaan pakollista määrittää. Määritimme tunnistustavaksi käyttäjätunnus/salasana-lomakkeen (Secure Name/Password -Form), jossa käyttäjä tunnistautuu käyttäen eDirectory-tunnuksiaan.



Kuva 13: Suojatut resurssit Jirassa

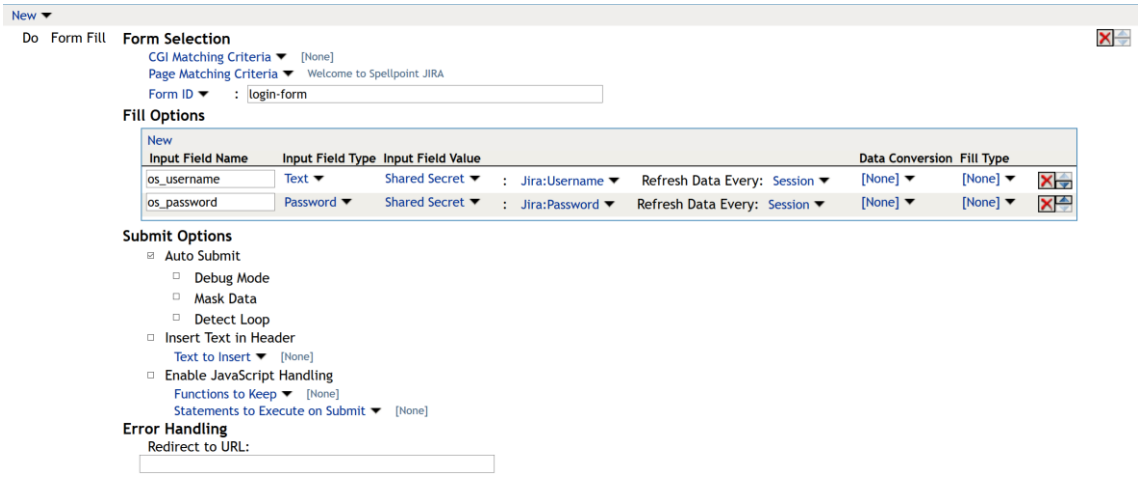
Suojattuja resursseja täytyi tehdä Jira-palvelua varten kolme kappaletta. Dashboard (/secure/dashboard.jsp) on uudelleenohjausta varten. Se kattaa Jiran toisen kirjautumisikkunan, jota ei haluttu ottaa käyttöön kertakirjautumisen yhteyteen. Siihen on määritelty

uudelleenohjaus Jira (/Login.jsp) -nimiseen suojattuun resurssiin. Jira on tehty kirjautumista varten. Siihen on kytketty lomakkeentäyttömenetelmää käyttävä kirjautuminen. Root (/*) on tehty kattamaan koko palvelu. Sen avulla saadaan palvelu kokonaan käyttäjien käyttöön. Kuvassa 14 on esitetty Jira-palvelun kirjautumislomake.

```
<form id="login-form" class="aui" action="/login.jsp" method="post">
  <div class="form-body">
    <fieldset>
      <div class="field-group">
        ::before
        <label accesskey="u" for="login-form-username">
          <u>U</u>
          sername
        </label>
        <input id="login-form-username" class="text medium-field" name="os_username" value="" type="text"></input>
        ::after
      </div>
      <div class="field-group">
        ::before
        <label id="passwordlabel" accesskey="p" for="login-form-password"></label>
        <input id="login-form-password" class="text medium-field" name="os_password" type="password"></input>
        ::after
      </div>
```

Kuva 14: Jira-kirjautumislomake

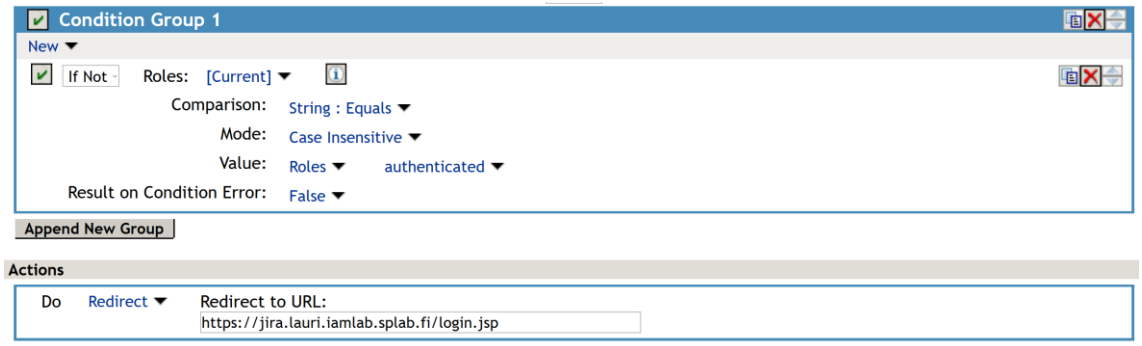
Kirjautumislomakkeen tiedot täytyi tutkia kohdejärjestelmän lähdekoodista. Oli myös kirjoitettava sääntö, jossa tunnistetaan lomakkeen sisältävä sivu. Lomakkeen sisältämään sivun tunnistamiseen on monta eri tapaa. Tunnistus voidaan tehdä käyttäen lomakkeen nimeä, sivulla esiintyvää tekstiä tai URL-osoitteessa olevaa REST- tai SOAP-kutsun osaa. Tässä tapauksessa käytettiin sekä lomakkeen nimeä että sivulla esiintyvää tekstiä lomakkeen tunnistamiseen. Lomake oli helposti tutkittavissa internetselaimella. Kuvassa 15 on nähtävissä, kuinka lomakkeentäyttö on luotu käyttäen kohdejärjestelmän lähdekoodin tietoja kirjautumislomakkeesta.



Kuva 15: Jira-lomakkeentäyttö

Kirjautumislomakkeen tulkinnan jälkeen lomakkeentäyttömenetelmä oli yksinkertainen toteuttaa. Kirjautumislomakkeen kenttien nimet tuli täyttää niille varatuille paikoille.

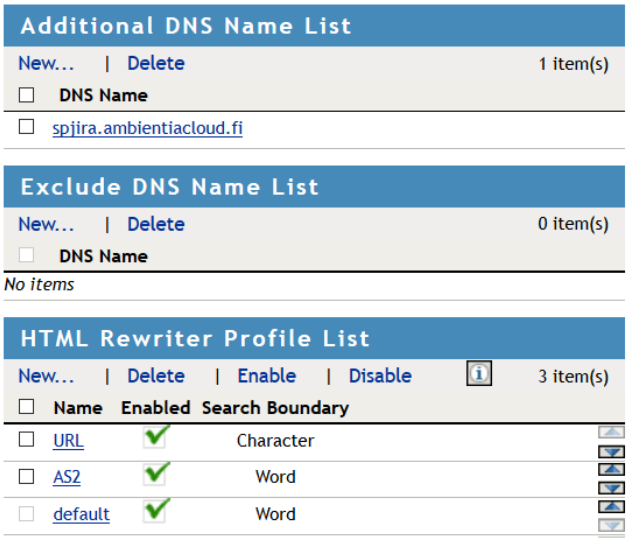
Jirassa oli kaksi eri URL-osoitetta, joista käyttäjä pystyi kirjautumaan sisään palveluun. Kirjautuminen uudelleenohjattiin aina käyttämään samaa kirjautumisikkunaa. Uudelleenohjaus tehtiin käyttäen tuotteen sisäisiä rooleja. Kuvassa 16 on esitetty uudelleenohjausta varten tehty konfiguraatio.



Kuva 16: Jira-uudelleenohjaus

Uudelleenohjausta varten tehty sääntö tarkastaa käyttäjän sen hetkiset roolit. Mikäli käyttäjältä puuttuu authenticated-rooli, hänet ohjataan kirjautumaan kirjautumisikkunaan. Authenticated-rooli on tuotteen sisäinen rooli, joka myönnetään käyttäjälle tämän kirjauduttuaan kertakirjautumisjärjestelmään. Ehdon alin rivi kertoo sen, mitä tehdään, jos vertailua ei ole mahdollista tehdä esimerkiksi tapauksessa, joissa yhteyksissä käyttäjähakemiston kanssa on jotain vikaa. Tässä ehdossa määriteltiin uudelleenohjaamaan käyttäjä kirjautumissivulle.

NAM-välityspalvelimen avulla julkaistiin kohdejärjestelmät eri URL-osoitteessa kuin niiden sovelluspalvelimet olettavat. Järjestelmän lähdekoodi kuitenkin sisälsi viitteitä todelliseen URL-osoitteeseen, jolloin kaikki komponentit eivät näkyneet oikein. Tähän NAM:issa on ratkaisuna HTML-uudelleenkirjoitus (rewriting). Sen avulla pystyttiin uudelleen kirjoittamaan sivun sisältämiä URL-osoitteita tai muita tekstejä. Kuvassa 17 on nähtävissä Jira-järjestelmälle luodun välityspalvelimen HTML-uudelleenkirjoituskonfiguraatio.



Kuva 17: HTML-uudelleenkirjoitus

Kohdejärjestelmän oikea DNS-nimi oli lisättävä vaihtoehtoiseen DNS-listaan, koska tällöin NAM osaa toimia oikein kohdatessaan kyseisen osoitteen. Määriteltiin myös 2 uutta profiilia uudelleenkirjoitukselle. Uudelleenkirjoitusprofiileja on kahta eri tyyppiä: Word ja Character. Word-tyyppinen profiili vaihtaa sivulla esiintyvän tekstin seasta sanoja. Jos etsitty sana olisi esimerkiksi ’tieto’, se vaihtaisi sanat tieto ja tietokone. Se ei kuitenkaan vaihtaisi sanaa lentokone. Character-tyyppinen profiili etsii myös sanoja sivun tekstistä. Jos etsitty sana olisi esimerkiksi ’kone’, se vaihtaisi sanat: lentokonehuolto, lentokone ja konehuone. Eli nämä ovat kaksi erilaista etsintämenetelmää, joista voi valita tarvitsemansa.

Confluence-palvelulle kertakirjautuminen oli huomattavasti yksinkertaisempi toteuttaa. Confluencelle oli vain yksi kirjautumissivu ja HTML-uudelleenkirjoitusta ei tarvittu sen sisällön näyttämiseen. Confluencelle kuitenkin luotiin suojatut resurssit ja lomakkeentäyttö täysin samoin periaattein kuin Jiralle tehtiin.

Vahvaa tunnistusta varten määriteltiin Google Autheticatorin -tunnistusprofiili. Aina käyttäjän kirjautuessa kertakirjautumisjärjestelmään tulee tämän kirjoittaa salasanan jälkeen Google Authenticator -mobiilisovelluksesta saatu pääsykoodi.

Näiden konfiguraatioiden jälkeen kertakirjautumisjärjestelmä pystyi tarjoamaan pääsyn kahteen kohdejärjestelmään yhden kirjautumisen jälkeen.

5 Johtopäätökset

Työn jälkeen ensimmäinen johtopäätös oli, että kertakirjautumisen toteuttamiseen kannattaa soveltaa siihen suunniteltua pääsynhallintatuotetta. Pääsynhallintatuotteen avulla on jatkossa joustavampi mukautua siihen, mihin suuntaan yritys kehittyy.

Toinen johtopäätös on, että PK-yritys voi käyttää täysin samoja tuotteita kuin suuremmat yrityksetkin. Tämä on mahdollista, koska yleensä lisenssihinnoittelu menee käyttäjämäärän mukaan. Pieniä hintaeroja voi olla, sillä tuotteiden lisenssihinnat neuvotellaan aina tapauskohtaisesti, mutta tämä ei ole niin merkittävä summa, että se vaikuttaisi projektin budjettiin radikaalisti pienellä käyttäjämäärällä.

Kolmantena johtopäätöksenä on, että toteutuskustannus / henkilö kasvaa yrityskoon pienentyessä. Tällä tarkoitetaan sitä, että mikäli kertakirjautumisprojektin toteutus ostetaan ulkoiselta taholta, saattaa järjestelmän implementaatiokustannukset suhteessa käyttäjämäärään nousta suureksi verrattuna isompiin yrityksiin. Tämä johtuu siitä, että samojen ominaisuuksien implementointi pääsynhallintatuotteella on aivan yhtä työlästä 100 käyttäjälle kuin 100 000 käyttäjälle. Tämä on samalla myös huomioitava IAM-palveluja tarjoavissa yrityksissä. Eli olisi tuotteistettava helposti implementoiva, joka sisältäisi yleisimmät vaatimukset toteuttavan kertakirjautumisratkaisun.

Neljäs johtopäätös on, että tuotevalinta kannattaa tehdä huolellisesti. Kannattaa valita tuote, joka vaatii mahdollisimman vähän kustomointia toteuttaakseen kertakirjautumisen vaatimukset. Tällöin tarvitsee kehittää mahdollisimman vähän omia lisäosia kertakirjautumisen toteutukseen ja pääsynhallintatuote toimii parhaalla mahdollisella tavalla. Suurin osa valmiista tuotteista on kuitenkin todella monipuolisesti muokattavissa erilaisiin vaatimuksiin. Suuri kustomoinnin määrä voi vaikeuttaa ylläpitoa, koska tuotteen toimittajat eivät suunnittele tuotteen päivityksiä niin, että kaikki omat kustomoinnit toimisivat päivityksien jälkeen.

6 Yhteenveto

Työssä toteutettiin kertakirjautumisjärjestelmä Spellpoint Oy:lle. Työ toteutettiin käyttäen erillistä NetIQ Access Manager -pääsynhallintatuotetta. Kertakirjautuminen suunniteltiin niin, että siinä ei olisi yhtäkään korvaamatonta komponenttia. Tulevaisuudessa voitaisiin

siis vaihtaa mikä tahansa komponentti ilman, että yrityksen sisäinen ympäristö pitäisi suunnitella täysin uudestaan. Toteutus suunniteltiin myös niin, että se olisi mahdollisimman soveltuva PK-yrityksen käyttöön. Suunnittelu onnistui hyvin ja tämän vuoksi toteutus oli vaivatonta tehdä. Työn toteutus onnistui, ja kaikki siihen asetetut tavoitteet saavutettiin. Aikataulu piti koko projektin ajan, ja työ saatiin tehtyä tavoiteaikataulussa. Työssä tehty toteutus oli kertakirjautumisjärjestelmäprojektin ensimmäinen vaihe. Teknisen toteutuksen kehittämistä jatketaan ja toteutusta laajennetaan tämän työn ulkopuolisissa projekteissa.

Toteutuksessa tehdyt integraatiot tehtiin käyttäen pääsynhallintajärjestelmän lomakkeentäyttömenetelmää. Lomakkeentäyttömenetelmä täyttää kirjautumislomakkeen käyttäjän huomaamatta ja tarjoaa näin kertakirjautumisen palveluun.

Tulevaisuudessa integraatiot tullaan vaihtamaan selainkertakirjautumisessa yleisesti käytettyyn luottamusliitäntäpohjaiseen kertakirjautumiseen. Tämä on mahdollista, kun kohdejärjestelmiin tulee SAML-tuki. Myös käyttäjähakemiston vaihtamista tullaan analysoimaan tarkemmin tulevaisuudessa.

Lähteet

1. CISSP Study Guide, Eric Conrad, Seth Misenar, Joshua Feldman 2010. Luettu 25.5.2016.

2. Secure Authentication With Single Sign-On (SSO) Solutions. Verkkodokumentti. Lawton, Stephen. 6.1.2015. <http://www.tomsitpro.com/articles/single-sign-on-solutions,2-853.html>. Luettu 30.5.2016.

3. How Shibboleth Woks: Basic Concepts. Verkkodokumentti. <https://shibboleth.net/about/basic.html>. Luettu 1.6.2016.

4. 5 Big Business Benefits of Using SSO (Single Sign-on). Verkkodokumentti. Villanueva, John Carl. 11.2.2014. <http://www.jscape.com/blog/bid/104856/5-Big-Business-Benefits-of-Using-SSO-Single-Sign-On>. Luettu 3.6.2016.

5. Forgotten Passwords cost Companies $200,00 a Year. Verkkodokumentti. Goldman, Jeff. 17.10.2014. <http://www.esecurityplanet.com/network-security/forgotten-passwords-cost-companies-200000-a-year.html>. Luettu 3.6.2016.

6. Security Assertion Markup Language (SAML) 2.0 Technical Overview. Ragouzis, Nick. Hughes, John. Philpott ,Rob. Maler, Eve. Madsen, Paul. Scavo, Tom. 25.3.2008. Verkkodokumentti. <https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf >. Luettu 15.6.2016.

7. Samoilla tunnuksilla eri yrityksiin. Verkkodokumentti.Lahti, Jarmo. 31.5.2007.<http://www.digitoday.fi/data/2007/05/31/samoilla-tunnuksilla-eri-yrityksiin/200713363/66>. Luettu 15.6.2016

8. Active Directory Federation Services. Verkkodokumentti. <https://msdn.microsoft.com/en-us/library/bb897402.aspx>. Luettu 20.6.2016.

9. Kerberos Protocol Tutorial. Verkkodokumentti. Ricciardi, Fulvio. 27.11.2007. <http://www.kerberos.org/software/tutorial.html>. Luettu 1.7.2016.

10. HTTP Authentication. Verkkodokumentti. <https://www.httpwatch.com/httpgallery/authentication/>. Luettu 3.7.2016

11. Two-factor authentication: What you need to know (FAQ). Verkkodokumentti. Rosenblatt, Seth. Cipriani, Jason. 15.7.2015. <http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/>. Luettu 10.7.2016.

12. What is application access and single sign.on with Azure Active Directory. Verkkodokumentti. Smalser, Aaron. 15.8.2016. <https://azure.microsoft.com/en-us/documentation/articles/active-directory-appssoaccess-whatis/>. Luettu 11.7.2016

13. ITIL – A guide to access management. Verkkodokumentti. <https://www.ucisa.ac.uk/~/media/Files/members/activities/ITIL/service_operation/access_management/ITIL_a%20guide%20to%20access%20management%20pdf.ashx>. Luettu 15.7.2016

14. Pienet ja keskisuuret yritykset. Verkkodokumentti. <http://www.stat.fi/meta/kas/pienet_ja_keski.html>. Luettu 15.7.2016.

15. Haka Identity Federation. Verkkodokumentti. <https://www.csc.fi/-/haka-kayttajatunnistusjarjestel-1>. Luettu 28.7.2016.

16. PKI (public key infrastructure). Verkkodokumentti. Rouse, Margaret. <http://searchsecurity.techtarget.com/definition/PKI>. Luettu 28.7.2016

17. NetIQ Access Manager 4.2. Verkkodokumentti. <https://www.netiq.com/documentation/access-manager-42/>. Luettu 1.7.2016.

Lähteet tarkastettu 21.9.2016.

Tunnistamisteknologiat

Radius (Remote Authentication Dial-In User Service) on tunnistamisteknologia, jossa palvelimet tunnistavat ja valtuuttavat käyttäjän (http://searchsecurity.techtarget.com/definition/RADIUS).

X.509 sertifikaatti on digitaalinen varmenne, jolla pystytään varmentamaan käyttäjien julkiset avaimet.

Riskipohjainen tunnistaminen (RBA, Risk Based Authentication) on menetelmä, jossa järjestelmä laskee käyttäjälle riski-indeksin, jonka perusteella käyttäjälle valitaan tunnistautumistapa. Esimerkiksi pienen riskin käyttäjä voi kirjautu salasanalla ja tunnuksella, mutta suuren riskin käyttäjän täytyy tunnistautua vahvasti.

Aikapohjainen salasanan (OTP, Time Based One-time Password Algorithm) on algoritmi, joka luo salasanan, jossa kyseinen kellonaika on yksi tekijä salasanassa (http://searchsecurity.techtarget.com/definition/time-based-one-time-password-TOTP).

Sosiaalinen tunnistautumisessa käyttäjä tunnistautuu, jonkin sosiaalisen median käyttäjätunnuksilla.

OpenID on ns. internetin ajokortti. Se on tietoa, jota käyttäjä pystyy itse määrittelemään itsestään. Verkkopalvelut pystyvät tunnistamaan käyttäjän käyttäen tätä tietoa (http://openidexplained.com/).