TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

KARI HARJULA

REST-KUTSUJEN SEKÄ XDS-TEKNIIKAN AVOIMEN LÄHDE-KOODIN JÄRJESTELMIEN MAHDOLLISUUDET SOSIAALI- JA TERVEYDENHUOLLON TIETOPALVELUSSA

Diplomityö

Tarkastaja: professori Jarmo Harju
Tarkastaja ja aihe hyväksytty
Tieto- ja sähkötekniikan tiedekunta-neuvoston kokouksessa 5. marras-kuuta 2014

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Tietotekniikan koulutusohjelma
HARJULA, KARI: REST-kutsujen sekä XDS-tekniikan avoimen lähdekoodin järjestelmien mahdollisuudet sosiaali- ja terveydenhuollon tietopalvelussa
Diplomityö, 92 sivua
Huhtikuu 2015
Pääaine: Tietoliikennetekniikka
Tarkastaja: professori Jarmo Harju
Avainsanat: XDS, REST, IHE, FHIR, profiili, tapahtuma, toimija

Tällä hetkellä Suomen potilastietojärjestelmien tila on hyvin monimuotoinen ja sekava, erilaisia järjestelmiä on todella paljon, jopa yhden sairaanhoitopiirin sisällä. Nykyiset järjestelmät eivät myöskään yleensä vaihda tietoa keskenään. Työssä ensiksi selvitetään Integrating the Healthcare Enterprise (IHE) -organisaation tarjoamien yhdentämisprofiilien rakennetta ja toimintaa. Sen jälkeen tutkitaan avoimen lähdekoodin toteutuksien tarjontaa ja ominaisuuksia. Lopuksi tutustutaan myös FHIR-standardin ominaisuuksiin. Näiden taustatutkimusten tuloksena arvioidaan esiteltyjen vaihtoehtojen käyttökelpoisuutta Medbit Oy:n tarpeisiin.

Integrating the Healthcare Enterprise -organisaatio on keskeinen toimija terveydenhuollon IT-järjestelmien kehityksessä. Organisaatio julkaisee profiileja, jotka sisältävät ratkaisun johonkin olemassa olevaan yhdentämisongelmaan. Profiilien tarjoamat ratkaisut näihin ongelmiin käyttävät olemassa olevia standardeja sekä toimivat yhteistyössä järjestelmän sisällä olevien muiden toimijoiden kanssa. Tärkeimpiä ja tietopalvelun toiminnan kannalta keskeisimpiä profiileja on useita ja ne tulee myös olla järjestelmässä tuettuna, jotta tietopalvelun toiminnallisuus kattaa tarvittavat osa-alueet ja se voidaan määritellä luotettavaksi. IHE-profiilien lisäksi FHIR-standardin mahdollisuudet tulee ottaa huomioon uuden tietopalvelun suunnittelussa. FHIR:n helpommin omaksuttava ja tehokkaampi lähestymistapa sekä yhteneväisyys XDS-profiilin kanssa ovat sen ehdottomia etuja.

Työn aihepiiriin kuuluu myös avoimen lähdekoodin ohjelmistototeutusten tutkiminen, niiden ominaisuuksien tarkastelu ja käyttökelpoisuuden arviointi. Saatavilla olevista avoimen lähdekoodin toteutuksista löytyi vaihtelevaa tietoa niiden käytöstä sekä kehityksestä. Toteutuksista on löydettävissä harkinnan arvoisia vaihtoehtoja myös Medbit Oy:n tarpeisiin.

Eri toteutusten valinnan lisäksi tulee myös miettiä käyttökelpoisuutta käyttökohdetta ajatellen. Avoimen lähdekoodin toteutuksien mahdollisuuksia tulee myös verrata valmiin kaupallisen XDS-yhteensopivan järjestelmän käyttämiseen. Paras vaihtoehto avoimen lähdekoodin toteutukselle olisi toteuttaa sitä käyttämällä jokin tietty toiminnallisuus tulevassa tietopalvelussa. Näin voidaan kokeilla kyseisen toteutuksen käyttökelpoisuutta käytännössä, ennen kuin aletaan toteuttaa kokonaista järjestelmää sitä hyödyntäen.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY
Master's Degree Programme in Information Technology
HARJULA, KARI: Possibilities of REST calls and open source systems with XDS methods in social and healthcare information service
Master of Science Thesis, 92 pages
April 2015
Major: Communications Engineering
Examiner: Professor Jarmo Harju
Keywords: XDS, REST, IHE, FHIR, profiles, actors, transactions

The current situation with Finnish electronic health record systems is very complex and complicated. There are lots of different EHR systems even within one hospital district and the EHR systems are not exchanging information with each other. At first in this thesis the IHE profiles and their structure and functionality will be introduced. Next the open source implementations that are using IHE profiles will be introduced as well as the FHIR standard. At the end of this thesis the results of the research will be evaluated from Medbit Oy's point of view.

Integrating the Healthcare Enterprise (IHE) organization is an essential actor in the development of healthcare EHR systems. IHE defines profiles that include a solution for existing integration problems within an EHR system. The solutions for the problems are using existing standards and those are working together with the other actors within the same information service. There are several important and essential profiles and all of them need to be supported in the information service. This requirement is needed in order to include all the necessary sectors and to meet the requirements of a trusted environment. In addition to the IHE profiles the FHIR standard needs also to be considered in the design of the new information service. FHIR standard's easier and more effective approach for development and common features are FHIR's biggest advantages.

Investigating the open source applications that are using IHE profiles is also one of the main parts of this thesis. This included research work, comparing the features of the implementations and evaluating the usage of the implementations. Various results were found about the usage and development of the available open source implementations. Regarding the needs of Medbit Oy there are also usable open source implementations.

In addition to the selection of the implementations also the usability in the real environment should be considered. The possibilities of open source implementations should also be compared to commercial products that are using XDS technique. The best usage for open source implementation would be to use it for developing some precise function in the upcoming information service. It means that the implementation would be tested in practice properly by using it for that exact functionality. After that it would be easier to evaluate whether the implementation is also usable for larger parts of the information service.

ALKUSANAT

Tämä diplomityö on tehty opinnäytteeksi Tampereen teknilliselle yliopistolle diplomi-insinöörin tutkintoon. Työn tilaajana on ollut Medbit Oy:n kehittämispalvelut-osasto ja diplomityö on kirjoitettu vuosien 2014-2015 aikana. Diplomityön tarkastajana on toiminut tietotekniikan laitoksen professori Jarmo Harju Tampereen teknillisestä yliopistosta ja ohjaajana kehityspäällikkö Matti Koskivirta Medbit Oy:sta. Opintoni ovat olleet hyvin pitkäaikainen prosessi, koska työnteko ja muu elämä on syönyt aikaani opiskelulta. Loppujen lopuksi pääsin kuitenkin siihen pisteeseen, että diplomityö oli ainoa jäljellä oleva asia tutkinnostani. Kirjoitusprosessi oli pitkä ja loppua kohti maali tuntui koko ajan vain siirtyvän kauemmaksi. Valmista kuitenkin lopulta tuli ja siksi haluan kiittää työni ohjaajaa ja tarkastajaa ohjauksesta, kommenteista ja neuvoista pitkin kirjoittamisprosessin eri vaiheita. Haluan kiittää myös isääni oikoluvusta ja pilkuntarkoista korjausehdotuksista työn loppuvaiheessa. Lopuksi haluan erityisesti kiittää Reettaa kärsivällisyydestä ja ymmärryksestä kirjoitusprosessin aikana, sekä työn oikoluvusta ja korjausehdotuksista.

Tampereella 21.4.2015

Kari Harjula

SISÄLLYS

TERMIT JA NIIDEN MÄÄRITELMÄT

Asynchronous Web Services Exchange	Web-pohjaisten palveluiden viestien vaihtotapa, jossa lähetystiheys ei riipu vastaustiheydestä
C-MOVE	DICOM-käsky, jolla pyydetään kaikki hakuehtoon liittyvät DICOM-instanssit hakukohteelta
CDA	XML-pohjainen kliinisten dokumenttien merkintästandardi (Clinical Document Architecture)
CCOW	HL7-standardin protokolla, joka mahdollistaa sovellusten potilastietojen synkronoitumisen (Clinical Context Object Workgroup)
DICOM	Lääketieteen kuvantamistietojen käsittelyn standardi (Digital Imaging and Communications in Medicine)
EHR	Sähköinen potilaskertomus (Electronic Health Record)
EKG	Sydänsähkökäyrä eli elektrokardiogrammi
FHIR	HL7-organisaation julkaisema standardikehys (Fast Healthcare Interoperability Resources)
GSDF	Digitaalisten harmaasävykuvien parannusfunktio (Grayscale Standard Display Function)
HIMSS	Voittoa tavoittelematon organisaatio USA:ssa, joka kehittää terveydenhuollon palveluita informaatioteknologian kautta (Health Information Management Systems Society)
HL7	Kansainvälinen sovelluskerroksen standardien kokoelma kliinisten tietojen siirtoa varten (Health Level 7)
ICSA Labs	Organisaatio, joka tarjoaa resursseja tutkimukseen, sertifiointiin ja testaukseen tietoturvaan liittyvissä asioissa (International Computer Security Association)
IHE	Organisaatio, joka pyrkii edistämään sähköistä tiedonjakoa terveydenhuollon organisaatioissa (Integrating the Healthcare Enterpise)
IHE-sertifikaatti	Todistus siitä, että IHE-profiileja tukeva tuote on testattu riippumattoman kolmannen tahon toimesta
MTOM/XOP	Tiedon optimointimenetelmä, joka pienentää siirrettävän tiedon määrää, sekä mahdollistaa metatiedon erottelun varsinaisesta informaatio-osasta (Message Transmission Optimization Mechanism/XML-binary Optimized Packaging)
PACS	Kuvantamistietojen tallennusteknologia (Picture Archiving and Communication Systems)
PHI-informaatio	Suojattu potilastieto, jonka perusteella pystyy yksilöimään tietyn henkilön (Protected Health Information)
Profiili	IHE:n määrittelemä viitekehys, joka sisältää tarkat määritelmät yhdentämisen toteutusta varten

RFC	Kommentoitavana oleva IETF:n standardi, joka käsittelee yleensä Internet-protokollia (Request for Comments)
SCP	DICOM-standardin määritelmä palvelinsovellukselle (Service Class Provider)
SCU	DICOM-standardin määritelmä asiakassovellukselle (Service Class User)
SOAP	XML-kieleen pohjautuva tietoliikenneprotokolla, joka mahdollistaa prosessien etäkutsun (Simple Object Access Protocol)
SOP	DICOM-standardin luokka, joka yhdistää informaatio-objektin ja DICOM-palveluelementit (Service Object Pair)
SQL	Kyselykieli, jolla tietokantaan voi tehdä hakuja (Structured Query Language)
Syslog	Standardi tietokoneviestien tallentamiseen
Tapahtuma	Toimijan suoritettava tehtävä, joka on määritelty profiilissa (Transaction)
Tekninen viitekehys	IHE:n julkaisema resurssikokoelma, joka sisältää profiileja terveydenhuollon eri osa-alueille (Technical Framework)
Testaustapahtuma	IHE:n järjestämä tapahtuma, jossa sovelluskehittäjät testaavat IHE-profiileja hyödyntäviä implementaatioita (Connectathon)
TLS	Salausprotokolla, jolla voidaan salata liikenne verkon yli tapahtuvassa tietoliikenteessä (Transport Layer Security)
Toimija	Profiilissa määritelty käsiteltävään informaatioon liittyvien toimien suorittaja (Actor)
UDP	Yhteydetön tiedonsiirtoprotokolla (User Datagram Protocol)
URI	Merkkijono, jolla määritellään jokin resurssi. Esimerkiksi URL-osoite (Uniform Resource Identifier)
WADO	Web-pohjainen DICOM-objektien näyttämisen määrittelevä standardi (Web Access to DICOM Persistent Objects)
XDS	IHE-profiili dokumenttien jakamista varten (Cross-enterprise Document Sharing)
XDS-hoitoyhteisö	Maantieteellisesti yhtenevä kokonaisuus sosiaali- ja terveyspalveluja tarjoavia tahoja, jotka soveltavat samoja käytäntöjä (XDS Affinity Domain)
XDS-I	IHE-profiili sellaisten dokumenttien jakamista varten, missä on myös kuvantamistietoja (Cross-enterprise Document Sharing for Imaging)
XML	Tekstimuotoinen merkintäkieli, joka sisältää sekä varsinaisen tiedon, että myös sen merkityksen. (Extensible Markup Language)

1 JOHDANTO

Tietotekniikan merkittävä osuus jokapäiväisessä työssä on nykyään arkipäivää lähes joka työpaikalla. Myös lääkärin ammatissa tietotekniikka on ollut merkittävässä roolissa jo pitkän aikaa ja sähköinen potilastietojärjestelmä on yksi tärkeimmistä lääkärin työkaluista. Tämän perusteella voisi olettaa, että potilastietojärjestelmä olisi luotettava ja vaivaton käyttää. Näin ei kuitenkaan aina ole ja nykyisiä käytössä olevia potilastietojärjestelmiä on moitittu monimutkaisiksi ja hankaliksi käyttää.

Näiden ongelmien lisäksi Suomessa on tällä hetkellä käytössä useita erilaisia ja keskenään yhteensopimattomia potilastietojärjestelmiä, jopa saman sairaanhoitopiirin sisällä. Tämän työn tilaaja Medbit Oy toimii pääasiassa Varsinais-Suomen ja Satakunnan sairaanhoitopiirien alueella tietohallintopalvelujen tuottajana. Jo näissä sairaanhoitopiireissä käytössä olevia tietojärjestelmiä on useita: Varsinais-Suomessa muun muassa Effica, Pegasos, Uranus, Mediatri ja Abilita, sekä Satakunnassa Effica ja Pegasos. [1]

Tällä hetkellä käytössä olevia järjestelmiä ei ole suunniteltu alun perin kommunikoimaan ja jakamaan tietoa muiden järjestelmien kanssa. Tämän diplomityön aihe perustuu sähköisten potilastietojärjestelmien sisältämien tietojen jakamisen tarpeeseen ja miten se olisi tällä hetkellä järkevintä toteuttaa. Työn taustalla on Medbit Oy:n tarve arvioida kansainvälisellä tasolla määriteltyä XDS-tekniikkaa potilastietojen toimittaja- ja tuoteriippumattomassa jakamisessa, sekä kartoittaa myös XDS-yhteensopivien Open Source tai Freeware -järjestelmien käyttökelpoisuutta, eli niiden tukemia ominaisuuksia tässä tarkoituksessa.

Työ koostuu tutkielmasta, jossa ensin tutkitaan työn taustaan olennaisesti liittyviä tekniikoita sekä toteutuksia. Tutkielmaosuuden pohjalta muodostetaan päätelmät, jossa ehdotetaan tutkielman lopputuloksena parhaat vaihtoehdot Medbit Oy:n tarpeisiin. Tutkielman aluksi käydään läpi useimpien IHE-profiilien takana olevan SOAP-protokollan ja REST-arkkitehtuurityylin ominaisuuksia ja niiden välisiä eroja. Sen jälkeen esitellään IHE organisaationa ja esitellään sen toimintaa. IHE:n yleisen esittelyn lisäksi tarkastellaan sen tarjoamia yhdentämisprofiileja ja esitellään näistä tulevan tietopalvelun kannalta tärkeimmät ja keskeisimmät profiilit omina lukuinaan.

IHE:n yhdentämisprofiileja on olemassa kaiken kaikkiaan paljon, koska ne on tehty kattamaan kaikkia terveydenhuoltoon liittyviä aloja, sekä niiden taustalla olevia palveluita. Yhdentämisprofiileista on tässä työssä rajattu mukaan olennaisimmat sillä perusteella, että niitä tullaan tarvitsemaan XDS-yhteensopivan tietopalvelun toteuttamista ajatellen. Käytännössä tämä sisältää potilastietojärjestelmissä olevien dokumenttien ja kuvantamistietojen turvalliseen jakamiseen liittyviä yhdentämisprofiileja. Keskeisimpien profiilien tarkempien esittelyiden lisäksi esitellään tiiviimmin muutamia XDS-

tekniikkaan liittyviä profiileja. Lisäksi vertaillaan IHE-profiileja hyödyntävän tietopalvelun ominaisuuksia tällä hetkellä käytössä olevan, REST-arkkitehtuurityyliä hyödyntävän tietopalvelun kanssa.

Lisäksi omassa luvussaan tutkitaan tarjolla olevia avoimen lähdekoodin toteutuksia, jotka käyttävät näitä IHE:n tarjoamia profiileja, sekä ovat niiden kanssa yhteensopivia. Työn loppuosassa esitellään myös uusin HL7:n julkaisema FHIR-standardikehys, joka haluttiin ottaa myös mukaan työn aihepiiriin sitä kohtaan sähköisten potilastietojärjestelmien markkinoilla esiintyvän mielenkiinnon vuoksi. Tässä päällimmäisenä syynä on FHIR:n erilainen, helpompi lähestymistapa. Lopuksi omassa luvussaan arvioidaan sen mahdollisuuksia tulevan tietopalvelun käytössä IHE-profiilien lisäksi, sekä esitellään avoimen lähdekoodin toteutusvaihtoehdoista tehdyt loppupäätelmät ja ehdotukset.

2 LÄHTÖKOHDAT

Medbit Oy:n tämänhetkinen tietopalvelu on toteutettu REST:iin perustuvalla tekniikalla. REST-tietopalvelu on toteutettu siten, että se on tulevaisuudessa myös mahdollisimman pitkälle yhteensopiva jotakin uudempaa tekniikkaa hyödyntävän tietopalvelun kanssa.

Markkinoiden tarpeesta johtuen REST-arkkitehtuurityyliin perustuva järjestelmä toteutetaan välivaiheena, ennen siirtymistä esimerkiksi XDS-tekniikkaa hyödyntävään järjestelmään. Uusien tekniikoiden hyödyntäminen lähitulevaisuudessa on kuitenkin myös tarpeellista, jotta Medbit Oy voi tarjota asiakkailleen tulevaisuutta ajatellen sellaisia järjestelmiä, jotka mahdollistavat tiedonjaon myös oman toimialueen ulkopuolelta, eli käyttävät esimerkiksi IHE:n määrittelemiä profiileja.

2.1 Tietopalveluiden vaatimukset

Medbit Oy:lla on tietyt tietovarannot ja -lähteet sekä yksinkertaiset tietotarpeet, joita silmällä pitäen uudet tietopalvelut rakennetaan. Tietolähteinä oman toiminta-alueen sisällä toimivat muun muassa potilastietorekisterit sekä useat erilliset erilaisia kuvantamistietoja tekevät kuvantamislaitteet. Tämän lisäksi tietovarantoina on muun muassa Kelan ylläpitämä kansallinen potilastiedon arkisto, joka tulee sisältämään muun muassa arkistoituja potilas- sekä reseptitietoja. Suurimpana ongelmana tietovarannoissa on niin sanotut vanhenevat (legacy) tietovarantoina toimivat arkistot, joita on edelleen säilytettävä ja toiminnallisuus varmistettava potilastietojen säilytyksestä määritellyn lain mukaisesti [2].

Medbit Oy:n tietotarpeet ovat verrattaen yksinkertaiset, tärkein tarve on potilastietojen haku eri tavoin tietopalveluista. Kliinisessä työssä eli potilaan terveydenhoitoon liittyvissä toimissa tiedetään yleensä aina mistä potilaasta on kyse, kun hänen tietojaan haetaan tai ollaan lisäämässä tietopalveluihin. Tässä tapauksessa hakukriteerinä on jokin potilaan identifioiva tieto, esimerkiksi henkilötunnus.

Toinen tärkeä Medbit Oy:n tarjoamien tietopalvelujen tietotarve on tieteellisiin tutkimuksiin liittyvät haut. Tieteellisessä tutkimuksessa tiedonhaku on erilaista, koska siinä haetaan tietopalveluista tietystä potilaasta riippumattomia tietoja. Hakukriteereinä eivät ole jonkin tietyn potilaan tiedot, vaan esimerkiksi jokin tietty diagnoosi, tietyt mitta-arvot tai jotakin muuta vastaavaa tietoa, joka liittyy tehtävään tutkimukseen.

2.2 REST-arkkitehtuurityyli

REST (Representational State Transfer) on abstrakti arkkitehtuurityyli, jota käytetään verkkopohjaisten sovellusten tai palveluiden toteutuksessa. Tunnetuin REST:n arkkiteh-

tuurimallia noudattava järjestelmä on WWW (World Wide Web), jota varten se on myös alun perin kehitetty. Pääasiallinen tarkoitus REST:n kehitykselle oli web-protokollien kehityksen hallitseminen.

REST itsessään ei määrittele miten eri komponentit toteutetaan tai miten ne toimivat protokollatasolla. Sen sijaan REST määrittelee arkkitehtuurityylille tiettyjä rajoitteita, jotka mahdollistavat sen vaatimusten täyttymisen. Näitä rajoitteita ovat asiakas-palvelin-malli, tilattomuus, välimuisti, yhdenmukainen rajapinta, kerroksittainen järjestelmä sekä ladattava koodi. [3]

2.3 SOAP-standardi

REST ja SOAP (Simple Object Access Protocol) tarjoavat molemmat oman ratkaisunsa siihen, miten tarjota web-palveluita. Näistä kahdesta tekniikasta SOAP on vanhempi ja tästä syystä myös vakiinnuttanut asemansa sekä metodinsa. Microsoft kehitti alun perin SOAP:n, koska aikaisemmin ei ollut luotettavasti toimivia web-palveluiden viestinvälitysprotokollia.

SOAP on protokolla, joka tarjoaa web-palveluja varten rakenteisen informaation välityksen. SOAP käyttää XML-muotoista tekstiä, eikä se ole rajoitettu johonkin tiettyyn siirtoprotokollaan. SOAP:iin pohjautuvat palvelut, kuten esimerkiksi IHE-profiileista suurin osa, määrittelevät tarkasti välitettävien viestien rakenteen. SOAP:n turvallisuus on hoidettu WS-turvallisuusstandardeilla, jotka toimivat päästä-päähän asti yhteyksissä. SOAP:n etuna on, että se on hyvin laajennettavissa, mutta todellisuudessa siitä ei tarvitse hyödyntää kuin pieni osa riittävän toiminnallisuuden saavuttamiseksi. XML-kielellä toteutetut pyynnöt ja vastaukset voivat helposti olla hyvin monimutkaisia, ja joissakin ohjelmointikielissä ne pitää vielä toteuttaa manuaalisesti. Tästä voi muodostua ongelmia, koska SOAP sisältää sisäänrakennetun virheenkäsittelyn, eikä se hyväksy virheitä. Jos pyynnössä havaitaan virhe, vastaus sisältää saatavilla olevat tiedot virheestä, joten korjaaminen on helpompaa. [4]

Tämä voi kuitenkin helpottua sillä, mitä ohjelmointikieltä käytetään, sillä esimerkiksi .NET:llä ohjelmoitaessa ei tarvitse itse tuottaa XML:iä. Yksi etu SOAP:n käytössä on myös WSDL (Web Services Description Language). Se sisältää määritelmän siitä, miten web-palvelu toimii. Jos palvelussa määritellään viite WSDL:ään, voi integroitu kehitysympäristö (IDE) automatisoida prosessin kokonaan. Esimerkiksi tämän vuoksi SOAP:n käytön vaikeus riippuu merkittävästi siitä, millä ohjelmointikielellä järjestelmää toteutetaan. [4]

Yleinen mielipide on, että SOAP on monimutkainen ja vaikea käyttää, mikä on sinällään totta. Pahimmillaan vaadittavat XML-rakenteet on luotava joka kerta erikseen koodin suoritusta varten. Näin on esimerkiksi käytettäessä JavaScript-ohjelmointikieltä. Tähän REST tarjoaa kevyemmän vaihtoehdon. REST perustuu yksinkertaisten URL-osoitteiden käyttämiseen pyyntöinä sen sijaan, että pyynnöt pitäisi muodostaa XML:llä joka kerta. Toisin kuin SOAP:ssa, REST:llä ei ole pakko käyttää XML:ää pyyntöjen

vastauksissa. REST:n ideana on, että tarvittaessa vastaukset voidaan tuottaa siinä muodossa, mistä se on helppo käsitellä kyseessä olevalla ohjelmointikielellä. [4]

2.4 REST:n ja SOAP:n vertailu

Etuna REST-arkkitehtuurityylillä toteutetussa järjestelmässä on palvelun keveys ja helppous, SOAP-protokollaan pohjautuva IHE-profiileja käyttävä palvelu on taas toimiessaan robustimpi eli vakaampi, mutta samalla myös kankeampi konfiguroitava. Alla on listattu molempien toteutustapojen merkittävimpiä etuja:

SOAP-edut

- Se on riippumaton ohjelmointikielestä, alustasta ja siirtotavasta (REST vaatii vähintään HTTP-protokollan).
- SOAP:n toiminta hajautetuissa organisaatioympäristöissä (REST olettaa suoran päästä-päähän-kommunikaation).
- SOAP on standardisoitu.
- Se sisältää merkittävän laajennettavuuden sisältämiensä WS-standardien vuoksi.
- SOAP:ssa on sisäänrakennettu virheenkäsittely.
- Tiettyjä ohjelmointikieliä käyttämällä saavutetaan automaatiota.

REST-edut

- REST ei vaadi kalliita työkaluja web-palvelun kanssa toimiakseen.
- Siinä on loivempi oppimiskäyrä, kuin SOAP:ssa.
- SOAP käyttää XML:ää kaikkiin viesteihin, REST voi käyttää myös muita (pienempiä) viestimuotoja eli REST on tehokkaampi.
- REST:n nopeus on parempi, se ei vaadi laajempaa prosessointia.
- REST on suunnittelufilosofialtaan lähempänä muita web-teknologioita. [4]

Molemmilla toteutustavoilla on omat hyvät puolensa, joten on enemmän kiinni tulevasta toimintaympäristöstä, kumpi toteutustapa näistä palvelee paremmin tarkoitustaan. Medbit Oy:n toimintaympäristöä ajatellen REST-tietopalvelu on jo käytössä, SOAP:n (IHE-profiilien) käyttöönotosta ei ole vielä tehty päätöksiä. Muun muassa tämän työn sisältö vaikuttaa osaltaan siitä asiasta tehtäviin päätöksiin. Joka tapauksessa käyttöönotettavat tekniikat tullaan rakentamaan siten, että ne toimivat sekä rinnakkain että myös pystyvät kommunikoimaan keskenään.

2.5 Integrating the Healthcare Enterprise

Sähköisten potilastietojärjestelmien sekä terveydenhuollon IT-palveluiden liittyvissä standardeissa kansainvälinen toimija on muun muassa organisaatio nimeltä IHE, jonka toimintaa ja sen tarjoamia palveluita esitellään tässä kohdassa tarkemmin.

Aluksi käydään läpi IHE:n historiaa ja toimintaa organisaationa, jonka jälkeen esitellään IHE:n nykyisin tarjoama IHE-sertifikaatti. Lopuksi esitellään vielä IHE:n toimintaan olennaisena osana kuuluvat komiteat.

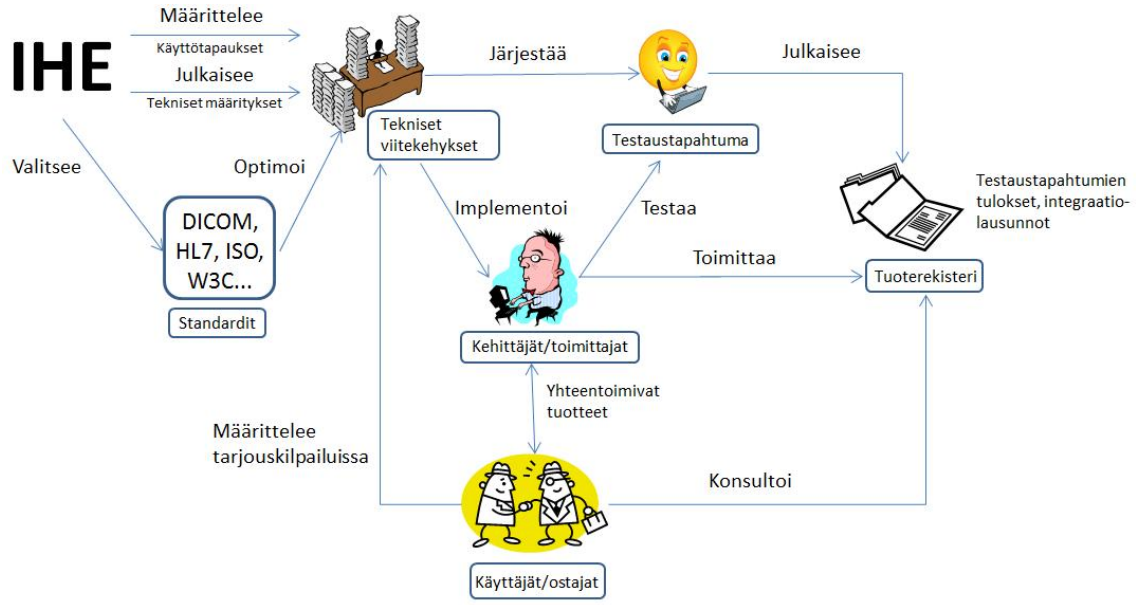
2.5.1 IHE-organisaation taustat

Integrating The Healthcare Enterprise (IHE) on riippumaton kansainvälinen organisaatio, joka on lähtöisin Illinoisista Yhdysvalloista. Organisaatio koostuu terveydenhuolto-alan ammattilaisista ja organisaatioista. IHE on perustettu vuonna 1998 radiologien ja IT-asiantuntijoiden toimesta. [5]

IHE toimii nykyään maailmanlaajuisesti, sen kehityskomiteoita toimii tämän työn kirjoitushetkellä 17 eri maassa. Näitä maita ovat Itävalta, Yhdysvallat, Kanada, Ranska, Saksa, Italia, Alankomaat, Luxemburg, Espanja, Sveitsi, Turkki, Iso-Britannia, Australia, Kiina, Japani, Korea ja Taiwan. Uusien paikallisten kehityskomiteoiden perustamista varten mikä tahansa IHE:n jäsenorganisaatio voi antaa ehdotuksen IHE:n kansainväliselle johtokunnalle. [6]

Organisaation tavoitteena on edistää terveydenhuollon IT-järjestelmissä olevan tiedon mahdollisimman tehokasta jakamista organisaatioiden kesken. IHE:n päämääränä on olla toimija, joka tarjoaa rajapinnat, joiden kautta useiden standardien mukaiset dokumentit välitetään organisaatioiden välillä. Nämä tarjotut rajapinnat eivät kuitenkaan ota kantaa itse toteutustapaan, vaan se jätetään toteutusten implementoijille.

Rajapintojen kehitys IHE:llä on jatkuva prosessi, jossa kehitetään ja johon lisätään uusia profiileja ja niihin liittyviä ominaisuuksia sitä mukaa, kun niitä hyväksytään. IHE:llä on vuosittain tapahtuva nelivaiheinen toimintaprosessi, joka on havainnollistettu myös kuvassa 2.1, joka perustuu lähteeseen [7].



Kuva 2.1. *IHE-organisaation prosessikuvaus [7].*

1. Tekniset ja kliiniset asiantuntijat kokoontuvat ja määrittelevät informaation jakamiseen tarvittavia käyttötapauksia.
2. Tekniset asiantuntijat tekevät tarkat tekniset määrittelyt järjestelmien väliseen kommunikaatioon käyttäen näitä käyttötapauksia.
3. Ohjelmistoteollisuus käyttää näitä profiileja omissa terveydenhuollon IT-järjestelmissään.
4. IHE testaa näitä ohjelmistoteollisuuden sovellutuksia järjestämissään testaustapahtumissa (Connectathons). [7]

IHE on jaoteltu terveydenhuollon osa-alueiden mukaan eri luokkiin, joista julkaistaan erilliset tekniset rajapintakuvaukset (Technical Framework):

IHE Anatomic Pathology (ANAPATH)
IHE Cardiology (CARD)
IHE Dental (DENT)
IHE Endoscopy (ENDO)
IHE Eye Care (EYECARE)
IHE IT Infrastructure (ITI)
IHE Laboratory (LAB)
IHE Patient Care Coordination (PCC)
IHE Patient Care Device (PCD)
IHE Pharmacy (PHARM)
IHE Quality, Research and Public Health (QRPH)
IHE Radiation Oncology (RO)
IHE Radiology (RAD) [12]

Tässä työssä perehdytään pääasiallisesti IT Infrastructure -osion teknisiin rajapintoihin ja niiden sovellutuksiin. Muista osioista käydään läpi tarpeen mukaan työn kannalta olennaisia rajapintoja, esimerkiksi Radiology-osiosta XDS-I ja XCA-I -profiilien ominaisuuksia.

IT Infrastucture -osio tuottaa toimintaympäristöön liittyviä standardeihin perustuvia rajapintoja sähköisten potilastietojen jakamisen sekä potilashoidon edistämiseen. IT Infrastructure sai alkunsa vuonna 2003, sponsorina Health Information Management Systems Society (HIMSS). Tähän mukaan liittyi vuonna 2008 GIP-DMP (Groupement d'Intérêt Public pour le Dossier Médical Personnel) Euroopasta. Siitä lähtien nämä kaksi järjestöä ovat vastanneet IT Infrastructure Technical Framework -dokumenttien kehityksestä ja ylläpidosta. [8]

2.5.2 IHE-sertifiointi

Testaustapahtumien lisäksi yhteistyötä tekevät IHE USA ja ICSA Labs (International Computer Security Association) tarjoavat IHE USA -sertifiointia IHE-profiileja käyttäville terveydenhuollon IT-palveluille. Sertifikaatti tarkoittaa, että IHE-profiileja tukevan

tuotteen on testannut riippumattomaton kolmas osapuoli. Sertifioinnin edellytyksenä on, että tuote on osallistunut myös testaustapahtumaan. Esimerkkinä IHE-sertifioidusta tuotteesta on ensimmäisten tuotteiden joukossa IHE-sertifioitu InterSystems-yrityksen HealthShare-ohjelmistoalusta [9].

Vaatimus testaustapahtumaan osallistumisesta on määritelty, koska suoritettavat sertifiointitestit vaativat tietyn tason testattavalta tuotteelta ja tämän tason edellytykset on testattu jo aikaisemmin testaustapahtumassa. Sertifioinnin testaus ja sertifikaatti ovat molemmat ISO-standardin mukaisia ja sertifikaatti on voimassa kaksi vuotta kerrallaan. [10]

IHE-sertifikaattia ei vielä voi hakea kaikkia IHE-profiileja käyttäville tuotteille. Tämän työn kirjoitushetkellä sertifikaatti on haettavissa vain taulukossa 2.1 mainituille profiileille. Taulukko perustuu lähteeseen [11].

Taulukko 2.1. *Sertifioitavat IHE-profiilit [11].*

Osa-alue	Lyhenne	Profiilin nimi
ITI	ATNA	Audit Trail and Node Authentication
ITI	CT	Consistent Time
ITI	HPD	*Healthcare Provider Directory**
ITI	PDQ/ PDQv3	Patient Demographics Query
ITI	PIX/ PIXv3	Patient Identity Cross-Reference
ITI	RFD	*Retrieve Form for Data Capture**
ITI	XCA	Cross-Community Access
ITI	XDM	Cross-Enterprise Document Media Interchange
ITI	XDR	Cross-Enterprise Document Reliable Interchange
ITI	XDS.b	Cross-Enterprise Document Sharing
ITI	XUA	Cross Enterprise User Assertion*
LAB	XD-Lab	Sharing Lab Report*
PCC	IC	Immunization Content*
PCC	XDS-MS	Cross-Enterprise Document Sharing – Medical Summary*
PCC	XPHR	Exchange of Personal Health Record Content*
PCD	ACM	Alert Communications Management*
PCD	DEC	Device Enterprise Communication
PCD	IPEC	*Infusion Pump Event Communication**
PCD	PIV	Point of Care Infusion Verification
PCD	POI	*Pulse Oximetry**
QRPH	CRD	*Clinical Research Document**
RAD	XDS-I.b	Cross-Enterprise Document Sharing for Imaging*
RAD	SWF	Scheduled Workflow

Tähdellä merkityt profiilit on vuonna 2014 lisätty sertifioitavaksi. Sen lisäksi kursivoidulla tekstillä olevat profiilit ovat alustavassa testauksessa. [11]

2.5.3 Komiteat

ITI Technical Framework:n kehityksen ja ylläpidon vastuu kuuluu IHE:n alaisuudessa toimiville suunnittelukomitealle ja tekniselle komitealle. Ne koostuvat kansainvälisistä jäsenistä ja kaikki äänioikeutetut voivat halutessaan osallistua komiteoiden toimintaan.

Komiteoiden toimintaan osallistuminen on vapaaehtoista. Osallistuvien on kuitenkin otettava säännöllisesti osaa tapaamisiin ja puhelinkonferensseihin, jotta he säilyttävät äänioikeutensa päätöksissä.

Suunnittelukomitea

Suunnittelukomitean (Planning Committee) tehtäviin kuuluu profiilien kehittäminen ja arviointi. Suunnittelukomitea päättää, mitä osa-alueita teknisistä rajapinnoista kehitetään ja missä järjestyksessä. Komitea myös hoitaa kommunikaation ja kehityksen koordinoinnin muiden IHE:n osa-alueiden kanssa.

Tekninen komitea

Tekninen komitea (Technical Committee) suorittaa arvioinnin suunnittelukomitean tekemästä kehitysaikataulusta ja -prioriteeteista. Uusien hyväksyttyjen profiilien yksityiskohtainen dokumentointi kuuluu myös tekniselle komitealle, kuten myös varsinaisten IHE Technical Framework -dokumenttien ylläpito.

3 IHE-PROFIILIT

IHE määrittelee sähköisissä potilastietojärjestelmissä (Electronic Health Record, EHR) tarvittavia käyttötapauksia sekä julkaisee tekniset määrittelyt, joiden pohjalta muodostetaan niin sanottuja profiileja. Näitä profiileja hyödyntäen IT-järjestelmien palveluntarjoajat kehittävät omat sovelluksensa. Terveydenhuollon tietojärjestelmiä varten olevia profiileja on kymmeniä ja sitä mukaa kun uusia tarpeita esiintyy, niitä varten luodaan uusia profiileja.

IHE-profiilissa kuvataan tarkka ratkaisu johonkin alun perin esiintyneeseen yhdentämisongelmaan. Profiilissa määritellään, miten järjestelmän toimijat käyttävät standardeja ratkaistakseen ongelman ja toimiakseen yhteistyössä IHE-profiileja käyttävän järjestelmän sisällä. Profiili koostuu siihen liittyvistä toimijoista (IHE Actor) ja niiden käyttämistä tapahtumista (IHE Transaction). Profiilit sisältävät myös tarvittaessa riippuvuuksia toisiin profiileihin. Tällaisissa tapauksissa toimijan pitää muodostaa kaikki esiehdoissa mainitut tapahtumat muihin profiileihin, jotta varsinainen tapahtuma on mahdollinen ja luvallinen.

Tässä luvussa käydään läpi suunniteltavan tietopalvelun toiminnan kannalta olennaisimmat profiilit. Kustakin läpikäytävästä profiilista esitellään sen sisältämät toimijat ja tapahtumat sekä niiden tärkeimmät ominaisuudet.

IHE-toimija

IHE-toimija toimii profiilista riippuen informaation välittäjänä, tuottajana tai säilöjänä. Toimija määritellään sen mukaan, mikä on sen pääasiallinen tarkoitus profiilissa. Samaan toimijaan on mahdollista viitata myös muista profiileista samanaikaisesti, jos toimijan tehtävä on kaikissa niissä yhtenevä.

IHE-tapahtuma

Tässä diplomityössä sekä IHE:n dokumentaatioissa tapahtumalla tarkoitetaan toimijoiden välillä tapahtuvaa informaation välitystä. Informaatio välitetään profiilin ja toimijoiden vaatimien standardien mukaisia viestejä käyttäen.

Tapahtuma on aina kahden toimijan välillä ja yksi toimija voi suorittaa tapahtumia yhden tai useamman toimijan kanssa. Rekursoivia tapahtumia eli toimijan suorittamia tapahtumia itsensä kanssa ei ole määritelty IHE:n teknisissä viitekehyksissä.

3.1 Dokumenttien jakaminen

Tämän diplomityön taustalla olevista profiileista tärkein ja keskeisin on Cross-Enterprise Document Sharing (XDS), joka kuuluu IHE:n IT Infrastructure -luokkaan (ITI). ITI keskittyy tarjoamaan tehokkaat keinot sähköisiin potilastietoihin liittyvien tietojen hallitsemiseen ja välittämiseen eri järjestelmien kesken. Tähän käytetään sitä varten luotuja standardeja eli profiileja. XDS hallitsee sähköisiin potilastietojärjestelmiin liittyvien dokumenttien rekisteröinnin (eli haltuunoton järjestelmään), jakamisen ja pääsyn niihin saman toimialueen sisällä olevien organisaatioiden kesken [12].

Tässä työssä kirjainlyhenteellä XDS viitataan sekä XDS.a- että XDS.b-profiileihin. XDS.a-profiili on alkuperäinen toteutus, joka on vuodesta 2008 jätetty vanhentuneena pois ITI:n dokumenteista. Näiden kahden version erot on eritelty alla olevassa listassa:

XDS.b:n lisäominaisuuksia ovat
- päivitetyt web-palvelut, muun muassa WS-osoitteisto
- päivitetty rekisteristandardi (ebRIM ja ebRS 3.0)
- MTOM:n käyttö Provide and Register -tapahtumassa (ja myös uusi WS Retrieve tapahtuma)
- WS Retrieve - tällä korvattiin MTOM:ia käyttävä HTTP GET, ja joka voi vastaanottaa useita dokumentteja yhdessä pyynnössä.

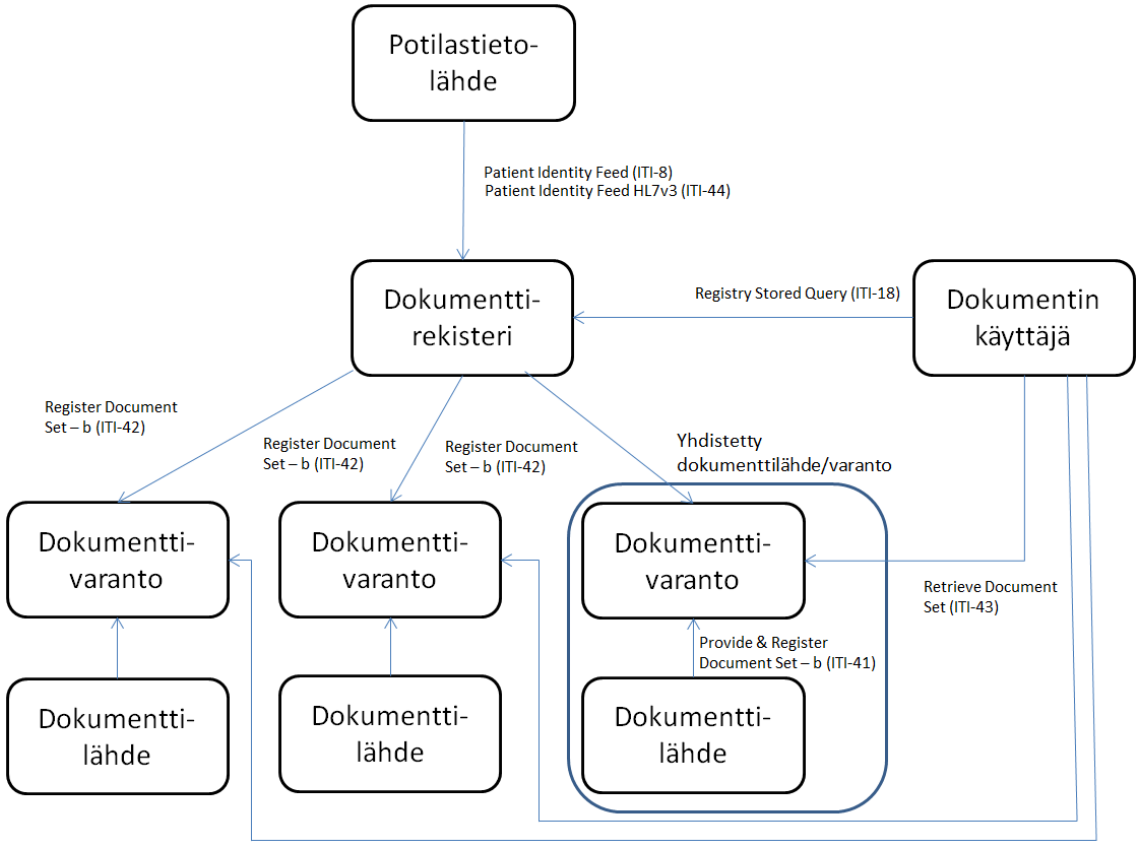
XDS.a:n ominaisuuksista jätettiin pois:
- SQL-kysely (tarkoittaa siis, että SQL on valinnainen XDS.a:n dokumenttirekisterin implementaatiossa)
- Tietojen vastaanottaminen HTTP GET:llä
- SOAP:n käyttö liitteiden yhteydessä. [13]

XDS-profiilin perusoletuksena on, että sitä käyttävä organisaatio kuuluu vähintään yhteen XDS-hoitoyhteisöön (XDS Affinity Domain). Tällä termillä tarkoitetaan hoito-organisaatioista koostuvaa terveydenhuoltopalveluita tarjoavaa yhteisöä. Lisäksi näillä organisaatioilla on lähes yhtenevät toimintaperiaatteet ja infrastruktuuri. Tällaisia voivat olla esimerkiksi jonkun tietyn sairaanhoitopiirin sairaalat ja terveyskeskukset tai puolustusvoimien varuskuntasairaalat. [12]

XDS-profiilien eräs vahvuus on niiden tukemat useat dokumenttimuodot, sillä profiilit pystyvät muuhunkin kuin vain esimerkiksi tekstipohjaisten dokumenttien välittämiseen. Dokumenttien sisällöllä on merkitystä ainoastaan siinä mielessä, että dokumenttien tiedostomuodot ovat jotakin sen tukemista standardeista. Tuettuja dokumentin muotoja ovat normaali teksti, muotoiltu/määrämuotoinen teksti (esimerkiksi HL7), kuvia (esimerkiksi DICOM) tai rakenteellista kliinistä informaatiota (esimerkiksi CDA-standardin mukaiset XML-pohjaiset dokumentit) sisältävät dokumentit [12].

3.1.1 XDS-toimijat

Kuvassa 3.1 on havainnollistettuna XDS-profiilin sisältämät toimijat ja tapahtumat ja niiden väliset suhteet. Toimijat käydään tarkemmin läpi tässä kohdassa ja tapahtumat seuraavassa kohdassa 3.1.2.



Kuva 3.1. *XDS-profiilin toimijat.*

Kuva 3.1. on tehty kuvaamaan sellaista tilannetta, missä järjestelmässä on useita dokumenttilähteitä ja -varantoja. Koska tämä on tyypillinen tilanne tietopalvelussa ja myös kuvaa Medbit Oy:n tietotarpeita, havainnollistettiin se myös kuvaan.

Dokumentin lähde

Dokumentin lähteen (Document Source) tehtävänä on tuottaa ja julkaista dokumenttivarantoon tallennettava tieto. Lähteen tulee myös välittää dokumentin metatiedot dokumenttivarannolle, jotta se voi toimittaa metatiedot edelleen dokumenttirekisterin haltuun. Kuten kuvassa 3.1 on havainnollistettu, dokumenttilähteitä ja -varantoja voi olla ja yleensä myös on useita yhtä dokumenttirekisteriä kohden. [12]

Dokumentin käyttäjä

Dokumentin käyttäjä (Document Consumer) tekee kyselyn dokumenttirekisterille tietyillä hakuehdoilla eli niiden metatiedoilla ja saa vastauksena näihin ehtoihin sopivat

dokumentit dokumenttivarannoilta. Kuten edellisessä kohdassa mainittiin, dokumenttivarantoja voi olla järjestelmässä enemmän kuin yksi. [12]

Dokumenttirekisteri

Dokumenttirekisterin (Document Registry) tehtävä on pitää kirjaa dokumenttivarantojen sisällöistä eli dokumenttirekisteri sisältää metatiedot olemassa olevista dokumenteista eri dokumenttivarannoissa. Dokumenttirekisteri vastaa dokumentin käyttäjän tekemiin kyselyihin sekä suorittaa uusien dokumenttien rekisteröinnin yhteydessä tarvittavat toiminnot.

Dokumenttivaranto

Dokumenttivaranto (Document Repository) on varsinaisen tiedon tallennuspaikka. Tiedot voivat olla hajautettuna yhteen tai useampaan dokumenttivarantoon samanaikaisesti. Dokumenttivaranto huolehtii myös dokumenttien rekisteröinnistä dokumenttirekisteriin.

Potilastietolähde

Potilastietolähde (Patient Identity Source) ylläpitää kaikille potilaille yksilöllisiä tunnisteita ja niistä muodostettua identiteettikantaa. Potilastietolähde tarkistaa myös dokumenttirekisterin käyttämien potilastunnisteiden yksilöllisyyden. [12]

Suomessa tarve potilastietolähde-toimijalle on melko pieni, koska täällä käytetään yksilöllisiä henkilötunnuksia kaikille Suomen kansalaisille. Henkilötunnusten perusteella potilaat voidaan yksilöidä eri järjestelmissä. Poikkeuksena tähän on kuitenkin esimerkiksi sellainen tilanne, jos suomalaiselle henkilölle suoritetaan sukupuolenvaihdos, jolloin henkilötunnus myös vaihtuu. Tässä tapauksessa kaksi eri henkilötunnusta voi siis viitata fyysisesti samaan ihmiseen.

Tällaisessa tapauksessa ongelmia voi tulla esimerkiksi Suomen lain suhteen, sillä henkilö ei enää välttämättä voi vaikuttaa omien, mutta edellisellä omalla henkilötunnuksella olevien tietojensa luovutukseen esimerkiksi isyyden ilmoittamisen suhteen keinohedelmöityksissä. Nämä tapaukset ovat kuitenkin melko harvinaisia, eivätkä ne vaikuta yksilöllisen henkilötunnuksen käytettävyyteen yleisellä tasolla.

Yhdistetty dokumenttilähde/varanto

Yhdistetyn dokumenttilähteen/varannon (Integrated Document Source/Repository) tehtävänä on sananmukaisesti yhdistää dokumenttilähteen ja dokumenttivarannon tehtävät. Tämä toimija on havainnollistettu kuvaan 3.1 tummansinisellä kehyksellä. Tällä voidaan myös korvata dokumenttivarannon tehtävä dokumenttisarjan rekisteröinnin (Register Document Set) tai dokumentin haku (Retrieve Document) -tapahtumien yhteydessä.

Esimerkkinä tällaisesta yhdistetystä toimijasta XDS:ää hyödyntävässä tietojärjestelmässä on ambulanssi eli sairaankuljetusauto, jolla on oma tietovaranto järjestelmässä ambulanssikäynteihin liittyvistä dokumenteista. Kun ambulanssi käy potilaskäynnillä, luo ambulanssin järjestelmä uuden dokumentin ja tallentaa sen saman tien ambulanssin

omaan tietovarantoon. Tässä tilanteessa ambulanssin rooli järjestelmässä on olla sekä dokumentin lähde, että dokumenttivaranto. [14]

3.1.2 XDS-tapahtumat

Alla olevassa taulukossa 3.1 on jaoteltuna XDS-profiilin sisältämät tapahtumat sekä niiden pakollisuus XDS-profiilin toiminnallisuuden kannalta. Taulukko perustuu lähteeseen [12]. Tässä kohdassa käydään läpi näiden tapahtumien tärkeimmät ominaisuudet.

Taulukko 3.1. *XDS-profiilin tapahtumat [12].*

Toimija	Tapahtuma	Pakollinen
Dokumentin käyttäjä	Registry Stored Query (ITI-18)	X
	Retrieve Document Set (ITI-43)	X
Dokumenttilähde	Provide and Register Document Set - b (ITI-41)	X
Dokumenttivarasto	Provide and Register Document Set - b (ITI-41)	X
	Register Document Set - b (ITI-42)	X
	Retrieve Document Set (ITI-43)	X
Dokumenttirekisteri	Register Document Set - b (ITI-42)	X
	Registry Stored Query (ITI-18)	X
	Patient Identity Feed (ITI-8)	
	Patient Identity Feed HL7v3 (ITI-44)	
Integroitu dokumenttilähde/rekisteri	Register Document Set - b (ITI-42)	X
	Retrieve Document Set (ITI-43)	X
Potilastietolähde	Patient Identity Feed (ITI-8)	
	Patient Identity Feed HL7v3 (ITI-44)	

Taulukkoon tähdellä merkitty potilastietolähde-toimija ei ole oleellinen osa järjestelmää, varsinkaan Suomessa. Täällä käytössä olevat yksilölliset henkilötunnukset ovat käytössä kaikilla Suomen kansalaisilla.

Provide and Register Document Set - b

Provide and Register Document Set - b -tapahtuma (ITI-41) suoritetaan dokumentin lähteen ja dokumenttivarannon välillä, kun dokumentin lähde välittää varsinaisen dokumentin ja siitä muodostetut metatiedot dokumenttivarannolle.

Dokumenttivaranto tallentaa dokumentit ja välittää vain niiden metatiedot edelleen dokumenttirekisterille Register Document Set - b -tapahtumaa (ITI-42) käyttäen. Register Document Set - b -tapahtuma on määritelty tarkemmin seuraavassa kohdassa. [15]

Register Document Set - b

Dokumenttivaranto aloittaa Register Document Set - b -tapahtuman (ITI-42). Sillä rekisteröidään yksi tai useampi dokumentti dokumenttirekisteriin välittämällä niiden metatiedot dokumenttirekisterille. Metatietojen perusteella dokumenttirekisteriin luodaan

uusi tieto XDS-dokumentista. Dokumenttirekisterin tehtävänä on kuitenkin tarkistaa metatietojen oikeellisuus ennen rekisteröintiä.

XDS-dokumentti voi olla myös moniosainen (esimeriksi MIME multipart document). Moniosainen XDS-dokumentti sisältää ensimmäisessä osassa pääasiallisen osuuden (primary part) ja loput osat ovat suoria liitteitä ensimmäiseen osaan. Tällaisia dokumentteja dokumenttivarannon pitää käsitellä yhtenä kokonaisuutena. Se tarkoittaa sitä, että moniosainen dokumentti tulee käsitellä palvelussa yhtenä kokonaisuutena riippumatta siitä, että se todellisuudessa on jaettu eri osiin. Tällaista kokonaisuutta kutsutaan nimellä multipart-rakenne. Silloin dokumenttivaranto ei prosessoi moniosaista rakennetta tai sen sisältöä XDS-profiilissa. Dokumenttien sisällön käsittely kuuluu dokumentin käyttäjän tai lähteen tehtäviin. [12]

Esimerkki MIME multipart -rakenteesta:

```
Content-Type: Multipart/Related; boundary=example-2

--example-2
Content-Type: text/plain

Text related to the PDF below is inserted here.
--example-2
Content-Type: application/pdf
Content-Transfer-Encoding: BASE64

BASE64 encoded PDF goes here
--example-2--
```

Ensimmäisellä rivillä tulee olla Content-Type -otsikon jälkeen merkkijono “Multipart/Related” ja sen jälkeen boundary-parametrina merkkijono, joka erottelee dokumentin eri osia. Edellä kuvatussa esimerkissä siis dokumentin multipart-osat eritellään boundary-parametrilla ”example-2”. Eri osat eritellään rakenteessa siten, että rivin alkuun tulee kaksi viivaa ja sen jälkeen boundary-parametri eli tässä tapauksessa riville on kirjoitettu ”--example-2”. Tyhjät rivit merkitsevät otsakkeen loppua (end of header). Esimerkissä yksi osa on text/plain -tyyppiä ja toinen osa ”application/pdf”, jonka sisältö pitää olla base64-koodattua sisältöä kyseisestä pdf-tiedostosta. [16]

Alla on lisäksi esimerkki kokonaisen multipart-dokumentin rakenteesta, jossa yhteen osaan on sisällytetty SOAP-osuus ja toisessa osassa on itse XML-tyyppiä oleva informaatio. Vastaavaa multipart-rakennetta voidaan käyttää siis myös XDS-profiilissa, esimerkiksi tässä luvussa esitellyssä Register Document Set - b -tapahtumassa. Tällaista dokumenttirakennetta on pystyttävä käsittelemään yhtenä kokonaisuutena.

Esimerkki multipart-dokumentin rakenteesta:

```
POST /ebxmlrr/registry/soap HTTP/1.1
Content-Type: multipart/related; type="text/xml"; boundary=----------
----------------7d4285f14803b8
SOAPAction: ""
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
```

```
Host: gunshot.ncsl.nist.gov:8080
Accept: */*
Connection: Keep-Alive
Cache-Control: no-cache
Content-Length: 1318

----------------------------7d4285f14803b8
Content-Type: text/xml

<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <SubmitObjectsRequest xmlns="urn:oasis:names:tc:ebxml-
regrep:registry:xsd:2.1">
      <LeafRegistryObjectList>
        <ExtrinsicObject id="doc_1" mimeType="text/xml"/>
      </LeafRegistryObjectList>
    </SubmitObjectsRequest>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
----------------------------7d4285f14803b8
Content-Type: text/xml
Content-Id: <doc_1>

<books>
  <book isbn="0345374827"><title>The Great Shark Hunt</title>
  <author>Hunter S. Thompson</author></book>
  <book><title>Life with Father</title><author>Clarence
Day</author></book>
</books>

----------------------------7d4285f14803b8--
```

[16]

Registry Stored Query

Dokumentin käyttäjä suorittaa Registry Stored Query -tapahtuman (ITI-18) dokumenttirekisterille. Dokumenttirekisteri etsii rekisteristä hakutuloksia käyttäjän suorittaman haun ehtojen perusteella ja palauttaa tuloksena löytyneet metatiedot. Tässä tapahtumassa dokumenttirekisterille annettu kysely tallennetaan yksilöllisellä tunnisteella dokumenttirekisteriin, jotta samaa onnistunutta kyselyä voi käyttää jatkossakin. Tämä yksilöllinen tunniste välitetään kyselyn (query request) mukana yhtenä parametrina. Kysely tallennetaan, jotta seuraavilla hakukerroilla sama kysely on valmiina ja se voidaan siksi todennäköisesti suorittaa nopeammin. [17, s.95]

Tässä menettelytavassa on muutamia etuja. Ensimmäinen etu on, että haitallisia SQL-tapahtumia (malicious SQL transactions) ei voida suorittaa. Yleensä haitallisilla SQL-tapahtumilla tarkoitetaan SQL-injektioita, joita käyttämällä saadaan aikaan haitallisia toimenpiteitä tietokantaan. Yksi parhaista ehkäisykeinoista tähän on parametrisoidut kyselyt. Tämä perustuu siihen, että kyselyn suorittajan syötteitä ei käytetä kyselyä valmistellessa, toisin sanoen injektiokoodia ei suoriteta tietokantahaun mukana lainkaan. Syötteet lisätään vasta silloin, kun tietokantasovellus tietää, miltä kyselyn tulee näyttää. Juuri tätä keinoa käytetään myös XDS-profiilin yhteydessä, jossa käytettävien

parametrien mukana välitetään myös yksilöllinen tunniste. Vastaavaa tekniikkaa SQL-injektioiden ehkäisykeinona käytetään myös tällä hetkellä käytössä olevan Medbit Oy:n REST-tietopalvelun toteutuksessa. [12]

Aikaisemmin Registy Stored Query -tapahtuman sijaan IHE-profiileissa oli käytössä Query Registry -tapahtuma (IHE-16). Suurin ero näissä tapahtumissa oli kyselyjen suorittamisessa: Registry Stored Query -tapahtuma poistaa suorien SQL-kyselyiden käytön tapahtumissa. Aikaisempi Query Registry -tapahtuman käyttö altisti dokumenttirekisterin muun muassa edellä mainituille palvelunestohyökkäyksille, joista IHE on pyrkinyt eroon tallennettujen kyselyiden avulla. Registry Stored Query -tapahtumassa tarvittava kysely talletetaan dokumenttirekisteri-toimijaan ja tapahtumassa viitataan tähän kyselyyn suoran SQL-kyselyn välittämisen sijaan. XDS-profiili ei ota kantaa siihen, miten tallennetut kyselyt on välitetty tai implementoitu dokumenttirekisteri-toimijaan. [17]

Registry Stored Query -tapahtuma tukee ainakin alla olevan taulukon 3.2 mukaisia valmiiksi määriteltyjä kyselyitä. Taulukon sisältö perustuu alkuperäiseen lähteeseen [17]. Tietoa on hyvin vähän tarjolla siitä, voiko omia kyselyitä määritellä näiden valmiiden tallennettujen kyselyiden lisäksi. Tämä ominaisuus olisi hyvin keskeisessä osassa tulevan tietopalvelun kannalta.

Taulukko 3.2. *Registry Stored Query -tapahtuman valmiit kyselyt [17].*

UUID (yksilöllinen tunniste)	Nimi
urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d	FindDocuments
urn:uuid:f26abbcb-ac74-4422-8a30-edb644bbc1a9	FindSubmissionSets
urn:uuid:958f3006-baad-4929-a4de-ff1114824431	FindFolders
urn:uuid:10b545ea-725c-446d-9b95-8aeb444eddf3	GetAll
urn:uuid:5c4f972b-d56b-40ac-a5fc-c8ca9b40b9d4	GetDocuments
urn:uuid:5737b14c-8a1a-4539-b659-e03a34a5e1e4	GetFolders
urn:uuid:a7ae438b-4bc2-4642-93e9-be891f7bb155	GetAssociations
urn:uuid:bab9529a-4a10-40b3-a01f-f68a615d247a	GetDocumentsAndAssociations
urn:uuid:51224314-5390-4169-9b91-b1980040715a	GetSubmissionSets
urn:uuid:e8e3cb2c-e39c-46b9-99e4-c12f57260b83	GetSubmissionSetAndContents
urn:uuid:b909a503-523d-4517-8acf-8e5834dfc4c7	GetFolderAndContents
urn:uuid:10cae35a-c7f9-4cf5-b61e-fc3278ffb578	GetFoldersForDocument
urn:uuid:d90e5407-b356-4d91-a89f-873917b4b0e6	GetRelatedDocuments

IHE-profiilien metatietojen kuvauskielenä käytetään ebXML RIM -standardia. Muun muassa suoritettavat kyselyt perustuvat tässä tapahtumassa ebXML Registry versio 3.0:aan [18]. Siinä määritellään tarkasti muun muassa dokumenttirekisterille suoritettavien kyselyiden protokollat ja niiden rakenne. Kyselyitä voi määritellä niin sanotusti AdHoc-periaatteella eli kysely suoritetaan samalla kun kommunikoidaan dokumenttirekisterin kanssa, eikä käytetä tallennettuja kyselyitä. Sen lisäksi ebXML Registry versio 3.0:n mukaan voidaan määritellä myös tallennettuja kyselyitä (Stored Queries) ja tätä määritelmää myös Registry Stored Query -tapahtuma käyttää XDS-profiilissa. Toisin

sanoen XDS-profiilin taustalla olevat standardit ainakin antavat mahdollisuuden myös yksilöllisten kyselyiden tekemiseen dokumenttirekisterille sekä niiden suoraan suorittamiseen. [18]

XDS-profiili itsessään ei määrittele selkeästi, onko yksilöllisiä hakuja mahdollista suorittaa XDS-tekniikkaa hyödyntävässä tietopalvelussa. Aikaisemman Query Registry -tapahtuman kautta tämä on ilmeisesti ollut mahdollista, mikä ei ole ollut järjestelmän kannalta kovin turvallista. Query Registry -tapahtuman käyttäminen sen poistuttua XDS-profiilista on ollut ainakin aluksi mahdollista, mutta ei pakollista. [19] Viimeisimmissä IHE-dokumenteissa mainitaan, että Query Registry -tapahtumaa ei enää käytetä lainkaan ja sen sijaan tulee käyttää Registry Stored Query -tapahtumaa.

Patient Identity Feed

Patient Identity Feed -tapahtuman (ITI-8) tarkoituksena on lisätä potilaiden yksilöllisiä tunnisteita ja siihen liittyvää demografista tietoa dokumenttirekisteriin sitä mukaa, kun niitä on rekisteröity tai mitä tahansa niihin liittyvää tietoa on muokattu XDS-hoitoyhteisössä. Taulukossa 3.2 on eritelty kaikki potilastietolähteen tukemat attribuutit, joita metatietoina voidaan välittää. Patient Identity Feed -tapahtuman toiminta vaikuttaa XDS-profiilin dokumenttirekisterin sisältöön ja sitä käytetään myös PIX-profiilissa (Patient Identity Cross-referencing) potilastietojen muutostenhallinnassa. Tarkemmin PIX-profiilin ominaisuuksista kerrotaan tämän työn kohdassa 3.8.

Patient Identity Feed -tapahtuman toimijoina XDS-profiilissa ovat potilastietolähde ja dokumenttirekisteri. Potilastietolähde ilmoittaa dokumenttirekisterille ja potilastunnisteiden ristiviittausten hallinnalle kaikista potilaan henkilötietoihin liittyvistä muutoksista. Dokumenttirekisteri käyttää potilastietolähteeltä saamiaan potilastunnisteita ja pitää huolen siitä, että päivitetyt XDS-dokumenttien metatiedot on liitetty oikean potilaan tietoihin. Dokumenttirekisteri myös päivittää potilaan identiteetin ajan tasalle dokumenttien metatiedoissa. Päivitykset tapahtuvat sitä mukaa, kun potilastietojen identiteeteissä tulee muutoksia, esimerkiksi jos niitä yhdistetään. [12]

Koska Suomessa on käytössä kaikille ihmisille henkilön yksilöivä henkilötunnus, tätä tapahtumaa ei tarvita kovin usein. Niissä tapauksissa tämä tapahtuma on hyödyllinen, kun jokin potilastietojen attribuuteista muuttuu. Normaalien henkilötunnusten lisäksi Suomessa on myös käytössä tietyissä tilanteissa väliaikaiset henkilötunnukset, joita nimitetään tilapäisiksi yksilöintitunnisteiksi. Tilapäistä yksilötunnistetta tarvitaan sellaisissa tilanteissa, joissa potilas ei tiedä omaa henkilötunnustaan tai ei pysty kertomaan sitä.

Nämä tilanteet tulevat esimerkiksi siinä tapauksessa kyseeseen, jos potilas on hyvin nuori tai vanha, tai kehitys- tai kielitasosta johtuen ei pysty kertomaan tai ei tiedä varsinaista henkilötunnustaan. Tämän lisäksi tilapäistä yksilöintitunnistetta käytetään myös silloin, jos henkilötunnusta ei saada selvitettyä. Tällainen tilanne on esimerkiksi silloin, kun potilaan tajuttomuuden vuoksi henkilötunnusta ei saada selville tai vastasyntyneellä vauvalla ei vielä ensimmäisten elintuntien aikana välttämättä ole väestörekisterikeskuksesta saatavaa varsinaista henkilötunnusta. [20]

Tähän asti tilapäinen yksilöintitunniste on ollut organisaatiokohtainen, mikä on asettanut omat haasteensa niiden käytölle. Tämä tarkoittaa sitä, että jos potilasta on hoidettu useammassa terveydenhuoltopalveluita tarjoavassa laitoksessa, on kaikkiin niihin pitänyt luoda oma tilapäinen tunnisteensa. Terveyden ja hyvinvoinnin laitos on käynnistänyt selvityksen aiheesta, miten nämä tunnisteet tulisi toteuttaa jatkossa, jotta ne toimisivat myös eri hoito-organisaatioiden kesken. Tulevissa, keskenään kommunikoivissa tietopalveluissa tällainen yhteensopivuus on erittäin tärkeää ja uudet tietopalvelut tulevat myös tukemaan sitä muun muassa XDS-tekniikan kautta. [20]

Suomen kohdalla henkilötietolaki myös kieltää tiettyjen arkaluonteisiksi luokiteltujen asioiden käsittelyn. Arkaluonteisiksi luokitellut asiat on lueteltu alla olevassa listassa.

”Arkaluonteisina tietoina pidetään henkilötietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan:

1) rotua tai etnistä alkuperää;
2) henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista;
3) rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta;
4) henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia;
5) henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka
6) henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.” [21]

Näin ollen potilaan identiteettiin liittyvien tietojen käsittelyssä on otettava huomioon Suomen lainsäädäntö ja jättää edellä mainitut asiat käsittelemättä järjestelmässä. Näitä poissuljettavia attribuutteja ovat taulukossa 3.3 esimerkiksi rotu (Race, item 113), etninen ryhmä (Ethnic Group, item 125) ja uskonto (Religion, item 120). Taulukko 3.3. perustuu alkuperäiseen lähteeseen [22].

Tähän on kuitenkin laissa määritelty poikkeus, jos arkaluonteisiksi luokiteltuihin tietoihin on erikseen saatu lupa potilaalta tai kyseessä on potilaan hoitotilanne. Hoitotilanteessa edellä mainittuun kohtaan 4) liittyviä tietoja voidaan käsitellä myös ilman erillistä lupaa. Vastaava poikkeus laissa on myös kohtaan 6) liittyvissä tiedoissa, jos potilasta hoidetaan sosiaalihuollon alaisuuteen liittyvissä asioissa. Suomen henkilötietolaki vaikuttaa näin ollen myös taulukon 3.3 sisältämiin attribuutteihin, joista on jätettävä pois edellä mainittuihin asioihin viittaavat attribuutit, ellei poikkeuksien myötä ole lain mukaan lupa käsitellä näitä tietoja järjestelmässä.

Taulukko 3.3. *HL7-standardin v. 2.3.1. mukaiset tuetut attribuutit [22].*

SEQ	LEN	DT	OPT	TBL#	ITEM#	ELEMENT NAME
1	4	SI	O		104	Set ID - Patient ID
2	20	CX	O		105	Patient ID
3	250	CX	R		106	Patient Identifier List
4	20	CX	O		107	Alternate Patient ID
5	250	XPN	R		108	Patient Name
6	250	XPN	R+		109	Mother's Maiden Name
7	26	TS	R+		110	Date/Time of Birth
8	1	IS	R+	1	111	Administrative Sex
9	250	XPN	O		112	Patient Alias
10	250	CE	O	5	113	Race
11	250	XAD	R2		114	Patient Address
12	4	IS	O	289	115	County Code
13	250	XTN	R2		116	Phone Number - Home
14	250	XTN	R2		117	Phone Number - Business
15	250	CE	O	296	118	Primary Language
16	250	CE	O	2	119	Marital Status
17	250	CE	O	6	120	Religion
18	250	CX	O		121	Patient Account Number
19	16	ST	R2		122	SSN Number – Patient
20	25	DLN	R2		123	Driver's License Number - Patient
21	250	CX	O		124	Mother's Identifier
22	250	CE	O	189	125	Ethnic Group
23	250	ST	O		126	Birth Place
24	1	ID	O	136	127	Multiple Birth Indicator
25	2	NM	O		128	Birth Order
26	250	CE	O	171	129	Citizenship
27	250	CE	O	172	130	Veterans Military Status
28	250	CE	O	212	739	Nationality
29	26	TS	O		740	Patient Death Date and Time
30	1	ID	O	136	741	Patient Death Indicator

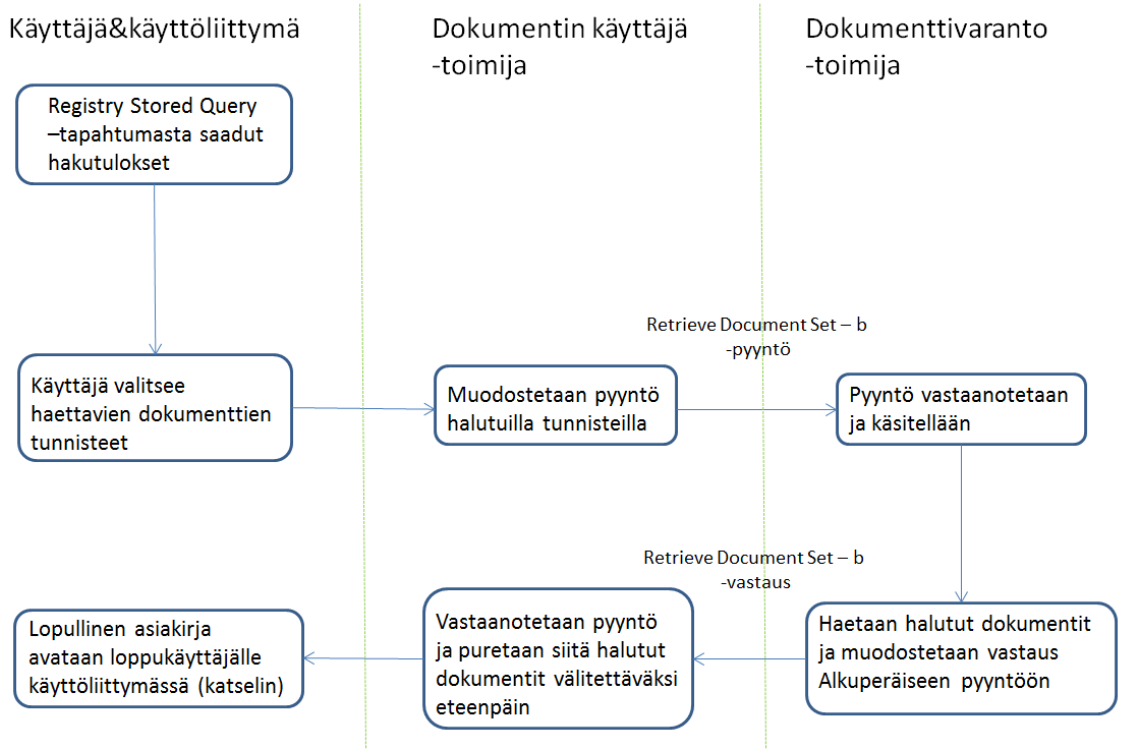
Taulukossa 3.3 käytetyt OPT-parametrit (Optional) ovat:

- R, vaatimus (Required)
- R2, vaatimus, joka on IHE:n määrittelemä parametrilaajennus. Jos lähettävä sovellus sisältää tietoa tälle tietoparametrille, on tietoparametri täytettävä tällä arvolla. Jos kyseistä arvoa ei ole tiedossa, tietoparametria ei lähetetä.
- R+, vaatimus, joka on IHE:n määrittelemä parametrilaajennus. Tämä tietoparametri on IHE:n vaatimus, joka on alun perin ollut valinnainen HL7:n standardissa.
- O, valinnainen tietoparametri (Optional) [23]

Nämä parametrit ovat lisätarkennusta alkuperäiseen HL7:n standardissa olleeseen attribuuttien kuvaukseen.

Retrieve Document Set

Retrieve Document Set -tapahtuman (ITI-43) alkutilanteessa dokumentin käyttäjällä on tiedossaan yksilöllinen tunniste XDSDocumentEntry. Näitä tunnisteita voi olla myös useampia, jos haluttuja dokumentteja on useampia. Tunnisteet on saatu onnistuneen Registry Stored Query -tapahtuman lopputuloksena. Kuvassa 3.2 on kuvattuna tämän tapahtuman logiikka.



Kuva 3.2. *Retrieve Document Set - b -tapahtuman logiikkakaavio.*

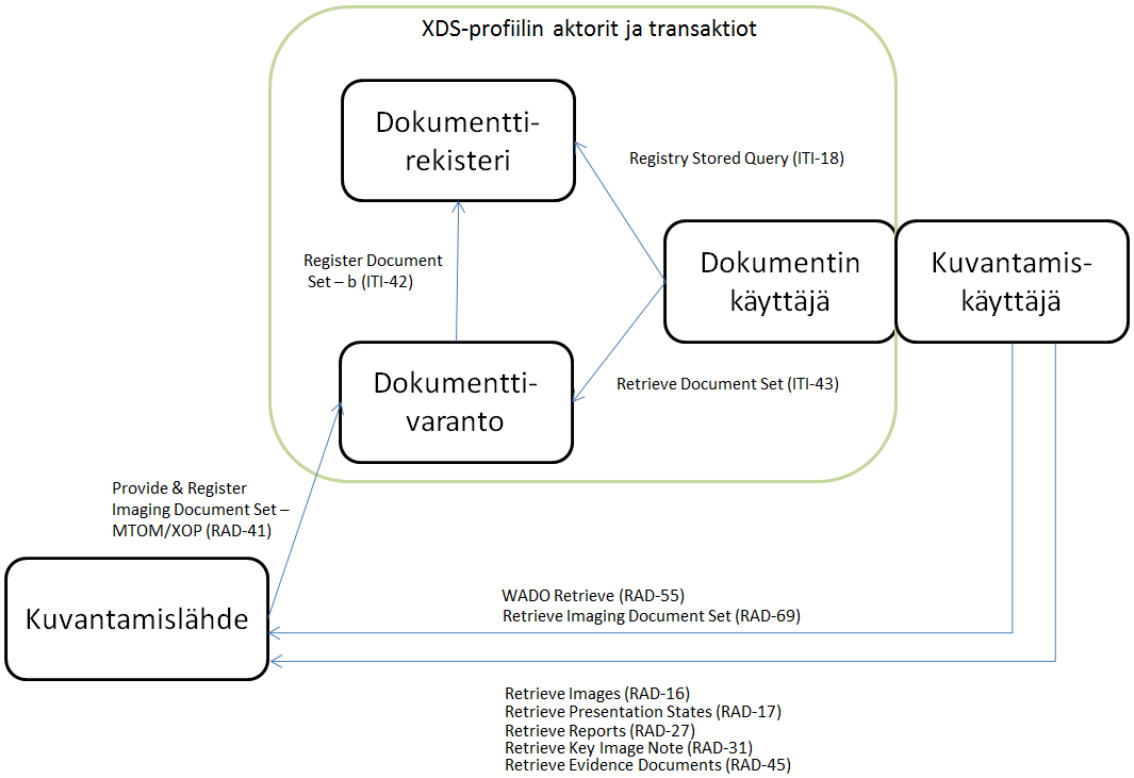
Dokumentin käyttäjä suorittaa pyynnön dokumenttivarannolle, jossa parametrina käytetään tätä yksilöllistä tunnistetta tai tunnisteita. Pyyntö muodostetaan XML-sanomaksi, joka sisällytetään SOAP-viestiin. Dokumenttivaranto vastaanottaa pyynnön ja käsittelee sen, jonka perusteella se muodostaa pyyntöön vastauksen.

Vastaus sisältää pyydetyt dokumentit tai virhekoodit, jos dokumentteja ei löytynyt tai niitä ei saatu haettua. Vastaus paketoidaan MIME-koodattuna ja lähetetään takaisin dokumentin käyttäjälle, jonka on pysyttävä käsittelemään vastaus siten, että XDS-dokumentit tai mahdolliset virheet suoritetussa haussa voidaan esittää käyttäjälle. [15]

3.2 Kuvantamisdokumenttien jakaminen

XDS-I -profiili (Cross-Enterprise Document Sharing for Imaging) pohjautuu XDS-profiiliin, mutta on siitä kehitetty laajempi versio, jossa on mahdollistettu myös potilastietoihin liitettyjen kuvantamis- tai signaalitietojen jakaminen (esimerkiksi EKG eli sydänsähkökäyrä tai magneettikuvauksen tulos). Tämä on vaatinut tiettyjä laajennuksia pohjalla olevaan XDS-profiiliin, koska nämä tiedot ovat usein yksittäiseltä kooltaan tai lukumääriltään suuria.

Kuvassa 3.3 on eroteltuna XDS-profiilin sisältämät toimijat ja tapahtumat vihreällä kehyksellä, jotta voidaan havainnollistaa, mitä lisätoiminnallisuutta kuvantamisominaisuuksien sisällyttäminen tuo mukanaan. Kuva perustuu alkuperäiseen lähteeseen [24]. XDS-I -profiilin toiminnallisuus alkaa siitä, että dokumentin käyttäjä suorittaa tarvitsemansa kyselyn Registry Stored Query -tapahtumaa käyttäen dokumenttirekisterille. Toiminta on siis vastaava, kuten XDS-profiilin tapauksessa.



Kuva 3.3. *XDS-I -profiilin kaaviokuva [24].*

XDS- ja XDS-I -profiilit eivät ole suunniteltu vastaamaan kaikkiin mahdollisiin organisaatioiden välisiin yhteystarpeisiin ja jotkut tietotarpeet vaativat toimiakseen myös muita IHE-profiileja. Sellaisia ovat esimerkiksi Patient Identifier Cross-Referencing (PIX), Audit Trail and Node Authentication (ATNA), Enterprise User Authentication (EUA), Cross-Enterprise User Authentication (XUA) ja Retrieve Information for Display (RID).

PIX-profiilia ei todennäköisesti Suomessa tarvita, koska täällä on käytössä ihmiset yksilöiviin henkilötunnuksiin perustuva järjestelmä. Joitakin tilanteita on tällä hetkellä tuettu vain osittain tai tuki on tulossa vasta tulevaisuudessa, kun IHE on määrittänyt uusia standardeja kyseisiä tietotarpeita varten. [24]

3.2.1 XDS-I -toimijat

Koska XDS-I -profiili perustuu XDS:ään, sisältyy sen toteutukseen kaikki samat toimijat mitä myös XDS:ään sekä tietyt kuvantamiseen liittyvät lisäominaisuudet. Edellä olleessa kuvassa 3.3 oli merkitty vihreällä reunuksella nämä XDS:n toimijat ja sen ulkopuolelle jäävät ovat XDS-I:n omia toimijoita.

Tässä kohdassa esitellään XDS-I -profiilin omat toimijat kuvantamislähde ja kuvantamiskäyttäjä. XDS-profiilin sisältämät toimijat on esitelty tarkemmin kohdassa 3.1.1.

Kuvantamislähde

Kuvantamislähteen (Imaging Document Source) tehtävänä on jakaa kuvantamistiedoissa olevia kuvia tai muita signaalitietoja XDS-hoitoyhteisössä oleville käyttäjille. Tähän asti kuvantamistietojen tallettamista ja katselua on terveydenhuollon organisaatioissa hoitanut PACS (Picture Archiving and Communication Systems). Siihen tallennetut kuvantamistiedot noudattavat DICOM-standardia (Digital Imaging and Communications in Medicine), joka on mahdollistanut kuvantamistietojen siirrettävyyden ja katseltavuuden myös muualla, kuin siinä sairaalassa missä kuvat on alun perin otettu.

XDS-I -profiili on DICOM-standardin kanssa yhteensopiva, joten kun kuvantamislähde haluaa jakaa kuvantamistietoja XDS-I -profiilia käyttäen, kuvantamistiedoista luodaan DICOM-julkaisudokumentti (DICOM manifest). Se sisältää viittaukset julkaistaviin DICOM-instansseihin eli varsinaisiin kuvantamistietoihin ja tämä julkaisudokumentti välitetään metatietojen kanssa dokumenttivarannolle. Varsinaisia kuva- tai signaalitiedostoja tai -objekteja ei välitetä dokumenttivarannolle, vaan kuvantamislähteen tehtävänä on vain välittää ne saataville niiden sisältämien metatietojen avulla. [25]

DICOM-julkaisudokumentin julkaisun lisäksi kuvantamislähteen on pystyttävä julkaisemaan myös kuvantamislausuntoja (Imaging Report), jotka ovat joko CDA- tai PDF-tiedostomuodossa. Nämä lausunnot ovat XDS-dokumentteja vastaavia asiakirjoja. Kuvantamislausunnot sisältävät dokumentin katselleen lääkärin tai muun hoitohenkilökuntaan kuuluvan henkilön dokumenttiin lisäämiä tietoja kyseisten signaali- tai kuvantamistietojen tutkimisen jälkeen. [24]

Kuvantamiskäyttäjä

Kuvantamiskäyttäjä (Imaging Document Consumer) toimii tietojärjestelmässä samassa roolissa XDS-dokumentin käyttäjän kanssa. Dokumentin käyttäjä tekee hakupyynnön dokumenttirekisterille, johon dokumenttivaranto vastaa listalla sopivia DICOM-julkaisudokumentteja. Dokumentin käyttäjä valitsee näistä sopivimman julkaisudokumentin ja pyytää tätä dokumenttivarannolta. Dokumenttivaranto palauttaa julkaisudokumentin dokumentin käyttäjälle, joka välittää sen edelleen kuvantamiskäyttäjälle. [26]

Kuvantamiskäyttäjän tehtävänä on ottaa yhteys kuvantamislähteeseen ja luoda kuvantamislähteen kanssa DICOM-yhteys (DICOM association) tekemällä pyynnön DICOM-julkaisudokumentissa olevasta tiedosta. Kun yhteys on luotu, kuvantamislähde lähettää haetun DICOM-objektin kuvantamiskäyttäjälle, joka tekee tarvittavia toimenpiteitä tuloksena annetulle objektille. Näin saadaan haun kohteena ollut kuvantamistieto käyttäjälle nähtäväksi. [24, s.44]

XDS-I -kuvantamiskäyttäjänä voidaan käyttää kahdentyyppistä tietojärjestelmää. Näiden rakenteellisena erona on se, ovatko dokumentin käyttäjä (XDS) ja kuvantamiskäyttäjä (XDS-I) yhdessä yksi toimija vai kaksi erillistä toteutusta. Jos tämä on toteutettu järjestelmässä yhteisenä toimijana, pitää myös XDS-I -kuvantamiskäyttäjän pystyä

käsittelemään vastaanottamansa informaatio ja käyttämään sitä DICOM-objektien kutsumisessa [24]

Jos nämä edellä mainitut toimijat ovat erillisiä toteutuksia, on kyseessä niin sanottu katselin kuvantamiskäyttäjän osalta. Siinä tapauksessa katselinta varten on toteutettava myös oma käyttöliittymänsä. Käyttöliittymää tarvitaan DICOM-julkaisudokumentin ja hakutulosten tarkastelua varten, jolloin tiedonsiirto tapahtuu dokumentin käyttäjänä toimivan järjestelmän ja kuvantamiskäyttäjänä toimivan katselin-sovelluksen välillä. [24]

Riippumatta kuvantamiskäyttäjätoimijan toteutustavasta on sen pystyttävä käsittelemään DICOM-julkaisudokumentin sisältämää informaatiota, DICOM-objekteja ja -kuvatiedostoja. DICOM-standardin käyttö tulee siis toteuttaa alusta loppuun kuvantamistietojen katseluun asti, eikä toiminnallisuutta saa toteuttaa muilla keinoin.

3.2.2 XDS-I -tapahtumat

Tässä kohdassa käydään läpi XDS-I -profiilin tapahtumat ja niiden tärkeimmät ominaisuudet. Tapahtumat ovat myös listattuna kootusti taulukossa 3.4, joka perustuu alkuperäiseen lähteeseen [24]. Taulukossa on myös eriteltynä tapahtumien pakollisuus.

Taulukko 3.4. *XDS-I toimijat ja tapahtumat [24].*

Toimija	Tapahtuma	Pakollinen
Kuvantamiskäyttäjä	Retrieve Images (RAD-16)	
	Retrieve Presentation States (RAD-17)	
	Retrieve Reports (RAD-27)	
	Retrieve Key Image Note (RAD-31)	
	Retrieve Evidence Documents (RAD-45)	
	WADO Retrieve (RAD-55)	
	Retrieve Imaging Document Set (RAD-69)	
Kuvantamislähde	Provide and Register Imaging Document Set - MTOM/XOP (RAD-68)	X
	Retrieve Images (RAD-16)	X
	Retrieve Presentation States (RAD-17)	X
	Retrieve Reports (RAD-27)	X
	Retrieve Key Image Note (RAD-31)	X
	Retrieve Evidence Documents (RAD-45)	X
	WADO Retrieve (RAD-55)	X
	Retrieve Imaging Document Set (RAD-69)	X

Retrieve Images

Retrieve Images -tapahtumaa (RAD-16) käyttävät sekä kuvan näyttäjä pyytäessään kuvia kuvavarannolta että myös kuvantamisdokumentin käyttäjä pyytäessään dokumentteja kuvantamislähteeltä. Molemmissa tapauksissa kun kuvanhakupyyntö on suoritettu, pyydetyt DICOM-kuvat välitetään kuvantamiskäyttäjälle tai katselimelle. [27]

Toimijoiden välinen liikenne tapahtuu DICOM-standardia käyttäen. Retrieve SOP -luokille (Retrieve Service-Object Pair) tulee tapahtumassa olla tuki. DICOM Storage SOP -luokat ovat tuettuina kuvavarannon tai kuvantamislähteen toimiessa tapahtumassa

SCU:na (Service Class User). Tästä löytyy tarkempi kuvaus DICOM 2011 PS 3.4 -standardin liitteestä C. [27]

Kuvavaranto tai kuvantamislähde vastaanottaa C-MOVE pyynnön, ja muodostaa DICOM-yhteyden katselimen tai kuvantamisdokumentin käyttäjän kanssa ja käyttää tarvittavaa DICOM Image Storage SOP -luokkaa haetun kuvan välittämiseen. C-MOVE -pyyntö on DICOM-komento, jolla kutsun suorittanut sovellus pyytää hakukohteelta kaikki saatavilla olevat hakuehtojen mukaiset DICOM-instanssit [28].

Katselimen tai kuvantamisdokumentin käyttäjän tulee tukea vähintään yhtä SOP-luokkaa. Tuki tarkoittaa samalla sitä, että järjestelmästä löytyy myös tuki näytölle. Taulukossa 3.5 on esitelty käytössä olevat DICOM SOP -luokat. Taulukko perustuu alkuperäiseen lähteeseen [27].

Taulukko 3.5. *SOP-luokkien UID-tunnisteet ja nimet [27].*

SOP-luokan UID-tunniste	SOP-luokan nimi
1.2.840.10008.5.1.4.1.1.1	Computed Radiography Image Storage
1.2.840.10008.5.1.4.1.1.2	CT Image Storage
1.2.840.10008.5.1.4.1.1.4	MR Image Storage
1.2.840.10008.5.1.4.1.1.20	Nuclear Medicine Image Storage
1.2.840.10008.5.1.4.1.1.128	Positron Emission Tomography Image Storage
1.2.840.10008.5.1.4.1.1.481.1	RT Image Storage
1.2.840.10008.5.1.4.1.1.7	Secondary Capture Image Storage
1.2.840.10008.5.1.4.1.1.6.1	Ultrasound Image Storage
1.2.840.10008.5.1.4.1.1.3.1	Ultrasound Multi-frame Image Storage
1.2.840.10008.5.1.4.1.1.12.1	X-Ray Angiographic Image Storage
1.2.840.10008.5.1.4.1.1.12.2	X-Ray Radiofluoroscopic Image Storage
1.2.840.10008.5.1.4.1.1.1.1	Digital X-Ray Image Storage – For Presentation
1.2.840.10008.5.1.4.1.1.1.1.1	Digital X-Ray Image Storage – For Processing
1.2.840.10008.5.1.4.1.1.1.2	Digital Mammography Image Storage – For Presentation
1.2.840.10008.5.1.4.1.1.1.2.1	Digital Mammography Image Storage – For Processing
1.2.840.10008.5.1.4.1.1.1.3	Digital Intra-oral X-Ray Image Storage – For Presentation
1.2.840.10008.5.1.4.1.1.1.3.1	Digital Intra-oral X-Ray Image Storage – For Processing
1.2.840.10008.5.1.4.1.1.77.1.1	VL Endoscopic Image Storage
1.2.840.10008.5.1.4.1.1.77.1.2	VL Microscopic Image Storage
1.2.840.10008.5.1.4.1.1.77.1.3	VL Slide-Coordinates Microscopic Image Storage
1.2.840.10008.5.1.4.1.1.77.1.4	VL Photographic Image Storage

Retrieve Presentation States

Retrieve Presentation States -tapahtumalla (RAD-17) on samat toimijat käyttäjänä kuin edellisen kohdan tapahtumalla (RAD-16), mutta kuvan sijaan tapahtumaa käytetään kuvan esitysmuodon (Presentation State) hakemiseen ja vastaanottamiseen kuvavarannolta tai kuvantamislähteeltä. Katselimen ja kuvantamiskäyttäjän tulee tukea kaikkia kuvamuunnoksia, jotka on määritelty DICOM 2011 PS 3.4:ssä (Grayscale Softcopy Presentation State Storage). On myös mahdollista, että useampia erilaisia Presentation State -parametreja voi viitata samaan kuvatietoon. [27]

Myös tässä tapahtumassa toimijoiden tulee tukea Retrieve SOP -luokkia (Study Root MOVE ja vaihtoehtoisesti Patient Root MOVE). Kuvavaranto tai kuvantamislähde vastaanottaa C-MOVE -pyynnön ja muodostaa DICOM-yhteyden katselimen tai kuvantamisdokumentin käyttäjän kanssa. Pyydettyjen Presentation State -objektien siirto tapahtuu käyttäen DICOM Grayscale Softcopy Presentation State Storage SOP -luokkaa. [27]

Katselimen tai kuvantamiskäyttäjän tehtävänä on käyttää aikaisemmin vastaanotettuja Presentation State -objekteja kuvatietoon ja muodostaa kuva katselua varten. Katselimen tulee tukea DICOM-standardin mukaista Grayscale Standard Display Function (GSDF) kuvanmuodostusta. Katselin tai kuvantamiskäyttäjä saattaa vastaanottaa myös ristiriitaista tietoa potilaasta jo aikaisemmin luodusta kyselystä. Tällainen tulee kyseeseen esimerkiksi silloin, jos potilaan nimi on muuttunut, mutta haku on tehty jo ennen nimenmuutosta. Esimerkiksi kun potilas on mennyt naimisiin, jolloin potilaan nimi on voinut vaihtua, ja kun kysely on tehty ja tallennettu järjestelmään jo ennen sitä. Nimenmuutoksen ajankohdan saa tarvittaessa selville myös XDS-profiilin potilastietolähteen kautta.

Ristiriitatilanteessa katselin tai kuvantamiskäyttäjä vastaanottaa Softcopy Presentation State -objekteja, jolla parametrit Study Instance UID, Series Instance UID ja SOP Instance UID pitävät paikkansa, mutta potilaan nimi on ristiriidassa niiden kanssa. Katselimen tai kuvantamiskäyttäjän tulisi tästä syystä aina käyttää lähiaikoina suoritettuja kyselyitä aikaisempien sijaan tai lyhyen ajan sisällä vastaanotettuja instansseja. Näin pystytään varmistamaan, että katselimelle tai kuvantamiskäyttäjälle näytetään varmasti viimeisin potilasinformaatio kuvavarannosta tai kuvantamislähteestä. [27]

Suomessa käytössä oleva henkilötunnusjärjestelmä helpottaa edellisen kappaleen tilannetta, jossa potilaan nimi on vaihtunut, koska suoritettavien kyselyiden hakuparametrina voidaan käyttää myös henkilötunnusta. Henkilötunnus pysyy todennäköisimmin muuttumattomatta myös nimenvaihdoksissa. Tähän on poikkeuksena potilaan sukupuolen vaihtuminen, jota voidaan pitää kuitenkin verrattain harvinaisena tilanteena.

Retrieve Reports

Retrieve Reports -tapahtumassa (RAD-27) pyydettyjä DICOM-standardisoituja raportteja siirretään kuvantamislähteeltä kuvantamiskäyttäjälle. Retrieve Reports -tapahtuman käyttäjinä on useita toimijoita, joista tämän työn kannalta olennaisimmat ovat kuvantamislähde ja -käyttäjä. Muita tapahtuman käyttäjiä ovat toimijat Report Manager, Report Repository, Report Reader ja External Report Repository Access.

Retrieve SOP -luokille (Study Root - MOVE ja valinnaisena Patient Root - MOVE) tulee olla tuki. Kuvantamisdokumentin käyttäjän pitää tukea myös DICOM Basic Text SR Storage SOP -luokkaa ja valinnaisesti myös DICOM Enhanced SR Storage SOP -luokkaa SCP:n roolissaan. Kuvantamislähteen SCU:n roolissa tulee tukea sekä DICOM Basic Text SR Storage SOP että DICOM Enhanced SR Storage SOP -luokkaa. [27]

C-MOVE -pyyntö lähetetään kuvantamiskäyttäjältä kuvantamislähteelle, pyynnön tulee tukea joko DICOM Study Root Query/Retrieve Information Model - MOVE SOP-

luokkaa tai DICOM Patient Root Query/Retrieve Information Model - MOVE SOP-luokkaa. Kuvantamislähde vastaanottaa C-MOVE -pyynnön ja muodostaa DICOM-yhteyden kuvantamiskäyttäjän kanssa ja käyttää raporttien siirtämiseen DICOM Structured Report Storage SOP -luokkia (Basic Text SR Storage SOP Class ja/tai Enhanced SR Storage SOP). [27]

Jos DICOM-standardin mukainen raportti viittaa muihin DICOM-objekteihin, on kuvantamiskäyttäjän päätettävissä näytetäänkö näitä tietoja käyttäjälle. Jos näitä viitattuja objekteja ei näytetä, on kuvantamiskäyttäjän joka tapauksessa ilmoitettava järjestelmän käyttäjälle, että raportissa on viittaus myös raportin ulkopuoliseen DICOM-objektiin. [27]

Raporteilla tässä tarkoitetaan esimerkiksi luvussa 3.2.1 mainittuja kuvantamislausuntoja, joita kuvantamistietoja tutkinut ja arvioinut lääkäri muodostaa omien tutkimustensa pohjalta. DICOM-standardisoidut raportit voivat sisältää myös muuta tietoa kuvantamislausuntojen lisäksi, esimerkiksi jonkin tietokonealgoritmin perusteella kuvasta muodostettua lisätietoa, kuten esimerkiksi mittaustietoa.

Retrieve Key Image Notes

Retrieve Key Image Notes -tapahtuman (RAD-31) käyttäjinä ovat katselin ja kuvavaranto tai kuvantamiskäyttäjä ja kuvantamislähde. Key Image Note (KIN) on erillinen IHE-profiili, jonka tarkoitus on mahdollistaa järjestelmän käyttäjän lisäämään yhteen tai useampaan kuvaan muistiinpanon. Tarkemmin tätä profiilia käsitellään kohdassa 3.3.

Retrieve Key Image Notes -tapahtumassa pyydetty DICOM Key Image Note siirretään kuvavarannolta tai kuvantamislähteeltä katselimelle tai kuvantamiskäyttäjälle tarkasteltavaksi KIN-profiilin merkitsemien kuvien kanssa. Retrieve (Study Root - MOVE ja mahdollisesti Patient Root - MOVE) SOP-luokille tulee olla tuki ja kuvavarannon sekä kuvantamislähteen tulee tukea DICOM Image Storage SOP -luokkia toimiessaan SCU:na. Kuvantamislähteen tulee varmistaa, että potilaan ja toimenpiteen tiedot ovat ajan tasalla KIN-objekteissa. [27]

Kuvavaranto tai kuvantamislähde vastaanottaa C-MOVE -pyynnön ja muodostaa DICOM-yhteyden katselimen tai kuvantamiskäyttäjän kanssa ja käyttää DICOM Key Image Storage SOP -luokkaa pyydettyjen KIN-objektien siirtämiseen. Katselin tai kuvantamiskäyttäjä voi halutessaan tukea myös kuvien näyttämistä muista tutkimuksista kuin siitä mihin kyseinen KIN-objekti viittaa. Lopuksi katselin tai kuvantamiskäyttäjä merkitsee kuvat ja muodostaa Key Image Note:n kuvaan.

Key Image Note voi viitata yhteen tai useampaan kuvaan kerralla ja yhtä kuvaa kohden voi olla useampia muistiinpanoja. On suositeltavaa, että viimeisimpänä vastaanotettu instanssi Key Image Note:sta on se, mitä tulee käyttää, jotta potilastietojen oikeellisuus pystyttäisiin varmistamaan. Näin siksi, jotta kuvantamislähteen tai kuvavarannon potilastiedot ovat varmasti ajan tasalla mahdollisten muutosten jäljiltä, eikä käytössä oleva Key Image Note viittaa vääriin, aikaisemmin voimassa olleisiin potilastietoihin. [27]

Retrieve Evidence Documents

Retrieve Evidence Documents -tapahtuman (RAD-45) käyttäjänä ovat katselin ja kuvavaranto tai kuvantamiskäyttäjä ja kuvantamislähde. Tapahtumaa käytetään pyydettyjen DICOM Evidence Document -dokumenttien siirtämiseen kuvavarannolta katselimelle tai kuvantamislähteeltä kuvantamiskäyttäjälle.

Tähän tapahtumaan tiiviisti liittyvä Evidence Document -profiili mahdollistaa tiedon muuntamisen pyydettyyn muotoon, tallentamisen ja hallinnoinnin vastaavalla tavalla kuten DICOM-kuvien tapauksessa. Tällaista tietoa ovat esimerkiksi neuvolamittaukset tai toimenpiteiden muistiinpanot. Evidence Document -tiedot voidaan tallentaa PACS:iin ja niitä voidaan hakea samalla kun haetaan DICOM-kuvia. Etuna tällaisten tietojen tallettamisessa on se, että tieto on silloin tallennettu koodattuna ja jäsennettynä. Tällöin tieto on varmasti tallennettu oikein ja sitä voidaan esimerkiksi automatisoidusti vertailla. Silloin voidaan olla varmoja, että lopputulos on luotettava. Esimerkiksi käytettäessä tutkimuksessa ultraäänilaitetta, joka tekee samalla myös mittauksia esimerkiksi sydänkuvista, voi luoda Evidence Document -dokumentin mitatuista arvoista ja tallentaa ne varantoon otettujen ultraäänikuvien kanssa.

Retrieve (Study Root - MOVE ja vaihtoehtoisesti Patient Root - MOVE) SOP -luokille tulee olla tuki, kun käytetään Retrieve Evidence Documents -tapahtumaa. SCU:na toimiessaan kuvavarannon tulee tukea DICOM Storage SOP -luokkaa ja kuvantamislähteen tulee tukea DICOM Storage SOP -luokkaa julkaistessaan jaettavia dokumentteja. [27]

Kuvavaranto tai kuvantamislähde vastaanottaa C-MOVE -pyynnön ja muodostaa DICOM-yhteyden katselimen tai kuvantamiskäyttäjän kanssa, sekä käyttää DICOM C-STORE -käskyä Evidence Document -objektien siirtämiseen. Koska katselin tai kuvantamiskäyttäjä voivat valita tehdystä kyselystä sopivia dokumentteja Template ID -parametriin pohjautuen, ei kuvavaranto tai kuvantamislähde saa palauttaa virheitä kuvavarannolle tai kuvantamislähteelle dokumentin sisällöstä. Virheen palauttamisen sijaan haun tulokset tulee hylätä ja jättää lähettämättä. [27]

Kun katselin tai kuvantamiskäyttäjä on vastaanottanut onnistuneesti Evidence Document -objektin, tulee vastaanottajan tulkita objekti käyttäjää varten. Jos katselin tai kuvantamiskäyttäjä ei pysty tulkitsemaan jotain osia kokonaan, on sen mahdollista ilmoittaa asiasta käyttäjälle ja kysyä, halutaanko muodostaa osittainen tulkinta tiedosta vai hylätä se kokonaan. Evidence Document -objekti voi sisältää myös viitteitä muunlaisiin Evidence-objekteihin. Katselimen tai kuvantamiskäyttäjän tulee aina pystyä tulkitsemaan joko kokonaan tai osittain kyseisen tiedon tai viitata johonkin ulkopuoliseen toimintoon, jolta tulkinta onnistuu. [27]

Jos katselin tukee myös Consistent Presentation of Images -profiilia, tulee sen myös näyttää kaikki tarjolla olevat esitysmuodot Evidence Document -objektista, jotka viittaavat kyseisiin kuviin. Jos tuki löytyy myös Key Image Notes -profiiliin, tulee sen myös aina tulkita kaikki Key Image Note -objektit joihin on viitattu Evidence-dokumentissa. [27]

WADO Retrieve

WADO Retrieve -tapahtuman (RAD-55) toimijoita ovat kuvantamiskäyttäjä ja kuvantamislähde. Tapahtuma mahdollistaa kuvantamiskäyttäjän pääsyn DICOM SOP -instansseihin web-pohjaisesta palvelusta HTTP(S)-protokollalla. [29]

Tapahtumassa kuvantamiskäyttäjä tekee HTTP GET -pyynnön, jolla pyydetään tiettyä DICOM-instanssia kuvantamislähteeltä. Kuvantamislähde vastaanottaa pyynnön, jos siinä ei ole virheitä sekä kokoaa vastauksen tarvittavalla sisällöllä (pyydetyn DICOM instanssin sisältö). Tämän jälkeen kuvantamislähde lähettää sen HTTP Response -pyynnön kanssa takaisin kuvantamiskäyttäjälle statuksella code 200 (OK). DICOM-instanssin tulee sisältää Study Instance UID:n (studyUID), Series Instance UID:n (seriesUID), ja SOP Instance UID:n (objectUID) HTTP Request-pyynnössä. Kuvantamiskäyttäjän pitää myös tietää parametreina web-palvelimen sijainti ja käytetty script-kieli, jotta tapahtuma onnistuu. Taulukossa 3.6 on eriteltynä WADO Retrieve -tapahtumassa käytettävissä olevat HTTP-pyynnön parametrit. Taulukko perustuu alkuperäiseen lähteeseen. [29]

Taulukko 3.6. *WADO HTTP-pyynnön parametrit [29].*

Nimi	Kuvaus	Vaatimus		Huom.
		Kuvantamis-dokumentin lähde	Kuvantamis-dokumentin käyttäjä	
requestType	Suoritetun http-pyynnön tyyppi, oltava "WADO"	R	R	
studyUID	Tutkimuksen yksilöllinen tunniste	R	R	
seriesUID	Sarjan yksilöllinen tunniste	R	R	
objectUID	Objektin yksilöllinen tunniste	R	R	
contentType	Vastauksen MIME-tyyppi	R+	R+	IHE-1,2
charset	Vastauksen merkistö	O	O	
anonymize	Objektin nimettömyys	O	O	
annotation	Objektin huomautus	O	O	IHE-3
rows	Pikselirivien lukumäärä	O	O	IHE-3
columns	Pikselisarakkeiden lukumäärä	O	O	IHE-3
region	Kuvan alue	O	O	IHE-3
windowCenter	Kuvan keskikohta	O	O	IHE-3
windowWidth	Kuvan leveys	O	O	IHE-3
frameNumber	Yksittäisen kuvakehyksen numero	O	O	IHE-3
imageQuality	Kuvanlaadun tekijä	O	O	IHE-3
presentationUID	Esitysobjektin yksilöllinen tunniste	O	O	IHE-3
presentationSeriesUID	Esitysobjektin kuvasarjan yksilöllinen tunniste	O	O	IHE-3
transferSyntax	Vastauksen sisältämän DICOM-objektin siirtomuodon yksilöllinen tunniste	O	O	IHE-3

IHE-1: DICOM PS 3.18:n mukaan taulukon 3.6 parametri contentType on valinnainen, mutta sille pitää silti olla tuki laajemman yhteensopivuuden vuoksi. Tarkemmin tämän parametrin ominaisuuksia on eritelty IHE RAD TF-3 -dokumentissa. [29, s. 123]

IHE-2: Tämän parametrin tulee olla yhteensopiva kuvantamisdokumentin käyttäjän määrittämän Accept-kentän kanssa HTTP-pyynnössä.

IHE-3: Koskee ainoastaan DICOM SOP -instanssia, jos se on kuvaobjekti.

Esimerkki WADO HTTP-pyynnöstä:

http://www.hospital.com/radiology/wado.php?requestType=WADO&studyUID=1.2.250.1.59.40211.12345678.678910&seriesUID=1.2.250.1.59.40211.789001276.14556172.67789&objectUID=1.2.250.1.59.40211.2678810.87991027.899772.2&contentType=application%2Fdicom

Jos kuvantamislähde ei pysty vastaamaan pyydetyillä MIME-tyypeillä contentType-parametrissa ja/tai Accept Field:ssä, tulee lähteen vastata koodilla 406 (Not Acceptable). Kuvantamislähteen tulee palauttaa koodi 404 (Bad Request), jos se ei pysty löytämään pyydettyä DICOM SOP -instanssia tai se ei tunnista HTTP-request URI:ssa olleita vaadittuja UID-arvoja. Paluukoodi 400 (Bad Request) palautuu siinä tapauksessa, jos mikä tahansa HTTP-kenttä tai vaadittu WADO HTTP -parametri puuttuu vastaanotetusta HTTP Request-URI:sta tai mikä tahansa syntaksivirhe on löydetty vastaanotetusta HTTP Request URI:sta. [29]

Retrieve Imaging Document Set

Retrieve Imaging Document Set -tapahtuma (RAD-69) on hyvin pitkälle yhtenevä XDS-profiilin yhteydessä käytettävän Retrieve Document Set -tapahtuman (ITI-43) kanssa, sillä siihen on lisätty lähinnä pieniä muutoksia kuvantamisdokumenttien välittämisen vuoksi. XDS-I -profiilissa tapahtumaa käyttää kuvantamisdokumentin käyttäjä vastaanottaessaan kuvantamisdokumentteja kuvantamislähteeltä.

Tämän lisäksi tätä tapahtumaa käytetään XCA-I -profiilissa (Cross-Community Access - Images). XCA-I -profiili on laajennus XCA-profiiliin, jota on käsitelty myöhemmin tässä työssä, kohdassa 3.11 XCA-profiili mahdollistaa diagnoosien ja kuvantamistietojen julkaisudokumenttien saatavuuden ja XCA-I -profiili mahdollistaa pääsyn näihin julkaisudokumentissa viitattuihin kuvantamistietoihin.

Dokumentin käyttäjä käyttää tätä tapahtumaa vastaanottamaan DICOM-objektien joukkoja kuvantamislähteeltä tai kuvantamisväylän valmistelijalta (Initiating Imaging Gateway). Kun dokumentin käyttäjä on suorittanut aikaisemmin kyselyn dokumenttivarannolle tietyistä dokumenteista Retrieve Document Set -tapahtumalla, saa kuvantamiskäyttäjä tätä kautta pääsyn kyseiseen julkaisudokumenttiin. Kuvantamiskäyttäjä purkaa tästä julkaisudokumentista tarvittavat parametrit, joita käyttämällä se saa luotua pyynnön kuvantamislähteelle. [29]

Pyynnön vastaanotettuaan kuvantamislähteen tai kuvantamisväylän valmistelijan tulee palauttaa kuvantamisdokumentti tai virhekoodi, jos palautus ei onnistu. Kuvatieto tulee muuntaa siihen DICOM-siirtomuotoon, joka on määritetty Retrieve Document Set -pyynnössä. Jos kuvatiedon muunnos ei onnistu yhdelläkään pyynnössä määritellyistä syntakseista, tulee palauttaa virheilmoitus kuvantamiskäyttäjälle. [29]

Provide and Register Imaging Document Set - MTOM/XOP

Provide and Register Imaging Document Set - MTOM/XOP -tapahtuman (RAD-68) käyttäjänä on kuvantamislähde, joka toimittaa kokoelman XDS-dokumentteja dokumenttivarannolle talletettavaksi ja rekisteröitäväksi dokumenttirekisterille (Repository Submission Request). Tapahtuma pohjautuu ITI-41:een, johon se tuo lisänä uusia dokumentin sisältötyyppejä. Provide and Register Document Set - MTOM/XOP pystyy välittämään:

- metatietoja nollasta tai useammasta uudesta dokumentista
  (jos metatiedossa on nolla dokumenttia, sitä voidaan käyttää kuvaamaan viitteitä sisältäviä kansioita, jotka viittaavat aikaisemmin toimitettuihin dokumentteihin)
- yksi XDSDocumentEntry dokumenttia kohden metatietojen sisällä
- Submission Set -määritelmä, joka sisältää linkityksen uusiin dokumentteihin ja viittaukset olemassa oleviin dokumentteihin
- nollan tai useamman XDS-kansion määritelmä sisältäen linkityksen uusiin tai olemassa oleviin dokumentteihin
- nolla tai useampia dokumentteja. [29]

Verrattuna XDS-tapahtumaan ITI-41 (Provide and Register Document Set-b) määrittelee seuraavat uudet dokumentin sisältötyypit (Document Content Type): [29]

1. DICOM SOP -instanssien kokoelmat
2. Kuvantamisen diagnostiikkaraportit

Jotta nämä uudet sisältötyypit ja niiden käyttö olisi tuettu, XDS-dokumentin metatiedot tarvitsevat uusia määrityksiä ja rajoitteita. Nämä ovat eriteltynä tarkemmin IHE Radiology Technical Framework Vol 3:ssa. [29]

3.3 Kuvantamisdokumenttien merkintä

Tässä kohdassa annetaan vain tiivis esittely kuvantamisdokumenttien merkintä -profiilista, koska tätä profiilia sivuttiin jo XDS-I -profiilia käsittelevässä kohdassa 3.2. Key Image Note -profiili (KIN) mahdollistaa kuvien merkitsemisen myöhempää käyttöä varten. KIN-profiilin merkintä tarkoittaa varsinaista otsikkokenttää sekä valinnaista kommenttikenttää, jossa voi eritellä tarkemmin muistiinpanon syytä. Käyttötarkoituksia muistiinpanoille on useita, esimerkiksi konsultaatiot muulta hoitohenkilökunnalta, kuvan laatuun liittyvät kommentit tai opetustarkoitukseen valittavat materiaalit. IHE:n julkaisuissa on myös mainittu, että vaikka KIN-muistiinpanot täyttävät myös määritelmän Evidence Document -dokumenteista, on KIN-muistiinpano sen erikoistapaus, mikä käsitellään erikseen historiallisista syistä. [24]

Käytettäville otsikoille on määritelty lista, joilla selviää, miksi kuvia on merkitty näillä muistiinpanoilla. Nämä otsikot on listattu alla olevaan taulukkoon 3.7, joka perustuu alkuperäiseen lähteeseen [30].

Taulukko 3.7. *KIN-muistiinpanojen määritellyt otsikot [30].*

Käytetty koodaus	Koodin lukuarvo	Koodin selite	Selite englanniksi
DCM	113000	Kiinnostava	Of Interest
DCM	113001	Hylätty laadun vuoksi	Rejected for Quality Reasons
DCM	113002	Lähete	For Referring Provider
DCM	113003	Kirurgia	For Surgery
DCM	113004	Opetus	For Teaching
DCM	113005	Konferenssi	For Conference
DCM	113006	Terapia	For Therapy
DCM	113007	Potilas	For Patient
DCM	113008	Vertaisarviointi	For Peer Review
DCM	113009	Tutkimus	For Research
DCM	113010	Laatuongelma	Quality Issue
DCM	113013	Kuvasarjan paras	Best In Set
DCM	113018	Tulostus	For Printing
DCM	113020	Raportin liitteeksi	For Report Attachment
DCM	113030	Julkaisudokumentti	Manifest
DCM	113031	Allekirjoitettu julkaisu	Signed Manifest
DCM	113032	Valmis opiskelusisältö	Complete Study Content
DCM	113033	Allekirjoitettu valmis opiskelusisältö	Signed Complete Study Content
DCM	113034	Valmis hankittu sisältö	Complete Acquisition Content
DCM	113035	Allekirjoitettu valmis hankittu sisältö	Signed Complete Acquisition Content
DCM	113036	Kuvakehysten lukumäärä	Group of Frames for Display
DCM	113037	Hylätty potilasturvallisuuden vuoksi	Rejected for Patient Safety Reasons

Otsikot on määritelty DICOM:n toimesta ja se sisältyy CID 7010:iin (Key Object Selection Document Title) DICOM PS3.16:ssa [30]. Yksi KIN-merkintä voi viitata useisiin kuviin samassa tutkimuksessa tai useita KIN-merkintöjä voi viitata samaan kuvaan. Sen lisäksi, että KIN-merkintä viittaa kuvaan, voi se viitata myös tiettyyn esitystilaan (Presentation State).

Tämä on mahdollista siksi, että merkintä voi liittyä juuri johonkin tiettyyn esitystilaan kuvasta, esimerkiksi ikkunan leveys, zoom tai kääntö. Kuvanäyttö voi käyttää tätä tietoa, jos se tukee sekä KIN-profiilia, että Consistent Presentation of Images -profiilia. [24] KIN-profiili ei liity kovin läheisesti tämän työn taustalla olevaan projektiin, joten toistaiseksi sitä ei käsitellä tämän enempää tässä työssä.

3.4 Järjestelmän aika

Consistent Time -yhdentämisprofiili (CT) on määritelty siksi, että sitä käyttämällä voidaan varmistaa samassa järjestelmässä olevien kaikkien laitteiden järjestelmäajan ja aikaleimojen olevan yhtenevät. Tässä profiilissa on ajan synkronoinnin mediaanivirhe määritelty olemaan alle yhden sekunnin, joka on riittävä useimpiin tarpeisiin [12]. Ottaen huomioon IHE-profiileja käyttävien järjestelmien luonteen, on tämä IHE Technical Framework -dokumentin määrittelemä alle sekunnin mediaanivirhe kuitenkin hieman liian sallivasti määritelty. Toteutettavissa järjestelmissä tulisi mediaanivirheen maksimi määritellä selvästi pienemmäksi.

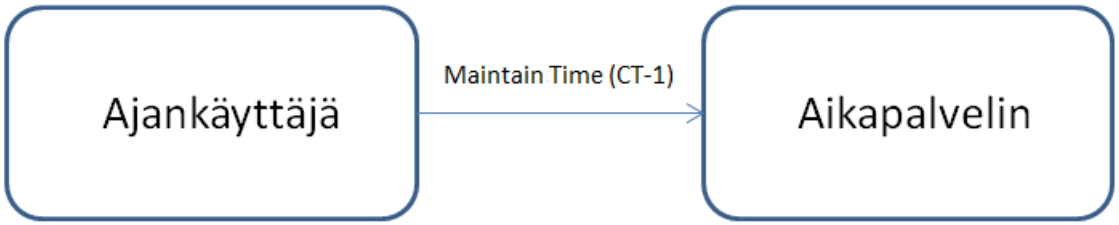
CT-profiili määrittelee synkronointimekanismin toimijoiden ja tietokoneiden välille. Useat infrastruktuuri-, turvallisuus- ja pääsyprofiilit vaativat yhdenmukaisen kel-

lonajan suurissa tietokoneverkoissa. CT-profiili vaatii Network Time Protocol -ajan (NTP) käytön, joka on määritelty RFC 1305:ssa [31]. Kun aikapalvelin (Time Server) on yhdistetty ajankäyttäjän kanssa (Time Client), ajankäyttäjän tulee käyttää NTP:tä. Jos jotkut käyttäjät eivät ole yhdistetty aikapalvelimeen, SNTP:tä voidaan käyttää (Simple Network Time Protocol). [12]

Consistent Time oli alun perin osa radiologian turvallisuusprofiileja (Radiology Basic Security Profile), mutta nykyisin sillä on käyttöä myös muissa IHE:n viitekehyksissä, joten siitä on muunnettu erillinen oma profiilinsa. Tämä muutos on toteutettu siten, että olemassa oleviin profiileihin ei ole tehty muutoksia niiden vaatimuksiin. [12]

3.4.1 CT-toimijat

CT-profiili on rakenteeltaan yksinkertainen, siinä on kaksi toimijaa ja niiden välillä yksi tapahtuma. Nämä on havainnollistettu alla olevaan kuvaan 3.5, joka perustuu alkuperäiseen lähteeseen [12]. Tässä kohdassa esitellään toimijat ja seuraavassa kohdassa 3.4.2 niiden välillä suoritettava Maintain Time -tapahtuma.



Kuva 3.5. *CT-profiilin toimijat [12].*

Aikapalvelin

Aikapalvelin eli Time Server on järjestelmässä keskitetty palvelin, jonka käyttäjinä ajankäyttäjät (Time Client) ovat. Aikapalvelimen tulee tarjota NTP-aikaa ajankäyttäjille.

Ajankäyttäjä

Ajankäyttäjä kuvaa järjestelmässä yksittäistä tietokonetta tai päätelaitetta, jonka tehtävänä on päivittää synkronoitu NTP-aika aikapalvelimelta. Jos synkronoidun NTP-ajan päivitys ei se jostakin syystä onnistu, niin siinä tapauksessa käytetään SNTP-protokollaa.

3.4.2 Maintain Time -tapahtuma

Maintain Time (ITI-1) on ainoa CT-profiilin tapahtuma. Maintain Time -tapahtuman tehtävänä on sananmukaisesti mahdollistaa käytettävän kellonajan synkronointi ja ylläpito aikapalvelimen ja ajankäyttäjien välillä.

Maintain Time -tapahtumaa käytetään kaikissa sellaisissa profiileissa, jotka tarvitsevat luotetun tiedon järjestelmän ajasta. Tämän tapahtuma on käytössä muun muassa seuraavassa kohdassa 3.5 esiteltävässä profiilissa.

3.5 Tunnistautuminen ja auditointi

Audit Trail and Node Authentication (ATNA) -profiili mahdollistaa potilastietojen käsittelyssä vaadittavat turvallisuus- ja luottamuksellisuusominaisuudet sekä tiedon eheyden ja käyttäjätilien käyttövalvonnan. Tällaista ympäristöä nimitetään turvallisuusympäristöksi (Security Domain) ja se skaalautuu yksittäisestä osastosta (department) kokonaiseen organisaatioon (enterprise) sekä päättyen XDS-hoitoyhteisöön (XDS Affinity Domain). ATNA-profiilin määritelmässä turvallisuusympäristön sisällä tulee olla voimassa:

1. Kaikki laitteet ovat tunnistautuneita (host authenticated). Tämä tunnistautuminen määrittää laitteen olevan tunnettu sairaalan turvallisuusjärjestelmille ja se omaa tietyt turvallisuusnäkökohdat. Tuntemattomille laitteille voidaan halutessaan myös antaa pääsy, mutta ne eivät pääse kuin tiettyihin rajattuihin julkisiin resursseihin.
2. Laitteiden tunnistautuminen määrittelee, annetaanko laitteelle tai sen käyttäjälle automaattisesti jotakin oikeuksia vai ei. Käytännössä näillä automatisoiduilla määrityksillä on kriittinen rooli.
3. Luotettu laite (secure node) on vastuussa riittävien oikeuksien antamisessa muille käyttäjille. Tähän kuuluu tyypillisesti käyttäjien tunnistautuminen ja valtuuttaminen. Tunnistautumisessa pitää ottaa huomioon sekä mahdollinen turvallisuusriski että potilaan terveyteen vaikuttava tekijät sen suhteen, jos ylimääräiset tunnistautumisen tarpeet viivästyttävät potilaan tarvitsemaa hoitoa.
4. Luotetun laitteen on myös tarjottava turvallisuusauditointi, jolla voi seurata kaikkia turvallisuuspoikkeamia ja -tapahtumia. Terveydenhuollon yhteydessä auditointilokeilla on enemmän käyttöarvoa, kuin tiukoilla pääsyvalvonnan mekanismeilla. Käyttöarvolla viitataan siihen, että potilastiedot sisältävät paljon luottamuksellista tietoa. Näihin tietoihin hoitohenkilökunnan tulee päästä tarvittaessa helposti käsiksi, joten tietojen käytönvalvonta on tärkeämpi ominaisuus kuin pääsynvalvonta. On parempi tilanne, että tietoihin hoitoa tarjoavissa organisaatioissa pääsee valvotusti käsiksi, kuin että potilas pahimmillaan kuolee käsiin, kun hoitohenkilökunta ei tiedä esimerkiksi potilaan allergioita. [12]

Tätä mallia on ajateltu erityisesti siltä kannalta, että eteen tulee myös sellaisia tilanteita, missä tietoa vaihdetaan laitteiden välillä ja tallennetaan vastaanottajan päässä. Tämä on osittain tehty sillä oletuksella, että terveydenhuollossa tulee eteen sellaisia tilanteita, missä verkkoyhteydet eivät toimi tai niiden käyttö on hyvin rajoitettua. [12]

ATNA-profiilin hallinnolliset oletukset on kuvattu alla olevassa listassa:

1. Kaikkien niiden järjestelmien, jotka kuuluvat suojattuun toimialueeseen (secure domain), tulee implementoida luotettu laite (secure node) -toimija ATNA-profiilia varten.
2. Kaikkien luotetun laitteen sovelluksien tulee täyttää ATNA:n vaatimukset, riippumatta siitä ovatko ne IHE-toimijoita vai eivät. Vaatimukset koskevat kaikkia tietokoneavusteisia tapahtumia, missä luodaan, haetaan, päivitetään tai poistetaan suojattua potilasinformaatiota (PHI, Protected Health Information). Tämä koskee kaikkia PHI-informaatioon kohdistuvia toimenpiteitä, ei pelkästään IHE:n määrittelemiä ja IHE-toimijoiden suorittamia toimenpiteitä.
3. IHE määrittelee ainoastaan sellaiset turvallisuusmääritykset, jotka liittyvät IHE:n terveydenhuollon sovellutuksiin. Se ei ota kantaa muihin turvallisuusnäkökohtiin, kuten esimerkiksi suojautumiseen verkkohyökkäyksiltä tai virustartunnoilta. Jäljitysmekanismin (Audit Trail) pääasiallinen tarkoitus on tallentaa tietoa PHI-informaatioon liittyvistä toimista, ei seurata IHE-tapahtumia.
4. Mobiililaitteilla on myös mahdollista käyttää ATNA-profiilia, mutta mobiililaitteisiin liittyviä erityistoimenpiteitä tai näkökohtia ei käsitellä tässä profiilissa.
5. ATNA-profiili olettaa, että organisaatiossa toimivassa järjestelmässä fyysinen pääsynhallinta, henkilöstön pääsyoikeudet ja muu organisaatioon kuuluva tietoturvan hallinta on hoidettu siinä laajuudessa, että voidaan sanoa organisaation täyttävän turvallisuus- ja yksityisyysmääräykset. [12]

Yllä olevaan listaan määritellyt hallinnolliset oletukset kuvaavat ATNA-profiilia käyttävän järjestelmän ominaisuuksia. Näitä ominaisuuksia järjestelmän oletetaan sisältävän, kun siinä on tuki ATNA-profiilille.

3.5.1 Tunnistautuminen

ATNA-profiilin pääsynvalvonta hoidetaan rajoittamalla verkkoyhteyksiä laitteiden välillä ja rajoittamalla pääsy laitteille vain valtuutetuille käyttäjille. Luotettujen laitteiden välinen liikenne suojatussa toimialueessa on rajoitettu ainoastaan sen toimialueen luotetuille laitteille. Luotetut laitteet rajoittavat pääsyn ainoastaan luotetuille käyttäjille paikallisen tunnistautumisen ja pääsykontrollin määritysten mukaan. [12]

Käyttäjän tunnistautuminen

ATNA-profiili vaatii ainoastaan paikallisen käyttäjän tunnistautumisen. Profiilin määritelmä antaa vapauden luotetulle laitteelle käyttää haluamaansa käyttäjän tunnistautumistapaa, sitä ei ole rajoitettu mihinkään tiettyyn tunnistautumistapaan. [12]

Yhteyden tunnistautuminen

Kaksisuuntainen sertifikaatteihin perustuva laitetunnistautuminen kaikkien laitteiden välillä on vaatimuksena ATNA-profiilissa. Käytetyissä standardeissa on kaikissa määritelty sertifikaattiin perustuva tunnistautuminen. Näitä standardeja ovat DICOM, HL7 ja HTML. Sertifikaattiin perustuvaa tunnistautumista käytetään käyttäjän tunnistautumisen sijaan. Yhteydet laitteisiin, jotka eivät ole kahdensuuntaisesti tunnistautuneet, tulee joko estää tai suunnitella siten, ettei niillä ole pääsyä PHI-informaatioon. Jos käytössä on sellaisia protokollia, mitä ei ole määritelty IHE-profiileissa, tulee niiden käyttöön toteuttaa kahdensuuntainen tunnistautuminen. ATNA-profiili ei ota kuitenkaan siihen kantaa, miten tämä toteutus tulee tehdä. [12]

Edellä mainittu vaatimus voidaan täyttää myös siten, että varmistetaan täydellinen fyysinen järjestelmän verkkotietoturva tiukalla konfiguraatiohallinnalla. Tällä tarkoitetaan sitä, että mikään ei-luotettu laite ei voi saada pääsyä mihinkään osaan verkkoa. Luotettu laite -toimija tulee olla konfiguroitavissa näillä molemmilla edellä mainituilla menetelmillä. Sen tulee siis tukea sekä kaksisuuntaista sertifikaatteihin perustuvaa tunnistautumista laitteiden välillä että pystyä myös toimimaan fyysisesti varmistetun verkkotietoturvan omaavassa verkossa, eli tukea tällaisen verkon määrittelemää tiukkaa tietoturvaominaisuuksien hallintaa. [12]

IHE ei edellytä, että liikenne siirtoverkossa on salattua, koska useimmat sairaaloiden verkot sisältävät asianmukaisen tietoturvallisuustason. Vaatimuksena ATNA-profiilissa on Transport Layer Security (TLS) -salausmekanismin käyttö kaikissa luotettujen laitteiden välisessä liikenteessä. Näin saadaan käteltyä myös salaus laitteiden välille, jos ne sitä pyytävät ja tukevat. Tällä mahdollistetaan IHE:n määritelmillä luotetun laitteen asennus ympäristöön, missä verkko ei ole muulla tavalla jo luotettu. [12]

XDS-tekniikkaa edeltävän REST-arkkitehtuurityyliin perustuvan järjestelmän on myös täytettävä riittävät turvallisuusvaatimukset. REST-palveluun voi tulla jatkossa myös ulkoverkosta suoritettavia pyyntöjä, joten tietoturvallisuus on otettava siinä laajuudessa myös huomioon. Tietosuojan vuoksi kaikki palvelussa tapahtuva liikenne on toteutettu HTTPS-protokollaa käyttäen. HTTPS-protokollassa kaikki liikenne salataan SSL/TLS-protokollan avulla. Tämän lisäksi palvelussa on niin sanottu whitelist-taulukko, jossa on listattuna kaikki sallitut ulkoiset IP-osoitteet. Tämän lisäksi käytössä on myös blacklist-taulukko, jossa estetään tarvittaessa tietyn sallitun IP-avaruuden sisältä tiettyjä IP-osoitteita tai -avaruuksia. [32]

3.5.2 Jäljitysmekanismi

ATNA-profiilin jäljitysmekanismilla (Audit Trail) on toteutettu järjestelmän käyttäjien käytönseuranta. Jäljitysmekanismin tulee antaa turvallisuushenkilölle pääsy suorittamaan auditointi toimialueen turvamääräyksiin, etsiä mahdollisia rikkomuksia sekä PHI-informaation asiattomia luonteja, katseluja, muokkauksia tai poistoja. Tärkeimpiä jäljitystietoja ovat kenen potilaan tietoja on tutkittu, ketkä käyttäjät tietoja ovat tutkineet ja mitä käyttäjän tai laitteen tunnistautumiseen liittyviä virheitä on raportoitu. [12]

Medbit Oy:n REST-palvelussa kirjoitetaan lokiin kaikki REST-kutsut parametreineen sekä myös kaikki viitteet jokaisen REST-kutsun tuloksista aikaleimoineen. Näiden tietojen tallennusta ei voi estää tai ohittaa ja kaikki tiedot kirjoitetaan tietokantaan siinä aikajärjestyksessä, kun ne on palvelussa suoritettu. [32]

3.5.3 Jäljitysviestien siirto

ATNA-profiili määrittelee Syslog-protokollien käytön mekanismina auditointiviestien tallennukseen auditointitietovarantoon. Syslog on standardi, jolla tallennetaan tietokoneen suorittamien viestien tallentaminen (logging). Syslog-standardi on määritelty RFC 5424:ssä. Kaksi vaihtoehtoista siirtotapaa auditointiviestien tallennukseen on määritelty ATNA-profiilin määritelmässä:

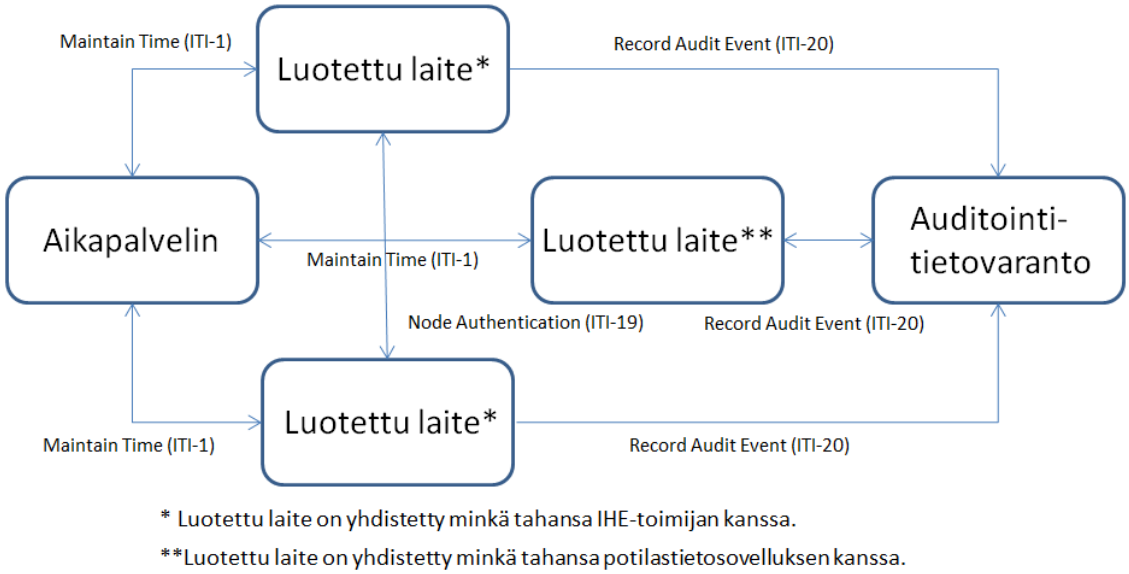
1. Syslog-viestien siirto käyttäen UDP:tä.
   Tässä siirtotavassa on useita tiedossa olevia rajoitteita:
   - Lähettäjälle ei ole olemassa mitään varmuutta siitä, että lähetetty viesti on vastaanotettu määränpäässä.
   - Auditointiviestejä ei ole mahdollista salata.
   - Sertifikaattitunnistautuminen lähettävien laitteiden ja auditointitietovarannon välillä ei ole mahdollista.
   - Viestejä voi korvautua toisilla viesteillä tai hukkua. [12]
2. Syslog-viestien siirto käyttäen TLS:ää. Tässä siirtotavassa syslog-viestien lähetys muotoillaan lähetettäväksi streaming-protokollan yli, jonka suojauksessa käytetään TLS:ää. Näin ollen TLS:ää käyttämällä ei ole vastaavia rajoitteita viestien siirrossa, koska se tarjoaa mekanismit edellä mainittujen rajoitteiden ratkaisemiseksi. [12]

Syslog-viestien tallennus on toteutettu soveltuvin osin myös REST-palveluun, jossa viestit tallennetaan sisäisesti ilman viestien siirtoja suoraan palvelun omaan tietokantaan [32].

3.5.4 ATNA-toimijat

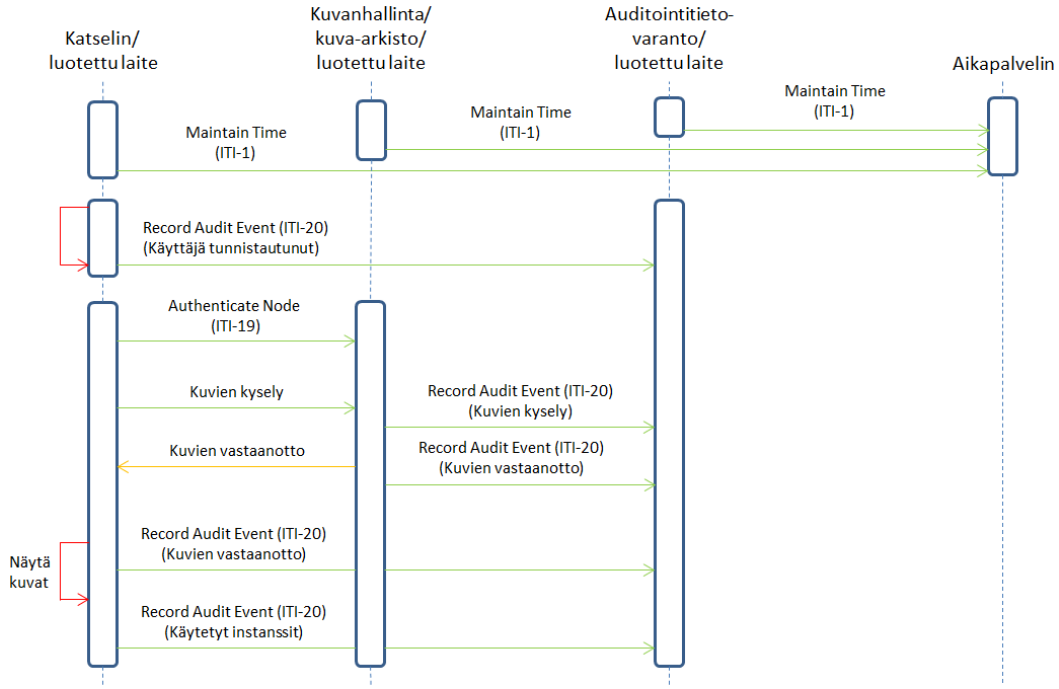
Jos IHE-implementaatio tukee ATNA-profiilia, tulee siinä tapauksessa kyseisen toimijan yhdistyä luotetun laitteen kanssa. ATNA:n määritelmässä on vaadittu, että kaikki IHE-toimijat ja mikä tahansa muu toiminta tässä implementaatiossa tulee tukea ATNA:aa [12].

Kuvassa 3.6 on havainnollistettu ATNA-profiilin toimintaa, siihen on merkitty kyseisen profiilin toimijat ja niiden väliset tapahtumat. Kuva 3.6 perustuu alkuperäiseen lähteeseen [12]. Kuvassa on myös määritelty profiiliin kahta eri tyyppiä luotettuja laitteita, sellainen joka on yhdistetty potilastietosovelluksen kanssa, sekä sellainen joka on yhdistetty minkä tahansa muun IHE-toimijan kanssa.



Kuva 3.6. *ATNA-profiilin toimijat [12].*

Kuvassa 3.7 on esitelty prosessikaavion muodossa auditointiviestien välitys. Kyseessä on sellainen tilanne, jossa katselin tekee kyselyn jostakin tietystä katselimen käyttäjän haluamasta kuvasta.



Kuva 3.7. *Luotetun laitteen ja auditointiviestien prosessikaavio.*

Kaikki toimijat järjestelmässä toimivat luotettuina laitteina ja näin ollen voivat käyttää Record Audit Event -tapahtumaa auditointiviestien välitykseen auditointitietovarastolle. Toimija voi olla mikä tahansa IHE-toimija tai mikä tahansa potilastietosovellus, joka on yhdistetty luotetun laitteen kanssa.

Auditointitietovarasto

Käyttäjälokien hallinta ATNA-profiilissa suoritetaan standardeihin perustuvan keskitetyn auditointitietovarannon (Centralized Audit Record Repository) avulla. Kaikki käyttäjien tapahtumista kerättävät tiedot kaikista IHE-toimijoista tallennetaan auditointitietovarantoon, jonka avulla tietojen muokkaamisen mahdollisuus on pienempi ja organisaation osastoja on helpompi auditoida. Jos laitteet ovat poiskytkettynä verkosta, niiden tulee tallentaa käyttäjätiedot auditointitietovarantoon seuraavan suojattuun verkkoon yhdistämisen jälkeen.

Luotettu laite

Luotettu laite (Secure Node) tulee sisältää:

1. Authenticate Node -tapahtuman kaikille verkkoyhteyksille, jotka voivat paljastaa yksityistä potilasinformaatiota.
2. Kaikki käyttäjän paikallisesti suorittamat toimet, eli esimerkiksi sisään ja uloskirjaukset, tulee suojata vain todennetuille käyttäjille (authorized users).
3. Auditointitapahtumien tallennus (Record Audit Event), kuten määritelty ITI IF-2a -dokumentin kohdassa 3.20. [12]

Luotettu sovellus

Luotetun laitteen (Secure Node) ja luotetun sovelluksen (Secure Application) erona on taustalla olevan käyttöjärjestelmän ja muun ympäristön suojaustaso. Luotettu laite sisältää kaikki tietoturvan eri ominaisuudet, käyttäjän tunnistautumisen, tiedostojärjestelmän suojaukset ja käyttöympäristön suojaukset.

Luotettu sovellus on tuote, joka ei sisällä käyttöympäristön suojauksia. Luotettu sovellus sisältää suojauksen ainoastaan sovelluksen ominaisuuksiin. [12]

Auditointitietovaranto

Auditointitietovarannon (Audit Repository) tulee tukea molempia tiedonsiirtomekanismeja, eli Syslog-viestien siirto tulee olla mahdollista UDP:tä ja TLS:ää käyttäen. Auditointitietovarannon tulee tukea myös mitä tahansa IHE:n määrittelemän auditointiviestin muotoa, kun viestit on lähetetty jommalla kummalla edellä mainitulla tiedonsiirtomekanismilla.

Näiden lisäksi auditointitietovarannon pitää sisältää tuki tietojen suojaukselle ja käyttäjien pääsynvalvonnalle. ATNA-profiili ei määritä muita tehtäviä auditointitietovarannolle, mutta oletetaan, että useimmat tietovarannot suorittavat tarkastuksia, raportointia, tallennusta ja niin edelleen. [12]

3.5.5 ATNA-tapahtumat

Tässä kohdassa esitellään tarkemmin ATNA-profiilin toimijoiden väliset tapahtumat. Tapahtumien lisäksi käydään läpi profiilin toiminnassa keskeinen paikallisen käyttäjän

tunnistautuminen. Tämä toiminnallisuus kuuluu keskeisenä osana ATNA-profiilin ominaisuuksiin.

ATNA-profiilin toiminnallisuutta verrataan myös REST-arkkitehtuurityyliä hyödyntävään tietopalveluun. REST-palvelussa on toteutettu vastaavat ominaisuudet, jotta saavutetaan vastaava järjestelmän turvallisuustaso sekä mahdollistetaan järjestelmien yhteensopivuus.

Maintain Time

Viitaten tämän työn lukuun 3.4., Maintain Time -tapahtuma (ITI-1) kuuluu osaksi Consistent Time -profiilia. Tapahtuman tehtävänä on synkronoida järjestelmässä käyttämä kellonaika yhtenevästi koko järjestelmän laitteiden kesken. Maintain Time -tapahtuma käyttää joko NTP- tai SNTP-protokollaa asiakassovelluksen (Time Client) ja aikapalvelimen (Time Server) välillä tapahtuvaa kommunikointia varten.

Authenticate Node

Kun on tarve vaihtaa tietoa kahden laitteen välillä, paikallinen luotettu laite esittelee oman identiteettinsä vieraalle luotetulle laitteelle (remote secure node) ja tunnistaa sen identiteetin. Kun tämä yhteinen tunnistautuminen on suoritettu ja kahden laitteen välille on muodostettu suojattu yhteys, voidaan suorittaa muita suojattuja tapahtumia. Authenticate Node -tapahtumaa (ITI-19) tulee käyttää jokaiseen DICOM-, HTTP- tai HL7-yhteyteen. Tämän lisäksi luotettu laite tunnistautuu myös käyttäjän kanssa, joka yrittää käyttää kyseistä laitetta. Käyttäjän tunnistautuminen on paikallinen toimenpide, joten sen toteutuksessa ei tarvitse ottaa yhteyttä vieraaseen laitteeseen. [17]

Paikallinen organisaatio, esimerkiksi XDS-hoitoyhteisö, tekee itse päätöksen siitä, mitä metodeja käytetään verkkoyhteyksien tunnistautumista varten. Tunnistautuminen voi perustua kokonaan luotetun ketjun muodostamiseen valittujen varmentajien kanssa (Certificate Authority), kokonaan laitekohtaisten varmenteiden jakamiseen tai näiden edellä mainittujen yhdistelmiin. [17]

Kun paikallinen luotettu laite tunnistaa vierasta luotettua laitetta, tulee sen pystyä tekemään varmenteen vahvistus perustuen luotetun varmentajan allekirjoitukseen tai pystyä tekemään suora varmennus luotettujen varmenteiden perusteella. Jos varmenteen vahvistaminen epäonnistuu, tulee paikallisen laitteen estää verkkoyhteydet tai rajoittaa niitä vain vieraan ei-luotetun laitteen käyttöä varten. [17]

Luotetun laitteen ei tule vaatia mitään tiettyjä varmenteen attribuutteja, mutta sen ei myöskään tule hylätä varmenteita, missä on tuntemattomia attribuutteja tai parametreja. Huomionarvoista on, että yleensä laitevarmenteita varten CN on isäntänimi (hostname). Isäntänimen käyttäminen ei tuo mitään lisäturvallisuutta, vaan aiheuttaa vain uuden mahdollisen virhetilanteen (esimerkiksi DNS-virhe). Yhteisen tunnistautumisen suorittamiseen käytettävät varmenteet tulee olla X509-varmenteita, jotka perustuvat RSA-avaimeen [33]. Varmenteen avain tulee olla 1024-4096 bittiä pitkä. Avaimen pituus valitaan paikallisesti sovittujen käytäntöjen (policy) mukaan. Käytettävien varmenteiden

voimassaoloajan maksimi tulee myös määritellä käytettävien turvallisuuskäytäntöjen mukaan. IHE:n viitekehyksen mukainen voimassaoloajan suositus on kaksi vuotta. [17]

IHE ei ole määrittänyt tarkkaa toimintatapaa siihen, miten päätetään, onko laite valtuutettu suorittamaan tapahtumaa vai ei. Tämä voidaan suorittaa esimerkiksi käyttämällä luotettuja varmenteita, perustuen johonkin attribuutin arvoon varmenteissa, hallinnoimalla pääsylistoja tai jollain muulla vastaavalla menettelytavalla.

REST-palvelussa on erikseen määriteltävissä ne osapuolet, jotka voivat hakea tietoja palvelusta myös ilman potilaan identifioivaa tietoa, esimerkiksi potilaan henkilötunnusta. Tällä tavalla tietoja voidaan hakea palvelussa myös tiedon sisällön perusteella, jolloin potilaan yksilöivä tieto ei selviä hakijalle, eikä näin ollen myöskään kyseisen potilaan todellinen identiteetti. [32]

Paikallisen käyttäjän tunnistautuminen

Luotettu laite aloittaa tunnistautumisprosessin, kun käyttäjä haluaa kirjautua laitteelle. Laitteen vastuulla on, ettei käyttäjälle myönnetä pääsyä luottamukselliseen potilasinformaatioon ennen kuin paikallisen käyttäjän tunnistautuminen on suoritettu onnistuneesti. Paikalliskäyttäjän tunnistautuminen ei ole IHE:n määrittelemä tapahtuma, vaikka se voi määrittää järjestelmän, joka tunnistautumisen suorittaa. [17]

Tämä tunnistautuminen tapahtuu paikallisesti luotetulla laitteella ja käyttäjän identiteetti tulee varmistaa esimerkiksi käyttäjänimellä ja salasanalla, biometrisella tunnisteella (esimerkiksi sormenjälkilukija) tai jonkinlaisella tunnistekortilla. Käyttäjä kirjautuu sisälle käyttämällä jotakin omaa henkilökohtaista tunnistetta. Tunnisteiden tulee olla yksilöllisiä koko luotetussa toimialueessa. Yhdellä käyttäjällä voi olla useampia henkilökohtaisia tunnisteita ja luotettu laite tulee olla konfiguroitavissa siten, että se sisältää listan sille valtuutetuista käyttäjistä. Toimintatavat henkilökohtaisten tunnisteiden määrittämiselle ja jakamiselle kuuluu jokaisen terveydenhuollon organisaation omiin tietoturvamäärityksiin. Näiden määritysten kehittäminen ei kuulu IHE:n viitekehykseen. [17]

REST-palvelussa toteutetaan vastaavaa periaatetta, kuin ATNA-profiilin määritelmä käyttäjän tunnistautumiseen. REST-palvelu ei myöskään ota kantaa siihen, miten käyttäjä on tunnistautunut alun perin järjestelmään. Kutsujan yksilöllinen tunniste FP, sekä sitä vastaava yksilöllinen Salt-arvo tulee löytyä REST-palvelusta, jotta järjestelmä vastaa tehtyihin kutsuihin. Sen lisäksi REST-palvelu vaatii myös, että kutsuissa on aina kutsujan antama SSO- tai UAD-arvo, jolla määritellään kutsujan ”sormenjälki” järjestelmään. Myös nämä kaikki kutsujaan liittyvät tiedot tallennetaan kaikissa tilanteissa tietokantaan REST-palvelun lokitietoihin. [32]

Record Audit Event

Record Audit Event -tapahtuman (ITI-20) käyttäjänä toimivat mitkä tahansa IHE-toimijat, jotka tukevat Audit Trail and Node Authentication -profiilia kommunikoidakseen auditointitietovarannon kanssa. Auditointiloki (Audit Log) on muistio kaikista käyttäjien mihin tahansa tietoon tekemistä toimista. Toimia ovat kyselyt, katselut, lisäykset, muutokset ja poistot. IHE-toimija luo merkinnän auditointitietovarannon audi-

tointilokiin, kun IHE-tapahtumaan liittyvä toimi tapahtuu tai myös siinä tapauksessa, jos toimi ei liity mihinkään tapahtumaan. [17] Alla olevaan taulukkoon 3.8 on listattu auditointimerkinnän aiheuttavat toimenpiteet. Taulukko perustuu alkuperäiseen lähteeseen [17].

Taulukko 3.8. *Auditointimerkinnän muodostavat toiminnot [17].*

Tapahtuma	Kuvaus	Lisätietoa
Actor-start-stop	Minkä tahansa toimijan käynnistys tai sammutus. Ei koske laitteiston käynnistystä ja sammutusta.	DICOM PS 3.15 A.5.3 “Application Activity”
Audit-Log-Used	Jokin muu kuin auditointiviestien tallennus on vieraillut tai muokannut auditointitietovarastoa.	DICOM PS 3.15 A.5.3 “Audit Log Used”
Begin-storing-instances	Aloita SOP-instanssien tallennus. Tämä voi koostua useammista instansseista.	DICOM PS 3.15 A.5.3 “Begin Transferring DICOM Instances”
Health-service-event	Jokin instanssi tai hoitotoimenpide on varannut ajan tai suorittanut terveydenhoitoa. Tämä sisältää ajanvarauksen, herätteen, päivitykset tai muutokset, hoitotoimenpiteen suorituksen tai loppuunsaattamisen ja keskeytyksen.	IHE Extension (ITI TF-2a:3.20.7.3) “Health Services Provision Event”
Instances-deleted	SOP-instanssit on poistettu tietystä tutkimuksesta. Yksi tapahtuma kattaa kaikkien instanssien poiston tietystä tutkimuksesta.	DICOM PS 3.15 A.5.3 “DICOM Instances Accessed” or “DICOM Study Deleted”
Instances-Stored	Järjestelmään on tallennettu instanssi tietystä tutkimuksesta. Yksi tapahtuma kattaa kaikkien instanssien tallennuksen tietystä tutkimuksesta.	DICOM PS 3.15 A.5.3 “DICOM Instances Transferred”
Medication	Lääkemääräys ja hallinnolliset toimenpiteet instanssissa tai hoitotoimenpiteessä. Tämä sisältää tilauksen, jakelun, toimituksen ja keskeytyksen.	IHE Extension (ITI TF-2a:3.20.7.3) “Medication Event”
Mobile-machine-event	Siirrettävä laite liittyy tai poistuu luotetulta toimialueelta.	DICOM PS 3.15 A.5.3 “Network Entry”
Node-Authentication-failure	Luotetun laitteen tunnistautuminen on epäonnistunut TLS-kättelyssä, eli virheellinen sertifikaatti.	DICOM PS 3.15 A.5.3 “Security Alert”
Order-record-event	Tilausvahvistus luotu, katseltu, muokattu tai poistettu. Tähän liittyvä toimija on tilauksen toimeenpanija. Tämä sisältää tilauksen, päivitykset tai muokkaukset, toimitus, vahvistus ja keskeytys.	DICOM PS 3.16 Annex D “Order Record”
Patient-care-assignment	Potilaan hoitoon liittyvän henkilöstön määritys. Sisältää kaikki hoitohenkilökuntaan luettavat henkilöt. Sisältää hoitoroolien muutokset tai valutuutukset.	IHE Extension (ITI TF-2a:3.20.7.3) “Patient Care Resource Assignment”
Patient-care-episode	Eriteltävät hoitotoimenpiteet tai ongelmat, mitä ilmeni annettavassa hoidossa. Tämä sisältää hoidon aloituksen, päivitykset tai muutokset, lopputuloksen, hoidon valmistumisen ja keskeytyksen.	IHE Extension (ITI TF-2a:3.20.7.3) “Patient Care Episode”
Patient-care-protocol	Potilaan liittäminen johonkin hoitoprotokollaan. Tämä sisältää hoidon aloituksen, päivitykset tai muutokset, lopputuloksen, hoidon valmistumisen ja keskeytyksen.	IHE Extension (ITI TF-2a:3.20.7.3) “Patient Care Protocol”
Patient-record-event	Potilastieto luotu, muokattu tai katseltu.	DICOM PS 3.16 Annex D “Patient Record”
PHI-export	Minkä tahansa suojatun potilastiedon vienti järjestelmästä. Tieto voi olla fyysisellä medialla tai esimerkiksi sähköpostilla. Myös mikä tahansa tuloste, paikallinen tai etätulostus, joka tulostaa suojattua potilastietoa.	DICOM PS 3.15 A.5.3 “Export”
PHI-import	Minkä tahansa suojatun potilastiedon tuonti järjestelmään. Informaatio voi olla fyysisellä medialla tai sähköisesti esimerkiksi sähköpostilla.	DICOM PS 3.15 A.5.3 “Import”
Procedure-record-event	Toimenpide suoritettu, muokattu, katseltu tai poistettu.	DICOM PS 3.16 Annex D “Procedure Record”
Query Information	Kysely on vastaanotettu, joko osana IHE-tapahtumaa tai osana muiden tuotteiden toimintoja. Esimerkiksi PIX, PDQ tai XDS-kysely. Huom. Tämän tarkoitus on tallentaa lokia kyselytapahtumasta ja sen parametreista.	DICOM PS 3.15 A.5.3 “Query”

Security Alert	Turvallisuuteen liittyvät toimenpiteet, luo, muokkaa, poista, kysely sekä näytä seuraavat: 1) Konfiguraatio- ja muut muutokset, esimerkiksi ohjelmistopäivitykset, jotka vaikuttavat suojattua tietoa käsitteleviin ohjelmistoihin tai laitteistoihin. 2) Turvallisuuteen liittyvät attribuutit ja auditoitavat tapahtumat. Sisältää sovellusten toiminnot, joita käytetään esim. potilastiedon hallintaan, kliinisiin prosesseihin, metodeihin (esimerkiksi WSDL, UDDI), ohjelmien luontiin tai ylläpitoon. 3) Turvallisuustoimialueet, esimerkiksi laitoksittain. 4) Turvallisuuskategoriat tai ryhmittelyt toiminnoille tai tiedolle, esim. potilastiedon hallinta, potilashoito, kliiniset toimenpiteet. 5) Hyväksyttävät pääsyoikeudet, jotka liittyvät toimintoihin tai tietoon, esimerkiksi luonti, luku, päivitys, poisto. Sisältää myös tiettyjen toimintojen suorittamisen tai manipuloimisen. 6) Käyttäjien turvallisuusroolit, sisältää useita toimien mukaan jaettuja kategorioita, kuten tietohallinto, vastaanotto, hoitajat, lääkärit, spesialistit. 7) Käyttäjätilit, sisältää salasanamääritykset ja muut tunnistautumistiedot. Sisältää myös käyttäjätilien roolimuutokset ja käyttöoikeudet. 8) Luvattomat käyttäjien yritykset käyttää tietohallinnollisia toimintoja. 9) Auditoinnin käyttö ja käytön poisto. 10) Käyttäjän tunnistautumisen poisto. 11) Hätäpääsytoiminto (lasinrikkomismoodi) Kaikki tietohallinnolliset toimenpiteet tulee aina auditoida.	DICOM PS 3.15 A.5.3 "Security Alert"
User Authentication	Tämä viesti kuvaa käyttäjän sisään- ja uloskirjautumisen, onnistui se tai ei.	DICOM PS 3.15 A.5.3 "User Authentication". For log off based on inactivity, specify UserIsRequestor=false in the User element to indicate that this was not user initiated.
Study-Object-Event	Tutkimus on luotu, muokattu, katseltu tai poistettu. Tällä määritellään sekä uusien instanssien lisäyksen olemassaoleviin tutkimuksiin, kuin myös kokonaan uuden tutkimuksen lisäyksen.	DICOM PS 3.15 A.5.3 "DICOM Instances Accessed"
Study-used	Jostain tietystä tutkimuksesta on luotu, muokattu tai käytetty SOP-instanssia. Yksi tapahtuma kattaa kaikki käytetyt instanssit.	DICOM PS 3.15 A.5.3 "DICOM Instances Accessed"

IHE määrittelee useita vaihtoehtoisia muotoja auditointimerkinnöille (Audit Record) ja tulevaisuudessa näiden lukumäärä tulee kasvamaan. IHE-toimijan tulee käyttää yhtä tai useampaa näistä määritellyistä formaateista. Kaikki tarjolla olevat formaatit ovat määritelty XML-muodossa. [17]

Tällä hetkellä auditointimerkintälistassa ovat mahdollisia:

1. IHE Audit Trail -jäljitystietomuoto, joka perustuu IETF-, HL7- ja DICOM-organisaatioiden kehittämiin ja julkaisemiin standardeihin.
2. IHE Provisional Audit Record -jäljitystietomuoto, joka on alun perin määritelty osaksi IHE Radiology Technical Framework -viitekehystä. Tätä ei nykyisin enää käytetä. Uusien sovellusten tulisi käyttää uudempaa IHE Audit Trail -muotoa. [17]

Kun luotettu laite tai sovellus luo auditointimerkinnän, sen tulee siirtää merkintä mahdollisimman pian auditointitietovarannolle. Jos tietovaranto ei ole saatavilla, laitteen tai sovelluksen tulee tallettaa tiedot paikalliseen puskuriin, kunnes auditointitietovaranto on jälleen saatavilla. Toisin sanoen, luotetuilla laitteilla ja sovelluksilla tulee pystyä tallettamaan tietoja myös paikallisesti ja niillä on oltava tallennustilaa paikallisten tietojen tallentamista varten. Tietoja ei tarvitse kuitenkaan pystyä tallettamaan paikallisesti lopullisesti, vaan ne voidaan poistaa siinä vaiheessa, kun ne on saatu siirrettyä myös auditointitietovarannolle. [17]

Syslog-viestien luonti ja välitys suoritetaan RFC 5424:n mukaisesti. ATNA-toimijoiden tulee ottaa seuraavat asiat huomioon:

- XML-muodossa oleva auditointiviesti voi sisältää Unicode-merkkejä, jotka on koodattu UTF-8:lla. Tämän etuna on se, että syslog-protokollan hallintaan käytettäviä merkkejä ei käytetä muuhun tarkoitukseen. Näin ollen auditointitietovarantojen on pystyttävä käsittelemään UTF-8 merkistökoodausta.
- PRI-parametri (priority) tulee asettaa arvoon 10 (turvallisuus/tunnistautumisviesti). Useimmat viestit tulisi sisältää vakavuusarvo (severity) 5 (normaali, mutta merkittävä). Sovellukset voivat valita myös arvon 4 (varoitus), jos se sopii auditointiviestin informaatioon. Tämä tarkoittaa sitä, että suurimmalle osalle auditointiviestejä PRI-parametri sisältää arvon 85. Edellä mainittu severity-arvo lasketaan priority-arvosta vähentämällä priority-arvosta facility-arvo joka on kerrottuna luvulla kahdeksan. Auditointitietovarantojen pitää pystyä vastaanottamaan ja käsittelemään mitä tahansa PRI-parametrin arvoja.
- Syslog-viestin otsikossa (HEADER) oleva MSGID-arvo tulee asettaa arvoon IHE+RFC-3881.
- ATNA-auditointiviesteissä STRUCTURED-DATA-arvoa ei käytetä, koska MSG-parametri sisältää itsessään jo rakenteista tietoa.
- MSG-parametrin tulee olla XML-muodossa (määritelty RFC 3881:ssä). [17]

3.6 Potilastietojen luovutus

Basic Patient Privacy Consents -profiilia (BPPC) käytetään potilaan antamien suostumusten tallentamiseen potilastietojärjestelmään. Suostumukset liittyvät potilaan omiin potilastietoihin ja niiden luovuttamistarkoituksiin. Profiili täydentää XDS-profiilia tarjoten mekanismin hallita suostumusten tallennusta ja käyttöä XDS-hoitoyhteisön sisällä sekä niiden yhdentämiseen pääsynvalvontamekanismeihin. Jos BPPC-profiilia ei ole käytössä XDS-hoitoyhteisössä, tulee silloin käyttää yksittäisen dokumentin julkisuus- ja käyttösääntöjä. [12]

Terveydenhuoltopalveluita tarjoavat organisaatiot (esimerkiksi terveyskeskukset ja sairaalat) käyttävät monentyyppistä tietoa hoidossa. Näiden tietotyyppien luottamuksellisuus on määritelty eri tasoille. Esimerkiksi jotkut potilaan tiedot voivat olla kaikille näkyvillä, jotkut vain sairaalan henkilökunnalle ja jotkut tiedot ainoastaan hoitaville lääkäreille. Tällaisia tietotyyppejä ovat esimerkiksi potilaan demografiset tiedot, läheisten yhteystiedot, vakuutustiedot, ravintoon liittyvät tiedot, yleiset kliiniset tiedot sekä yksityiset kliiniset tiedot. Nämä kaikki tiedot voidaan julkaista erillisinä dokumentteina, joille kaikille annetaan erilaiset luottamuksellisuustunnukset (confidentialityCode). Tämä mekanismi ei ole pelkästään BPPC-profiilin ominaisuus, mutta sitä hyödynnetään yksityisyys- ja turvallisuussäädöksissä. [12]

Edellä mainittuja tietotyyppejä hyödyntävät terveydenhuoltoa tarjoavissa laitoksissa useat henkilöt erilaisissa tehtävissä. Se, mitä tietoja kukin henkilö saa nähtäväkseen, on

juuri sitä, mihin BPPC-profiilia käytetään XDS-hoitoyhteisössä. XDS-hoitoyhteisö voi luoda erilaisten toimintakoodien listan, joka määrittelee potilaan yksityisyystoimialueen (Patient Privacy Domain). Tätä säädellään potilaan yksityisyystunnisteilla (Patient Privacy Policy Identifier), joka taas määrittelee dokumenttien jakamista. Jokainen yksityisyystunniste määrittelee yksilöllisesti yksityisyyssäännöksen (Privacy Policy), mikä tulee eritellä lakitekstinä. Tällä tarkoitetaan sitä, että ketkä saavat tietoja käyttää, miten tietoja saa käyttää, millä rooleilla tietoja pääsee käyttämään, minkälaisissa olosuhteissa ja niin edelleen. [12]

3.6.1 BPPC-profiilin käyttötapauksia

Tämän kohdan alla käydään läpi tyypillisimpiä BPPC-profiilin käytännön käyttötapauksia. Käyttötapaukset ovat peräisin alun perin USA:sta, kuten IHE ja sen julkaisemat profiilit. Tämän vuoksi käyttötapauksissa käytetyt termit ja perusteet pohjautuvat muun muassa USA:n terveydenhoitoon liittyvään sanastoon ja lainsäädäntöön.

Lopuksi tässä kohdassa käydään säännöstöjen yhteenvedon lisäksi läpi Suomessa käyttöönotettavaa valtakunnallisen potilastiedon arkistoa. Tästä esitellään tärkeimpiä ominaisuuksia ja palvelun sekä sen käyttöönoton tämänhetkistä tilannetta.

Epäsuora ja suora suostumus

BPPC-profiili tukee sekä epäsuoraa (Implied Consent) että suoraa (Explicit Consent) suostumusta potilastietojen jakamiseen. Epäsuora suostumus tarkoittaa lähinnä sitä, että sellainen tilanne on normaali, missä dokumentin käyttäjä ei löytäisi mitään merkintää siitä, että potilas on hyväksynyt omien tietojensa jakamisen. Tässä tapauksessa hyväksyntää ei järjestelmässä olisi myöskään vaadittu. BPPC-profiiliin on toteutettu molemmat suostumustavat siksi, jotta profiili olisi käytettävissä myös sellaisissa maissa, missä ei vaadita suoraa suostumusta. [12] Esimerkiksi USA:ssa vaaditaan potilaalta kirjallinen suostumus, ennen kuin hänen potilastietojaan voidaan jakaa [34].

Opt-In

Opt-In tarkoittaa sitä, että potilaan on ensiksi hyväksyttävä omien tietojensa jakaminen ennen kuin mitään dokumentteja on varsinaisesti jaettuna järjestelmässä. Kun lupa on annettu, XDS-hoitoyhteisön järjestelmänvalvojat määrittävät seuraavaksi tiedoille säännöt siitä, mitä jaetaan, milloin jaetaan, missä sitä voidaan käyttää, ja niin edelleen.

Näille säännöille tulee olla myös sellainen rajoittava XDS-hoitoyhteisön sääntö (XDS Affinity Domain Policy), jolla kielletään kaikkien tietojen jako. Kielto on voimassa siihen asti, kun potilas on suoraan ilmoittanut hyväksyntänsä minkään itseään koskevien tietojen jakamiseen. [12]

Opt-Out

Tämä termi tarkoittaa päinvastaista toimintaa, kuin Opt-In eli kun potilas hakeutuu hoitoon, eikä halua omia tietojaan jaettavaksi mihinkään hoitolaitoksen ulkopuolelle. Tässä

tapauksessa kaikkien potilaan tietojen käyttö kielletään, eli potilaan mahdollisia edellisiäkään tietoja ei tule enää jakaa, eikä myöskään uusien hoitotoimenpiteiden pohjalta tallennettuja tietoja. Tämän toiminnon vaatima toiminnallisuus tulee olla myös otettuna huomioon XDS-hoitoyhteisön järjestelmissä. [12]

Wet Signature

Wet Signature, eli niin sanotulle oikealle allekirjoitukselle on myös BPPC-profiilissa tuki. Allekirjoituksella suoritettu suostumus tallennetaan käyttämällä XDS-SD -profiilia (XDS Scanned Document Profile). Tässä tapauksessa myös XDS-SD -profiilille tulee olla tuki järjestelmässä. [12]

Advanced Patient Privacy Consents

Advanced Patient Privacy Consents tarkoittaa sitä, jos normaalit hyväksyntäsäännöt eivät riitä, vaan XDS-hoitoyhteisö tarvitsee tuen laajemmille potilastietosuostumuksille. Näihin tapauksiin BPPC-profiili antaa tarvittavan tuen implementaatioille, jotka nämä säännökset toteuttaisivat, mutta ei ota kantaa siihen, miten ne tulisi tehdä. [12]

Yksi esimerkki tällaisten tarkempien hyväksyntöjen käytöstä on henkilökohtaisesti eriteltävät hyväksynnät potilastietojen jakamiselle. Tässä tapauksessa määritellään yksittäisiä henkilöitä hoito-organisaatiosta, jotka saavat ainoastaan nähdä potilaan tietoja.

Creating Patient Privacy Policies

Yhden Patient Privacy Policy -toimialueen säännöstö koostuu useista säännöstön sisällä olevista potilaan yksityisyyssäännöstöistä. Yksittäinen säännöstö kuvaa kyseessä olevan suojatun tiedon käytön vastaavalla tavalla kuin se on kuvattu potilaalle hänen hyväksyntäänsä varten. BPPC-profiili ei itsessään määrittele sen tarkemmin näiden säännöstöjen sisältöä tai niiden kehittämistä. Profiili olettaa, että yleinen Patient Privacy Policy -toimialue koostuu sen sisällä olevista tarkemmista säännöstöistä, joista jokaista voi käyttää yksitellen tai niitä voi käyttää myös yhdistelminä tietyntyyppisiä dokumentteja varten. [12]

Yksi säännöstö määrittelee sen, kenellä on tietoihin pääsy ja millaista tämä tieto on. Näiden säännöstöjen julkaisemisen toimintatapaa ei ole määritelty profiilissa sen tarkemmin. Säännöstöt on pystyttävä toteuttamaan sellaisilla teknologioilla, että kaikilla järjestelmään kuuluvilla laitteilla on pääsy toimialueeseen. Jokainen säännöstö saa oman yksilöllisen tunnisteensa (OID). Tätä tunnistetta käytetään silloin, kun etsitään potilaan hyväksyntöjä tietyille säännöstöille. [12]

XDS-hoitoyhteisössä käytetyt yksityisyyssäännöstöt poikkeavat yleensä XDM- tai XDR-profiileihin tarvittavista säännöstöistä, koska niissä dokumentteja siirretään poikkeavalla tavalla. XDM- ja XDR-profiileissa käytetään erillistä siirtomediaa, joten säännöstöt tulee myös määritellä niiden mukaan.

Yhteenveto säännöstöjen luonnista ja julkaisusta

IT Infrastructure Technical Framework:ssa on tiivistetty säännöstöjen luonnista seuraava lista:

1. Patient Privacy Policy Domain -toimialue laatii yleiset yksityisyyssäännöstöt.
2. Patient Privacy Policy Domain -toimialue sisältää pienen kokoelman yksityisyyssäännöstöjä, jotka vastaavat pitkälti tämänhetkisiä käytössä olevia hyväksyntäkaavakkeita.
3. Jokaiselle säännöstölle annetaan yksilöllinen tunniste (OID), joka on nimeltään Patient Privacy Policy Identifier.
4. Patient Privacy Policy Domain -toimialueen säännöstö ja kaikki sen sisältämät säännöstöt tulee julkaista jollakin tavalla. Tämän tulee olla vähintään paikallisen lainsäädännön mukaisesti toteutettu.
5. Kun potilas hyväksyy säännöstön, Patient Privacy Policy Acknowledgement Document -dokumentti julkaistaan sen Patient Privacy Policy -tunnisteen kanssa, jonka potilas hyväksyi. [12]

Suomen valtakunnallinen potilastiedon arkisto

Suomessa ollaan parhaillaan ottamassa käyttöön maanlaajuisesti valtakunnallista potilastiedon arkistoa, joka sisältää potilastietoja eri terveydenhuollon yksiköistä. Potilastiedon arkistoon liittyminen toteutetaan vaiheittain vuosien 2013-2015 aikana. Näitä arkistoon tallennettuja potilastietoja hoidon kohteena olevien potilaiden on mahdollista tarkastella itsenäisesti. Tälle arkistolle on annettu nimi Kanta-arkisto ja siihen liittyvästä Omakanta-palvelusta voi suorittaa omien sähköisten potilas- ja reseptitietojen tarkastelua. Tiedonhallintapalvelun rekisterinpitäjänä toimii Kansaneläkelaitos (Kela). Tavoitteena Kanta-arkiston käyttöönotossa on, että tulevaisuudessa kaikki Suomen sähköiset potilas- ja reseptitiedot olisi tallennettu järjestelmään ja myös potilaiden käytettävissä. Näiden lisäksi arkistoon tallennetaan potilaan antamat suostumukset tietojen luovutukseen, mahdolliset luovutuskiellot, näiden suostumusten ja kieltojen peruutukset, hoitotahto, potilaan kanta elinluovutukseen ja tieto siitä, että potilasta on informoitu valtakunnallisista tietojärjestelmäpalveluista [35].

Potilas voi aina rajoittaa antamiensa suostumusten laajuutta tekemällä tietojen luovutusta rajaavia kieltoja. Kieltoja on mahdollista tehdä esimerkiksi jotakin tiettyä hoitokäyntiä varten tai johonkin tiettyyn toimintayksikköön liittyviä tietoja varten. Kaikki potilastiedon arkistoa varten annettavat kiellot ja suostumukset on annettava kirjallisina. Virallisia lomakkeita saa terveydenhuoltopalveluita tarjoavista toimintayksiköistä ja ne on aina allekirjoitettava. Suostumukset ja kiellot voi tehdä toimintayksikössä paikan päällä tai suoraan internetissä Omakanta-verkkopalvelun kautta.

Tästä syystä potilastiedon arkisto tulee toimimaan eräänlaisena päärekisterinä (master), koska kansallisen arkiston on sisällettävä aina ajantasaiset tiedot. Aikaisemmin tehtyjä kieltoja tai suostumuksia on mahdollista poistaa tai muokata jälkikäteen milloin vain. Koska tällä hetkellä potilastiedon arkisto on käytössä vain osittain, on suostumus-

ten ja kieltojen antaminen mahdollista vain niissä terveydenhuollon toimintayksiköissä, missä potilastiedon arkisto on otettu jo käyttöön. [35]

3.6.2 BPPC-toimijat ja -tapahtuma

Kuten kuvaan 3.8 on havainnollistettu, BPPC-profiili sisältää kaksi toimijaa, jotka ovat sisällöntuottaja (Content Creator) ja sisällönkäyttäjä (Content Consumer). Kuva perustuu alkuperäiseen lähteeseen [12]. Sananmukaisesti sisällöntuottaja tuottaa sisällön ja sisällönkäyttäjä käyttää sitä. Sisällön jakaminen tai siirtäminen määritellään niitä koskevissa IHE-profiileissa.

Dokumenttilähde tai kannettavan median luoja (Portable Media Creator, esimerkiksi muistitikku, CD tms.) voi toimia sisällöntuottaja-toimijana. Dokumentin käyttäjä, dokumentin vastaanottaja (Dokument Recipient) tai kannettavan median sisällyttäjä (Portable Media Importer) voivat toimia sisällönkäyttäjä-toimijana.

Kuva 3.8. *BPPC-profiilin toimijat [12].*

BPPC-profiili sisältää ainoastaan yhden tapahtuman, joka on nimeltään Share Content. Tapahtumaa käyttää sisällöntuottaja, joka jakaa sisältöä sisällönkäyttäjälle, jos potilas on antanut suostumuksensa jaettavana olevaan sisältöön.

3.6.3 Turvallisuusnäkökohtia

XDS-hoitoyhteisöön tallennettuja suostumuksia koskettavat myös yksityisyyssäännöstöt. Patient Privacy Policy Acknowledgement -dokumentti itsessään voi sisältää tietoa potilaan terveydentilasta, esimerkiksi jos hän on kuolemansairas ja haluaa olla kertomatta sitä asiaa perheenjäsenilleen, mutta muut hoitotiedot voi kertoa. Näin ollen kyseistä hyväksyntädokumenttia ei siis voisi näyttää perheenjäsenille, koska diagnoosi voisi selvitä jo näkemättä varsinaista diagnoosidokumenttia.

Potilastietoihin liittyvien yksityisyyssäännöstöjen toteuttaminen terveydenhoitolaitosten käyttöön sisältää erilaisia riskejä ja vaatii erilaisen lähestymistavan kuin vastaavien säännöstöjen toteutus muun alan laitoksiin. Tämä johtuu siitä, että jos pääsy kriittisiin potilastietoihin jää saamatta, voi se aiheuttaa vakavaa loukkaantumista tai pahimmillaan kuoleman potilaalle. Nämä riskit on tiedostettava ja tasapainoiltava sen ja mahdollisten seuraamusten välillä, jos yksityisiä tietoja jostain syystä pääseekin vääriin käsiin virheellisten säännöstöjen takia. Tämän takia XDS-hoitoyhteisön tulisi aina ottaa

potilaiden hyväksynnät kirjallisena, jotta edellä mainittuja tilanteita pystyttäisiin välttämään.

Yksi turvallisuustekijä on kattava auditointi ja seuranta kaikesta potilastietoon liittyvistä tapahtumista. Hoitohenkilökunnan oletetaan käyttävän omia valtuuksiaan oikein, eikä suorittaa aiheettomia potilastietojen tarkistuksia tai muokkauksia. Järjestelmien käyttöä myös seurataan jatkuvasti, ettei väärinkäytöksiä tapahtuisi. Tämän strategian vuoksi tekninen komitea (ITI Technical Committee) on luonut ATNA-profiilin, joka on myös pakollisena vaatimuksena XDS-profiilin käyttämiselle.

XDS-hoitoyhteisön sisällä on päätettävä myös sellainen riski, että miten jaetaan kaikkein arkaluontoisimmat informaatiot (esimerkiksi mielenterveyteen liittyvät asiat). Yksi strategia tähän olisi, että tällaista informaatiota ei jaettaisi toimialueen sisällä, vaan jakaminen tapahtuisi ainoastaan XDR- tai XDM-profiileja käyttämällä.

3.7 Skannattujen dokumenttien jako

Sairaaloiden ja terveyskeskuksien potilastietoihin sisältyy paljon sellaista materiaalia, joka on tallennettu perinteiselle paperille, filmille sekä sähköiseen muotoon ja skannereiden tallentamiin tallennusmuotoihin. Näitä ei ole suunniteltu alun perin sairaanhoidon dokumentoinnin tarpeisiin, eikä niissä ole mekanismeja dokumentteihin liittyvien metatietojen tallettamiseen. On tärkeää saada liitettyä metatiedot alkuperäisiin hoitodokumentteihin, jotta voidaan säilyttää potilastietojen eheys, kuten se on alkuperäisessäkin lähteessä kirjoitettu. [12]

Profiilin sisältö on tarkoitettu käytettäväksi XDS-, XDR- ja XDM-profiileissa. Profiilin vaatimat toimenpiteet sisällöntuottajalle ja -käyttäjälle toteutetaan ohjelmistolla, joka luo lopullisen potilastietodokumentin ja/tai käyttää profiilin tarjoamia dokumentteja, sen sijaan että tämän suorittaisi valmiiksi jokin tietty skannaustekniikka. [12]

XDS-SD -profiili (Cross-Enterprise Document Sharing of Scanned Documents) määrittelee sen, miten metatiedot yhdistetään. Metatiedot sisältyvät jäsennellysti HL7 CDA R2 -otsakkeeseen tai ne ovat sellaisessa PDF- tai plaintext-muotoisessa dokumentissa, joka sisältää kliiniset hoitotiedot. Tämän lisäksi profiili määrittelee CDA R2 -otsakkeen osat, jotka vähintään on oltava dokumenttien kirjausta varten. Tällaisia osia ovat potilaan identiteetti, potilaan demografiset tiedot, skannerin identiteetti, skannausteknologia, skannausaika sekä paras mahdollinen tiedon julkaisuinformaatio. Tietyt osat CDA R2-otsakkeesta, sekä lisäinformaatio dokumentin rekisteröinnistä käytetään täyttämään XDS Document Entryn metatietoja. [12]

3.7.1 Sisällön käyttötapauksia

Tässä kohdassa esitellään tyypillisimpiä XDS-SD -profiilin toimintaan liittyviä käyttötapauksia. Nämä ovat käytännössä erilaisilla tavoilla skannattavia dokumentteja.

Näiden käyttötapausten osuus potilastietojärjestelmissä pienenee koko ajan, koska jatkuvasti vähennetään paperilla olevien dokumenttien käyttöä. Näin ollen vähitellen

paperilta skannattavat dokumentit poistuvat, mutta niille on silti oltava toiminnallisuus järjestelmissä kaiken varalta.

Muistiinpanot potilastietojen lomakepohjissa

Lomakepohjiin kirjoitetut muistiinpanot (Text Chart Notes) ovat yleensä käsinkirjoitettuja potilastietoja tai taulukkomuistiinpanoja. Nämä ovat yleensä monisivuisia selostuksia, jotka sisältävät valmiita lomakepohjia, joissa on käsinkirjoitetut tulokset, tulostettuja dokumentteja ja nämä kaikki on tallennettu erilaisilla tiedostomuodoilla.

Asianmukainen tiedostomuoto on PDF tai plaintext, jos tekstin rakenne on ainoa, mikä tarvitsee välittää eteenpäin. PDF on tiedostomuotona suositelluin, koska sillä saadaan tallennettua alkuperäinen teksti mahdollisimman tarkkaan kaikkine mahdollisine muistiinpanoineen.

Kaaviot, taulukot ja/tai kuvaajat

Esimerkkejä tällaisista ovat kasvukäyrät ja sikiön seurantakaaviot. Kuvaajat tulisi ensisijaisesti muodostaa PDF-tiedostoiksi ja kuvatiedostoja tulisi välttää. Esimerkiksi JPEG-tiedostojen häviöllinen pakkaustapa huonontaisi skannaustulosta alkuperäiseen dokumenttiin verrattuna. [12]

OCR-tekniikalla skannatut dokumentit

OCR-tekniikalla (Object Character Recognition) skannaus ei pysty lukemaan kaikkea mahdollista tietoa potilastietodokumenteista, jotka voivat sisältää tekstin lisäksi myös muuta tietoa. Siksi tällaiset dokumentit tulisi ensin muuntaa PDF-tiedostoiksi, joihin voi sitten hyödyntää OCR:ää, normaalia tekstiskannausta sekä skannattujen kuvien erittelyä. [12]

3.7.2 XDS-SD -toimijat ja -tapahtumat

XDS-SD -profiilissa on kaksi toimijaa, sisällöntuottaja ja sisällönkäyttäjä. Toimijat ovat siis samat, kuin BPPC-profiilissa, ja niiden käyttötarkoitus on myös yhtenevä, kuten kuvassa 3.8 on esitelty. Sisällöntuottaja antaa sisällön ja sisällönkäyttäjä hakee sitä.

Dokumenttilähde tai kannettavan median luoja voi toimia profiilissa sisällöntuottajana. Dokumentin käyttäjä, dokumentin vastaanottaja tai kannettavan median sisällyttäjä voi toimia sisällönkäyttäjänä.

Skannattujen dokumenttien sisällön prosessikuvaus

XDS-SD -profiili olettaa XDS-SD -dokumentin luonnissa seuraavia asioita:

1. Paperilla oleva dokumentti skannataan ja siitä muodostetaan PDF-dokumentti. Vaihtoehtoisesti sähköinen dokumentti muunnetaan tarvittaessa PDF- tai plaintext-tiedostomuotoon. (ITI TF-3: 5.2.1&5.2.1.1)

2. Ohjelmisto tuottaa käyttäjän syötteen avulla (esimerkiksi syöttää dokumentin otsikon, luottamuksellisuuskoodin, alkuperäisen julkaisijan), muodostaa CDA R2 -otsakkeen ja liittää tuotettuun PDF- tai plaintext-tiedostoon. (ITI TF-3: 5.2.3)
3. XDS-metatiedot tuotetaan CDA -otsakkeessa olevista tiedoista ja saatavilla olevista lisäinformaatioista. (ITI TF-3: 5.2.2)
4. Valmis XDS-SD -dokumentti ja siihen liittyvät metatiedot lähetetään tapahtumilla Provide or Register Document Set (ITI-15 tai ITI-41) XDS/XDR-profiileissa tai Distribute Document Set on Media Transaction (ITI-32) XDM-profiilissa. [12]

3.8 Potilastunnisteiden ristiviittaukset

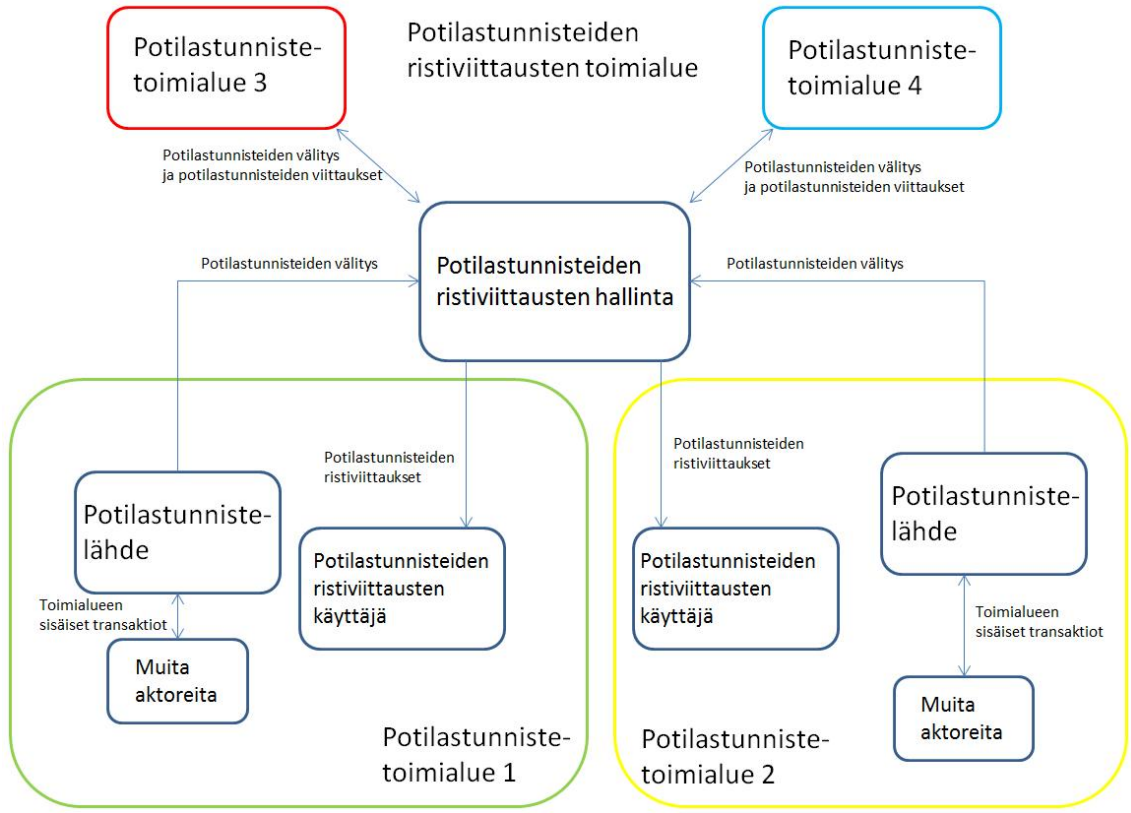
Patient Identifier Cross-referencing -profiili (PIX) on tarkoitettu kaikenkokoisille terveydenhoitopalveluita tarjoaville laitoksille (esimerkiksi sairaala, terveyskeskus, klinikka). PIX-profiili tukee potilastunnisteiden ristiviittauksia useista potilastunnistetoimialueista.

Tämä on mahdollistettu kahdella vuorovaikutuksella. Potilaan yksilöivän informaatio siirretään lähteeltä potilastunnisteiden ristiviittauksien hallinnalle (Patient Identifier Cross-reference Manager) ja on mahdollista lukea ristiin viitattujen tunnisteiden listoja joko kysely/vastaus-periaatteella tai päivitysilmoituksilla. Määrittelemällä nämä tiettyjen toimijoiden suorittamat tapahtumat, PIX-profiili ei määrittele niiden lisäksi mitään tiettyjä säännöstöjä tai ristiviittausalgoritmeja. [12]

Tämä profiili on alun perin tehty sellaisien maiden terveydenhuoltojärjestelmiä varten, joissa potilaan tunniste voi vaihdella alueittain. Suomessa tätä ei esiinny, joten Suomen rajojen sisäpuolella oleviin XDS-yhteensopiviin järjestelmiin tämän profiilin käyttö ei ole välttämätöntä. Se on kuitenkin tarpeen silloin, jos potilaisiin ei viitata suoraan henkilötunnuksilla vaan käytössä on jokin muu tunnistejärjestelmä.

3.8.1 PIX-toimijat

Kuvassa 3.9 on kuvattu PIX-profiilin toimijoiden ja tapahtumien rakenne. Kuvaan on esitetty neljä eri potilastunnistetoimialuetta havainnollistamaan tilanne, jossa toimialueita on useita. Näistä toimialueet 1 ja 2 on esitetty tarkemmin, jotta selviää mitä toimintoja niiden sisällä tässä profiilissa on. Kuva perustuu alkuperäiseen lähteeseen [12].



Kuva 3.9. *PIX-profiilin toimijat [12].*

Potilastunnistetoimialueita voi olla järjestelmässä useampiakin kuin neljä. Tässä kohdassa esitellään kuvassa olevat PIX-profiilin toimintaan liittyvät toimijat.

Potilastunnistelähde

Potilastunnistelähde (Patient Identity Source) ilmoittaa potilastunnisteiden ristiviittauksien hallinnalle (Patient Identifier Cross-reference Manager) kaikista potilastunnisteisiin liittyvistä muutoksista, esimerkiksi luonti, päivitykset tai yhdistämiset.

Potilastunnisteiden ristiviittausten hallinta

Potilastunnisteiden ristiviittausten hallinta (Patient Identifier Cross-reference Manager) toimii erillisten potilastunnistetoimialueiden välissä niiden tietoja yhdistävänä toimijana. Potilastunnistelähteet tuottavat informaatiota potilastunnisteista omilta toimialueiltaan, joita ristiviittausten hallinta hallinnoi ja päivittää kaikkien toimialueiden saataville.

Ristiviittausten hallinnan konfiguraatioon määritellään etukäteen ristiviittausten käyttäjät, jotka haluavat päivitykset uusista tai muuttuneista ristiviittauksista järjestelmässä. Ristiviittausten hallinta tekee ilmoituksen tarjolla olevista päivityksistä. Näihin ilmoituksiin käytetään PIX Update Notification -tapahtumaa (ITI-10). Potilasinformaation välitykseen käytetään HL7:n yleiskäyttöistä "Update Person Information"-viestejä. [17]

Potilastunnisteiden ristiviittausten käyttäjä

Potilastunnisteiden ristiviittausten käyttäjä (Patient Identifier Cross-reference Consumer) vastaanottaa ilmoituksia potilastunnisteiden aliasten muutoksista potilastunnisteiden ristiviittausten hallinnalta. Ristiviittausten käyttäjä -toimija käyttää näitä tietoja informaatiolinkkien päivitykseen erillisillä potilastunnistetoimialueilla.

3.8.2 PIX-tapahtumat

Tässä kohdassa käydään läpi PIX-profiilin sisältämät tapahtumat ja niiden tärkeimmät ominaisuudet. Muut tapahtumat ovat PIX-profiilille yksilöllisiä, paitsi Patient Identity Feed, joka toimii myös XDS-profiilin yhteydessä.

Patient Identity Feed

Tämän tapahtuman sisältö on käyty läpi tarkemmin XDS-profiilin yhteydessä kohdassa 3.2.4. PIX-profiilin yhteydessä tämän tapahtuman toimijana toimii potilastunnisteiden ristiviittausten hallinta, joka hallinnoi potilastunnisteiden ristiviittauksia eri potilastunnistetoimialueilla. Potilastunnisteiden ristiviittausten hallinta muokkaa ristiviittauksia sen mukaan, miten niitä potilastietolähteet eri toimialueilta hallinnalle päivittävät.

PIX Query

PIX Query (ITI-9) -tapahtuman käyttäjinä toimivat potilastunnisteiden ristiviittausten käyttäjä ja hallinta. Potilastunnisteiden ristiviittausten käyttäjä tekee tapahtumassa pyynnön ristiviittausten hallinnalle, joka sisältää ristiviittausten hallinnan tuntemia potilastunnisteita, joita vastaavia tunnisteita sen tarvitsee tietää muilta potilastunnistetoimialueilta.

Ristiviittausten hallinta käsittelee pyynnön ja suorittaa potilastunnisteiden ristiviittaukset sen hallinnoimien toimialueiden sisällä. Tämän jälkeen ristiviittausten hallinta palauttaa ristiviittausten käyttäjälle listan pyyntöä vastaavia potilastunnisteita, jos niitä on saatavilla muilla potilastietotoimialueilla. [17]

Jos potilastunnisteiden ristiviittausten hallinnan palauttama lista potilastunnisteita sisältää useita tunnisteita yhden toimialueen sisälle, potilastunnisteiden ristiviittausten käyttäjän tulee joko käyttää kaikkia toimialueelle annettuja potilastunnisteita tai hylätä kaikki toimialueelle annetut potilastunnisteet. Tämä vaatimus on määritelty siksi, että potilastunnisteiden ristiviittausten hallinnan on mahdollista käsitellä useita identiteettejä yhdelle potilaalle saman toimialueen sisällä. Tällä tarkoitetaan sitä, että ristiviittausten hallinta pystyy tarvittaessa yhdistämään oikein eri tunnisteisiin liittyvät tiedot. Jos ristiviittausten hallinta ei pysty tällaista suorittamaan, kaikki tunnisteet on mahdollista hylätä, jolla estetään ristiviittausten käyttäjää esittämästä virheellistä tietoa potilastunnisteista. [17]

PIX Update Notification

Kuten edellisen kohdan PIX Query -tapahtumassa, PIX Update Notification -tapahtuman (ITI-10) käyttäjinä ovat potilastunnisteiden ristiviittausten käyttäjä ja hallinta. Tässä tapahtumassa potilastunnisteiden ristiviittausten hallinta suorittaa ilmoitukset potilastunnisteiden ristiviittausten muutoksesta ristiviittausten käyttäjille, jotka ovat ilmoittaneet mielenkiinnon tällaisten tietojen muutoksista tehtäviin ilmoituksiin. Ilmoituksia haluavat käyttäjät asetetaan ristiviittausten hallinnan konfiguraatioon. PIX Update Notification -tapahtuma käyttää ilmoituksien tekemiseen HL7:n Update Person Information -viestejä. [17]

Tämä tapahtuma on toiminnaltaan yhtenevä PIX Query -tapahtuman kanssa myös tilanteessa, jossa ristiviittausten hallinnan toimittamassa listassa on useampi potilastunniste yhden toimialueen sisältä. Kuten edellisessä kohdassa kerrottiin, tässä tilanteessa potilastunnisteiden ristiviittausten hallinnan tulee joko käyttää kaikki tarjotut potilastunnisteet annetulta toimialueelta tai hylätä ne kaikki.

Patient Identity Management

Patient Identity Management -tapahtuman (ITI-30) käyttäjinä toimivat potilaan väestötilastojen käyttäjä (Patient Demographics Consumer) sekä potilaan väestötilastojen hoitaja (Patient Demographics Supplier). Tämän tapahtuman tarkoituksena on välittää potilaan demografisia tietoja potilastietotoimialueen sisällä. Potilaan demografisilla tiedoilla tarkoitetaan tässä yhteydessä potilaan yksilöiviä tietoja sekä identiteettiä. Tämän lisäksi tietoihin sisällytetään tietoja potilaaseen liittyvistä henkilöistä, kuten esimerkiksi omaishoitaja, omalääkäri ja lähisukulaiset. [15]

Tapahtuma sisältää toiminnallisuuden potilaiden luontiin, päivitykseen, yhdistämiseen, liittämiseen ja erottamiseen toisistaan. Potilastietojen tyypille on tapahtumassa määritelty tiettyjä luokkia: potilaan oikea nimi, VIP (Very Important Person, jos järjestelmään on määritelty tällainen status tärkeitä henkilöitä varten) tai tuntematon potilas. Tätä tapahtumaa voidaan käyttää myös ensiavussa sekä vuodepotilaille (potilas, joka viettää sairaalassa yön) että poliklinikkapotilaille (potilas, jota hoidetaan vastaanotolla) ja ambulanssihoidossa. [15]

3.9 Synkronoidut potilastiedot sovelluksissa

Patient Synchronized Applications Profile (PSA) -profiili mahdollista yhden potilaan valinnan käytettäessä useampia terveydenhuollon sovelluksia yksittäisellä työasemalla. Tämä tarkoittaa sitä, että kun yhdessä sovelluksessa valitsee jonkin tietyn potilaan tiedot tarkasteltavaksi, aiheuttaa se myös muiden sovellusten siirtymisen näyttämään saman potilaan tietoja. [12] Suomessa tätä vastaavaa toiminnallisuutta kutsutaan myös nimellä minimikontekstinhallinta [36].

PSA-profiili käyttää HL7 CCOW -standardia, erityisesti Patient Subject Context Management -ominaisuutta siitä. CCOW (Clinical Context Object Workgroup) on HL7-organisaation määrittelemä standardi, joka on suunniteltu vähentämään kirjautumisen

määrää eri järjestelmiin sekä minimoimaan turhaa monimutkaisuutta eri järjestelmien yhtäaikaiselle toiminnalle. [37]

CCOW-standardi käyttää hyväkseen Single Sign On -metodia, mikä mahdollistaa käyttäjän pääsyn eri järjestelmiin yhdellä kirjautumisella. CCOW mahdollistaa tarkasteltavan potilaan asiayhteyden muutoksen eli eri järjestelmien käyttämisen sekä vaihtamisen samanaikaisesti. CCOW-standardi toimii sekä asiakas-palvelin- että verkkopohjaisissa sovelluksissa. [38]

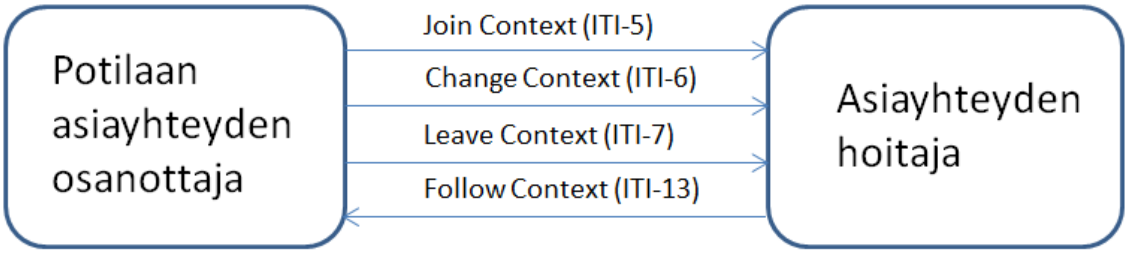
PSA-profiili keskittyy jakamaan vain CCOW:n Patient subject -parametria. PSA tarkentaa CCOW:n patient subject -määritelmää keskittymällä potilastunnisteeseen, jotta saadaan varmistettua sen oikeellisuus PSA-profiilia tukevissa eri sovelluksissa. [12]

3.9.1 PSA-toimijat

Pääasiallisesti PSA-profiilin toimijoina ovat potilaan asiayhteyden osanottaja (Patient Context Participant) ja asiayhteyden hoitaja (Context Manager). Potilaan asiayhteyden osanottajan tarkoitus on tukea kaikkia profiilin tapahtumia sekä vastata kaikkiin potilaan asiayhteyteen liittyviin muutoksiin. Tässä asiayhteydellä (context) tarkoitetaan muun muassa sitä, mitä järjestelmiä avataan, kun potilaan tiedot otetaan tarkasteltavaksi. Valittaviin järjestelmiin vaikuttaa esimerkiksi se, mitä kyseisestä potilaasta on tutkittu ja missä järjestelmissä hänestä on tietoja.

Asiayhteyden hoitajan ominaisuuksiin voi kuulua muutakin, kuin CCOW asiayhteyden hoitajan tehtävät (CCOW context manager). Se voi sisältää myös muita komponentteja, kuten esimerkiksi asiayhteyden hallintarekisterin (context management registry) ja potilastunnisteiden yhdistäjä (patient mapping agent). Potilastunnisteiden yhdistäjä on CCOW Context Agent -tyyppi, joka mahdollistaa uusien tunnisteiden lisäämisen automaattisesti jo olemassa olevalle objektille. Yhdistäjät eivät näy sovelluksille erillisinä toimijoina järjestelmässä, vaan ne toimivat ainoastaan asiayhteyden hoitajien kanssa. [39]

Kuvassa 3.10 on havainnollistettu profiilin toimijat ja niiden välissä suoritettavat tapahtumat. Kuva perustuu alkuperäiseen lähteeseen [12].



Kuva 3.10. *PSA-profiilin toimijat ja tapahtumat [12].*

3.9.2 PSA-tapahtumat

PSA-profiilin tapahtumia on neljä, Join Context, Change Context, Leave Context, Follow Context. Nämä kaikki tapahtumat suoritetaan kahden PSA-profiilin toimijan välillä. Tässä kohdassa käydään tapahtumat läpi ja esitellään niistä tärkeimmät ominaisuudet.

Join Context

Join Context -tapahtumaa (ITI-5) käyttävät potilaan asiayhteyden osanottaja (Patient Context Participant), käyttäjän asiayhteyden osanottaja (User Context Participant) ja asiakassovelluksen tunnistautumisagentti Client Authentication Agent. Tapahtumaa käyttämällä toimijat voivat etsiä ja liittyä sisällönhallintaistuntoon (context management session) sillä työasemalla, mistä käyttäjä on potilastietoja hakemassa. [17]

Asiayhteyden osanottaja paikallistaa asiayhteyden hoitajan toteutuksen ja kun viite tähän on vastaanotettu, asiayhteyden osanottaja käyttää join-metodia, johon vastauksena saadaan yksilöllinen osanottotunniste (participant identifier). Tätä tunnistetta käyttämällä käyttäjän asiayhteyden osanottaja ja asiakassovelluksen tunnistautumisagentti suorittavat keskinäisen tunnistautumisen. Tunnistautuminen tapahtuu tätä yksilöllistä osanottotunnistetta ja jaettua salausavainta käyttämällä kaksivaiheisessa tunnistautumisprosessissa. Tunnistautumisen lopputuloksena molemmat osapuolet jakavat julkiset avaimet keskenään. [17]

Jos tämän tapahtuman toteutus muodostaa kahden tai useamman asiayhteyden osanottajan ryhmiä, tämä tapahtuma tulee suorittaa ainoastaan kerran, kun sovellus käynnistetään. Kaikille osanottajille tulee jakaa sama asiayhteys ja jos vähintään yksi toimijoista on käyttäjän asiayhteyden osanottaja tai asiakassovelluksen tunnistautumisagentti, tapahtuman pitää sisältää kaksivaiheinen tunnistautuminen. Ryhmien tapauksessa toimitaan siis kuten kahden toimijan välisessä yhteyden muodostuksessa. [17]

Change Context

Change Context -tapahtuman (ITI-6) tarkoitus on sallia asiayhteyden osanottaja -toimijaa tukevan sovelluksen muuttaa yhden tai useamman asiayhteyden kohteen arvoa. Samalla pakotetaan muiden asiayhteyden osanottajien synkronoituminen tähän uuteen asiayhteydessä esiintyvään arvoon. [17]

Tällä tapahtumalla on kaksi määräävää tekijää. Yksi tekijä on, että tapahtuma sisältää useita vaiheita. Näitä vaiheita ovat asiayhteyden muutokseen pakottaminen, muiden osanottajien kartoittaminen ja viimeisenä vaiheena päätös siitä, julkaistaanko asiayhteyden muutos vai ei. Toinen tekijä tapahtumassa on, että asiayhteyden vaihtaminen sisältää tietyn aiheen. Potilaan asiayhteyden muutos -toimijalle vaihtuva aihe on potilas ja asiakassovelluksen tunnistautumisagentille vaihdettava aihe on järjestelmän käyttäjä. Ne sovellukset, joissa on toteutettu ainoastaan potilaan asiayhteys, ei niiden tule odottaa käyttäjäaiheen asiayhteyden muuttumista. [17]

Leave Context

Leave Context -tapahtuman (ITI-7), joka tukee samoja toimijoita kuin edellisien lukujen tapahtumat, tarkoituksena on lopettaa osanotto sisällönhallintaistunnossa, johon toimija on ottanut osaa. Tämä tapahtuu siten, että asiayhteyden osallistuja -toimija ilmoittaa asiayhteyden hoitajalle, että osallistuja on poistumassa asiayhteydestä. [17]

Tapahtumassa käytettävät metodit on esitelty HL7 Context Management ”CCOW” -standardeissa, joista asiayhteyden osallistuja voi valita toteutuksessa käytettävän teknologian. Asiayhteyden hoitajan on tuettava molempia teknologioita, riippumatta siitä kumpaa toinen liittyvä osapuoli tulee käyttämään. [17]

Follow Context

Tätä tapahtumaa (ITI-13) suorittamalla asiayhteyden hoitaja -toimija pystyy pakottamaan muut osallistujat synkronoitumaan uusiin asiayhteydessä esiintyviin arvoihin. Follow Context -tapahtuma perustuu myös HL7:n sisällönhallinnan standardeihin, joiden määrittelemiä metodeja käyttämällä esimerkiksi potilaan asiayhteyden osanottaja seuraa potilasaihetta ja käyttäjän asiayhteyden osanottaja seuraa käyttäjäaihetta. [17]

3.10 Usean potilaan kyselyt

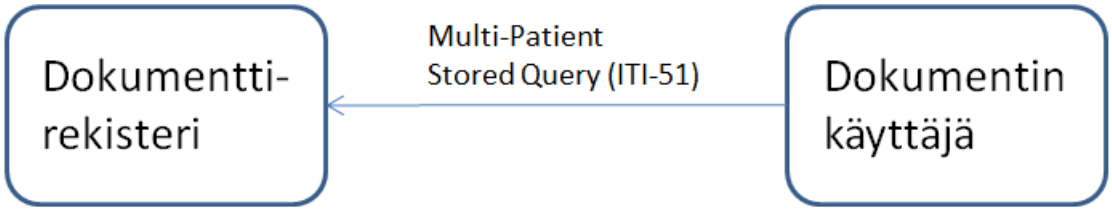
Multi-Patient Queries -profiili (MPQ) mahdollistaa kyselyiden yhteenliittymisen dokumenttirekisteriä varten. Nämä kyselyt perustuvat joihinkin tiettyihin kriteereihin alueilta, joista suoritetaan tietoanalyysia. Tällaisia analyyseja ovat esimerkiksi terveydenhuoltoa tarjoavien laitosten tai henkilöiden laaduntarkkailu, kliininen tutkimus tai kansanterveyden seurannat.

Parhaimmillaan MPQ-profiili on käytössä silloin, kun on tarve suorittaa sellaisia kyselyitä dokumenttivarannolle, missä haetaan tuloksena listausta potilaista, jotka täyttävät tietyt kriteerit. Tällä hetkellä XDS-profiili tukee ainoastaan yksittäisestä potilaasta tehtäviä hakuja (Stored Query -tapahtuma). MPQ-profiili laajentaa tätä toiminnallisuutta ja sillä voidaan suorittaa esimerkiksi hakuja dokumenttivarannolta sellaisilla kriteereillä, joista palautuu tietyn diagnoosin saaneet potilaat, esimerkiksi kaikki viime vuonna todetut influenssatapaukset.

Medbit Oy:n REST-palvelussa käytettävissä REST-kutsuissa tällaista tilannetta vastaa sellainen kutsu, missä PAT-tietoa ei ole annettu lainkaan, mutta sen sijaan annettuna on esimerkiksi jokin hakuehto parametrilla E. Hakuparametri E tarkoittaa sitä, että palvelusta haetaan tietoa suoraan varsinaisen tietosisällön perusteella. Näin saadaan haettua jokin tietty lista potilaita, jotka täyttävät hakuehdossa määritellyn kriteerin. [32]

3.10.1 MPQ-toimijat

Tässä profiilissa olevat toimijat ovat dokumenttirekisteri ja dokumentin käyttäjä, eli kyseessä ovat samat toimijat, joita muun muassa XDS-profiili käyttää.



Kuva 3.11. *MPQ-profiilin toimijat ja niiden välinen tapahtuma [12].*

Nämä ovat suoraan MPQ-profiilin kanssa vuorovaikutuksessa olevia toimijoita, välillisesti yhteydessä olevia toimijoita ei kuvassa 3.11 ole eriteltynä selvyyden vuoksi. Kuva perustuu alkuperäiseen lähteeseen [12].

3.10.2 Multi-Patient Stored Query -tapahtuma

Multi-Patient Stored Query -tapahtuma (ITI-51) on johdettu Registry Stored Query -tapahtumasta, jota käytetään muun muassa XDS-profiilin yhteydessä. Suurin ero tapahtumien välillä on suoritettavien kyselyiden määrä. [17]

Dokumentin käyttäjä suorittaa Multi-Patient Stored Query -kyselyn dokumenttirekisterille haluamillaan hakuehdoilla. Dokumenttirekisteri vastaa käyttäjälle listan dokumentteja, jotka sisältävät useita potilaita näillä hakuehdoilla. Vastaus sisältää kaikkien dokumenttien tunnisteet ja sijainnit yhdessä tai useammassa dokumenttivarastossa. [12]

3.11 Dokumenttikyselyt yli toimialuerajojen

Cross-Community Access -profiili (XCA) tarjoaa mahdollisuuden suorittaa potilastietokyselyjä muihin kuin oman yhteisön järjestelmiin. Yhteisöksi tässä määritellään terveydenhuoltopalveluita tarjoavien laitosten tai organisaatioiden ryhmittymiä, jotka ovat sopineet yhteistyöstä ja yhtenevistä säännöstöistä (policies). Näiden päämääränä on kliinisten dokumenttien jakaminen tiettyä mekanismia käyttäen. [12]

Yhteisöön kuuluvien laitosten tai organisaatioiden tarjoamien terveydenhoitodokumenttien tyypillä ei ole merkitystä, yhteisöt eritellään toisistaan yksilöllisellä tunnisteella nimeltään homeCommunityId. Jos laitos/organisaatio kuuluu jo johonkin yhteisöön, ei se estä samanaikaisia yhteyksiä muihin yhteisöihin. Tällaiset yhteisöt voivat olla esimerkiksi XDS-hoitoyhteisöitä, missä dokumenttien jakaminen on määritelty XDS-profiilin mukaan tai mitä tahansa muita tyyppejä riippumatta siitä, mikä niissä toimii sisäisenä jakotapana. [12]

XCA-profiilissa tulee ottaa tiettyjä turvallisuusnäkökohtia huomioon. Osa näistä on suosituksia ja osa vaatimuksia. Seuraavat asiat tulee olla toteutettuna kaikissa XCA-toimijoissa:

- Kaikki XCA-toimijat tulee ryhmitellä ATNA-profiilin luotetun laitteen kanssa (tai luotetun sovelluksen kanssa) sekä CT-profiilin ajankäyttäjän kanssa.

- Dokumentin metatietojen tulee sisältää SHA1-hash-arvo dokumentin sisällöstä. Sovellusten tulee pystyä vahvistamaan dokumentin SHA1-hash-arvo metatietojen SHA1-hash-arvolla, jos mahdollinen korruptoituminen on havaittu.
- Dokumentin käyttäjä -implementaatioiden tulee kyetä hallitsemaan ylikuormitustilanteita, jotka johtuvat suuresta vastauksien määrästä. Dokumentin käyttäjän tulee siinä tilanteessa pystyä lopettamaan tiedon lukeminen ja sulkea siihen liittyvä liityntäpiste (socket). Valmistelevan ja vastaavan väylän (Initiating and Responding Gateway) tulee vastata yhteyden katkaisuun lopettamalla vastausten käsittely.
- Dokumentin käyttäjän ei tule luoda sellaisia Registry Stored Query -kyselyjä, jotka eivät ole tiettyyn potilaaseen liittyviä. Tämä tarkoittaa sitä, että käyttäjän tulee käyttää hakutoimenpiteissä joko potilastunnistetta tai yksilöllistä dokumentin tunnistetta.
- Kyselyt, joista vastaus on tuntematon potilastunniste, tulee palautua joko nolla dokumenttia ilman muuta informaatiota tai XDSUnknownPatientId -parametrilla. Tämä riippuu siitä, mikä on palvelun paikallinen säännöstö. Tämä koskee potilastunnisteita, jotka ovat oikeassa tai väärässä formaatissa. Koska virheellisestä tunnisteesta ei palauteta virhekoodia, pyritään tällä vähentämään tiedonkalastelua. Tämä koskee ainoastaan kyselyihin vastaavaa liitäntää. [12]

IHE:n määrittelemä suositus sisällön eheydestä on, että dokumentit voidaan allekirjoittaa digitaalisesti käyttämällä DSG-yhdentämisprofiilia (Document Digital Signature). Tämän suosituksen noudattaminen implementaatioissa on vapaaehtoista IHE:n mukaan. [12]

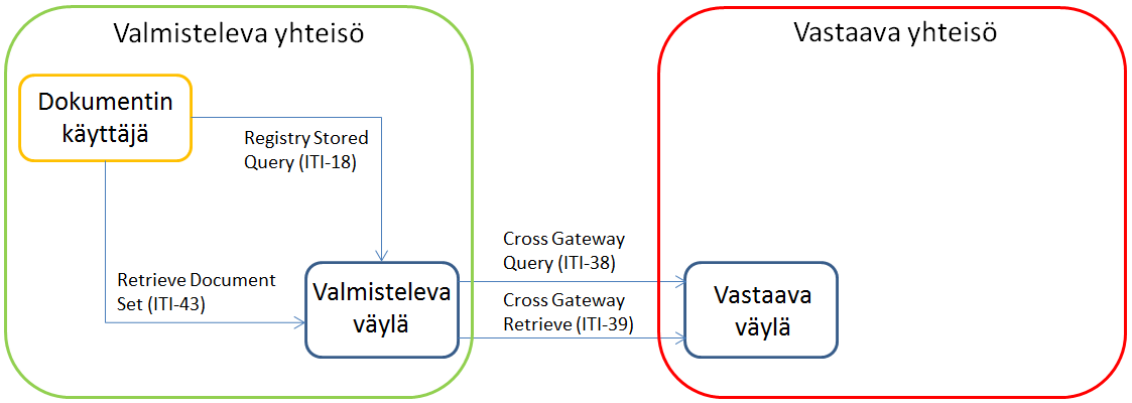
Palveluiden tuottajille, XDS-hoitoyhteisölle ja organisaatioille IHE kohdistaa alla olevassa listassa olevia suosituksia:

- Varmuuskopiointi rekisterin metatiedolle, varantojen dokumenteille ja vastaaville liitännöille on suositeltavaa.
- Kaikkien implementaatioiden suositellaan varmistamaan, että kaikki käsitelty ja vastaanotettu tieto on eheää tai jokin virheilmoitus on annettu järjestelmään.
- Verkon tietoturva suositellaan varmistamaan palvelunestohyökkäyksiä (Denial of Service) vastaan kaikissa verkkolaitteissa.
- Auditointilokia ja luvattomia toimia listaavia tahoja varten tulisi olla olemassa prosessi.
- Järjestelmien suunnittelussa tulisi ottaa huomioon myös mahdolliset verkkohyökkäykset sekä järjestelmän korruptiosta toipuminen. [12]

Järjestelmän käyttöön valittaviin säännöstöihin ei XCA-profiili ota kantaa. Kaikilla yhteisöillä voi olla omat profiilinsa, jotka ovat erilaisia muiden yhteisöjen kanssa. Tämä on otettu XCA-profiilin luonnissa huomioon, eikä sen toiminnalle aiheudu ylimääräistä työtä riippuen siitä, mitä säännöstöä missäkin profiilia tukevassa yhteisössä käytetään.

3.11.1 XCA-toimijat

Kuvassa 3.12 on XCA-profiilin kuvaus sisältäen sen toimijat ja tapahtumat. Kuvassa on piirrettynä yksi valmisteleva ja vastaava yhteisö, mutta valmisteleva yhteisö voi olla yhteydessä myös useampiin vastaaviin yhteisöihin. Kuva perustuu alkuperäiseen lähteeseen [12].



Kuva 3.12. *XCA-profiilin toimijat ja tapahtumat [12].*

Valmisteleva väylä

Valmistelevalla väylällä (Initiating Gateway) on useita tehtäviä XCA-profiilissa. Näitä tehtäviä ovat rekisterikyselyn prosessointi potilastunnistepyynnöstä (Registry Stored Query), väylien välisen kyselyjen potilastunnistevastausten prosessointi, UUID-pohjaisten kyselypyyntöjen ja niiden vastausten prosessointi sekä tarvittaessa myös paikallisten dokumenttikyselyiden käsittely. Valmisteleva väylä voi ottaa yhteyden yhteen tai useampaan yhteisöön kerrallaan. [12]

Vastaava väylä

Vastaava väylä (Responding Gateway) käsittelee saamansa potilastunniste- sekä UUID-kyselyt valmistelevalta väylältä ja kokoaa vastaukset niihin valmistelevaa väylää varten. Tämän lisäksi vastaava väylä käsittelee dokumenttien vastaanoton yhdistymällä dokumentin käyttäjän kanssa ja suorittamalla tarvittavat kyselyt dokumenttivarannoille. Jos pyyntö sisältää useita dokumentteja erillisiin dokumenttivarantoihin, tulee vastaavan väylän kyetä ottamaan yhteys näihin kaikkiin. [12]

3.11.2 XCA-tapahtumat

Tässä kohdassa käydään läpi XCA-profiilin sisältämät tapahtumat. Nämä kaksi tapahtumaa ovat Cross Gateway Query ja Cross Gateway Retrieve, jotka suoritetaan valmistelevan ja vastaavan yhteisön välillä.

Cross Gateway Query

Cross Gateway Query -tapahtuma (ITI-38) perustuu Registry Stored Query -tapahtumaan, jota muun muassa XDS-profiilissa käytetään. Tallennettujen kyselyiden

vaatimukset ovat samat, samoin paluutiedon valintamahdollisuudet. Eroja Registry Stored Query -tapahtumaan ovat:

- Tapahtuma on käytössä valmistelevan ja vastaavan väylän välillä.
- Jos yhteisöjen välisissä kyselyissä ei ole määritelty potilastunnistetta, valmisteleva väylä määrittelee homeCommunityId-parametrin.
- HomeCommunityId-parametri palautetaan kaikkien vastausten mukana.
- Vastaavien väylien tulee tukea Asynchronous Web Services Exchange -optiota tässä tapahtumassa.
- Asynchronous Web Services Exchange on valinnainen ominaisuus valmistelevalla väylällä (ITI TF-1: 18.2.2.)
- Jos tallennetut kyselyt, jotka perustuvat sellaisiin ominaisuuksiin, mitä yhteisö ei välttämättä tue (esimerkiksi kansioita), voi vastaava väylä vastata nollalla hakutuloksella. [15]

Asynchronous Web Services Exchange liittyy web-pohjaisten palveluiden viestien vaihtoon. Tässä tapauksessa lähettäjän ei tarvitse odottaa vastausta lähettämistään paketeista, vaan sille riittää vastaanottajan ilmoittama hyväksyntä (acknowledgement). Lähettäjä olettaa tässä tapauksessa, että vastaanottaja lähettää vastauksen myöhemmin ja voi lähettää tarvittaessa uusia paketteja. Kun vastaanottaja on prosessoinut pyynnön, se lähettää vastauksen uudella HTTP-yhteydellä. Asynchronous Message Exchange mahdollistaa tuen myös sellaisille verkkoympäristöille, missä esiintyy paljon yhteysviiveitä. [40]

Asynchronous Message Exchange:n yhteydessä toimintamekanismeja on muutamia, joista IHE on päätynyt tukemaan WS-osoitteistuksen ReplyTo-otsikkoelementtiä ja kahden kaksisuuntaisen SOAP-viestin tekniikkaa. Ensin mainittu tarkoittaa lähinnä sitä, että alkuperäisen kyselyn lähettäjä määrittelee ReplyTo-otsikkoelementissä vastauksen lähetettäväksi erillisellä HTTP-yhteydellä. Näin voidaan hoitaa vastausten ja kyselyiden prosessointi Web-palveluiden Infrastructure-kerroksen kautta, eikä sovellusten itsensä tarvitse tietää tästä mitään.

Tämän lisäksi toinen mahdollinen tekniikka on kahden kaksisuuntaisen SOAP-viestin käyttö. Tämä tekniikka toimii erityisesti silloin, kun kyseessä on pitkä viive viestien toimittamisessa. Pääasiallinen hyöty tämän tekniikan käytöstä on sovellustason ilmoitukset (acknowledgement) pyyntö- ja vastausviestien perillemenoista ja onnistuneesta käsittelystä. IHE nimittää tätä viivästyneeksi vastaukseksi (deferred response). HL7 V3:ssa on myös tälle tuki, joten se on tuettu myös XCPD-profiilissa (Cross-Community Patient Discovery) tällä hetkellä. Muissa IHE-profiileissa tätä ei toistaiseksi käytetä, vaan niiden yhteydessä käytössä on edellä mainittu WS-osoitteistuksen ReplyTo-otsikkoelementin hyödyntäminen. [40]

Cross Gateway Retrieve

Cross Gateway Retrieve -tapahtuma (ITI-43) perustuu jo aikaisemmin tässä työssä esiteltyyn Retrieve Document Set -tapahtumaan. Eroina näiden tapahtumien välillä ovat:

- Cross Gateway Retrieve -tapahtuma suoritetaan samojen toimijoiden välillä kuin Cross Gateway Query eli valmistelevan ja vastaavan väylän välillä.
- HomeCommunityId-parametri on tapahtumassa pakollinen.
- Vastaavan väylän on tuettava Asynchronous Web Services Exchange -optiota tätä tapahtumaa käytettäessä.
- Valmistelevalle väylälle edellä mainittu optio on valinnainen kuten Cross Gateway Query -tapahtuman tapauksessa. [15]

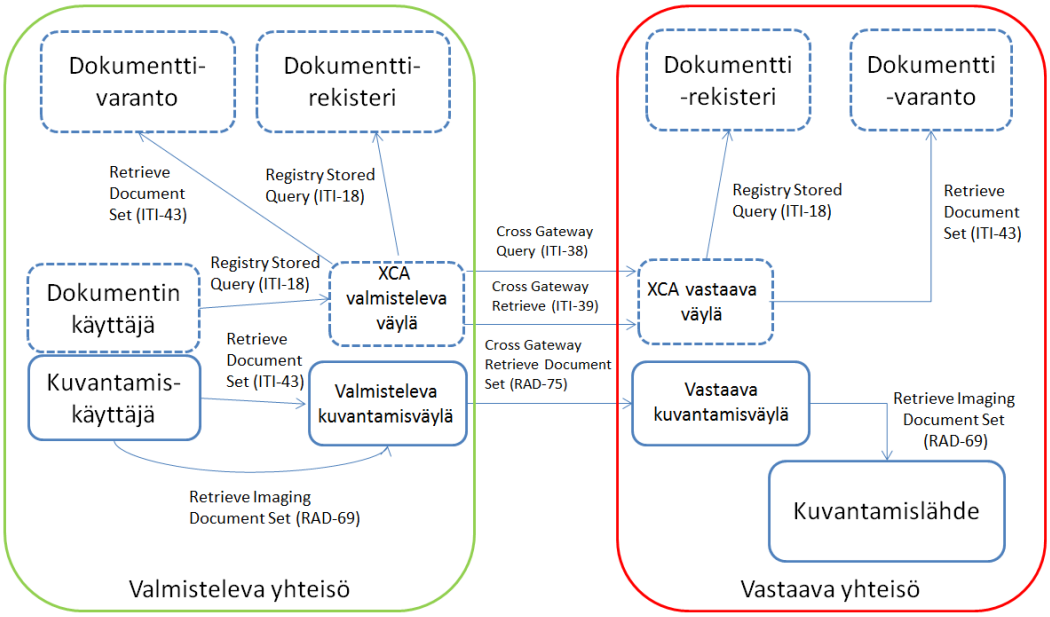
3.12 Kuvantamisdokumenttikyselyt yli toimialuerajojen

Cross-Community Access for Imaging -profiili (XCA-I) laajentaa edellisessä kohdassa 4.11 esitellyn XCA-profiilin ominaisuuksia kattamaan myös kuvantamistietoja muista yhteisöistä. XCA-profiili tarjoaa tuen suorittaa kyselyjä ja hakea kuvantamistietoja muista yhteisöistä oman paikallisen yhteisön lisäksi. [24]

XCA-profiili tarjoaa pääsyn diagnoosiraportteihin ja kuvantamistietojen julkaisudokumentteihin. XCA-I -profiili mahdollistaa pääsyn näissä julkaisudokumenteissa viitattuihin kuvantamisobjekteihin tai muihin mahdollisiin liitteisiin. [24]

3.12.1 XCA-I -toimijat

Kuvassa 3.13 on eroteltu katkoviivoin ne toimijat, jotka eivät ole suoraan XCA-I -profiilin kanssa tekemisissä. Ne on merkitty kuvaan siksi, että voidaan havainnollistaa sitä, mitä kaikkia toimijoita liittyy XCA-I -profiilin toimintaan. Kuva perustuu alkuperäiseen lähteeseen [24].



Kuva 3.13. *XCA-I -profiilin toimijat ja tapahtumat [24].*

Tässä kohdassa käydään läpi kuvassa 3.13 yhtenäisin viivoin merkityt toimijat ja niiden tärkeimmät ominaisuudet. Katkoviivoilla merkityt toimijat on käyty läpi aikaisemmin kohdassa 3.1.1 XDS-profiilin toimijoiden yhteydessä.

Kuvantamiskäyttäjä

Tämä toimija on esitelty jo aikaisemmin XDS-I -profiilin yhteydessä kohdassa 3.2.1. Kuvantamiskäyttäjän tehtävä tässä profiilissa on suorittaa tarvittaessa kyselyjä sekä paikallisesti yhteisön sisällä että myös erillisille yhteisöille valmistelevan kuvantamisväylän kautta. Kuvantamiskäyttäjä käyttää Retrieve Imaging Document Set -tapahtumaa, joka sisältää tietyt vaadittavat parametrit. Suoritettavan kyselyn vastauksena saadaan kuvantamistietojen julkaisudokumentti, joka sisältää parametreja vastaavat tiedot. [24]

Jos tapahtuma suoritetaan oman yhteisön sisällä, on silloin homeCommunityId-parametrina oman kotiyhteisön tunniste. Tämän perusteella tapahtuma suoritetaan suoraan paikalliselle kuvantamisdokumenttilähteelle. [24]

Kuvantamislähde

Kuvantamislähde on myös esitelty tarkemmin jo aikaisemmassa kohdassa 3.2.1 XDS-I -profiilin toimijoiden yhteydessä. Kuvantamislähteen tehtävänä on vastata sille suoritettuihin kyselyihin ja välittää vastauksissa tarvittavat kuvantamistiedot vaadituilla parametreilla. Jos kyseessä on paikallinen yhteisö, niin Retrieve Imaging Document Set -tapahtumaa käyttämällä kyselyn kuvantamislähteelle suorittaa kuvantamiskäyttäjä.

Jos kyseessä on erillinen yhteisö, välitetään sama tapahtuma ensin valmistelevalle kuvantamisväylälle, joka välittää kyselyn vastaavalle yhteisölle. Vastaavassa yhteisössä vastaava kuvantamisväylä suorittaa tämän tapahtuman lopulta vastaavan yhteisön kuvantamislähteelle.

Valmisteleva kuvantamisväylä

Valmistelevan kuvantamisväylän tehtäviin kuuluu Retrieve Imaging Document Set -tapahtuman käsittely. Valmistelevan kuvantamisväylän tulee päättää, mihin vastaaviin kuvantamisväyliin ja missä yhteisöissä sen tulee kysely välittää. Tässä työvälineenä käytetään homeCommunityId-parametria, jonka perusteella saadaan selvitettyä oikea vastaava kuvantamisväylä.

Käsiteltävä tapahtuma voi sisältää useamman kuin yhden yksilöllisen homeCommunityId-parametrin, joten valmistelevan kuvantamisväylän pitää pystyä käsittelemään useampi pyyntö samalla kerralla ja hallita myös kaikki niistä saatavat tulokset. Valmisteleva kuvantamisväylä käyttää homeCommunityId-parametria Cross Gateway Retrieve Imaging Document Set -tapahtumassa vastaavan kuvantamisväylän kanssa. [24]

Vastaava kuvantamisväylä

Vastaava kuvantamisväylä vastaanottaa ja käsittelee valmistelevalta kuvantamisväylältä saadun Cross Gateway Retrieve Imaging Document Set -tapahtuman. Tämän pohjalta vastaava kuvantamisväylä suorittaa Retrieve Imaging Document set -tapahtuman kuvantamislähteelle, jonka kohde selviää tapahtuman Retrieve Location UUID -parametrista. Jos Cross Gateway Retrieve Imaging Document Set -tapahtuma sisältää useiden dokumenttien pyynnöt useilla eri Retrieve Location UUID -parametreilla, tulee vastaavan kuvantamisväylän pystyä suorittamaan tapahtuma useamman dokumenttilähteen kanssa, sekä käsitellä niiltä saatavat vastaukset. [24]

3.12.2 XCA-I -tapahtumat

Tässä kohdassa on käyty läpi vain ne tapahtumat, jotka ovat suoraan tekemisissä XCA-I -profiilin kanssa. Kuvassa 3.13 nämä tapahtumat suoritetaan niiden toimijoiden välillä, joiden tekstien kehykset on piirretty kuvaan yhtenäisin viivoin.

Retrieve Imaging Document Set

Retrieve Imaging Document Set -tapahtuma (RAD-69) on esitelty tarkemmin jo kohdassa 3.2.2. Samaa tapahtumaa käytetään myös XDS-I -profiilissa kuvantamiskäyttäjän ja kuvantamislähteen välillä. XCA-I -profiilissa tätä tapahtumaa käytetään kuvantamiskäyttäjän ja valmistelevan kuvantamisväylän välillä sekä vastaavan kuvantamisväylän ja dokumenttilähteen välillä.

Kuvantamiskäyttäjä käyttää tätä tapahtumaa saadakseen halutut DICOM-objektit valmistelevalta kuvantamisväylältä. Erillisessä yhteisössä sijaitseva vastaava kuvantamisväylä käyttää tätä tapahtumaa myös saadakseen haluttuja DICOM-objekteja sen kanssa samassa yhteisössä olevalta kuvantamislähteeltä.

Cross Gateway Retrieve Imaging Document Set

Cross Gateway Retrieve Imaging Document Set -tapahtuma (RAD-75) perustuu edellisessä kohdassa kuvattuun Retrieve Document Set -tapahtumaan. Tiettyjä eroja tapahtumien välillä kuitenkin löytyy:

- Cross Gateway Retrieve Imaging Document Set -tapahtuma suoritetaan valmistelevan ja vastaavan kuvantamisväylän välillä.
- HomeCommunityId-parametri on pakollinen, eli siltä osin poikkeaa Retrieve Document Set -tapahtumasta, jossa se on valinnainen.
- Vastaavan kuvantamisväylän pitää sisältää Asynchronous Web Services Exchange -tuki.

3.13 Mobiili pääsy potilastietoihin

MHD-profiili (Mobile access to Health Documents) on suunniteltu erityisesti mobiililaitteita varten. MHD-profiili on saanut alkunsa vuonna 2012, jolloin määriteltiin yksinkertainen RESTful API -rajapinta XDS-ympäristöön (XDS-, XCA-, XDR- ja XDM-profiilit).

MHD-profiili on tällä hetkellä kehitettävänä IHE:llä, Volume 1 on julkaistu lokakuussa 2014, Volume 2 ja 3 ovat edelleen kehityksen alla. FHIR-standardin syntymisen myötä nämä MHD-profiilin uudet versiot volume 2 ja 3 tulevat perustumaan FHIR-standardiin [41]. FHIR (Fast Healthcare Interoperability Resources) standardikehys esitellään tarkemmin tämän työn luvussa 5.

Tällä hetkellä IHE:n MHD-profiili on trial-tilassa eli se on toistaiseksi keskeneräinen versio. MHD-profiilin tämänhetkinen versio pidetään myös niin sanottuna stable-versiona eli toiminnaltaan vakaana siihen asti, kunnes FHIR:n kehitys etenee. Kun FHIR:sta saavuttaa myös stable-tilan julkaisuissaan, päivitetään MHD-profiilia toimimaan sillä hetkellä viimeisimpien FHIR:n määritelmien kanssa yhteen. [42]

Tämän rajapinnan kautta on määritelty tietyt tapahtumat:

- välittää dokumentteja ja metatietoja (mobiililaitteesta) vastaanottajalle
- hakea toimitettujen dokumenttien metatietoja kyselyparametrien perusteella
- etsiä metatietoja sisältäviä dokumentteja kyselyparametrien perusteella
- vastaanottaa jonkin tietyn dokumentin kopioita

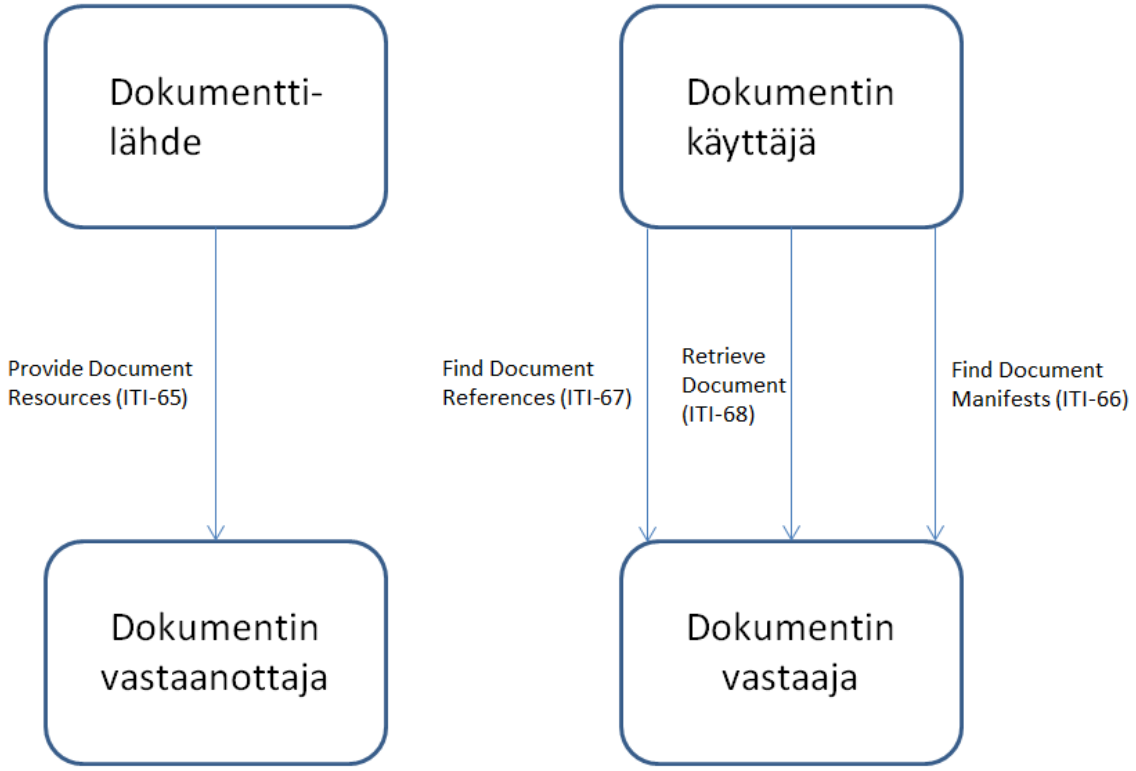
MHD-profiilia ei ole suunniteltu XDS-profiilin korvaajaksi, vaan se on suunniteltu mobiilien tai muuten rajoittuneiden päätelaitteiden käyttöä varten. Tällaisia rajoittuneita päätelaitteita voivat olla esimerkiksi niin sanotut itsepalvelupäätteet tai sähköiset mittalaitteet. Itsepalvelupäätteellä tarkoitetaan esimerkiksi sellaisia käytäväkoneita, joilla potilaat voivat syöttää omia tietojaan järjestelmään, esimerkiksi ilmoittautumisen yhteydessä. Sähköisellä mittalaitteella tarkoitetaan sellaisia laitteita, jotka tallentavat potilaan terveyteen liittyviä tietoja sekä voivat lähettää mittaustietoja potilasta hoitavalle organisaatiolle (esimerkiksi sydämentahdistin).

MHD-profiilin tapahtumat käyttävät hyväkseen dokumentin sisältöön ja metatietoihin liittyviä konsepteja XDS-profiilista ja yksinkertaistavat niiden teknologiaa mahdollisimman paljon. MHD-profiilin ominaisuudet painottuvat XDS-profiilin käytetyimpiin ominaisuuksiin, eikä se yritä edes kattaa kaikkea mahdollista toiminnallisuutta XDS-rakenteesta. MHD-profiili määrittelee tietyn URL-rakenteen, missä on pakollisena parametrina potilastunniste. Tämä on siis perinteinen REST-arkkitehtuurityylin määritelmä, joka painottaa tämän profiilin tapahtumien olevan potilaskeskeisiä. [43]

Kuvassa 3.14 on esitelty MHD-profiilin tärkeimmät toimijat ja tapahtumat. Dokumenttilähde ja dokumentin käyttäjä -toimijat on suunniteltu siten, että ne voidaan toteuttaa mobiililaitteeseen. Silti nämä toimijat pystyvät tarjoamaan riittävän

toiminallisuuden, jotta voidaan tukea useita sovellutuksia ja käyttötapauksia. Kuva 3.14 perustuu alkuperäiseen lähteeseen [43].

Dokumentin vastaanottaja ja dokumentin vastaaja on suunniteltu siten, että ne toteutetaan palvelujärjestelmään, eikä niillä ole rajoitettua, mobiililaitteille tarkoitettua toimintaympäristöä.



Kuva 3.14. *MHD-profiilin tärkeimmät toimijat ja tapahtumat [43].*

MHD-profiilissa olevat tapahtumat vastaavat XDS-profiilin tapahtumia seuraavasti:

- MHD Provide Document References -tapahtuma vastaa XDS Provide and Register -tapahtumaa.
- MHD Find Document References -tapahtuma vastaa XDS Registry Stored Query - FindDocuments -tapahtumaa.
- MHD Find Document Manifests -tapahtuma vastaa XDS Registry Stored Query - FindSubmissionSets -tapahtumaa.
- MHD Retrieve Document -tapahtuma vastaa XDS Retrieve Document Set -tapahtumaa. [43]

MHD-profiilin tapahtumissa on myös rajoituksia, missä ne eivät suoraan vastaa XDS-profiilin toimijoita:

- MHD Provide Document Resources -tapahtumaa ei voi käyttää korvaamaan olemassa olevaa dokumenttia tai tekemään muunnosta siitä.
- MHD Retrieve Document -tapahtuma voi vastaanottaa yhden dokumentin kerrallaan.
- MHD Find Document References ei tue XDS Registry Stored Query -tapahtuman tallennettua GetRelatedDocuments -kyselyä.

- MHD Provide Document Resources ei voi luoda tai päivittää kansioita. [43]

MHD-profiili tarjoaa resurssit tiettyihin REST-operaattoreihin omien tapahtumiensa kautta. Alla olevassa taulukossa 3.9 on eritelty tämän diplomityön kirjoitushetkellä määritellyt metodit ja resurssit. Taulukko perustuu alkuperäiseen lähteeseen [43].

Taulukko 3.9. *MHD-profiilin metodit ja resurssit [43].*

HTTP metodi	Document Entry -tapahtumat	Document Submission Set -tapahtumat	Document-tapahtumat
GET	Find Document Reference (ITI-67)	Find Document Manifest (ITI-66)	Retrieve Document (ITI-68)
PUT	Kielletty	Kielletty	Kielletty
POST	Provide Document Resources (ITI-65)		
DELETE	Kielletty	Kielletty	Kielletty
UPDATE	Kielletty	Kielletty	Kielletty
HEAD	Ei määritelty	Ei määritelty	Ei määritelty
OPTIONS	Ei määritelty	Ei määritelty	Ei määritelty
TRACE	Ei määritelty	Ei määritelty	Ei määritelty

MHD-profiilin turvallisuus

Kun puhutaan mobiileista päätelaitteista, tulee turvallisuuteen myös kiinnittää erityistä huomiota. Laitteet ovat usein langattomia, joten niitä on vaikeampi fyysisesti hallita. Yleensä HTTP-protokollaa ja REST:iä käyttävät järjestelmät eivät käsittele niin arkaluonteisia asioita, kuten potilastietojärjestelmät. Näin ollen järjestelmän turvallisuuteen tulee kiinnittää erityistä huomiota myös MHD-profiilissa. IHE suosittelee, että sovelluskehittäjät määrittelevät riskianalyysin sovelluskehitykseen ja että sitä myös käytetään tuotantoympäristössä.

3.14 Muita merkittäviä IHE-profiileja

Tässä luvussa käydään hieman suppeammin läpi muita tietopalvelun toimintaan liittyviä IHE-profiileja. Tulevan tietopalvelun toiminnan kannalta tässä luvussa esiteltävät profiilit eivät ole yhtä olennaisessa osassa kuin edellisessä luvussa tarkemmin läpikäydyt profiilit, mutta niille voi tulla käyttöä tulevaisuudessa. Nämä profiilit esitellään lähinnä yleisellä tasolla, jotta lukijalle käy selville niiden tarkoitus XDS-tekniikkaa hyödyntävän tietopalvelun osana.

3.14.1 Patient Demographics Query

Patient Demographics Query -profiili (PDQ) tarjoaa keinot hajautetusti toimiville sovelluksille hakea potilastietolistoja potilasinformaatiopalvelimelta perustuen tiettyihin ha-

kukriteereihin. Vastauksena palautuu suoraan sovellusten käyttöön potilaan demografisia sekä mahdollisesti potilaskäynteihin liittyviä tietoja.

On todettu, että sellaisissa tilanteissa, missä aineistoa on olemassa todella paljon ja johon sisältyy paljon lasten potilastietoja, on ylimääräinen demografinen tieto erittäin hyödyllistä. Tällaisia tilanteita ovat esimerkiksi julkiset terveystietokannat tai vastaavat laajat rekisterit. Lasten potilastietojen vaikutus selittyy sillä, jos lapsia on useampi ja ne ovat samanikäisiä, esimerkiksi kaksosia. Kaksosilla on tiedoissaan huomattavan paljon yhteneviä tietoja, kuten esimerkiksi sukunimi, syntymäaika ja vauvana sekä lapsena suoritetut tarkastukset on todennäköisesti myös tallennettu samoille päivämäärille. [12]

Tällöin suoritettaessa hakuja aineistoihin niin sanottujen väärien positiivisten tulosten todennäköisyys kasvaa, jos lisäinformaatiota ei ole käytettävissä. PDQ-profiili tarjoaa tarkentavia parametreja demografisiin tietoihin, millä pyritään minimoimaan virheitä hakutuloksiin. Näitä parametreja ovat esimerkiksi äidin tyttönimi, potilaan kotipuhelinnumero, potilaan monikkosynnyttämisen indikaattori, potilaan syntymäjärjestys, viimeinen päivitysaika/-päiväys tai viimeinen päivityspaikka. [12]

3.14.2 Cross-Enterprise Document Reliable Interchange

Cross-Enterprise Document Reliable Interchage -profiili (XDR) tarjoaa luotettavan siirtomedian yhden potilaan dokumenttien jakamiseen, jos siihen ei ole käytettävissä valmista infrastruktuuria, kuten esimerkiksi XDS-dokumenttirekisteriä ja -varantoa. XDR-profiili tukee Provide and Register Set -tapahtuman uudelleenkäyttöä, jossa Web-palvelut toimivat siirtotienä. Siirto tapahtuu suoraan dokumenttilähteeltä dokumentin käyttäjälle, eikä välissä ole dokumenttivarantoa tai -rekisteriä.

XDR tukee samoja dokumenttityyppejä, kuin XDS- ja XDM-profiilit. Määrittelyssä ei ole uusia metatietotyyppejä tai viestityyppejä. XDR käyttää hyväkseen XDS-metatietoja, joista se painottaa potilaan ja dokumenttien tyyppien tunnisteita, metatietojen kuvaustietoja ja niiden välisiä suhteita. [12]

XDR-profiili määrittelee ainoastaan sähköisen siirtomekanismin hoitodokumentteja varten, siirrettävä sisältö määritellään IHE:n PCC-osiossa (Patient Care Coordination). XDR:ää ei ole suunniteltu muuhun kuin potilaisiin liittyvien kliinisten dokumenttien siirtämiseen, eikä hoitamaan kaikkea organisaatioiden välistä sähköisten potilaskertomusten tietoliikennettä. XDR-profiilin tuki olisi hyvä olla olemassa sitä varten, jos dokumenttivaranto ja/tai dokumenttirekisteri eivät ole jostain syystä saatavilla. Näissä tapauksissa XDR toimisi varalla olevana siirtotienä dokumenteille eri hoito-organisaatioiden välillä.[12]

3.14.3 Cross-Enterprise Document Media Interchange

Cross-Enterprise Document Media Interchange -profiili (XDM) mahdollistaa dokumenttien jakamisen tiettyjen tunnettujen siirtomedioiden välityksellä. Tätä profiilia käyttämällä potilaan on mahdollista käyttää fyysistä siirtomediaa omien potilastietojen-

sa siirtoon. XDM tukee myös useiden potilaiden tiedostojen siirtoa yhdellä tiedonsiirtotapahtumalla.

Yleisimpiä tämän profiilin käyttötapauksia ovat tiedonsiirto lääkäriltä potilaalle ja edelleen lääkärille, potilaalta lääkärille tai lääkäriltä lääkärille. Lääkäri-potilas-lääkäri tarkoittaa sitä, että potilas saa esimerkiksi yleislääkäriltä diagnoosin ja potilastiedot, jotka potilas voi viedä mukanaan haluamalleen erikoislääkärille. Potilas-lääkäri -tilanne tarkoittaa sitä, että kun potilaalle on luovutettu potilastiedot aikaisemmin ja hän tulee hoitoon uudelleen eri paikkaan, niin hänellä on mukanaan aikaisemmat potilastiedot, jotka hän luovuttaa uudelle lääkärille vastaanotolla. Lääkäri-lääkäri-tilanteessa ensimmäisellä vastaanotolla käyneen potilaan lääkäri voi lähettää sähköpostitse potilaan tiedot suoraan seuraavalle erikoislääkärille. Tämä ei tosin ole Suomessa sallittua, ellei sähköposti ole salatussa muodossa.

Yhteistä näille käyttötapauksille on, että ne kaikki ovat ihmisten välistä kommunikaatiota. Tästä syystä XDM-profiili on suunniteltu käyttäen helppokäyttöisiä siirtomedioita, kuten jo olemassa olevia sähköpostisovelluksia, kirjoittavia CD-asemia ja USB-portteja. XDM ei lisää näihin siirtomedioihin mitään luotettavuutta lisääviä ominaisuuksia ja se vaatii, että käyttäjiltä löytyy arvostelukykyä siihen, että hän pystyy valitsemaan oikeat potilaat ja tarvittavat tiedot sieltä tallennettavaksi siirtomedialle. [12]

XDM-profiili ei ota kantaa siirrettävien dokumenttien tiedostomuotoihin, se tukee samoja tiedostomuotoja, kuin XDS ja XDR. XDM ei myöskään määrittele mitään uusia metatietoja, vaan se käyttää vastaavalla tavalla XDS:n tarjoamia metatietoja, kuten XDR. [12]

Hakemisto- ja tiedostorakenne on määritelty XDM-profiilissa, jotta tallennus onnistuu siirtomedioille. Rakenne sisältää erilliset alueet jokaiselle potilaalle ja se on tuettuna kaikilla viitatuilla mediatyypeillä. Rakenne ja mahdolliset siirtomediat on valittu niin, että media on toiminut myös radiologiassa, tarkemmin PDI-profiilin käytössä (Periodontal Disease Index). Valitut siirtomediat ovat laajasti käytössä olevia tallennustapoja, CD-R, USB-muistit/kiintolevyt, ja sähköpostin liitetiedosto ZIP-muotoon pakattuna. Tämän profiilin käytössä on hyvä ottaa huomioon myös tallennusmedioiden kehittyminen ja niiden vaikutus käytettäviin siirtomedioihin, nykyisin kirjoittavat CD-asemat alkavat poistua varsinkin kannettavista tietokoneista.

4 AVOIMEN LÄHDEKOODIN XDS-SOVELLUKSET

Tämän diplomityön yksi osio on kartoittaa olemassa olevia avoimen lähdekoodin (open source) tai freeware-lisenssillä tehtyjä toteutuksia XDS-aihepiiristä. Tässä luvussa perehdytään eri toteutuksiin, suoritetaan vertailua tärkeimmistä ominaisuuksista ja arvioidaan niiden käyttökelpoisuutta käytännön toteutuksessa Medbit Oy:n XDS-projektin yhteydessä.

Tämän diplomityön tapauksessa keskitytään tarkasteltavissa ohjelmissa avoimen lähdekoodin sovelluksiin. Avoin lähdekoodi tarkoittaa ohjelmistokehityksessä sellaista menetelmää, jossa käyttäjälle tarjotaan mahdollisuus tutkia ohjelmiston lähdekoodia ja muokata sitä haluamakseen. Tällaiset sovellukset ovat yleensä ilmaisia tai niiden hinta on hyvin pieni. Avoimeen lähdekoodiin kuuluu myös vapaus käyttää ohjelmistoa mihin tahansa kehittäjän haluamaan käyttötarkoitukseen. Tämän luvun seuraavissa kohdissa esitellään tärkeimmät ominaisuudet tutkituista avoimen lähdekoodin toteutuksista. Tarkastellut avoimen lähdekoodin toteutukset perustuvat vuoden 2011 tilanteeseen. Löydettyjen toteutusten lisäksi pyrittiin etsimään myös uudempia varteenotettavia toteutuksia, mutta tuloksetta.

Freeware-lisenssillä tehdyt sovellukset jätetään kokonaan tarkemman tarkastelun ulkopuolelle sovellusten luonteen ja turvallisuussyiden vuoksi. Freeware-sovellus on jonkin ohjelmistokehittäjän omaa tuotantoa ja sitä jaetaan yleensä ilmaiseksi muiden käyttöön. Avoimesta lähdekoodista eroten freeware-sovellukset ovat suljettuja eli lähdekoodia ei ole saatavilla. Näin ollen niistä ei tiedetä mitä kaikkea ohjelmat tekevät tai jättävät tekemättä ohjelman suorituksen aikana.

4.1 O3-XDS

O3-XDS on avoimella lähdekoodilla tehty ohjelmisto, joka tarjoaa IHE-yhteensopivan rekisterin ja tietovarannon. Sen on tehnyt Open Three (O3) Consortium -niminen avoimen lähdekoodin projekti, jonka päämääränä oli kehittää sairaaloiden välistä yhdentymistä. Tällä hetkellä projektin verkkosivut eivät ole enää olemassa, eikä mitään muutakaan varsinaista dokumentaatiota O3-XDS:stä valitettavasti ole enää saatavilla.

4.2 IheOS

IheOS eli IHE Open Source on projekti, joka sai alkunsa XDS-standardia luotaessa tehdystä referenssitestiympäristöstä, jonka toteutti NIST (National Institute of Standards

and Technology). Tällä testiympäristöllä on tällä hetkellä tuki IHE-profiileille XDS.b, XDR (täydet ja rajoitetut metatiedot), XDM, XCA, MPQ, ATNA ja XCPD.

4.3 Open eHealth Integration Platform

IPF eli Open eHealth Integration Platform on laajalti USA:ssa ja Euroopassa käytössä oleva avointa lähdekoodia käyttävä sovellutus IHE standardeista. IPF on laajennos Apache Camel routing and meditation -moottoriin. Se tukee myös DSL:ää (Domain Specific Language), jotta sekä yleiskäyttöiset että tarkemmin määritellyt yhdentymismallit, kuten HL7-pohjainen yhdentymisratkaisu, olisivat mahdollisia. Näitä DSL:iä voidaan laajentaa vielä Groovyn ominaisuuksilla. IPF:n voi helposti sulauttaa Java-sovelluksiin ja siinä on myös tuki OSGi-ympäristöstä sisäiselle käyttöönotolle (deployment). IPF:stä löytyy tuki useiden IHE-profiilien toimijoille. Näitä profiileja ovat XDS, PIX, PDQ, PIXv3, PDQv3, QED, XCPD, XCA, XCA-I, XCF, XPID ja PCD.

IPF on hyvin dokumentoitu heidän omalla wiki-sivullaan ja informaatiota on muutenkin hyvin saatavilla. IPF:ää myös kehitetään edelleen ja uusia versioita sekä dokumentaatiota on päivitetty wiki-sivustolle myös vuoden 2015 aikana. IPF:ää on tähän mennessä käytetty useissa projekteissa sekä Pohjois-Amerikassa että Euroopassa ja sen komponentteja on testattu IHE:n testaustapahtumissa useita kertoja.

4.4 HIEOS

HIEOS (Health Information Exchange Open Source) on avointa lähdekoodia hyödyntävä implementaatio, jonka on kehittänyt Vangent Inc. niminen organisaatio. HIEOS tukee XDS- ja XCA-profiileja. Dokumentaatiota on vähän saatavilla ja wiki-sivuston viimeisin päivitys on tapahtunut vuonna 2011.

Tämän perusteella HIEOS ei ole enää jatkuvan kehityksen kohteena, uusin tarjolla oleva versio on HIEOS 2.0. Tuoreimpia kysymyksiä HIEOS:n nykytilanteesta on kirjoitettu implementaation verkkosivulle vuonna 2014. Niihin ei kuitenkaan toistaiseksi ole tullut mitään vastausta kehittäjiltä. [44]

4.5 Open Health Tools

Open Health Tools -projekti sisältää laajan IHE-profiilituen. Tuettuja profiileja ovat ATNA, MPQ, PAM, PIX, PDQ, SVS, XCA, XDS ja XUA. Näiden lisäksi Open Health Tools:lla on useita palvelinosion aliprojekteja:

- OpenXDS, XDS-profiilin implementointi sisältäen rekisterin ja tietovarannon.
- OpenATNA, ATNA-profiilin implementaatio sisältäen Audit Record -tietovarannon.
- OpenPIXPDQ, PIX ja PDQ -profiilien implementoinnit.

Open Health Tools -projekti on toteutettu myös Java-ohjelmointikielellä, kuten suurin osa tässä luvussa esitellyistä avoimen lähdekoodin toteutuksista. Tämän projektin etuna on jo alun perin samalle perusalustalle suunnitellut aliprojektit ja niiden saumat-

tomasti toimiva yhteistyö. Nämä implementaatiot ovat myös helposti käyttöönotettavia, mutta projektin dokumentaatio on joiltakin osin hieman puutteellinen. [45]

4.6 CONNECT

CONNECT oli alun perin suunniteltu USA:n terveysvirastojen toimesta heidän omaan käyttöönsä, mutta nykyisin se on kenen tahansa käytettävissä avoimen lähdekoodin lisenssillä. CONNECT on nykyisin laajalti käytössä, tuotannossa yli 20 organisaatiossa.

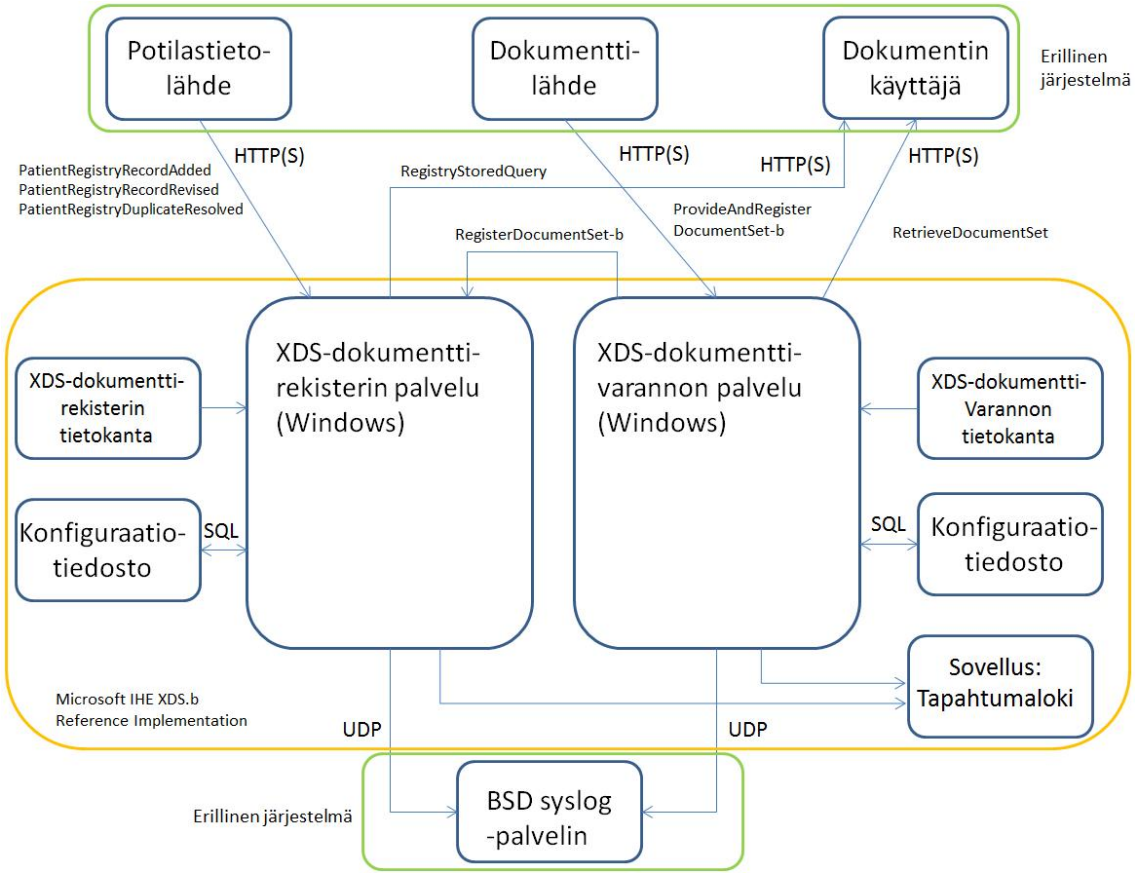
CONNECT on dokumentoitu kattavasti ja eri versioiden ominaisuudet on eroteltu omina taulukoinaan. IHE-profiileihin liittyvä tarkka informaatio on hieman haasteellista löytää projektin sivustolta CONNECT:n modulaarisen rakenteen ja suuren dokumenttimäärän vuoksi. CONNECT:lla on tuki HITSP:n (Healthcare Information Technology Standards Panel) määrittelyihin, jotka perustuvat IHE:n profiileihin XDR, XCA ja ATNA, mutta suoraan ilmoitettua tukea näille ei löydy. Tästä syystä CONNECT:n tiedoissa ominaisuustaulukoissa 4.2 ja 4.3 ei ole merkitty yhteensopivuuksia. Näin ollen tämän toteutuksen käytännön hyödyntämistä Medbit Oy:n tarpeisiin ei voi suositella.

4.7 Cross-Enterprise Document Sharing XDS.b

Cross-Enterprise Document Sharing XDS.b (CodePlex) on Microsoft Connected Health Platform:n (CHP) tekemä avoimen lähdekoodin ratkaisu, joka perustuu IHE:n XDS-profiiliin. Tämä ratkaisu toteuttaa sekä dokumenttirekisterin, että dokumenttivarannon, molemmat Async-optiolla. Tässä on myös tuki ATNA-profiilin asiakassovelluksen lokien tallennukselle ja luotettu laite -toimijalle. Tämä Microsoftin tekemä ratkaisu toimii ainoastaan Windows-alustoilla.

Tässä toteutuksessa käytetyt teknologiat ovat .NET 3.0 (WCF), Microsoft Enterprise Library ja SQL Server 2005. Sen lisäksi, että toteutus sisältää XDS-dokumenttivarannon ja XDS-dokumenttirekisterin, on siinä myös Test Harness -sovellus, jolla voi suorittaa toiminnallisia testejä kaikille tuetuille XDS-tapahtumille. Dokumenttirekisterin ja dokumenttivarannon palvelut on toteutettu WCF-palveluna (Windows Communication Foundation) Windowsissa. WCF on viitekehys, jolla rakennetaan palvelutyyppisiä sovelluksia. WCF mahdollistaa muun muassa asynkronisen viestiliikenteen palvelun toimijalta toiselle. [46, 47]

ATNA-profiilin lokien tallennustuen lisäksi tässä XDS-implementaatiossa kerätään lokeja eri tavoilla. Dokumenttirekisteri ja dokumenttivaranto tallettavat sovellustietoja, kuten esimerkiksi sovelluksen käynnistyksiä ja sammutuksia, Windowsin Application Event Log -lokiin. Tämän lisäksi toteutukseen kuuluu erillinen järjestelmä, BSD syslog -palvelin (RFC3164), joka toimii auditointilokien tallennuspaikkana, jos tätä ei ole toteutettu ATNA-profiilin toiminnallisuudella. Kuvaan 4.1 on piirretty tämän sovellutuksen tarkempi toimintakaavio. Kuva perustuu alkuperäiseen lähteeseen [46].



Kuva 4.1. *Kaaviokuva: Microsoft IHE XDS.b Reference Implementation. [46]*

Uusin saatavilla oleva versio on julkaistu helmikuun 1. päivä vuonna 2012, eikä sen jälkeen ole tullut uusia päivityksiä julkaisuun. Toteutuksesta löytyy hyvin dokumentaatiota, mutta perustuen toteutuksen verkkosivuihin, ne saattavat olla osin puutteellisia. Viimeisimmän version julkaisussa on kommentteja pääosin puutteellisista/virheellisistä skripteistä sekä virheellisestä dokumentaatiosta, joten materiaaliin tulee suhtautua pienellä varauksella. Yksittäinen kommentti löytyi myös viimeisimmän version puolesta, jossa mainittiin, että materiaalin sync-hakemistosta löytyvät dokumentaatiot ovat ajan tasalla ja eivät sisältäisi edellä mainittuja virheitä. [48]

4.8 Ominaisuustaulukot

Tässä kohdassa avoimen lähdekoodin toteutusten ominaisuuksia kootaan yhteen ja esitellään ominaisuustaulukoiden muodossa. Taulukossa 4.1 esitellään toteutusten tärkeimpiä ominaisuuksia koottuna yhteiseen taulukkoon. Taulukosta on havaittavissa yhteneviä piirteitä eri toteutuksissa, muun muassa valtaosa on tehty Java-ohjelmointikielellä sekä ne ovat web-pohjaisia. Eniten eroja muihin tarkasteltuihin toteutuksiin löytyy Microsoftin tekemästä CodePlex:stä. Se on toteutettu Windows-pohjaisena C#- ja .NET-kielillä ja se käyttää tietokantanaan MS-SQL:ää.

Taulukko 4.1. *Avointa lähdekoodia hyödyntävien sovellusten ominaisuudet.*

	Lisenssi	Tekijä	Kieli	Alusta	Käyttöliittymä	Tietokanta
O3-XDS	GNU GPL	O3 Consortium	Java, PHP	Cross-Platform	Web-pohjainen	JDC
IheOS	Julkinen	NIST	Java	Cross-Platform	Web-pohjainen	JDC
IPF	Apache	Open eHealth	Java, Groovy	Cross-Platform	Web-pohjainen	JDC
HIEOS	Muu	Vangent	Java	Cross-Platform	Web-pohjainen	JDBC
OpenXDS*	Julkinen	Misys OSS	Java	Cross-Platform	Web-pohjainen	JDC
OpenPIXPDQ*	Julkinen	Misys OSS	Java	Cross-Platform	Web-pohjainen	JDBC
OpenATNA*	Julkinen	Misys OSS	Java	Cross-Platform	Web-pohjainen	JDBC
CONNECT	BSD	USA:n terveysvirasto	Java	Cross-Platform	Natiivi	JDBC (mySQL)
CodePlex	Microsoft PL	Microsoft	C#/.NET	Windows	Windows	MS-SQL

* Open Health Tools:n osatoteutus

Seuraavassa taulukossa 4.2 on esitelty eri avoimen lähdekoodin toteutusten sisältämä yhteensopivuus yleisimpien IHE-profiilien toimijoille. Taulukko 4.2 perustuu alkuperäiseen lähteeseen [45]. Taulukosta on nähtävissä, että yksi laajinta toimijatukea tarjoaa IPF. Samoin CodePlex:n toteutuksen rajoittuneisuus XDS-profiiliin näkyy taulukosta, sillä XDS ja XDS-I -profiilien sisältämien toimijoiden lisäksi muita toimijoita ei ole tuettu.

Taulukko 4.2. *Profiili- ja toimijatuki avoimen lähdekoodin sovelluksissa [45].*

						Open Health Tools				
Profiili	Toimija	O3-XDS	IheOS	IPF	HIEOS	Open XDS	Open PIXPDQ	Open ATNA	CONNECT	CodePlex
CT	Time Client	X	X	X	X	X	X	X		X
ATNA	Audit Record Repository	X	X					X		
	Secure Node	X	X	X	X			X		X
	Secure Application					X	X			X
PIX	Patient Identity Source			X						
	Patient Identity Cross-Reference Manager			X			X			
	Patient Identity Cross-Reference Consumer			X						
PDQ	Patient Demographics Supplier			X			X			
	Patient Demographics Consumer									
XDS.a	Document Registry	X		X						
	Document Repository	X		X						
	Document Source	X		X						
	Document Consumer	X		X						
XDS.b	Document Registry		X	X	X	X				X
	Document Repository		X	X	X	X				X
	Document Source			X						
	Document Consumer			X						X
XDS-I	Document Registry		X		X	X				X
	Document Repository		X		X	X				
	Imaging Document Source									
	Imaging Document Consumer	X								
XDR	Document Source		X							
	Document Recipient		X							
XCA	Initiating Gateway		X		X	X				
	Responding Gateway		X		X	X				
XDM	Portable Media Creator	X								
	Portable Media Importer									
MPQ	Document Consumer				X					
	Document Registry				X					

Seuraavan sivun taulukko 4.3 sisältää edellistä taulukkoa vastaavasti yleisimmät IHE-profiilit, joista on eriteltynä niiden sisältämät tapahtumat. Taulukkoon 4.3 on merkitty näiden eri avoimen lähdekoodin toteuksien sisältämä yhteensopivuus profiilien tapahtumille. Taulukko 4.3 perustuu alkuperäiseen lähteeseen [45]. Myös tästä taulukosta on huomattavissa taulukon 4.2 kohdalla mainitut seikat, IPF:n sisältämä tapahtumatuki on kattavimpia tarkastelluista toteutuksista ja CodePlex:n painotus XDS-profiilitukeen rajoittaa myös sen tapahtumatuen monipuolisuutta.

Taulukko 4.3. *Profiili- ja tapahtumatuki avoimen lähdekoodin sovelluksissa [45].*

Profiili	Tapahtuma	O3-XDS	IheOS	IPF	HIEOS	Open Health Tools Open XDS	Open PIXPDQ	Open ATNA	CONNECT	CodePlex
CT	Maintain Time [ITI-1]	X			X	X	X	X		
ATNA	Authenticate Node [ITI-19]	X		X	X	X	X	X		
	Record Audit Event [ITI-20]	X		X	X	X	X	X		
PIX	Patient Identity Feed [ITI-8]	X		X	X	X	X			
	PIX Query [ITI-9]	X		X			X			
	PIX Update Notification [ITI-10]			X			X			
	Patient Identity Management [ITI-30]									
PDQ	Patient Demographics Query [ITI-21]			X			X			
	Patient Demographics and Visit Query [ITI-22]			X						
XDS.a	Query Registry [ITI-16]	X		X						
	Provide and Register Document Set [ITI-15]	X		X						
	Register Document Set [ITI-14]	X		X						
	Retrieve Document [ITI-17]	X		X						
XDS.b	Registry Stored Query [ITI-18]			X	X	X				X
	Provide and Register Document Set-b [ITI-41]			X	X	X				X
	Register Document Set-b [ITI-42]			X	X	X				X
	Retrieve Document Set [ITI-43]			X	X	X				X
XDS-I	Retrieve Images [RAD-16]	X								X
	Retrieve Presentation States [RAD-17]	X								X
	Retrieve Reports [RAD-27]	X								X
	Retrieve Key Image Note [RAD-31]	X								X
	Retrieve Evidence Documents [RAD-45]	X		X	X					X
	WADO Retrieve [RAD-55]	X		X						X
	Retrieve Imaging Document Set [RAD-69]			X						
	Provide and Register Imaging Document Set – MTOM/XOP [RAD-68]									
XDR	Provide and Register Document Set-b [ITI-41]									
XCA	Cross Gateway Query [ITI-38]				X					
	Cross Gateway Retrieve [ITI-39]				X					
XDM	Distribute Document Set on Media [ITI-32]									
MPQ	Multi-Patient Stored Query [ITI-51]				X					

Poikkeuksena edellä olleissa toimija- ja tapahtumataulukoissa on CONNECT, jolle tarkkaan määriteltyä yhteensopivuutta IHE-profiileille ei ollut vahvistettavissa. Tästä syystä edellä mainituissa taulukoissa ei kyseisen toteutuksen kohdalle ole merkitty lainkaan toimija- tai tapahtumatukea. IheOS:n kohdalla myös tapahtumatuki on tyhjä taulukossa 4.3, koska kyseinen toteutus sisältää käytännössä testausalustan joka tukee vain taulukossa 4.2 mainittuja toimijoita.

5 FHIR-STANDARDI

Uusin haastaja ja vaihtoehto tulevista teknologioista on HL7-organisaation julkaisema standardikehys FHIR (Fast Health Interoperable Resources). FHIR hyödyntää uusimpia web-standardeja ja siinä keskitytään yhdistämään hyvät puolet jo olemassa olevista HL7:n V2- ja V3- sekä CDA-määrityksistä. Määrityksiä on kehitetty vuodesta 2011 lähtien, aluksi työnimellä ”Resources for Healthcare” ja myöhemmin sen tilalle valittiin nimi FHIR, joka äännetään kuten sana ”tuli” englanniksi (fire). [49]

FHIR:iin perustuvat ratkaisut koostuvat komponenteista, joista käytetään nimeä resurssit. Resurssit ovat modulaarisia ja niitä pyritään koostamaan mahdollisimman helposti joihinkin olemassa olevien järjestelmien ongelmien ratkaisua varten. FHIR:ää voidaan käyttää useissa käyttöympäristöissä ja se on myös sellaiseksi alun perin suunniteltu, esimerkiksi suurten terveyspalvelujen tuottajien välisessä tiedonsiirrossa, pilvipalveluissa tai mobiiliratkaisuissa. [49]

FHIR:n määritys on tehty ainoastaan toteuttajia varten ja sen dokumentaatio on myös tehty siltä kannalta ajateltuna. Kaikki resurssit tulee olla myös ilmaistavissa selkokielisellä tavalla. FHIR poikkeaa myös HL7:n V2- ja V3-määrityksistä, koska se on alusta lähtien perustunut avoimeen lähdekoodiin.

5.1 FHIR-määritys ja toteutustavat

Määritys on jaettu kolmeen osa-alueeseen:

- Taustadokumentaatio, resurssien ymmärtämisessä ja niiden käytössä tarvittava materiaali.
- Implementaatio, miten resursseja käytetään eri käyttöympäristöissä.
- Resurssimääritykset, joissa eritellään ja määritellään käytettävät resurssit tarkemmin. [49]

Toteutustapoja FHIR:ssä on neljä: REST, dokumentit, viestit ja palvelut. Resurssien sisältö tulee olla sama riippumatta siitä, mikä näistä tavoista on käytössä. Toteutustapojen lisäksi myös rajoituksia ja profiileja voidaan käyttää.

FHIR-standardissa määritellään resurssi seuraavasti:

- Sillä on oma identiteettinsä (URL-osoite), jolla siihen voidaan osoittaa.
- Se on jonkin FHIR:n määritelmässä olevan resurssin tyyppinen.
- Se sisältää tietyt rakenteiset tietotyypit, jotka on määritelty jossakin resurssissa.
- Resurssin sisältö on kuvattu sen sisältämässä, selkokielisesti kuvatussa XHTML-muodossa.

- Resurssin sisältö voi muuttua myöhemmin.

Resursseilla on useita esitysmuotoja ja resurssi on validi, jos se täyttää edellä mainitut ehdot sekä se on XML- tai JSON-muodossa, kuten FHIR:ssä on määritelty. Myös muut esitysmuodot ovat mahdollisia, mutta niitä ei ole määritelty FHIR:n määrityksessä. [50]

RESTful API-rajapinnat

FHIR:ssä resursseja on mahdollista käyttää RESTful-rajapinnalla. REST:n käyttäminen ei ole pakollista, käyttö riippuu muusta toimintaympäristöstä. REST-rajapintaan kuuluvat URL-osoite ja HTTP-pohjaiset transaktiot Create, Retrieve, Update ja Delete. FHIR:n operaatioille on määritelty vastaavuudet ja mallit sekä edellä mainittuihin operaatioihin että URL-osoitteen ja HTTP:llä välitettävien sanomien sisältöjen suhteen. Resursseista voidaan myös muodostaa dokumentteja ja lähettää ryhmässä. FHIR tarjoaa myös sanomanvälityskehyksen, joka perustuu tapahtumiin.

REST-rajapinta määrittelee FHIR:n resurssit operaatioina ja ne kohdistetaan resursseihin, joita hallitaan omina kokoelminaan. Palvelin päättää, mitä interaktioita on saatavilla ja mille resurssityypeille löytyy järjestelmästä tuki. FHIR-palvelimilta löytyy myös tuki binääriresursseille. Tämä tarkoittaa siis sitä, että binääriresurssi voi sisältää käytännössä mitä tahansa ja sisältö tallennetaan sellaisenaan.

Sanomat ja dokumentit

Kun joltakin tietyltä ajanhetkeltä käsitellään tietty resurssikokoelma, määritellään se dokumentiksi. Se voi olla joko niin sanottu standalone-dokumentti, kuten esimerkiksi CDA tai jokin yhdistetty resurssityyppi. Dokumentti voidaan välittää esimerkiksi linkitettyjen resurssien joukkona tai ATOM-syötteenä (XML-pohjainen dokumenttitiedostomuoto). REST:iä ei ole pakko käyttää dokumenttien siirrossa, dokumentit voidaan lähettää myös esimerkiksi SOAP-sanoman sisältönä tai sähköpostina. FHIR REST -palvelimen avulla dokumentteja voidaan säilyttää ja vastaanottaa. Dokumentit käsitellään ja säilytetään siinä muodossa kun ne on vastaanotettu eli niitä ei tarvitse purkaa. [49, 50]

Kuten dokumentin kohdalla, myös sanoma määritellään kokoelmana resursseja, jotka lähetetään jonkin tietyn tapahtuman lopputuloksena. Sanomat tukevat pyyntö/vastaus-metodia ja ne ovat tapahtumapohjaisia, tarvittaessa myös asynkronisia. FHIR-standardi olettaa, että sovellusten välillä siirretään tietoa jollakin siirtotavalla, mutta se ei ota kantaa siihen, miten se käytännössä toteutuu. Yksi vaatimus tiedonsiirrolle kuitenkin on: kaikki liikenne tulee lähettää johonkin tunnettuun osoitteeseen ja vastaukset palautetaan viestien lähettäjälle. [49]

Palvelut

Edellisessä kohdassa mainittuja sanoma- tai dokumenttipohjaisia toteutuksia ei FHIR:n määritelmän mukaan ole pakko käyttää, vaan resurssien välitykseen käytettävä liikenne

voidaan toteuttaa millä tahansa sopivalla tekniikalla. Yksi tapa tähän on käyttää resursseja parametreina palvelurajapinnoissa. FHIR ei määrittele tarkemmin mitään tiettyä palvelurajapintaa, vaan olettaa, että resursseja pystytään hyödyntämään muiden standardien ja toteutusten palvelurajapintojen kautta. [49]

5.2 Yhteensopivuus ja laajennettavuus

FHIR sisältää sisäänrakennetun laajennusmekanismin, jonka avulla implementaatioiden tekijät voivat lisätä uusia resursseja toteutettavaan järjestelmään. Laajennusmekanismin määritelmänä käytetään nimeä, arvoa ja linkkipistettä. Linkkipiste sisältää tiedon perusresurssin elementin tai toisen laajennuksen kiinnittämisestä laajennukseen. [49]

5.3 Esimerkkejä FHIR-käyttöympäristöistä

Sähköinen potilastietojärjestelmä tarjoaa RESTful API -rajapinnan, joka mahdollistaa potilaiden pääsyn omiin tietoihinsa. Yleensä pääsy tapahtuu jonkin kolmannen osapuolen tarjoaman sovelluksen tai portaalin avulla. Tässä käyttöympäristössä sähköinen potilastietojärjestelmä mahdollistaa seuraavia palveluita:

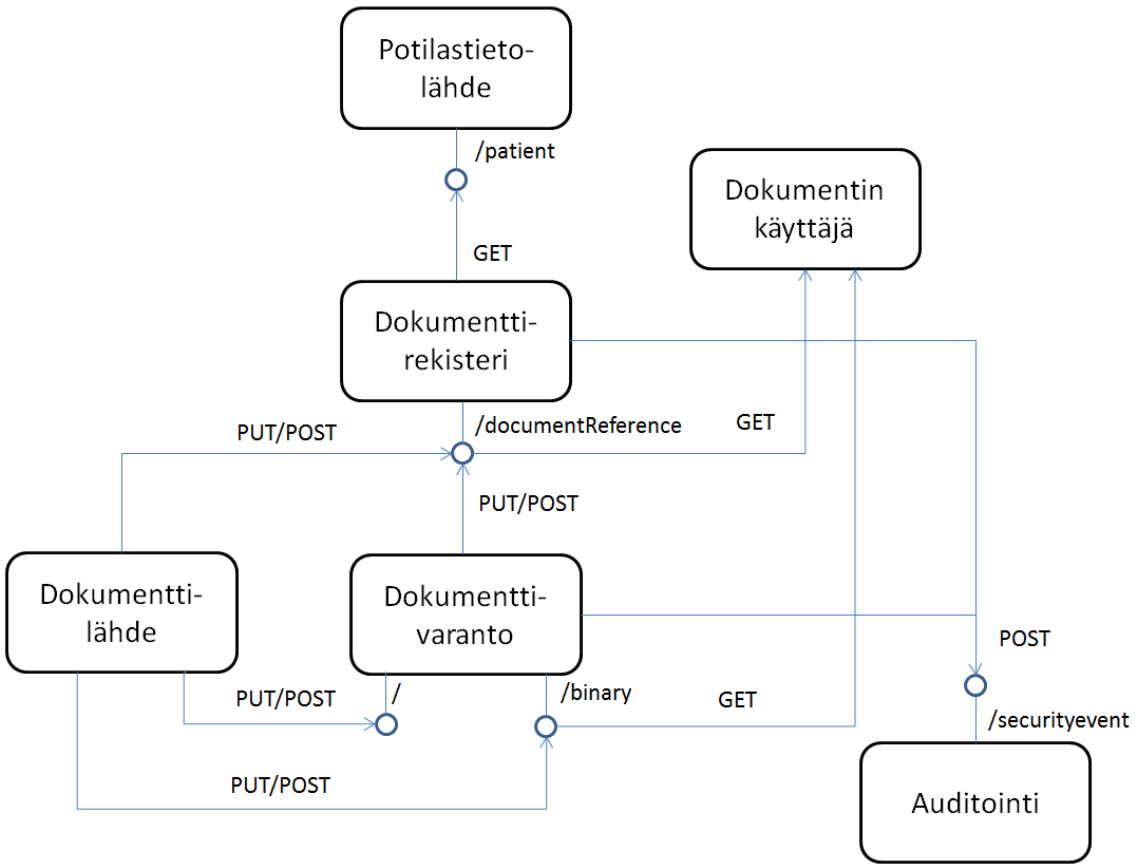
- Potilaan tai käyttäjän kirjautuminen ja tunnistaminen ulkoisen palvelun avulla (esimerkiksi OpenID, Facebook, Google).
- Tunnistautuminen soveltuvan OAuth-palvelimen avulla.
- Sähköiseen potilaskertomukseen liittyvä FHIR-palvelin, joka tukee haku- ja lukuoperaatioita, esimerkiksi potilasresursseihin, dokumenttiviittauksiin, havaintoihin, diagnooseihin ja lääkitykseen.
- Potilaskertomuksen määrittelemät lisätoiminnallisuudet. [49]

FHIR mahdollistaa myös IHE:n XDS-profiilia vastaavan toiminnallisuuden. XDS-profiilin toteutuksessa sitä voidaan käyttää olemassa olevan XDS.b-rajapinnan takana ja sen avulla voidaan tarjota esimerkiksi käyttöliittymä mobiililaitteita varten tai yhdistää dokumenttien jako muuhun FHIR-rajapinnan toiminnallisuuteen. Tässä asiayhteydessä käytettäviä resursseja ovat muun muassa:

- DocumentReference-viittaus, joka ilmoittaa dokumentin sijainnin järjestelmässä.
- XDS-profiili, joka kuvaa XDS-toteutuksen yksityiskohtia dokumenttiviittauksiin liittyen.
- Binäärituki, jonka avulla voidaan säilyttää binääridokumentteja FHIR-palvelimella.
- Potilas, terveydenhuollon ammattilainen ja organisaatio, sekä niiden tunnistaminen.
- SecurityEvent, jolla seurataan dokumenttirekisterin ja tietovaraston käyttöä. [49]

5.4 FHIR:n ja XDS:n yhteneväisyydet

FHIR:lla ja XDS-profiililla on yhteisiä piirteitä, kuten alla olevasta kuvasta 6.1 voi päätellä. Kuva perustuu alkuperäiseen lähteeseen [41]. Siinä on XDS-profiilin toimijoiden välille kuvattu FHIR:n resursseja ja päätepisteitä XDS-profiilin tapahtumien sijaan. Tässä ei ole kyse siitä, että FHIR voisi suoraan korvata XDS-profiilin, vaan FHIR:n käytön helppous voi sopivissa tilanteissa olla hyvin houkutteleva vaihtoehto natiiville XDS-profiilin käytölle. Sen sijaan erityisesti laajemmissa ympäristöissä natiivin XDS-profiilin rajapinnat voivat olla vaatimuksena onnistuneelle toteutukselle. [41]



Kuva 6.1. *FHIR ja XDS yhdistettynä samaan kuvaan [41].*

Yllä olevassa kuvassa 6.1 FHIR:n resursseilla on korvattu XDS:n tapahtumat, joista esimerkkinä seuraava tapahtuma:

- Dokumenttilähde toimittaa dokumentin ja sen metatiedot dokumenttivarannolle tapahtumana. Tästä esimerkkinä lääkityksen päivitys (medication update).
- Dokumenttivaranto päivittää dokumenttirekisterin tiedot lähettämällä resurssin dokumenttirekisterin DocumentReference-päätepisteeseen.
- Dokumentin käyttäjä etsii dokumentteja suorittamalla kyselyn dokumenttirekisterin DocumentReference-päätepisteelle ja vastaanottaa dokumentin GET-metodilla dokumenttivarannon /binary-päätepisteestä.

Tästä tapahtumasta tallennetaan auditointitieto SecurityEvent. [41]

5.5 FHIR:n nykytila

Syyskuussa 2013 julkaistut FHIR-määritykset annettiin laajempaan arvioon HL7-äänestyksen yhteydessä. Joulukuussa 2013 määrityksiä aloitettiin korjaamaan havaittujen tarpeiden mukaan. Samalla määritykset jaettiin kahteen versioon, syyskuussa julkaistu versio sekä kehittyvä versio. Kehittyvään versioon tehdään korjauksia havaittujen ongelmien perusteella sekä tätä versiota kehitetään edelleen. [49]

Syyskuusta 2012 lähtien on järjestetty Connectathon-testaustapahtumia FHIR-standardin toteutuksia varten. Nämä testaustapahtumat ovat luonteeltaan vastaavia, kuin IHE:n testaustapahtumat, niissä testataan ohjelmistokehittäjien tekemiä toteutuksia. Siitä huolimatta, että FHIR-standardin määritys on keskeneräinen, on sen kokeilukäyttö jo mahdollista. Aluksi kehityksen pääpainona on perusresurssien dokumentointi, sekä käytännön kokemusten ja esimerkkien hankkiminen. [49]

Tällä hetkellä julkaistu versio FHIR:stä on DSTU (First Draft Standard for Trial Use) ja HL7:n tavoitteena on julkaista uusia DSTU-versioita noin kahden vuoden välein, joissa esitellään uusia resursseja ja korjauksia edellisissä versioissa todettuihin virheisiin. FHIR:n normatiivinen versio on tavoitteena julkaista 2,5 vuoden sisällä. FHIR:n julkaisija haluaa mahdollisimman paljon kokemusta käytännön implementaatioista ennen kuin eri versioiden takaisinpäin yhteensopivuus voidaan julkaista virallisesti. [51]

Joulukuussa 2014 HL7 julkaisi Agronaut-projektin, jonka tarkoituksena on nopeuttaa FHIR-standardin kehitystä. Projekti lisää rahoitusta ja poliittista tahtoa julkaista FHIR-implementaatio-ohjeita ja profiileja kysely/vastaus- ja dokumenttien vastaanottoon toukokuuhun 2015 mennessä. [52]

5.6 FHIR:n hyödynnettävyys

FHIR:n kehittäjien mukaan standardia voidaan käyttää yleisesti muun muassa organisaation tai laitoksen sisäistä yhteensopivuutta varten, taustajärjestelmiin (esimerkiksi taloushallinto), alueelliseen terveystiedonsiirtoon (RHIO), kansallisiin terveystietojärjestelmiin, sosiaalista internetiä (terveys) varten ja mobiilisovelluksiin. Edellä mainituista kaksi viimeistä kohtaa, sosiaalinen internet ja mobiilisovellukset on arvioitu olevan todennäköisimpiä soveltamisalueita tulevaisuudessa. [49]

FHIR on toiminut myös muiden standardijärjestöjen kanssa yhteistyössä, joista syntyneitä tai syntyviä lopputuloksia ovat:

- IHE: Tutkimuksessa - FHIR for MHD (mobile XDS - Mobile Access to Health Documents).
- DICOM: Kiinnostusta - kuvien metatiedot RESTful-tyyppisesti.
- W3C: Semantic health group ja RDF, RIM-pohjainen semantiikan tarkistus.

Myös muiden standardijärjestöjen kanssa tapahtuva yhteistyö on mahdollista. Suomessa todennäköisimpiä soveltamiskohteita ovat erilaiset mobiili- ja asiointipalvelut tai palveluhakemistot, joissa turvallisuusvaatimukset eivät ole kovin tiukkoja. [49]

6 PÄÄTELMÄT

Tässä luvussa kootaan yhteen tämän diplomityön tutkimusten lopputulokset. IHE-profiilien käyttökelpoisuuden arviointi, avoimen lähdekoodin toteutusten esittely sekä FHIR-standardin mahdollisuudet käsitellään kukin omissa kohdissaan.

Sähköisten potilastietojärjestelmien tulevaisuus on tällä hetkellä muutoksen alla. Erilaisia järjestelmiä on lukemattomia määriä ja niissä pyritään koko ajan pääsemään yhtenäiseen, keskenään kommunikoivaan rakenteeseen. Tämän lisäksi potilashoidossa potilaan rooli kasvaa hoitoprosessissa. Potilas pyritään saamaan osallistumaan aktiivisemmin omaan hoitoprosessiinsa, esimerkiksi varaamaan aikaa sähköisesti, tutkimaan ja jakamaan omia tietojaan potilastietorekisterissä.

Muita mahdollisia tulevaisuuden käyttökohteita sähköisissä järjestelmissä voisivat olla esimerkiksi erilaiset potilasportaalit, missä on keskitetysti kaikki tarjolla oleva tieto näkyvissä potilaille sekä tähän mahdollisesti sisällytettyjä virtuaalisia yhteisöjä, esimerkiksi vertaistukea jotakin sairauksia sairastaville potilaille. Tällä tarkoitetaan siis eräänlaista hoitoyhteisöjen sisäistä, kliinisen tiedon sosiaalista mediaa.

Näiden lisäksi kaikki sähköisten potilastietojärjestelmien sisältämä tieto sekä niihin nykyisin tallennettava tieto tulisi pyrkiä hyödyntämään mahdollisimman tehokkaasti. Paine tämän asian edistämiseen kasvanee jatkuvasti, koska ns. big-data eli isojen tietomäärien louhiminen ja hyödyntäminen mahdollisimman tehokkaasti on koko ajan kasvattamassa suosiotaan. Tietomäärien tehokkaaseen hyödyntämiseen on myös terveydenhuollossa suuri tarve, esimerkiksi eri sairauksien tutkimuksessa, niin uusien kuin vanhojenkin.

6.1 IHE-profiilien käyttökelpoisuus

IHE:n julkaisemat profiilit ovat saavuttaneet viime vuosina jalansijaa maailmalla sähköisissä potilastietojärjestelmissä. Suomessa niiden hyödyntäminen ei ole tähän mennessä vielä saavuttanut laajaa käyttäjäkuntaa. Näin lähinnä siksi, koska IHE-profiilit laajenivat ensin Eurooppaan isoihin valtioihin ja nyt sitä kohtaan on ilmennyt mielenkiintoa myös Suomessa.

Tämän työn yksi tarkoitus oli tehdä tutkimusta IHE:n profiileista ja esitellä lopputuloksena niistä olennaisimmat tulevan tietopalvelun toiminnan kannalta. Keskeisiä profiileja löytyi useita ja lopputuloksena kaikista näistä keskeisistä profiileista on kirjoitettu esittelyt siinä laajuudessa, missä ne tulisi ottaa huomioon.

Koska SOAP-protokollan käyttö on melko kankeaa ja samaan aikaan vakaata, toimivat useimmat IHE:n profiilit myös vastaavalla tavalla. Suurin syy tälle on siinä, että ne perustuvat SOAP-protokollaan. Tietynlainen kankeus ilmeni muun muassa XDS-

profiilin sisältämissä kyselyissä. Tarkemmin sanottuna omien kyselyiden tuottaminen ei ole niin yksinkertaista kuin voisi kuvitella. Tämänhetkinen XDS-profiili tukee käytännössä vain etukäteen tallennettuja kyselyjä, eikä niitäkään voi itse täysin määritellä. Tallennettavat kyselyt perustuvat valmiisiin XDS-profiilin tarjoamiin parametreihin ja attribuutteihin. Aikaisemmissa versioissa oli mahdollista muokata kyselyitä vapaammin, mutta se ominaisuus on poistettu SQL-kyselyiden tekemiseen liittyvistä turvallisuussyistä.

XDS tulee XDS-I:n ohella olemaan keskeisin profiili IHE:n profiileja käytettäessä, joten pelkästään IHE:n profiileja hyödyntävää tietopalvelua ei voi täysin suositella. Medbit Oy:n tietotarpeista olennaisimpia ovat erityyppisten hakujen tekeminen dokumenttirekistereille ja -varannoille ja kyselyt tulisi olla hyvinkin yksilöllisiä esimerkiksi attribuuttien suhteen. Valmiina tarjotut attribuutit ja parametrit eivät näitä tarpeita pysty täysin kattamaan.

Näistä rajoitteista huolimatta IHE:n profiileissa on paljon sellaisia ominaisuuksia, jotka olisivat uutta tietopalvelua ajatellen käyttökelpoisia. Myös muun muassa FHIR:n ja XDS:n yhdistelmänä julkaistava seuraava versio MHD-profiilista vaikuttaa mielenkiintoiselta ja ehdottomasti harkinnan arvoiselta vaihtoehdolta.

6.2 Avoimen lähdekoodin toteutusten mahdollisuudet

Tämän diplomityön yhtenä tavoitteena oli kartoittaa tarjolla olevia avoimen lähdekoodin toteutuksia, jotka hyödyntävät IHE-profiileja. Näistä tärkeimpänä profiilitukena toteutuksilla tulisi olla XDS, jotta voidaan arvioida näiden toteutusten käyttökelpoisuutta tulevaisuudessa Medbit Oy:ssä käyttöönotettavassa järjestelmässä. Kuten edellä olleesta taulukosta 4.1 voidaan lukea, on lähes kaikki tutkitut avoimen lähdekoodin järjestelmät toteutettu Java-ohjelmointikielellä. Näistä järjestelmistä tekee poikkeuksen CodePlex, jonka toteutukseen on käytetty C#- ja .NET-kieliä. Järjestelmä toimii ainoastaan Windows-ympäristössä, koska kyseinen toteutus on avoimesta lähdekoodista huolimatta Microsoftin tekemä tuote. Se ei sisällä muuta toiminnallisuutta, kuin XDS- ja XDS-I -profiilien tuen.

Suurin osa käsitellyistä vapaan lähdekoodin toteutuksista on kehitetty 2010-luvun taitteessa, mutta niiden kehitystä ei ole jatkettu viimeisinä vuosina juurikaan. Yksiselitteistä syytä tähän ei löytynyt, mutta tarjolla olevien kaupallisten toteutusten (esimerkiksi InterSystems:n HealthShare-alusta) markkina-asema on varmasti osaltaan vaikuttanut avointen sovellutusten asemaan. Avoimista toteutuksista O3-XDS-niminen toteutus oli osa projektia, joka on jo päättynyt. Ilmeisesti tästä syystä toteutusta ei ole enää kehitetty eikä siitä ole enää verkkosivuja tai muuta dokumentaatiota tarjolla.

Näistä tarkastelluista toteutuksista parhaiten dokumentoitu ja edelleen kehitetty on IPF eli Open eHealth Integration Platform. Sille on myös listattu useita jo olemassa olevia käyttökohteita USA:ssa ja Euroopassa, joten löydettyjen tietojen perusteella tämä toteutus voisi olla harkitsemisen arvoinen vaihtoehto myös Medbit Oy:lle toteutettavan järjestelmän osaksi. Tätä järjestelmää tulisi tarkastella vielä tarkemmin, sekä pyrkiä

testaamaan sen toimintaa käytännössä, jotta voidaan varmistua sen käyttökelpoisuudesta Medbit Oy:n omiin tarkoituksiin ja tarpeisiin.

IPF:n versio on päivittynyt viimeksi vuonna 2013, jolloin otettiin käyttöön IPF 2.6. Tästä versiosta uusin versio vuoden 2015 alussa on 2.6.6. Tämän lisäksi IPF:n lähdekoodia päivitetään aktiivisesti, master branch -julkaisussa on tuoreimmat lähdekoodimuutokset suoritettu vuonna 2015.

Toinen harkitsemisen arvoinen vaihtoehto olisi CodePlex, joka on Microsoftin tekemä avoimen lähdekoodin toteutus. Tässä on melko rajatut ominaisuudet, mutta se on ohjelmoitu C#/.NET-kielillä, joten se sopisi helposti nykyiseen sovellusympäristöön. CodePlex:n selvä rajoite on sen rajalliset ominaisuudet, sillä siihen on toteutettu ainoastaan XDS-profiilin tuki. Näin ollen se vaatisi ympärilleen paljon työtä, jotta tuki muillekin tarvittaville profiileille olisi mahdollista.

Käytännön hyödyntämistä varten tulee erityisesti arvioida Medbit Oy:n tarpeet ja vähimmäisvaatimukset XDS-tekniikkaa käyttävälle sovellukselle, jotta voidaan tehdä luotettavaa vertailua tutkittujen avoimen lähdekoodin toteutusten ja mahdollisten kaupallisten tuotteiden väliltä. Tietopalvelussa käsiteltävien tietojen luonteen vuoksi tämä vertailu on erittäin tärkeää, esimerkiksi potilasturvallisuus ei saa vaarantua missään tilanteessa.

Avoimen lähdekoodin toteutusten kiistaton etu on niiden hinta. Toteutusten hyödyntäminen on ilmaista, koska lähdekoodi on avointa. Kaupallisella vastineella on yleensä suuri alkuinvestointi ja ylläpitoon liittyy yleensä myös lisäkustannuksia. Näiden vastapainona valmiilla tuotteella on myös toimivuustakuu sekä ylläpito ja päivitykset varmistettu. Valmiille kaupalliselle tuotteelle vastapainona avoimen lähdekoodin toteutukset on hyödynnettävissä vapaasti ilmaiseksi ja niitä voi kehittää vapaasti juuri oman käyttötarkoituksensa mukaan. Näin ollen avoimen lähdekoodin toteutuksen hyödyntämisessä on myös riskinsä, koska sen toimivuutta tuotantokäytössä ei ole tässä tietyssä käyttötarkoituksessa testattu.

Näistä tarkastelluista avoimen lähdekoodin toteutuksista ei todennäköisesti ole heti suoraan valmiuksia ainoaksi toteutukseksi Medbit Oy:n käyttöön, mutta yhdeksi osaksi isompaa kokonaisuutta olisi varmasti mahdollisuuksia. Tällaisessa käytössä toteutusta voisi käyttää niin sanottuna pilottihankkeena ja sen pohjalta arvioida sen laajentamista myös isompaan osaan tietopalvelua ja etenkin vastaanottavana osana nykyiselle REST-palvelulle.

6.3 FHIR-standardin mahdollisuudet

FHIR-standardi on lyhyestä historiastaan huolimatta sosiaali- ja terveydenhuollon sähköisten tietopalveluiden suosittu keskusteluaihe. Mielenkiinto FHIR-standardiin johtuu isolta osin sen uudesta, yksinkertaisesta lähestymistavasta. FHIR:n perustana olevat modernit verkkopalvelut helpottavat tietojärjestelmien välistä tiedonvaihtoa. FHIR:ssä ei ole välttämätöntä lähettää kokonaisia dokumentteja riippumatta tietotarpeista, vaan

näistä dokumenteista voidaan hakea jotakin tiettyjä, tarkkaan määriteltyjä dokumentin osia.

Nykyhetkellä tapahtuvassa sähköisen potilastietojärjestelmän tiedonhaussa esimerkiksi C-CDA-standardi on suunniteltu siten, että siinä siirretään kokonaisia dokumentteja tiedonhaussa. Se tarkoittaa sitä, että jos hoitohenkilökunnan tarvitsee etsiä jokin yksittäinen tieto, esimerkiksi siviilisääty, järjestelmä joutuu sen vuoksi hakemaan kokonaisia dokumentteja sen hakuehtona olleen tietyn tiedon sijaan. Tämä ei ole tehokas hakutapa ja se kuormittaa järjestelmää selkeästi enemmän, kuin FHIR-standardin mahdollistamat niin sanotut täsmähaut.

FHIR-standardia hyödyntävät järjestelmät nopeuttavat ja nostavat sähköisten potilastietojärjestelmien tehokkuutta. Tämä on mahdollista edellisissä kappaleissa mainitulla tietokeskeisellä lähestymistavalla dokumenttikeskeisen lähestymisen sijaan. Tietokeskeisessä lähestymistavassa apuna ovat API-ohjelmointirajapinnat ja FHIR-standardin tarjoama resurssipohjaisuus. Resurssit ovat hyvin yksinkertaisia rakenteisia tietoja.

Kiistaton FHIR:n etu on myös sen mahdollisuus kuluttajalähtöisyyteen. Tämä tarkoittaa sitä, että FHIR:n teknologiaa voidaan hyödyntää myös potilashoidossa potilastietojen kautta. FHIR mahdollistaa ohjelmistokehittäjille pääsyn potilastietoihin siten, että haetaan ainoastaan tarvittavia tietoja ilman, että kaikki potilaan tiedot paljastuisivat samalla kertaa. Tämä avaa ohjelmistokehittäjille mahdollisuuden kehittää uusia, innovatiivisia sovelluksia, jossa hyödynnetään sähköisten potilastietojärjestelmien sisältämää tietoa, ennen kaikkea näiden ominaisuuksien hyödyntämistä mobiiliympäristössä. Tässä auttaa omat API-ohjelmistorajapinnat ja niiden tarkasti hallinnoitavissa olevat säännöstöt siitä, mitä niiden kautta näkee ja mitä ei.

Aikaisemmin HL7 v2 oli yleisin käytössä oleva standardi kliinisen tiedon siirrossa sähköisissä potilastietojärjestelmissä. HL7 v2:sta on julkaistu ensimmäinen versio vuonna 1987 ja viimeisin päivitys siihen on tehty vuonna 2011. Pitkän kehityskaaren myötä standardin ominaisuuksien rajojen lähestyessä luonnollinen jatkumo olisi seuraava HL7 v3 -standardi. HL7 v3:n versio julkiseen käyttöön julkaistiin vuonna 2005, mutta versiota luonnehditaan monimutkaiseksi ja sitä käyttävistä järjestelmistä tulee raskaita. Tämän lisäksi järjestelmien kehittäminen ja ylläpito on kalliimpaa. Pääosin näistä syistä HL7 v3 ei saavuttanut heti julkaisunsa jälkeen suurta suosiota, vaan sanomanvälityksenä käytettiin mahdollisuuksien mukaan mieluummin HL7 v2:ta sen yksinkertaisemman rakenteen vuoksi.

Tähän tilanteeseen FHIR-standardi on tehty tarjoamaan uuden vaihtoehdon. FHIR:n on sanottu yhdistävän HL7-standardin eri versioiden hyvät puolet sekä olemaan samalla myös helpommin omaksuttava kuin HL7 v3. FHIR:n etuna on myös se, ettei se vaadi niinkään erikoisosaamista terveydenhuollosta, vaan se perustuu HTTP-protokollaan, mikä on tuttu käytännössä kaikille ohjelmistoalan ammattilaisille.

6.4 Jatkokehitys

Diplomityötä varten suoritetut tutkimukset perustuvat teoriapohjaiseen tietoon edellä mainituista tutkimuskohteista, tietoa on hankittu pääosin verkosta löytyvästä materiaalista. Teoriapohjaisuudesta johtuen havaittuja tietoja ja lopputuloksia ei ole todennettu käytännössä esimerkiksi IHE-profiilien ja FHIR-standardin käytöstä tai avoimen lähdekoodin toteutuksien toiminnasta.

Näiden päätelmien todentaminen käytännössä tulisi kuitenkin ottaa huomioon seuraavana vaiheena ennen mahdollista käyttöönottoa. Diplomityön aihepiirin laajuudesta johtuen käytännön testejä ei pystytty mahduttamaan järkevästi työn lopulliseen sisältöön.

LÄHTEET

[1] Keso E. 2013. Onnistunut eResepti-hanke pohjana sähköiseen arkistoon siirtymisessä. [WWW]. [Viitattu 16.7.2014]. Saatavissa: http://atk-paivat.fi/2013/2013-05-28-03-04-keso.pdf

[2] Sosiaali- ja terveysministeriön asetus potilasasiakirjoista. A 298/2009, 2009. Saatavissa: http://www.finlex.fi/fi/laki/alkup/2009/20090298

[3] Pihlajaniemi J. 2012. REST-pohjaisen web-rajapinnan kehittäminen. Insinöörityö (AMK). Helsinki. Metropolia Ammattikorkeakoulu, tietotekniikan koulutusohjelma. 38 s. Saatavissa: http://www.theseus.fi/bitstream/handle/10024/43246/Pihlajaniemi_Jarmo.pdf

[4] Mueller J. 2013. Understanding SOAP and REST Basics. [WWW]. [Viitattu 5.3.2015]. Saatavissa: http://blog.smartbear.com/apis/understanding-soap-and-rest-basics/

[5] Wikipedia. Integrating the Healthcare Enterprise. [WWW]. [Viitattu 22.7.2014]. Saatavissa: http://en.wikipedia.org/wiki/Integrating_the_Healthcare_Enterprise

[6] National/Regional Deployment Committees. [WWW]. [Viitattu 30.7.2014]. Saatavissa: http://www.ihe.net/Governance/

[7] Integrating the Healthcare Enterprise. 2013. Engaging HIT Stakeholders in a Proven Process. [WWW]. [Viitattu 24.7.2014]. Saatavissa: http://www.ihe.net/IHE_Process/

[8] Integrating the Healthcare Enterprise. 2013. IHE IT Infrastructure. [WWW]. [Viitattu 12.9.2014]. Saatavissa: http://www.ihe.net/IT_Infrastructure/

[9] InterSystems Corporation. IHE Integration Statement & Certification. [WWW]. [Viitattu 12.9.2014]. Saatavissa: http://www.intersystems.com/our-products/healthshare/ihe-integration-statement-certification/

[10] Morrissey J. 2014. IHE Profiles and Certification Drive Interoperability. [WWW]. [Viitattu 23.7.2014]. Saatavissa: https://www.icsalabs.com/sites/default/files/WP15863.a.IHE%20Profiles%20and%20Certif%20Drive%20Interop.pdf

[11] IHE USA & ICSA Labs. 2013. IHE USA Certification Flyer. [WWW]. [Viitattu 23.7.2014]. Saatavissa: http://www.iheusa.org/docs/IHEUSAcertificationflyer_Final-01-2014.pdf

[12] Integrating the Healthcare Enterprise. 2013. IHE IT Infrastructure (ITI) Technical Framework Volume 1 (ITI TF-1) Integration Profiles. Revision 10.1. [WWW]. [Viitattu 16.7.2014]. Saatavissa: http://www.ihe.net/technical_frameworks/

[13] IHE Wiki. 2008. XDS-FAQ. [WWW]. [Viitattu 28.8.2014]. Saatavissa: http://ihewiki.wustl.edu/wiki/index.php/XDS-FAQ

[14] Hay D. 2013. FHIR and the Ambulance: Notification of XDS Documents. [WWW]. [Viitattu 31.7.2014]. Saatavissa: http://fhirblog.com/2013/12/06/fhir-and-the-ambulance-notification-of-xds-documents/

[15] Integrating the Healthcare Enterprise. 2013. IHE IT Infrastructure (ITI) Technical Framework Volume 2b (ITI TF-2b) Transactions Part B - Sections 3.29-3.64. Revision 10. [WWW]. [Viitattu 16.7.2014]. Saatavissa: http://www.ihe.net/technical_frameworks/

[16] IHE Wiki. 2011. Notes on XDS Profile. [WWW]. [Viitattu 24.9.2014]. Saatavissa: http://ihewiki.wustl.edu/wiki/index.php/Notes_on_XDS_Profile

[17] Integrating the Healthcare Enterprise. 2013. IHE IT Infrastructure (ITI) Technical Framework Volume 2a (ITI TF-2a) Transactions Part A - Sections 3.1-3.28. Revision 10.0. [WWW]. [Viitattu 16.7.2014]. Saatavissa: http://www.ihe.net/technical_frameworks/

[18] ebXML Registry Services and Protocols Version 3.0. OASIS Standard, 2 May, 2005. [WWW]. [Viitattu 4.3.2015]. Saatavissa: http://docs.oasis-open.org/regrep/regrep-rs/v3.0/regrep-rs-3.0-os.pdf

[19] Integrating the Healthcare Enterprise. 2007. IHE IT Infrastructure (ITI) Technical Framework Supplement 2007-2008. Registry Stored Query Transaction for XDS Profile (ITI-18). Trial Implementation Version. [WWW]. [Viitattu 16.12.2015]. Saatavissa: http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Supplement_XDS_Stored_Query_TI_2007_08_20-2.pdf

[20] Tilapäinen yksilöintitunniste sosiaali- ja terveydenhuollossa Versio 0.92. Esiselvitys 4/2014. [WWW]. [Viitattu 4.3.2015]. Saatavissa: http://www.thl.fi/attachments/oper/Lausuntopyynt%C3%B6_Tilap%20yksil%20tunniste_Esiselvitys%20luonnos%20v%200%2092_2014.pdf

[21] Henkilötietolaki. L 22.4.1999/523, 1999. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

[22] Health Level Seven. 1999. HL7 Messaging Standard, Version 2.3.1. [WWW]. [Viitattu 24.9.2014]. Saatavissa: http://www.pacs.hk/Doc/HL7/Hl7V231.pdf

[23] Integrating the Healthcare Enterprise. 2013. IHE IT Infrastructure (ITI) Technical Framework Volume 2x (ITI TF-2x). Volume 2 Appendices. Revision 10.0. [WWW]. [Viitattu 16.7.2014]. Saatavissa: http://www.ihe.net/technical_frameworks/

[24] Integrating the Healthcare Enterprise. 2013. IHE Radiology (RAD) Technical Framework Volume 1 (IHE RAD TF-1) Integration Profiles. Revision 12.0. [WWW]. [Viitattu 22.7.2014]. Saatavissa: http://www.ihe.net/technical_frameworks/

[25] IHE Wiki. 2013. Cross-enterprise Document Sharing for Imaging. [WWW]. [Viitattu 4.8.2014]. Saatavissa: wiki.ihe.net/index.php?title=Cross-enterprise_Document_Sharing_for_Imaging

[26] Koivu F. 2012. Cross-enterprise Document Sharing (XDS)- ja Cross-enterprise Document Sharing for Imaging (XDS-I) -integraatioprofiilit ja niiden hyödyntäminen Suomessa. Opinnäytetyö (AMK). Turku. Turun ammattikorkeakoulu, tietotekniikan koulutusohjelma. 125 s.

[27] Integrating the Healthcare Enterprise. 2013. IHE Radiology (RAD) Technical Framework Volume 2 (IHE RAD TF-2) Transactions. Revision 12.0. [WWW]. [Viitattu 16.7.2014]. Saatavissa: http://www.ihe.net/technical_frameworks/

[28] Software Programming for Medical Applications. [WWW]. [Viitattu 5.8.2014]. Saatavissa: http://dicomiseasy.blogspot.fi/2012/02/c-move.html

[29] Integrating the Healthcare Enterprise. 2013. IHE Radiology (RAD) Technical Framework Volume 3 (IHE RAD TF-3) Transactions (continued). Revision 12.0. [WWW]. [Viitattu 16.7.2014]. Saatavissa: http://www.ihe.net/technical_frameworks/

[30] Digital Imaging and Communications in Medicine (DICOM). Part 16: Content Mapping Resource. [WWW]. [Viitattu 4.3.2015]. Saatavissa: http://medical.nema.org/Dicom/2011/11_16pu.pdf

[31] Mills D.L. 1992. Network Time Protocol (Version 3) Specification, Implementation and Analysis. RFC 1305. IETF. Saatavissa: http://tools.ietf.org/pdf/rfc1305.pdf

[32] Harjula K., Koskivirta M. Turku 2015. Tekninen määrittely - Tietoaltaan REST-rajapinta. Medbit Oy. Julkaisematon määrittelydokumentti. 16 s.

[33] Cooper, et al. 2008. PKIX Certificate and CRL Profile. RFC 5280. IETF. Saatavissa: http://tools.ietf.org/pdf/rfc5280

[34] Health Information Privacy Law and Policy. [WWW]. [Viitattu 5.3.2015]. Saatavissa: http://healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange/health-information-privacy-law-policy#specific-legal-requirements

[35] Määrittelyt Potilastiedon arkistolle. 2015. [WWW]. [Viitattu 10.2.2015]. Saatavissa: http://www.kanta.fi/web/ammattilaisille/potilastiedon-arkiston-kayttonoton-kasikirja

[36] Minimikontekstihallinnan määrittely. Versio 3.0. 2006. [WWW]. [Viitattu 12.2.2015]. Saatavissa: http://www.kanta.fi/documents/3430315/0/kh_v3.doc

[37] Standards for health information systems: CCOW - Clinical Context Object Workgroup [WWW]. [Viitattu 8.8.2014]. Saatavissa: http://www.openclinical.org/std_ccow.html

[38] OrionHealth. CCOW Information: For the healthcare industry. [WWW]. [Viitattu 8.8.2014]. Saatavissa: http://www.ccow-info.net/

[39] Lead Technologies Inc. Context Agents. [WWW]. [Viitattu 8.8.2014]. Saatavissa: http://www.leadtools.com/help/leadtools/v18/dh/to/leadtools.topics.ccow~cw.topics.contextagents.html

[40] IHE Wiki. 2013. Asynchronous Messaging. [WWW]. [Viitattu 15.8.2014]. Saatavissa: wiki.ihe.net/index.php?title=Asynchronous_Messaging

[41] Hay D. 2013. FHIR and XDS – an Overview. [WWW]. [Viitattu 6.3.2015]. Saatavissa: http://fhirblog.com/2013/11/05/fhir-and-xds-an-overview/

[42] IHE Wiki. 2014. Mobile access to Health Documents (MHD). [WWW.] [Viitattu 19.2.2015]. Saatavissa: http://wiki.ihe.net/index.php?title=Mobile_access_to_Health_Documents_%28MHD%29

[43] Integrating the Healthcare Enterprise. 2014. IHE IT Infrastructure Technical Framework Supplement, Mobile access to Health Documents (MHD). Trial Implementation. [WWW]. [Viitattu 19.2.2015]. http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_MHD.pdf

[44] Health Information Exchange Open Source (HIEOS). [WWW]. [Viitattu 1.9.2014]. Saatavissa: http://sourceforge.net/p/hieos/

[45] Alves B. & Schumacher M. 2011. IHE Profiles Open-source and/or Free Implementations. [WWW]. [Viitattu 16.7.2014]. Saatavissa: http://publications.hevs.ch/index.php/attachments/single/328

[46] Microsoft Corporation. 2008. Whitepaper: Microsoft IHE XDS.b Reference Implementation. Introduction to Developing Document Source and Document Consumer Actors. [WWW]. [Viitattu 26.8.2014]. Saatavissa: http://www.microsoft.com/en-us/download/details.aspx?id=10850

[47] Microsoft Developer Network. What Is Windows Communication Foundation. [WWW]. [Viitattu 27.8.2014]. Saatavissa: http://msdn.microsoft.com/en-us/library/ms731082%28v=vs.110%29.aspx

[48] XDS.b Document Registry and Document Repository Solution Accelerator. 2012. January 2012 Release. [WWW]. [Viitattu 26.8.2014]. Saatavissa: http://ihe.codeplex.com/releases/view/81518

[49] Suhonen, et al. 2013. Fast Health Interoperability Resources - FHIR-standardin kuvaus ja arviointi. Versio 1.0. [WWW]. [Viitattu 6.3.2015]. Saatavissa http://www.hl7.fi/wp-content/uploads/FHIR-HL7fi-2013.pdf

[50] FHIR Resource Definitions. 2014. FHIR DSTU (v0.0.82.2943). [WWW]. [Viitattu 6.3.2015]. Saatavissa: http://www.hl7.org/implement/standards/fhir/resources.html

[51] Baltus M. 2015. HL7 FHIR Training Course. Afternoon slides, training course material. 70 p.

[52] Health Level Seven. 2014. HL7 Launches Joint Argonaut Project to Advance FHIR. [WWW]. [Viitattu 24.2.2015]. Saatavissa: http://www.hl7.org/documentcenter/public_temp_54B57D7B-1C23-BA17-0C6EEED16DABD85B/pressreleases/HL7_PRESS_20141204.pdf