



Luottamus. Tietoturva. Sähköiset palvelut.

LUOTI-julkaisuja 1/2006

INDICA2

Luotettavien ja turvallisten
yhteisöviestintäpalvelujen kehittäminen

LUOTI-pilottihanke
Loppuraportti

Sisällysluettelo

Termit ja lyhenteet	4
Tiivistelmä	5
1. Yleistä	6
1.1. Projektin kohde	6
1.2. Projektin tavoitteet ja rajaukset	6
1.3. Projektin menetelmät	7
2. Yhteisöviestintäkonsepti	8
2.1. Tausta	8
2.2. Yhteisöviestintäalusta	9
2.3. Yhteisöviestintäalustan käyttö	10
3. INDICA2	12
3.1. Hankekuvaus	12
3.2. Case – Uusi Kiss	13
3.3. Digitaalinen mobiilitelevisio, DVB-H	13
4. Tietoturvaongelmat palvelukehitysprosessissa	15
4.1. Liiketoimintaprosessien kuvaaminen	15
4.1.1. Havainnot liiketoimintaprosessien mallintamisesta ja kuvaamisesta	15
4.2. Riski- ja kontrolli-workshopit	16
4.2.1. Havainnot riski- ja kontrolli-workshopeista	17
4.3. Merkittävimmät esille tulleet tietoturvakysymykset	17
5. Tietoturvan ratkaiseminen tuotantoketjussa	22
5.1. Esimerkki vastuunjakomallista	23
6. Tietoturvaa koskevat menetelmät ja toimintatavat	24
6.1. Menetelmät ja toimintatavat palvelukehitysprosessissa	24
6.2. Käyttäjien tunnistaminen	24
6.3. Mobiilikansalaisvarmenne, sähköinen allekirjoitus ja tunnistaminen	25
7. Johtopäätökset	26

Termit ja lyhenteet

Creative Commons	Lisenssijärjestelmä, jonka avulla teosten julkaiseminen verkossa helpottuu siten, että muut tietävät, mitä niillä saa tehdä. Käyttämällä Creative Commons –lisenssiä säilyy tekijänoikeus teoksen tekijällä. Lisenssi sallii muiden kopioida ja levittää teosta, kunhan he antavat kunnian sen tekijälle ja noudattavat muita teoksen käytölle määriteltyjä ehtoja. Creative Commons –lisenssillä tekijä luopuu osasta teokseen kohdistuvia tekijänoikeuksiaan ja antaa haluamansa vapaudet teoksen käyttäjälle, katsojalle tai kokijalle. Erilaisilla lisenssityypeillä voidaan antaa muiden kopioida, jaella, näyttää, esittää ja muokata teosta sekä kaupallisessa että ei-kaupallisessa käytössä, jos he mainitsevat alkuperäisen tekijän nimen. Erilaisilla lisensseillä voidaan myös kieltää muokattujen versioiden tekemistä teoksesta.
INDICA2	Hanke, jossa kehitettiin mediayrityksille ja –yhteisöille jakelualusta digitaalisen median julkaisuun.
DVB-T	Maanpäällinen digi-tv.
DVB-H	Maanpäällisen digi-tv:n mobiiliversio.
3G	Matkapuhelintekniikan kolmas sukupolvi.
Visual Radio	Mobiililaitteissa toimiva näköradio; radiolähetys, johon on synkronoitu interaktiivista sisältöä.
GPRS	Matkapuhelintekniikan toisen sukupolven (GSM) tapa lähettää ja vastaanottaa dataa pakettikytkentäisesti.
Broadcasting	Yleislähetys, jossa lähetetty tieto saavuttaa useampia vastaanottajia yhdellä lähetyksellä. Käytetään esimerkiksi televisio- tai radiolähetyksissä.
Prepaid	Ennakkoon maksettu (anonyymi) matkapuhelinliittymä.
Audit-trail	Kirjausketju, tapahtumaketjun jäljitettävyyden ja todennettavuus.
DRM	Digitaalinen oikeuksien hallinta. Tekniikka, jolla estetään tai rajoitetaan kopioiden tekemistä, sisällön katselukertoja tai katselutapaa.
Phishing	Henkilötietojen tai muun arkaluonteisen tiedon kalastelu sähköpostiviesteillä, puhelimitse tai väärennetyillä verkkosivuilla rikollisiin tarkoituksiin.
PKI	Julkisen avaimen infrastruktuuri, salauksessa käytetty menetelmä, jossa luottamus perustuu kolmannen osapuolen varmennukseen toimijoiden henkilöllisyydestä.
Mobiilivarmenne	Tunnistautumis- ja allekirjoitusväline mobiililaitteisiin.
Vahva tunnistaminen	Tunnistusmenetelmä, jossa käyttäjät tunnistetaan käyttäjätunnus/salasana- paria tehokkaammalla tavalla, esimerkiksi biometriset menetelmät tai mobiilivarmenne.

Tiivistelmä

LUOTI on liikenne- ja viestintäministeriön tietoturvaohjelma vuosille 2005–2006. Sen tavoitteena on uusien sähköisten palvelujen tietoturvan kehittäminen. Ohjelmassa edistetään käytännön hankkeiden avulla uusia toimintamalleja, joissa tietoturva otetaan sähköisiin palveluihin mukaan jo niiden kehittämisen alkuvaiheessa. Ohjelman välillisenä tavoitteena on kuluttajien luottamuksen lisääminen uusiin sähköisiin palveluihin.

LUOTI-ohjelma valitsi ensimmäiset pilottihankkeensa vuoden 2005 loppupuolella. Monen toimijan välisillä viihdepalveluhankkeilla oli mahdollisuus hakea hankehaun kautta tietoturva-asiantuntijaa hankkeisiin ohjelman asiantuntijapoolista. Elisa ja SBS Finland Oy hakivat yhteiseen INDICA2-mobiili-tv-palvelukehityshankkeeseen ohjelman tarjoamaa asiantuntijapalvelua. Asiantuntijaksi valittiin KPMG Oy Ab.

INDICA2-hankkeessa kehitettiin uusia mobiili-tv sekä visual radio -tyyppisiä palveluja ja konsepteja sekä selvitettiin näihin liittyviä liiketoimintamalleja. INDICA2:n tavoitteena oli muun muassa kehittää uuden teknologian mahdollistamia, yhteisöjen sisäistä vuorovaikutusta ja viestintää tukevia palveluja.

LUOTI-ohjelman asiantuntijapalvelun tuloksena voidaan sanoa, että liiketoiminta-prosessin mallintaminen tuotekehitysprojektin alussa on haastavaa, mutta tietoturvallisuuden kannalta erityisen tärkeää. Liiketoimintaprosessikuvaukset osaltaan ohjaavat tuotettavan teknologian kehitystä ja toimivat siten myös tietoturvaratkaisujen perustana.

Pilottihankkeen kaltaisissa yhteisöviestinnällisissä palveluissa on paljon tekijänoikeuksiin ja eri toimijoiden vastuisiin liittyviä kysymyksiä. Näiden ratkaiseminen teknisesti ja sopimuksilla on tärkeää, jotta ne eivät muodostu esteeksi palvelun käytölle. Koska yhteisöviestintäpalvelut ovat kovaa vauhtia yleistymässä, nähdään näiden tekijänoikeuksiin ja eri toimijoiden vastuisiin liittyvien kysymysten työstäminen yleisissäkin foorumeissa palvelujen käyttöönottoa ja yleistymistä edistävänä toimenpiteenä.

Uusien tuotteiden kehityksessä tietoturvallisuudella on suuri merkitys, mutta samaan aikaan on varmistettava palvelun käytettävyys. Käytettävyys on yksi tärkeimmistä tekijöistä palvelun tai tuotteen yleistymisen kannalta.

Loppuraportin ovat laatineet Mika Laaksonen, Matti Järvinen ja Mika Iivari KPMG Oy Ab:stä. Kappaleen 2 kirjoittamisesta on vastannut Jonas Kronlund Elisa Oyj:n tutkimusyhteistyöyksiköstä.

1. Yleistä

INDICA2-hankkeessa on ollut tarkoituksena kehittää innovatiivisia mobiili-tv-palveluja ja selvittää niihin liittyviä liiketoimintamalleja. Tekniikkana hankkeessa on käytetty maanpäällisen digi-tv:n mobiililaitteisiin jatkokehitettyä versiota, DVB-H:ta. Tavoitteena on ollut kehittää muun muassa uuden teknologian mahdollistamia, yhteisöjen sisäistä vuorovaikutusta ja viestintää tukevia palveluja. Käytännössä tämänkaltaisten palvelujen avulla kuluttajat ja yhteisöjen jäsenet voivat itse vaikuttaa jaeltavan lähetyksen sisältöön tuottamalla ja jakelemalla sisältöä omatoimisesti. Interaktiivisen mobiilitelevision ja tämän mahdollistamien palvelujen kehityksessä on kuitenkin vielä paljon tietoturvan ja tekijänoikeuksien kannalta huomioitavia asioita. Tuotettaessa materiaalia yleiseen lähetykseen pitää kiinnittää huomiota lähetettävän tiedon oikeellisuuteen ja lainmukaisuuteen. Myös käyttäjien tunnistus asettaa haasteita palvelun toiminnalle, samoin kuin palvelun suojaaminen erilaisilta luottamuksellisen tiedon väärinkäytöksiltä. Vaikka palveluun liittyy riskejä, on se kuitenkin mahdollista toteuttaa turvallisesti varautumalla tietoturvakysymyksiin jo suunnitteluvaiheessa.

1.1. Projektin kohde

Projekti on osa liikenne- ja viestintäministeriön LUOTI-ohjelmaa. Tässä projektissa keskitytään LUOTI-ohjelman tavoitteissa määriteltyjen tekijöiden (ks. luku 1.2.) kartoittamiseen, analysointiin ja dokumentointiin.

Projektin kohteena oli Elisan ja SBS Finlandin INDICA2-hanke ja erityisesti siihen liittyvät tietoturvanäkökohdat. Case-esimerkkinä projektissa käytettiin Uusi Kiss -radiokanavan kautta tarjottavia mobiilipalveluja, joskin hankkeen aikana tarkasteltiin koko jakelualustan toimintaa laajemminkin.

1.2. Projektin tavoitteet ja rajaukset

LUOTI-ohjelman tarkoituksena on edistää käytännön hankkeiden avulla toimintamalleja, joissa tietoturva otetaan entistä paremmin mukaan sähköisten palvelujen kehittämiseen jo palvelujen kehittämisen alkuvaiheessa. INDICA2 ja sen case-esimerkki Uusi Kiss on LUOTI-ohjelman ensimmäinen pilottihanke.

Tavoitteena on auttaa Elisaa ja SBS Finlandia kehittämään luotettavaa, tietoturvallista ja käyttäjille helppokäyttöistä mobiilipalvelua sekä tuottaa LUOTI-ohjelmalle materiaalia, jonka avulla se voi edistää tietoturvallisuuden huomioimista uuden teknologian käyttöönotossa. Erityisesti projektin tavoitteena oli:

- Arvioida INDICA2-hankkeeseen liittyviä tietoturvariskejä huomioiden käytetyt teknologiat sekä liiketoimintaprosessit.
- Etsiä mahdollisten uusien tietoturvariskien ratkaisukeinoja.

- Määrittää tietoturva-vaatimukset palvelun kaupallistamiseksi (Case Uusi Kiss).
- Dokumentoida arviointien tulokset ja toimintamallit uusien tietoturvariskien vähentämiseksi.

Projektissa ei suoritettu palvelualustan tietoturvallisuuden teknistä testaamista, koska hankkeen omistaja, Elisa, ei nähnyt tarpeelliseksi prototyyppeillä olevan järjestelmän testaamista.

1.3. Projektin menetelmät

Projekti ja sen dokumentointi toteutettiin:

- Haastattelemalla INDICA2-hankkeen toteutuksen kannalta keskeiset henkilöt
 - Jonas Kronlund, Elisa ja
 - Henrik Laine, SBS Finland.
- Mallintamalla case-esimerkkinä olevan palvelun liiketoimintaprosessit.
- Järjestämällä riskien ja kontrollitoimenpiteiden tunnistamiseen tähtäävä workshop ja tätä täydentävä LUOTI-asiiantuntijapoolin workshop.
- Käymällä läpi INDICA2-hankkeeseen ja käytettyyn tekniikkaan liittyvää dokumentaatiota.

Havainnot analysoitiin KPMG:n menetelmiä hyväksikäyttäen. Projekti dokumentoitiin asiakkaan kanssa solmitun sopimuksen mukaisesti.

2. Yhteisöviestintäkonsepti

Tässä luvussa on kuvattu INDICA2-hankkeessa kehitettävien palvelujen yleisperiaatteita kuvaamalla yhteisöviestintäkonseptia. Yhteisöviestintäpalveluilla tarkoitetaan tässä tapauksessa erilaisille käyttäjäryhmille (yhteisöille) suunnattuja interaktiivisia mobiilipalveluja, joiden avulla käyttäjillä on mahdollisuus jakaa ja jalostaa itse tuotettua sisältöä.

2.1. Tausta

Matkapuhelimia ja niihin liittyviä uusia mahdollisuuksia käsitellään Suomessa usein teknologiavetoisesti unohtaen sisällöntuotantopuoli. YLE:n Mikael Jungner on todennut, että mobiilimediabisnes saadaan tuottamaan viipaloimalla tarjontaa pienillekin kohderyhmille ja tiivistämällä kännykälle tarjottavat tv-ohjelmat murto-osaan perinteisestä kestostaan.

Tällä hetkellä mobiilipuolella ei kuitenkaan löydy sisällöntuottajille helposti omaksuttavia ja edullisia palvelu-, testi- ja levitysympäristöjä. Niiden saatavuus edistäisi kuitenkin innovatiivisten sisältöjen ja palvelujen syntymistä ja varsinkin kulttuurisektorin tietoyhteiskuntavalmiuksien kehittämistä. Kutsukaamme tätä konseptia jatkossa *yhteisöviestinnän monikanavaiseksi palvelualustaksi*.

Myös kaupallisin perustein toimivat yritykset voivat hyötyä tällaisesta palvelualustasta. Tavoitteena voi sekä yhteisöjen että yritysten osalta olla toiminnan tukeminen ja tehostaminen, mutta miksei myös loppukäyttäjälle suunnattu kaupallinen toiminta. Alla esitellään muutama esimerkki tästä (Taulukko 1).

Yhteisöjen toiminnan tukeminen	Yritysten toiminnan tehostaminen	Yritysten kaupalliset palvelut
Festivaalit, esim. ISEA	Asiakasseminaarit	Kanavariippumattomat palvelut
Julkiset infopalvelut	Johdon esiintymiset	Kauppapaikat
Mediakeskukset, esim. LUME	Mainokset	Lisäarvopalvelut eri kanavassa
Mediayhteisöt, esim. Pixoff	Markkinointitapahtumat	Maksulliset ohjelmat
Oppilaitokset	Messut	Ohjelmalataukset
Seurakunnat	Osavuositarkastukset	Vuorovaikutteiset mainokset
Vähemmistöryhmät	Tuotelanseeraukset	Vuorovaikutteiset pelit

Taulukko 1. Esimerkkejä monikanavaisen palvelualustan asiakkaista ja niiden tarpeista

Internet-maailmassa löytyy useita sekä kaupallisia että ei-kaupallisia tahoja, jotka www-sivustonsa kautta tarjoavat videoiden julkaisutavan pienille toimijoille, esimerkiksi suomalainen Pixoff-yhteisö. Tämän lisäksi on myös kehitetty vapaata sisällönjakelua tukevia tekijänoikeusehtoja, esimerkiksi *Creative Commons* -lisenssi.

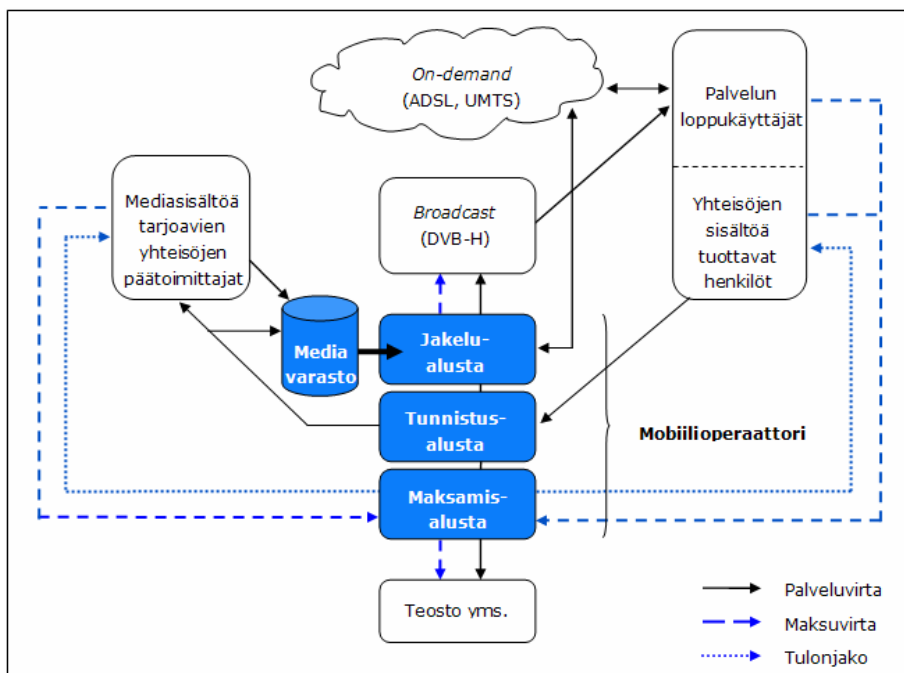
Vahva trendi maailmanlaajuisesti on, että palvelujen loppukäyttäjistä tulee sisällöntuottajia. Kokonainen videostudio voidaan rakentaa kannettavalla tietokoneella ja digitaalisella videokameralla ja sen käyttäjä voi langattomalla laajakaistayhteydellä toimia melkein täysin ajasta ja paikasta riippumatta. Kamerapuhelinten ympärille rakennetut palvelut ovat madaltaneet vielä enemmän sisällöntuotannon kynnyksiä, esim. Cell Journalist, OVAO, Scoopt, Spy Media jne.

Kiinnostusta julkaista omaa videosisältöä ja erityyppisiä ratkaisuja sitä varten löytyy siis Suomesta, mutta ei vielä tahoa, joka tarjoaisi tätä luotettavasti, kustannustehokkaasti ja monikanavaisesti.

2.2. Yhteisöviestintäalusta

Digita Oy:n Estradi-nimisessä kehitysprojektissa oli tarkoituksena tarjota yhteisöille mahdollisuus hyödyntää DVB-T-verkon vapaata kapasiteettia. Rekisteröityneet pilotti-asiakkaat toimittivat sisältöään DVD-levyillä ja varasivat ohjelma-aikaa www-käyttöliittymän kautta. Pilottiasiakkaiden laskutus tapahtui esim. pankkisiirtomaksulla ja tunnistauminen sisällöntoimituksen yhteydessä koodilla. Digita myi kuitenkin kaiken DVB-T-kapasiteetin kaupallisille toimijoille ja Estradi-palvelu jäi siksi pilottitasolle. Estradi oli Digitalille siinä mielessä ongelmallinen, että kyseinen yritys ei voi tarjota palveluja yksityishenkilöille eikä toimia sisältötoimialalla.

Luonnollinen tämänkaltaisen palvelun tarjoaja olisi mobiilioperaattori, joka pystyy tarjoamaan paremmin yksityishenkilöillekin tarvittavia laskutus- ja vahvoja tunnistaumisen ratkaisuja omassa samankaltaisessa palvelussa. Tätä palvelualustakonseptia kuvataan alla (Kuva 1).



Kuva 1. Yhteisöviestintäalustan mahdollistamia ansaintamalleja

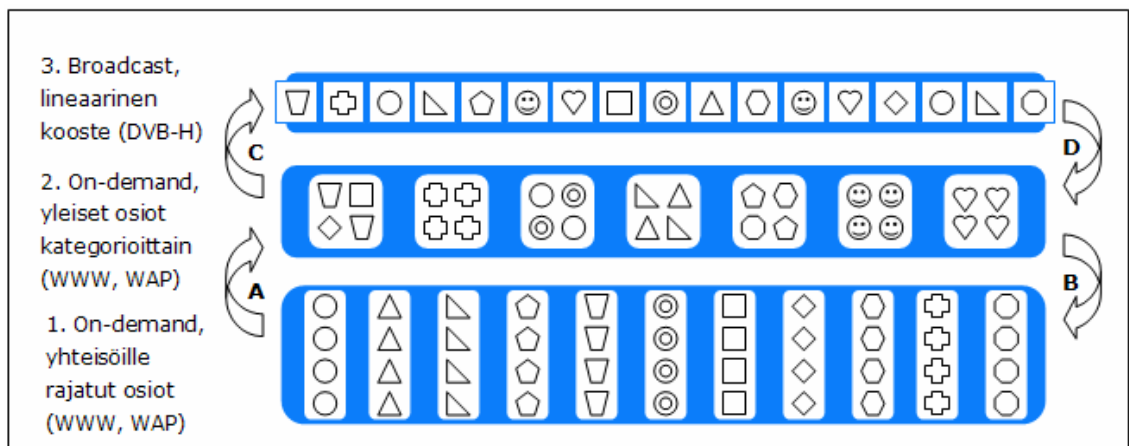
Digi-tv-puolella on jo kehitetty eräs kokonaiskonsepti (Kanava Viisi), joka idealtaan osittain vastaa yhteisöviestintäalustan massalähetyspuolta. Kanava Viisi ei myöskään tuottanut itse sisältöä, vaan toimi ainoastaan ohjelmasisällön kokoajana. Yhteisöllisyydellä oli lisäksi tärkeä rooli ohjelmavirrassa. Kanavan ansainta muodostui ohjelma-ajan myynnistä, lisäarvopalveluista ja mainostuloista. Kanava Viisi ei kuitenkaan enää ole saatavilla.

Elisan nykyinen yhteisöviestintäalustaprototyyppi tarjoaa www-pohjaisen hallintakäyttöliittymän, mediavaraston sekä mediapalvelinten ja monikanavaisten verkkoyhteyksien saatavuuden. Tavoitteena on vuoden 2006 aikana lisätä sisällöntuottajien tai yhteisöjen jäsenten vahvaa tunnistusta sekä valmiita ratkaisuja palvelujen interaktiivisuutta ja laskutusta varten.

2.3. Yhteisöviestintäalustan käyttö

Elisa kehitti alun perin yhteisöviestintäkonseptinsa kevään 2005 aikana Helsingin DVB-H-mobiili-tv-pilotin kokeellisiksi palveluiksi. Näitä palveluja yhdistettiin alkuvuonna 2006 kokonaisuudeksi, joka välittää digitaalista mediaa sekä yhdensuuntaisesti ja aikataulutetusti DVB-H-kanavaan että kaksisuuntaisesti ja on-demand-tyyppisesti matkapuhelin- tai laajakaistakanaviin.

Yhteisöviestintäpalvelu perustuu pitkälti kamerapuhelimella tallennettuun sisältöön, jota helppokäyttöisesti voidaan erillisen kamerapuhelimen client-sovelluksen kautta siirtää palvelimeen. Laajamittaisempaa videosisältöä voidaan toimittaa tietokoneen web-selaimen kautta. Yhteisöviestintäpalvelun katselijat voivat myös kuluttaa haluamansa sisällön joko matkapuhelimella tai tietokoneella. Palvelu mahdollistaa näin ollen sisällön tuotantoa ja katselua milloin ja mistä tahansa.



Kuva 2. Yhteisöviestintäalustan mahdollistamat sisältötasot

Yhteisöviestintäalusta mahdollistaa kolme sisältöpalvelujen päätasoa (Kuva 2):

1. **On-demand, yhteisöille rajatut osiot** – Palvelun web- tai wap-portaali tarjoaa eri yhteisöille suojattuja osuuksia, esim. <http://yhteiso.palvelu.tv>. Yhteisöt vastaavat oman osion sisällön tuottamisesta, valvonnasta ja käytöstä sekä tekijänoikeuksista. Yhteisön jäsenten lähettämän sisällön ns. moderointi tapahtuu yhteisön asettaman päätoimittajan toimesta, suojatun www-käyttöliittymän kautta.
2. **On-demand, yleiset osiot kategorioittain** – Yhteisön päätoimittaja voi valikoidusti siirtää sisältöä yleisen osion sisältökategorioihin, esim. <http://www.palvelu.tv/funny/> (Kuva 2, skenaario A). Yleinen osio toimii samalla eräänlaisena kauppapaikkana, joka luo kiinnostusta yhteisöä kohtaan (Kuva 2, skenaario B).
3. **Broadcast, lineaarinen kooste** – Yhteisön päätoimittaja voi lisäksi hakea oman yhteisön sisällöille aikaikkunoita yhteisöviestintää tukevan, jopa kaupallisen kanavan DVB-H-lähetyksessä (Kuva 2, skenaario C). Mobiili-tv-lähetys toimii houkuttimena yleiseen on-demand-osioon esim. ladattaviin maksullisiin sisältöihin (Kuva 2, skenaario D).

Yllä viitattiin siihen, että yhteisöviestintäalusta voisi tukea täysin kaupallisten mediakanavien ohjelmiakin. Voitaisiin esimerkiksi ajatella tietyn musiikkityylin ns. faniyhteisöä, jonka jäsenet omilla kamerapuhelimillaan otettujen videoklippien avulla esittelevät toisilleen mediavarastosta valittuja musiikkivideoita. Nämä henkilöt voivat silloin itse toimia video jockey -esittelijänä ja saada siitä tunnustusta omassa yhteisössään. Palvelu voisi esimerkiksi toimia radiokanavan sponsoroimana tai olla käyttäjille maksullinen.

3. INDICA2

3.1. Hankekuvaus

Elisa kehittää mediayrityksille ja -yhteisöille digitaalisen median jakelualustan, jonka liiketoiminta perustuu näiden tahojen kustannustehokkaan, monikanavaisen (ja erityisesti mobiiliin) digitaalisen median julkaisutarpeiden tyydyttämiseen. INDICA2-hankkeen tavoitteena oli muun muassa tunnistaa median jakelualustan kaupallistamisen edellytyksiä sekä rakentaa luotettava ja turvallinen toimintamalli. Lisäksi tavoitteena oli tunnistaa loppukäyttäjän tuottaman sisällön sekä yhteisöllisten sisällönjakelumekanismien haasteita ja toimenpiteitä erilaisten sisällönjakelumallien edistämiseksi.

Radiokanava Uusi Kiss oli esimerkki-case INDICA2-hankkeessa. Tuttu radiokanava lähetti myös monessa mielessä Visual Radio™:ta muistuttavaa näköradioversiota lähetyksestään, jossa perinteiseen radiosta kuuluvaan lähetykseen oli matkapuhelimessa kuuntelun lisäksi yhdistetty katseltavaa sisältöä. Sisällön katselemisen lisäksi käyttäjillä oli periaatteessa mahdollisuus tilata radiolähetykseen liittyviä taustakuvia tai soittoääniä matkapuhelimeensa.

Case-esimerkin lisäksi INDICA2-hankkeen tavoitteena oli mahdollistaa monipuolisempi sisällönjakelu, kuten esimerkiksi loppukäyttäjien ja kuluttajien tai yhdistysten toimintaa tukevan tiedon ja sisällön tuotanto sekä jakelu. Raportissa on käsitelty sekä Visual Radio -casea että varsinkin riski- ja kontrolli-workshopien analysoinnissa myös monipuolisempaa yhteisöjen välistä sisällönjakelua.

Kehitettävien palvelujen tavoitteet liittyvät kuluttajan näkökulmasta palvelun veloitusperusteiden selkeytymiseen, sisällön tuottamiseen ja palvelun korkeaan käytettävyyteen. INDICA2-hankkeessa tuotettavan mobiilidigi-tv-lähetyksen vastaanottamisesta ei tarvinnut maksaa, toisin kuin Visual Radio -tyyppisissä sovelluksissa, joissa käyttäjälle aiheutuu kuluja tiedonsiirrosta. Mobiilidigi-tv:n tapauksessa käyttäjä ei maksa peruslähetyksestä vaan ainoastaan tilaamastaan sisällöstä. Toisaalta käyttäjä joutuu investoimaan lähetyksen vastaanottoon kykenevään laitteeseen. Toinen loppukäyttäjän näkökulmasta tärkeä tavoite on sisällön tuottaminen. INDICA2-hankkeen tavoitteena oli mahdollistaa helposti sisällön tuottaminen jaeltavaan lähetykseen. Myös palvelun käytön helppous ja toimivuus ovat loppukäyttäjien näkökulmasta tärkeitä asioita. Tekniikan kehittyessä päätelaitteiden käytettävyys paranee ja käyttäjä saa entistä helpommin monimuotoisempaa sisältöä laitteeseensa.

Jakelualustan käyttäjiä ja kohdeasiakkaita ovat sellaiset tahot, joilla ei itsellään ole olemassa tarvittavia raskaita prosesseja ja järjestelmiä eikä tarvittavaa teknistä- ja tietoturva-osaamista. Tällaisia voivat olla esimerkiksi yhdistykset, jotka pystyvät palvelun avulla helposti jakamaan sisältöä, sekä sisällöntuottajat, jotka eivät halua alkaa rakentaa raskasta jakelukanavaa. Elisa toimii tässä mahdollistajana, jolla on hallussa prosessit ja järjestelmät.

Hankkeessa ei ollut tarkoitus rajoittaa johonkin tiettyyn tekniikkaan, esim. DVB-H, vaan pitää alustassa mukana tietynlaista verkkoagnostisuutta (laajakaista, 3G). Case-esimerkissä pääpaino oli kuitenkin DVB-H-tekniikassa sekä SMS- ja MMS-viestien hyväksikäytön tutkimisessa.

Jakelualustan tarjoama liiketoimintamalli perustuu kokonaan ulkopuolisten tahojen tuottaman sisällön jakeluun, jolloin varsinaisesta sisällöntuotannosta ei aiheudu operaattorille tai palveluntarjoajalle kustannuksia. Operaattorin ansainta muodostuu lähinnä ohjelma-ajan myynnistä, lisäarvopalveluista tulonjakoperiaatteella tai erillisten jakelualustojen Application Service Provider -tyyppisestä toiminnasta.

3.2. Case – Uusi Kiss

Uusi Kiss on osa eurooppalaista SBS Broadcasting SA:ta, joka harjoittaa radio-, TV- ja uusmediatoimintaa kymmenessä Euroopan maassa.

Uusi Kiss on SBS:n perinteinen FM-radiokanava, josta on olemassa myös Visual Radio -toteutus. SBS aloitti Visual Radio -lähetyskset Nokian kanssa yhteistyössä maaliskuussa 2005. Visual radio toimii siten, että päätelaite (matkapuhelin) vastaanottaa radion FM-signaalina ja kuvan GPRS:n kautta. GPRS-lähetys sisältää tietoa, jonka avulla kuva ja ääni synkronoidaan keskenään. Interaktiivisuus tarkoittaa toistaiseksi lähinnä soittoäänien ja taustakuvien tilaamista lähetyksen sisältöön liittyen. Jatkossa jakelukanavan kapasiteetin kasvaessa on tarkoitus jakaa myös esimerkiksi musiikkivideoita. Radiolähetyksen vastaanotto on ilmaista ja Visual Radion käytön hinta määräytyy operaattorin datapalvelumaksujen mukaan.

INDICA2-projektissa yhdistettiin Uusi Kiss -radiokanava, kuvasignaali ja interaktiivinen paluukanava käyttäen DVB-H-tekniikkaa sekä radiolähetyksen että kuvan välittämisessä. DVB-H-tekniikan avulla kuva ja ääni lähetetään broadcasting-tyyppisesti, jolloin kuluttajalle ei synny kustannuksia lähetyksen vastaanotosta toisin kuin Visual radio -tekniikkaa käytettäessä.

Koelähetyksen vastaanottamiseen projektissa käytettiin Nokian 7710 -älypuhelinia. Puhelimeen oli liitetty erillinen digisovitin.

3.3. Digitaalinen mobiilitelevisio, DVB-H

DVB-H (Digital Video Broadcasting -Handheld) on maanpäällinen digi-tv-standardi, joka pohjautuu yleisempään DVB-T-standardiin. Merkittävimpinä eroina DVB-T-standardiin on mobiililaitteille tärkeä pienempi virrankulutus ja parempi tuki liikkuvalla vastaanottimella. DVB-H-standardissa käytetään yleistä DVB-T-verkkoa IP-liikenteen välittämiseen, mikä tunnetaan yleisnimikkeellä IP-Datcasting. DVB-H-standardin mukaiset päätelaitteet vastaanottavat digi-tv-lähetyksen käyttäen maanpäällistä digi-tv-verkkoa (DVB-T). Signaalin siirtämiseen ei siten käytetä lainkaan matkapuhelinverkkoja. DVB-H ei ota kantaa videon pakkaukseen; tyypillisesti käytetään MPEG4-muotoista videoa.

DVB-H:ssa kanavanipun parametrit on asetettu siten, että mobiilivastaanoton vaatimukset, kuten virransäästö, on helpommin toteutettavissa. Kanavanipun koko voi olla 11 Mbit/s ja yhden kanavan vaatima datavirta on noin 256 kbit/s. Päätelaitteiden rajoitukset ruutukoon ja resoluution suhteen tuovat mobiili-tv:n palvelunkehitykseen omat erityispiirteensä, joista mm. kosketusnäytöt voivat tarjota uusia mahdollisuuksia esimerkiksi käyttöliittymien teossa. Lisäksi matkapuhelinten käyttötottumukset ovat erilaisia perinteiseen television katsomiseen verrattuna.

4. Tietoturvaongelmat palvelukehitysprosessissa

4.1. Liiketoimintaprosessien kuvaaminen

Koska tietoturvallisuuden on oltava osa liiketoimintaprosesseja eikä oma erillinen toimintonsa, on liiketoimintaprosessien ja mallien tunteminen tietoturvallisuuden kannalta ensiarvoisen tärkeää. INDICA2-projektissa on tunnistettu eri osapuolten rooleja ja tulonjakoa. Lisäksi Elisa on yhdessä SBS:n kanssa tehnyt mallinnuksen edellisissä luvuissa kuvatunlaisten palvelujen liiketoimintamallista. Tämän lisäksi on testattu ja kehitetty käytettävää tekniikkaa.

LUOTI-ohjelman asiantuntijapalvelua tarjonneet asiantuntijat lähtivät projektissa liikkeelle liiketoimintaprosessikuvausten tarkentamisella. Liiketoimintaprosessit mallinnettiin ja dokumentoitiin prosessitasolla eli toimintaa tarkennettiin sille tasolle kuin se tällä hetkellä oli mahdollista. Tässä käytettiin case-mallina SBS:n kanssa toteutettua visual radio-palvelua. Toiminnan kehittämisen kannalta on suositeltavaa, että Elisa ja SBS päivittävät prosessikuvauksia, mikäli niihin tulee muutoksia.

Valitut tekniset ratkaisut ovat tietoturvallisuuden kehittämisen kannalta sinänsä toisarvoisia. Liiketoiminnan vaatimukset määrittävät liiketoimintaprosessit, jotka asettavat vaatimuksia tietoturvalle. Valittujen teknisten ratkaisujen on mahdollistettava tietoturva vaatimukseen vastaaminen. Tuotekehitys- ja pilottiprojekteissa liiketoimintamallien sekä -prosessien huomioiminen on haastavaa, sillä kaikki liiketoiminnalliset näkökulmat eivät välttämättä ole vielä hahmottuneet. Ne tarkentuvat projektin aikana tai sen tuloksena. Tulevan tai ajatellun liiketoimintamallin ja prosessin vaatimukset on kuitenkin pyrittävä selvittämään ja mallintamaan mahdollisimman ajoissa, jotta ne voidaan huomioida teknologia- ja toteutusratkaisuja valittaessa. LUOTI-ohjelman INDICA2-hankkeessa prosessikuvauksia käytettiin kriittisten tietoturva vaatimusten, kontrollipisteiden ja vaatimusten tunnistamiseen. Niitä käytettiin järjestettyjen riski- ja kontrolli-workshopien järjestämisen apuvälineenä ja niillä ohjattiin osallistujien ajatuksia liiketoimintaprosessin kannalta kriittisiin kohteisiin. Samalla pyrittiin varmistamaan tietoturvallisuuden kattava huomiointi prosessin kaikissa vaiheissa.

4.1.1. Havainnot liiketoimintaprosessien mallintamisesta ja kuvaamisesta

Liiketoimintaprosessien mallintaminen kehitys- tai konseptiasteella olevien tuotteiden ja palvelujen osalta on haastavaa, mutta tietoturvallisuuden kehittämisen kannalta erittäin hyödyllistä ja tärkeää. Prosessit muodostavat perustan tietoturvallisuudelle ja asettavat tuote- tai palvelukehitysprojektien etenemisen reunaehdot, jotka teknisen ratkaisun on mahdollistettava.

Liiketoimintaprosessikuvausten havaittiin olevan tehokkaita keskustelun ohjaajia tietoturvallisuusriskejä ja kontrollitoimenpiteitä mietittäessä.

Liiketoimintaprosessin kuvaamisessa havaittiin, että mallintamisvaiheessa on hankalaa erottaa toisistaan case-tapauksen ja suunniteltavan, monimutkaisemman kokonaisuuden liiketoimintaprosesseja. Tämä on kuitenkin erittäin tärkeää, samoin kuin käyttää aikaa

siihen, että etsitään oikeita henkilöitä, joiden kanssa yhdessä rakennetaan ja mallinnetaan liiketoimintaprosesseja. Tietoturvan suunnittelussa tämä on erityisen tärkeää, jotta tietoturva-asioiden huomioiminen saataisiin mukaan heti projektin alusta lähtien eikä sitä mietittäisi vasta, kun tekniset ratkaisut on jo lyöty lukkoon. Tietoturva saadaan siis osaksi teknistä ratkaisua eikä sitä vain liitetä jälkeenpäin erillisenä osana toteutettuun ratkaisuun.

4.2. Riski- ja kontrolli-workshopit

Projektissa järjestettiin workshop-tilaisuuksia, joiden tarkoituksena oli kartoittaa INDICA2-hankkeen tietoturvauhkia sekä pohtia mahdollisia ratkaisuja niihin. Lisäksi tietoturva-kysymyksiä pohdittiin KPMG:n asiantuntijoiden kesken kartoituksilla ja erillisillä sisäisillä workshoppeilla. Tietoturvaongelmien ratkaisujen osalta pyrittiin lisäksi täsmentämään, onko kyseessä olemassa oleva ratkaisu, helposti käyttöönotettava ratkaisu vai toiminnan muuttamista tai uudelleensuunnittelua vaativa ratkaisu.

Ensimmäinen workshop järjestettiin 27.10.2005 ja siihen osallistui KPMG:n, Elisan sekä SBS:n edustajia. Workshopissa oli monenlaisia osallistujia: osalla oli vahva tekninen tausta, osalla liiketoimintaprosessien osaamista ja osalla hallinnollista osaamista. Myöhemmin havaittiin, että mukana olisi voinut olla myös henkilö, jolla olisi ollut erityistä osaamista lakiasioista.

Workshopissa käsiteltiin projektin yleisiä kysymyksiä sekä tarkempia teknisiä kysymyksiä liittyen projektissa käytettäviin tekniikoihin. Keskustelun pohjana ja ohjaajana toimivat aiemmin laaditut prosessikuvaukset. Riskien ja kontrollien kartoitus aloitettiin parityönä, jossa KPMG:n asiantuntijat ensin esittelivät prosessikuvaukset ja toimivat tämän jälkeen ryhmätyön vetäjinä esittäen ryhmille kysymyksiä, kuten:

- Mitä prosessin tässä vaiheessa teknisesti tapahtuu?
- Mitä jos tämä viesti ei mene perille?
- Varmistetaanko tässä, että...?
- Voiko palvelun käyttäjä tehdä näin?
- Oletteko ajatelleet mahdollisuutta, jossa...?
- Mitä tapahtuisi, jos...?

Ryhmiä työstämät riskit ja kontrollit kirjattiin ylös ja niitä käsiteltiin ja täsmennettiin vielä kaikkien osallistujien kesken käydyn keskustelun perusteella. Workshopissa laadittiin riski-kontrollimatriisi, johon kirjattiin eri käyttöskenaarioiden riskejä ja niihin liittyviä mahdollisia ratkaisuja.

LUOTI-asiantuntijapoolin workshop järjestettiin 23.11.2005. Workshopissa käsiteltiin projektiin liittyviä tietoturvauhkia yleisemmällä tasolla ja tekniset yksityiskohdat jätettiin hieman vähemmälle huomiolle Elisan liikesalaisuuksien varjelemiseksi. Keskustelu asiantuntijapoolin workshopissa oli vähemmän jäsenneltyä ja määrämuotoista kuin projektin sisäisessä workshopissa. Myös tässä tilaisuudessa pyrittiin kuitenkin seuraamaan liiketoimintaprosessikuvauksia ja käsittelemään asiat niiden pohjalta. Riski-kontrollimatriisia täydennettiin tässä workshopissa esille tulleilla riskeillä ja kontrollitoimilla. Silloin kun workshoppeissa nousi esille riskejä, joihin ei workshopin aikana kyetty löytämään tehokasta kontrollitoimenpidettä, KPMG:n asiantuntijat pyrkivät löytämään sellaisen jälkikäteen.

4.2.1. Havainnot riski- ja kontrolli-workshopeista

Workshopit, joissa mietitään hankkeeseen liittyviä tietoturvaongelmia ja ratkaisuja, ovat tehokas tapa jakaa tietoa sekä lisätä osallistujien tietoturvatietoisuutta. Osallistujilla oli erilaisista taustoistaan johtuen erilaisia ajatuksia mahdollisista riskeistä ja toimivista ratkaisuksista ja keskustelu tietoturvakysymyksistä oli vilkasta. Workshopissa toiset osallistujat pystyivät siten tuomaan esille näkökulmia, joita muut osallistujat eivät välttämättä olleet ajatelleet ja lukuisa määrä erilaisia riskejä ja kontroleja pystyttiin identifioimaan. Voidaankin sanoa, että workshopit saavuttivat hyvin tavoitteensa.

Workshop johti myös liiketoimintamallin osittaiseen muutokseen mm. siltä osin, että palveluja ei näillä näkymin tulla tarjoamaan Prepaid-liittymiin. Palvelun toiminta edellyttää, että tilaajien ja varsinkin sisällöntuottajien, jotka voivat olla myös yksityishenkilöitä, henkilöllisyys pystytään varmentamaan riittävän tarkasti. Prepaid-liittymissä henkilöllisyyttä ei pystytä varmentamaan riittävällä varmuudella, sillä näitä liittymiä pystyy ostamaan kuka tahansa ilman, että henkilöllisyyttä varmennetaan. Riskien katsottiin olevan tässä tapauksessa liian suuria sekä kontrollitoimenpiteiden toteuttamisen liian monimutkaista. Lisäksi asiakaskunta on Suomessa marginaalinen.

4.3. Merkittävimmät esille tulleet tietoturvakysymykset

Seuraavissa kappaleissa käydään läpi palvelun käytettävyyteen, toimintaan ja tietoturvaan liittyviä riskejä, jotka workshopeissa sekä KPMG:n analyysissä arvioitiin merkittäviksi. Jokaisen riskin perässä esitetään ehdotus riskin pienentämiseksi tai poistamiseksi.

Operaattorin vastuu materiaalista

RISKI: Järjestelmässä loppukäyttäjä pystyy itse julkaisemaan materiaalia. Käyttäjällä on siten mahdollisuus myös vahingossa tai tahallaan julkaista materiaalia, joka on laitonta. Tällaista materiaalia voi olla esimerkiksi lapsille haitallista aineistoa sisältävät kuvat tai herjaavat tekstit.

RATKAISUEHDOTUS: Sisältö on tarkastettava ennen kuin materiaali julkaistaan järjestelmässä. Lisäksi käyttäjien sopimuksiin on lisättävä kohdat, jotka käsittelevät laittoman materiaalin julkaisemista. Operaattorin täytyy lisäksi rakentaa audit-trail eli tieto siitä, keneltä viesti on vastaanotettu, milloin se on vastaanotettu, milloin se on julkaistu ja kuka sen on hyväksynyt julkaistavaksi.

Toimitetun materiaalin toimivuus

RISKI: Käyttäjä tilaa sisältöä, jonka kuvittelee toimivan omassa päätelaitteessaan. Toimitettu sisältö ei kuitenkaan jostain syystä toimi päätelaitteessa. Syynä voi olla esimerkiksi väärä kuvaformaatti tai muu yhteensopivuusongelma.

RATKAISUEHDOTUS: Järjestelmän on pyrittävä tunnistamaan päätelaite sekä rekisteröinnin että tilauksen yhteydessä, jolloin sisällön ja käyttäjän laitteen yhteensopivuus pystytään tarkistamaan. Tähän tarkoitukseen voidaan käyttää viestien otsikkotietoja, joita esimerkiksi GPRS-liikenne sisältää.

Käyttäjien turha laskutus

RISKI: Järjestelmässä saattaa monesta syystä tulla tilanne, jossa käyttäjä tilaa tuotteen, mutta ei sitä saa. Tällöin asiakasta saatetaan myös laskuttaa, vaikka hän ei tuotetta olisikaan saanut.

RATKAISUEHDOTUS: Järjestelmän täytyisi joka tilanteessa odottaa kuittausta mobiililaitteelta siitä, että se on saanut sisällön vastaan. Kuittaus ei kuitenkaan kaikilla tekniikoilla ole mahdollista toteuttaa luotettavasti. Tällaiseksi havaittiin esimerkiksi GPRS-viestit, joiden yhteydessä päätettiin, että asiakasta laskutetaan vasta sisällön lähetyksen yhteydessä.

Tunnistamisongelmat

RISKI: Normaalisti palvelua käyttävät henkilöt tunnistetaan puhelinnumeron perusteella. Järjestelmää voi kuitenkin päästä käyttämään henkilö, jota ei ole tunnistettu ollenkaan tai on tunnistettu toiseksi käyttäjäksi. Tällainen tulee kysymykseen esimerkiksi, kun palvelua yritetään käyttää selaimen kautta tai kun käyttäjä pystyy väärentämään puhelinnumeron.

RATKAISUEHDOTUS: Ongelmakohdat, kuten selaimen kautta käyttö, olisi järjestelmässä estettävä tai siihen pitäisi rakentaa luotettava käyttäjän tunnistus esimerkiksi siten, että ainakin rekisteröitymisen yhteydessä käyttäjälle lähetetään varmistusviesti matkapuhelimeen. Lisäksi järjestelmän kehityksessä on otettava huomioon se mahdollisuus, että jatkossa käytetään esimerkiksi vahvan tunnistamisen järjestelmiä. Tällä hetkellä vahvan tunnistuksen käyttö ei ole kovin yleinen, jolloin sen käyttöönotto todennäköisesti vähentäisi käyttäjien määrää merkittävästi ja ei siten ole liiketaloudellisesti perusteltua.

Ulkopuoliset kuuntelevat tiedonsiirtoa

RISKI: Järjestelmässä siirtyvä tieto saattaa olla sellaista, jota käyttäjät eivät haluaisi muiden pystyvän kuuntelemaan. Kuitenkin siirtokanavat, kuten GPRS, saattavat olla sellaisia, joita ulkopuoliset pystyvät kuuntelemaan. Tämä johtuu siitä, että tieto saattaa kulkea julkista verkkoa salaamattomana tai huonosti salattuna, jolloin ulkopuolisen tarvitsee vain olla oikeassa paikassa kuuntelemaan tiedonsiirtoa.

RATKAISUEHDOTUS: Tiedonsiirto on salattava riittävän hyvin. Salauksen toteuttamistapa riippuu monesta tekijästä, kuten avainten jakelusta, saatavilla olevista salauskomponenteista sekä päätelaitteiden laskentatehosta. Täten on vaikeaa antaa yleispätevää suositusta riittävän hyvästä salauksesta. Suosittelemme kuitenkin hyväksi havaittujen yleisten menetelmien käyttöä.

Sisältö muuttuu

RISKI: Järjestelmässä saatetaan siirtää tietoa, jonka oikeellisuus on tilaajalle tärkeää. Järjestelmässä tai viestiketjun aikana tieto voi kuitenkin muuttua siirrettäessä. Toistaiseksi palvelussa välitetään kuitenkin lähinnä viihdepalveluja, joiden sisältämän tiedon muuttuminen tiedonsiirron aikana on haitallista lähinnä vain siksi, että muuttunut sisältö ei välttämättä toimi asiakkaan päätelaitteessa.

RATKAISUEHDOTUS: Järjestelmässä on mahdollisuuksien mukaan salattava tieto, jolloin sen muuttaminen on vaikeaa.

Suljettujen asiakasryhmien jakaman tiedon laillisuus

RISKI: Suljettujen asiakasryhmien, kuten yhdistykset, sisällä tuotettava ja jaettava materiaali on lakien tai yhdistyksen toiminnan vastaista.

RATKAISUEHDOTUS: Sisältö on tarkistettava yhdistyksen ja mahdollisesti myös operaattorin toimesta. Lisäksi käyttäjien kanssa on tehtävä sopimukset, jotka kieltävät tällaisen materiaalin levittämisen.

Asiattomat käyttäjät pystyvät rekisteröitymään

RISKI: Rekisteröityminen voidaan hoitaa tekstiviestillä tai yhteisökäyttäjien tapauksessa käyttäjät rekisteröityvät yhteisön välityksellä. Käyttäjät, joilla ei ole oikeutta rekisteröityä (esimerkiksi alaikäiset) pystyvät rekisteröitymään.

RATKAISUEHDOTUS: Yhteisötapauksessa on kiinnitettävä huomiota yhteisön ylläpitäjien koulutukseen siinä, minkälaisia käyttäjiä järjestelmään sallitaan. Tekstiviestillä tapahtuvaan rekisteröintiin kannattaa lisätä käyttäjän iän ja henkilöllisyyden tarkistus puhelinnumeron perusteella. Tämäkin on usein hankalaa, sillä matkapuhelimet on rekisteröity vanhempien nimellä. Järjestelmässä on otettava suunnitteluvaiheessa huomioon vahvan tunnistuksen käyttäminen tulevaisuudessa, jonka avulla käyttäjä pystytään aukottomasti tunnistamaan.

Haittaohjelmat leviävät sisällön mukana

RISKI: Järjestelmässä jaettavaan sisältöön on mahdollista liittää erilaisia haittaohjelmia, kuten viruksia. Nämä saattavat aiheuttaa ongelmia käyttäjillä ja heikentää järjestelmän toimivuutta.

RATKAISUEHDOTUS: Jakelujärjestelmään on lisättävä automaattinen tarkistusmekanismi, joka poistaa sisältöön liittyvät haittaohjelmat, kuten mobiilivirukset.

Matkapuhelimen toiminta häiriintyy

RISKI: Monet käyttäjät pitävät matkapuhelimen päätarkoituksena puhelutoimintoja, jotka eivät saa häiriintyä. Järjestelmän käyttö saattaa kuitenkin häiritä päätelaitteen normaalia toimintaa.

RATKAISUEHDOTUS: Päätelaittevalmistajilta on edellytettävä prosessoinnin eriyttämistä laitetasolla. Tämä on hankalaa, joten palvelun tarjoajan kannattaa tutkia markkinoita ja suosittelua käyttäjille hyväksi havaittuja päätelaitemalleja sekä ilmoittaa käyttäjälle selvästi, mitkä ovat tuettuja päätelaitteita. Käyttäjälle on ilmoitettava, jos hän yrittää hankkia sisältöä, jonka tiedetään olevan yhteensopimaton käyttäjän laitteen kanssa.

Luottamuksellisen tiedon vuoto

RISKI: Operaattorilla on tallennettuna asiakastietoa ja tietoa järjestelmän käytöstä. Tämä on luottamuksellista tietoa, jota ulkopuolisten ei pitäisi pystyä lukemaan. Järjestelmän laitteet ovat kuitenkin yhteydessä julkisiin internet- ja GPRS-verkkoihin, jolloin ulkopuoliset saattavat pystyä murtautumaan järjestelmään.

RATKAISUEHDOTUS: Palvelimet on suojattava riittävällä tasolla, kuten palomureilla, ja operaattorin toiminnan täytyy muutenkin olla ammattimaisesti järjestettyä, mikä tarkoittaa palvelinten säännöllistä päivittämistä, turhien palvelujen poistamista ja muita tietoturvaa parantavia toimenpiteitä. Sovellustason palomuurien käyttöä kannattaa harkita sekä julkisiin verkkoihin olevat järjestelmät testata säännöllisesti tunnettujen tietoturva-aukkojen löytämiseksi ja tukkimiseksi.

Tekijänoikeuslain alaisen tai Creative Commons -lisenssin alaisen materiaalin kopiointi

RISKI: Materiaali, jota käyttäjät lataavat, saattaa olla tekijänoikeuslain alaista. Käyttäjät saattavat kopioida tällaista materiaalia toisten käyttöön. Järjestelmässä on tarkoitus levittää myös tietoa, jotka on julkaistu Creative Commons -lisenssin alla. Tällöin sisältöä voi vapaasti jakaa tekijän antamien ehtojen puitteissa. Henkilöt, jotka ovat tehneet Teoston kanssa sopimuksen ja siten luopuneet mahdollisuudestaan vapaasti päättää tekemänsä materiaalin jakelusta saattavat kuitenkin (vahingossa) antaa materiaalia jaettavaksi järjestelmään ja siten rikkoa Teoston kanssa tekemänsä sopimusta.

RATKAISUEHDOTUS: Tällä hetkellä on käytösäännöissä kiellettävä tekijänoikeuslain alaisen materiaalin levittäminen. Järjestelmää kehitettäessä on otettava huomioon mahdollinen DRM-järjestelmien käyttöönotto, joilla voidaan suojata sisältöä kopioimiselta. Sopimuksissa on otettava huomioon myös Creative Commons -lisenssin alaisen materiaalin osalta tilanne ja tehtävä selväksi käyttäjille, minkä lisenssin alla materiaali julkaistaan ja mitä se käyttäjältä edellyttää.

Phishing

RISKI: Käyttäjä (hyökkääjä) julkaisee materiaalia, joka sisältää linkin ulkoiseen sivustoon. Linkki ei kuitenkaan johda sivustolle, jolle käyttäjä olettaa sen ohjautuvan, vaan johonkin hyökkääjän rakentamaan sivustoon. Tämä sivusto voi muistuttaa sivustoa, jolle käyttäjä oikeasti haluaa. Tätä sivustoa apuna käyttäen hyökkääjä pyrkii saamaan selville muiden käyttäjien arkaluontoista tietoa, kuten salasanoja.

RATKAISUEHDOTUS: Sisältöä pitäisi tarkastaa manuaalisesti erityisen tarkasti linkkien osalta sekä mahdollisesti automaattisia työkaluja apuna käyttäen. Lisäksi phishing-hyökkäyksistä olisi tiedotettava nopeasti käyttäjille ja mahdollisesti automaattisesti estettävä käyttäjien pääsy tunnetuille phishing-sivustoille.

5. Tietoturvan ratkaiseminen tuotantoketjussa

Tuotantoketjussa yksi osapuoli ei pysty ratkaisemaan kaikkia tietoturvaan liittyviä ongelmia, vaan asioiden ratkaiseminen on monen toimijan vastuulla. Case-tapauksessa erilaisia toimijoita oli hyvin rajallinen määrä, mutta jatkossa käyttötapojen kehittyessä erilaisia osapuolia voi olla paljon enemmänkin.

Elisa voi käyttää eri alihankkijoita palvelun tekniikan kehittämiseen, jolloin alihankkijoiden rooli täytyy miettiä tarkasti suhteessa siihen, mikä heidän vastuunsa on palvelun tietoturvallisuuden suhteen.

Tekniikan lisäksi sisällöntarkastus voidaan ulkoistaa, jolloin tarkastajan kanssa on tehtävä tarkka sopimus siitä, mikä on soveliaista materiaalia ja mikä kumppanin rooli on.

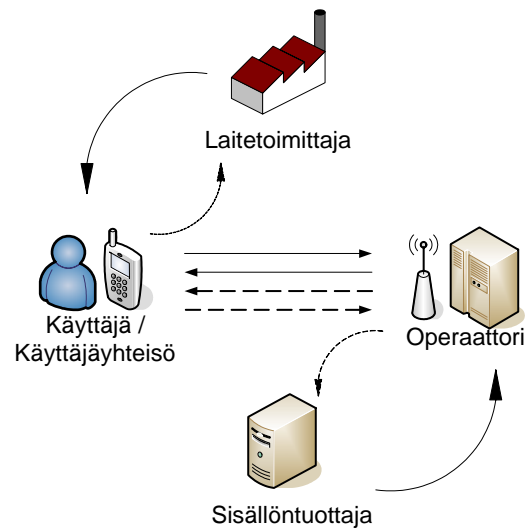
Sisällöntuotanto on jo case-esimerkissä ulkoistettu. Varsinkin silloin, jos sisällöntuottajien määrä kasvaa suureksi, tulee ongelmaksi se, miten toimitaan tilanteessa, jossa sisältö ei ole lainmukaista.

Alihankkijoiden ja ulkoistuskumppanien kanssa ongelma on myös siinä, kuka on vastuussa väärinkäytöksistä, jos alihankkijan ja kumppanien toimet ovat lainvastaisia. Tällöin saatetaan päätyä tilanteeseen, jossa Elisa on vastuussa alihankkijan virheestä. Tällaisilta tilanteilta on pyrittävä suojautumaan sopimuksin. Ongelmana tällöin on se, että vaikka alihankkija tai kumppani olisikin lopullisessa vastuussa virheestä, on Elisan imago jo vahingoittunut. Joka tapauksessa alihankkijoiden kanssa on kommunikoitava selkeästi tietoturva-vaatimuksista väärinkäytösten välttämiseksi.

Tietoturvan vastuunjaosta ei siis voi tehdä mitään yleistä mallia, vaan on jaettava vastuuta sopimuksin eri toimijoiden kesken. Tällöin suurimman pelurin, tässä tapauksessa Elisan, kannattaa toimia siten, että se sisällyttää tietoturvan vaatimukset muille toimijoille sopimustasolla. On kuitenkin muistettava, että sopimuksissakaan ei pystytä sopimaan kohtuuttomista vaatimuksista eli sopimuksista on tehtävä sellaiset, että ne ovat oikeudessakin päteviä. Kohtuullisuusvaatimus tulee esille varsinkin silloin, jos toisena osapuolena on yksityishenkilö sisällöntuottajana. Sopimuksia laadittaessa on mahdollisuuksien mukaan käytettävä sekä tekijänoikeuksiin että tietoturvaan erikoistuneita lakimiehiä.

5.1. Esimerkki vastuunjakomallista

Alla olevassa kuvassa on esitetty yksi mahdollinen vastuunjakomalli, jossa on kuvattu eri toimijat. Kuvassa normaalilla nuolella on kuvattu sisällön ja tuotteen virta sekä katkoviivalla esitetyllä nuolella rahavirta.



Kuva 3. Tuotantoketju

Sisällöntarjoaja vastaa tuottamansa sisällön lainmukaisuudesta ja oikeellisuudesta. Tässä kannattaa muistaa, että sisällöntarjoaja voi olla myös loppukäyttäjä, mikäli hän on sisältöä tuottavan yhteisön jäsen. Vastuut ja sopimuksen sisältö täytyykin määritellä eri tavalla suurille sisällöntarjoajille ja yksityishenkilöille.

Operaattori hoitaa käyttäjien tunnistuksen, sisällönjakelun oikeellisuuden ja keräämiensä rekisteritietojen luottamuksellisuuden varmistamisen.

Laitetoimittaja vastaa päätelaitteiden tekniikoiden yhteensovittamisesta turvallisella tavalla siten, että päätelaitteen eri toiminnot eivät haittaa laitteen muita toimintoja.

Käyttäjä vastaa oman päätelaitteensa ja tilatun materiaalin käytöstä asianmukaisella tavalla sopimusehtojen mukaisesti sekä käytettävien ohjelmien ajantasaisuudesta ja toimintakunnosta.

6. Tietoturvaa koskevat menetelmät ja toimintatavat

6.1. Menetelmät ja toimintatavat palvelukehitysprosessissa

Tietoturvan kehityksessä on hyvä lähteä liikkeelle palvelun vaarantavien riskien määrittämisestä. Tämän jälkeen kannattaa miettiä toimenpiteitä riskien minimoimiseksi tai välttämiseksi. Vertaamalla riskin suuruutta ja mahdollisten suojaustoimenpiteiden kustannuksia saadaan selville, mitkä suojautumismenetelmät ovat taloudellisesti kannattavia.

Riskien kartoituksessa kannattaa käyttää monenlaisia menetelmiä, joista esimerkkeinä tässä projektissa toimivat workshopit ja tarkistuslistat. LUOTI-projektin aikana pidettiin sisäisiä ja ulkoisia workshoppeja, joiden tuloksena oli listoja riskeistä ja suojaustoimenpiteistä. Elisän vastuulle jäi suojaustoimenpiteiden kannattavuuden arviointi.

Riskien määrittelytyö synnyttää hyvää materiaalia tietoturva vaatimusmäärittelyn perustaksi. Tätä vaatimusmäärittelyä voidaan hyödyntää alihankintatilauksia ja –sopimuksia tehtäessä. Tällöin on tosin samalla huomioitava, että riskien ja suojaustoimenpiteiden määrittely on tehtävä tarkalla tasolla.

6.2. Käyttäjien tunnistaminen

Perinteisesti matkapuhelimien käyttäjän tunnistuksen tarve on lähtenyt siitä ajatuksesta, että pystytään laskuttamaan oikeaa asiakasta tilatuista palveluista. Tämä on tärkeää myös INDICA2-hankkeen osalta. Kuitenkin INDICA2-hankkeessa käyttäjän tunnistus on oleellista myös siinä mielessä, että käyttäjä pystyy luomaan sisältöä. Käyttäjä pitää pystyä tunnistamaan, jotta tuotettu sisältö pystytään yksilöimään kyseiseen käyttäjään. Tällainen tarve saattaa tulla esille silloin, kun sisältö ei ole lain tai palvelun ehtojen mukaista ja sisällöntuottaja on pystyttävä jäljittämään. Lisäksi saattaa olla tarpeellista maksaa käyttäjälle tuotetusta sisällöstä.

Käyttäjän tunnistamisen menetelmä matkapuhelimella riippuu käytettävästä yhteystavasta. Soitettaessa tai SMS-viestiä käytettäessä yhteys voidaan yksilöidä käyttäjän SIM-korttiin ja sitä kautta käyttäjään. Tästä poikkeuksena esimerkiksi verkkopalvelut, joista voi lähettää ilmaiseksi SMS-viestejä.

Käytettäessä muita yhteystapoja, kuten GPRS-viestintää, muodostuu käyttäjän tunnistaminen hankalaksi. Käytännössä GPRS-verkko voidaan laskea julkiseksi verkoksi, jossa käyttäjän tunnistaminen ei voi perustua viestin otsikkotietoihin. Tällöin tarvitaan jokin parempi tapa tunnistaa käyttäjä, kuten käyttäjätunnus/salasana-pari. Palvelun käyttö voitaisiin mahdollistaa tiettyä client-ohjelmaa käyttäen, jolloin käyttäjän olisi pakko asentaa laitteeseensa ohjelma, jolla palvelua käytetään. Tällöin myös käyttäjän tunnistaminen helpottuisi.

6.3. Mobiilikansalaisvarmenne, sähköinen allekirjoitus ja tunnistaminen

INDICA2-projektin keskeisiä haasteita on käyttäjän tunnistaminen. Mikäli käyttäjä käyttää palvelua matkapuhelimella, voidaan käyttäjän tunnistus tehdä pohjautuen matkapuhelimen numeroon. Tämä on mahdollista esimerkiksi tekstiviestien kohdalla. GPRS-liikenteen osalta tunnistamisen toteuttaminen on jo hankalampaa. Lisäksi jatkossa palveluja saatetaan käyttää muillakin välineillä kuin matkapuhelimilla. Tällöin käyttäjän tunnistukseen olisi hyvä saada menetelmä, jolla käyttäjä voidaan aukottomasti tunnistaa.

PKI-teknologiaan perustuvilla varmennepalveluilla voidaan monipuolisesti suojata sähköistä viestintää ja asiointia. Sähköisellä allekirjoituksella voidaan yksiselitteisesti varmistaa allekirjoitetun tiedon ja allekirjoittajan yhteenkuuluvuus sekä allekirjoitetun tietosisällön muuttumattomuus. Henkilön tunnistamisen lisäksi voidaan varmentaa tietosisältöjen muuttumattomuutta ja alkuperää sekä salata niitä.

Mobiilivarmenteen käyttöönotto mahdollistaa vahvaa tunnistusta vaativien asiointipalvelujen käytön luotettavasti paikasta ja ajasta riippumatta. Mobiilivarmenteella varustettu matkapuhelin on tunnistautumis- ja allekirjoitusväline sähköisessä asiointissa ja kaupan- käynnissä. Varmennus voidaan tehdä myös puhelun aikana vaikkapa puhelinasiakas- palveluun.

Mobiilikansalaisvarmenne on SIM-korttiin liitetty kansalaisvarmenne. Se on valtion takaama sähköinen henkilöllisyys, joka on samaan tapaan Väestörekisterikeskuksen tuottama kuin jokaisen suomalaisen oma henkilötunnus. Matkapuhelimen käyttäjä voi jatkossa yhteneväisesti samaa tunnuslukua käyttäen tunnistautua erilaisiin sähköisiin asiointi- palveluihin. Mobiilikansalaisvarmenne on sähköisistä allekirjoituksista annetun lain vaatimukset täyttävä. Mobiilikansalaisvarmenne on myös yhdenmukainen muilla alustoilla toimivien kansalaisvarmenteiden kanssa ja se perustuu jo olemassa olevaan varmenneinfrastruktuuriin.

Julkisen avaimen menetelmään perustuva PKI-teknologia tekee sähköisestä allekirjoituksesta vähintään yhtä luotettavan kuin normaali allekirjoitus on. Allekirjoittamiseen tarvittava henkilön yksityinen avain on mobiilivarmenteessa luku-, kopio- ja kirjoitussuojattuna SIM-kortin mikrosirulla. Avaimien käyttö on suojattu tunnusluvulla ja henkilön varmenteet sekä sulkulista sijaitsevat Väestörekisterikeskuksen hakemistossa, josta ne haetaan tunnistustapahtuman aikana.

Mobiilivarmenteen takana oleva monimutkainen arkkitehtuuri on pyritty piilottamaan sekä palveluntarjoajilta että kuluttajilta. Kansallisen yhteistyön tuloksena tunnistautumistapa on tehty operaattorista riippumattomaksi. Käyttäjien on helppo omaksua palvelujen käyttölogiikka, kun yhdellä lyhyellä tunnusluvulla voidaan vahvistaa tunnistautuminen eri palveluissa. Palveluntarjoajille taas riittää jatkossa yksi tekninen rajapinta, jonka kautta saadaan käyttöön kaikkien verkko-operaattorien mobiilivarmenteet. Palveluntarjoaja tavoittaa kaikki asiakkaat yhden operaattorin palvelulla.

7. Johtopäätökset

Toimeksiannon aikana on tarkennettu ja mallinnettu liiketoimintaprosessia sekä tunnistettu sen avulla palveluihin liittyviä tietoturvauhkia. Jatkossa on olennaista, että tuotekehityksen yhteydessä päivitetään prosessikuvausta ja ratkaistaan sen perusteella esiin tulleet mahdolliset uudet uhkat. Jälkeenpäin tietoturvaongelmien korjaaminen on erittäin kallista ja työlästä. Tuotekehityksessä kannattaa jatkossakin harkita ulkopuolisen tietoturva-asiantuntijan käyttöä apuna, sillä monesti palvelunkehittäjien rooliin ei kuulu kaikkien tietoturvaan liittyvien asioiden miettiminen. Lisäksi uusien teknologioiden ja monikanavaisen palveluympäristön osalta organisaation sisällä ei luonnollisestikaan välttämättä ole riittävää asiantuntemusta eikä kykyä nähdä kaikkia ongelmia.

LUOTI-projektin tuloksena voidaan sanoa, että liiketoimintaprosessin mallintaminen tuotekehitysprojektin alussa on haastavaa, mutta tietoturvallisuuden kannalta erityisen tärkeää. Liiketoimintaprosessikuvaukset osaltaan ohjaavat tuotettavan tekniikan kehitystä ja toimivat siten myös tietoturvaratkaisujen perustana.

Pilottihankkeen kaltaisissa yhteisöviestinnällisissä palveluissa on paljon tekijänoikeuksiin ja eri toimijoiden vastuisiin liittyviä kysymyksiä. Näiden ratkaiseminen teknisesti ja sopimuksilla on tärkeää, jotta ne eivät muodostu esteeksi palvelun käytölle. Koska tämäntyyppiset palvelut ovat kovaa vauhtia yleistymässä, nähdään näiden tekijänoikeuksiin ja eri toimijoiden vastuisiin liittyvien kysymysten työstämistä yleisissäkin foorumeissa palvelujen käyttöönottoa ja yleistymistä edistävänä toimenpiteenä.

Eri toimijoiden vastuiden takia käyttäjien tunnistaminen luotettavasti on tärkeää. Matkapuhelin mahdollistaa käyttäjien tunnistuksen matkapuhelinnumeron avulla, mutta jo esimerkiksi GPRS-yhteyttä käytettäessä tunnistus ei ole yhtä luotettava. Mobiilikansalaisvarmenne tarjoaa vahvan tunnistamisen, mutta käyttäjiltä vaaditaan toistaiseksi lisäinvestointeja, mikä hidastaa palvelun leviämistä. Siksi ainakin alkuvaiheessa pitää keskittyä muihin käyttäjän tunnistusmenetelmiin.

Projektissa liiketoimintaprosesseja pystyttiin tehokkaasti hyödyntämään tietoturva-tietoisuuden lisäämisessä tuotantoketjun eri toimijoiden joukossa, potentiaalisten tietoturvauhkien kartoittamisessa sekä kontrollitoimien suunnittelussa.

Uusien tuotteiden kehityksessä tietoturvallisuudella on suuri merkitys, mutta samaan aikaan on huomioitava palvelun käytettävyys, joka on yksi palvelun tai tuotteen yleistymisen kannalta tärkeimmistä tekijöistä. Joidenkin tietoturvaratkaisujen käyttöönotto ei siksi välttämättä ole liiketoiminnallisesti järkevää, koska ne voivat tehdä palvelusta tai tuotteesta liian vaikeasti käytettävän. Tällöin se ei myöskään saavuta riittävän laajaa käyttäjäkuntaa. Mahdollisiin uusiin tietoturvaratkaisuihin on kuitenkin varauduttava jo tuote- ja palvelukehityksen alussa, jotta ratkaisut voidaan tarvittaessa ottaa käyttöön nopealla aikataululla ja ilman suuria järjestelmä- tai konseptimuutoksia.