



VALTIOVARAINMINISTERIÖ

Julkisen hallinnon ICT-toiminto

PERA-määrittely

VM125:06/2007

Liite 4.3

versio 1.0

8.12.2011

Julkishallinnon perustietovarantojen rajapinnat (PERA) -työryhmä

Tietovarantojen yhteinen rajapintaratkaisu

Määrittäviä VIA-palvelun tarjoamiksi yhteisiksi palveluiksi

Versio 1.0

Päiväys 8.12.2011



Sisällysluettelo

1 Johdanto.....	3
2 Rajaukset.....	3
3 Tietoturva	3
4 Saavutettavuus ja käytettävyys	3
5 Yleiset palvelut.....	4
5.1 Palvelurekisteri	4
5.2 Integraatioihin liittyvät tukipalvelut.....	4
6 Sovellus-sovellus integraatiot	5
6.1 Tunnistus	6
6.2 Valtuutus ja valtuuksien hallinta	6
6.3 Protokollan muunnospalvelut	6
6.4 Sanomien muunnospalvelut.....	7
6.5 Reitityspalvelut.....	7
6.6 Monitorointi ja raportointi.....	7
7 Aineistonvälitys	8
7.1 Tunnistus- ja valtuutuspalvelu	8
7.2 Aineistojen siirto.....	8
7.3 Tiedotuspalvelu.....	9
7.4 Monitorointi ja raportointi.....	10
8 Testiympäristöt	10
9 Muutoshistoria	11



1 Johdanto

Valtionhallinnon yhteisenä integraatiopalveluna VIA-palvelun tulee tarjota ratkaisuja, joilla PERA-määrittelyjen mukaisia palveluita saadaan julkaistua ja ylläpidettyä yksinkertaisemmin ja tehokkaammin. Tässä dokumentissa on kuvattu vaatimuksia näille ratkaisuille PERA-määrittelyjen näkökulmasta.

2 Rajaukset

VIA on tarkoitettu valtionhallinnon integraatiopalveluksi, mutta sen kautta valtionhallinnon palvelut voidaan tarjota koko julkishallintoon sekä yksityiselle sektorille. Valtion IT-palvelukeskus (VIP) tekee hallinnolliset sopimukset kuitenkin ainoastaan valtionhallinnon organisaatioiden kanssa.

VIA on ensisijaisesti tarkoitettu järjestelmien välisiin sovellus-sovellus-integraatioihin ja aineistonvälitykseen. Tämän takia tässä dokumentissa ei oteta kantaa, kuinka loppukäyttäjän asiakassovellukset olisi mahdollista integroida palveluihin VIAN avulla.

3 Tietoturva

Yleensä viestiliikenne VIAN, palvelua kutsuvan sekä palvelua tarjoavan järjestelmän välillä suojataan käyttäen HTTPS- tai SFTP-protokollaa. Valtion yhteistä VY-verkkoa käytettäessä VIAN ja palvelua tarjoavan organisaation välistä tietoliikennettä ei tarvitse salata, mikäli siirrettävät tiedot tietoturvaluokituksestaan sen mahdollistavat. Tällaisissa tapauksissa palvelua tarjoava organisaatio voi tarjota palvelut suoraan VIA:lle, ilman tunnistukseen tai salaamiseen tarkoitettuja ratkaisuja.

VIAN tarjoaman integraatoratkaisun eteen on sijoitettu erillinen palvelu suojaamaan järjestelmiä DoS-hyökkäyksiltä. Tällöin palvelua tarjoava organisaatio voi parantaa mahdollisuutta suojata omat palvelunsa DoS-tyyppisiltä palvelunestohyökkäykseltä julkaisemalla ne ainoastaan VIAN kautta. Lisäksi VIA voi rajoittaa välitettävien pyyntöjen määrää yksittäisille palveluille. Tämän toiminnallisuuden avulla palvelua tarjoava organisaatio voi suojata kutsuttavaa järjestelmää ylikuormittumiselta.

4 Saavutettavuus ja käytettävyys

Käytettäessä keskitettyä integraatiopalvelua saavutettavuudella ja käytettävyydellä on suuri merkitys. Tämän takia VIAN palvelut on jo nyt toteutettu niin, että arkkitehtuurissa ei ole yhtään yksittäistä teknistä kohtaa, jossa esiintyvä häiriö estäisi palvelun toimivuuden. Keskitetyssä integraatoratkaisussa myös kapasiteetin riittävyys ja palvelutason tasaisuus ovat haasteita tilanteissa, joissa useilla organisaatioilla on kuormitushuippu yhtä aikaa. Integraatiopalvelun nykyinen kapasiteetti mahdollistaa suuren volyymin sanomien välitykselle, mutta kapasiteettia voidaan tarvittaessa myös kasvattaa. Kapasiteetin riittävyyden varmistamiseksi VIP on toteuttanut valmiit suunnitelmat kuinka kapasiteettia saadaan tarvittaessa lisättyä. VIP toteuttaa jatkuvasti kapasiteetin ja käytettävissä olevien resurssien käytön seuranta.

Resurssien suunnittelun helpottamiseksi liittymien määrittelyssä tulee arvioida myös palvelupyyntöjen volyymit. Lisäksi palvelua käyttävän organisaation tulee informoida



myös VIAa, mikäli palvelupyyntöjen määrä tulee kasvamaan olemassa olevassa liittymässä merkittävästi.

VIA:n nykyiset ratkaisut tarjoavat jo nyt mahdollisuuden läpimenevien sanomien rajoittamiseen. Kriittisille, paljon käytettäville palveluille on mahdollista erottaa VIAssa omat domainit, jolloin nämä palvelut eivät häiritse muita palveluita.

5 Yleiset palvelut

5.1 Palvelurekisteri

PERA-määrittelytyön yhteydessä havaittiin tarve keskitetyille palvelurekisterille, johon voidaan sijoittaa eri organisaatioiden rajapintakuvaukset. Keskitetyllä palvelurekisterillä pyritään saamaan rajapintakuvaukset helposti saataville ja poistamaan tarve organisaatiokohtaisille palvelurekistereille.

VIA:n, VIPin tai jonkin muun valtiotason organisaation tulee tarjota tulevaisuudessa palvelurekisteri valtionhallinnon organisaatioiden palveluiden rajapintakuvauksille sekä muille palveluiden käyttöön liittyville hallinnollisille tiedoille. Luotavaan palvelurekisteriin tulee tallentaa PERA-määrityksen mukaisten palveluiden lisäksi muutkin olemassa olevat palvelut, jotta palvelurekisteristä saadaan kattava. Palvelurekisteriä hallinnoivan organisaation vastuu rajautuu rekisterin hallinnointiin. Palvelua tarjoava organisaatio on keskitetyn rekisterin käyttöönoton jälkeenkin vastuussa omien palveluidensa dokumentaatiosta ja muutoksenhallinnasta.

Palvelurekisterin tulee tarjota palveluiden ja välitettävien tietosisältöjen kuvaukset myös koneluettavassa muodossa, jotta palveluiden käyttöönotto olisi yksinkertaisempaa.

VIA:n tulee pitää kirjaa mitkä organisaatiot käyttävät mitäkin palvelua versiokohtaisesti. Nämä tiedot helpottavat olemassa olevien palveluiden muutoksenhallintaa. Lisäksi VIA:n tulee voida raportoida kutsujen volyymit tarvittaessa asiakaskohtaisesti, jotta palvelua tarjoava organisaatio näkee kuinka eri organisaatiot kuormittavat heidän palveluitaan.

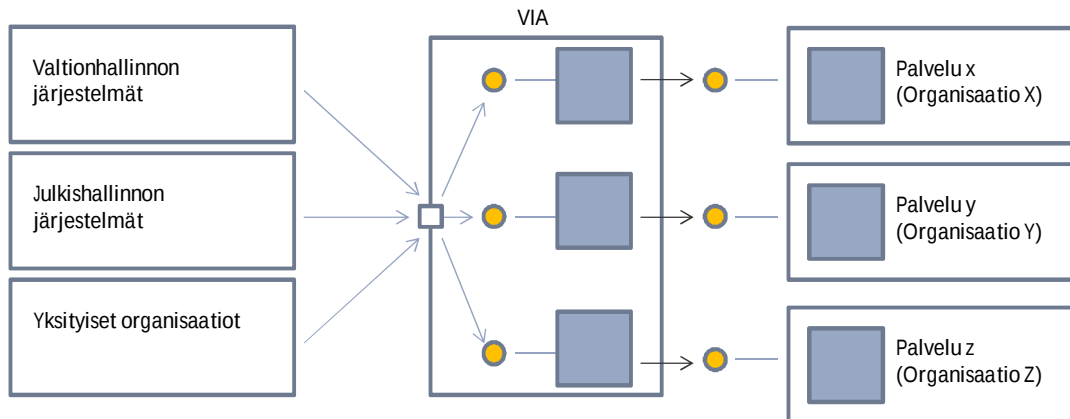
5.2 Integraatioihin liittyvät tukipalvelut

VIA:n tulee tarjota asiakkailleen tukipalvelut liittyen integraatiossa esiintyviin teknisiin ongelmiin. Tukipalvelu on tarkoitettu asiakasorganisaatioiden teknisten henkilöiden tueksi, ei loppukäyttäjän. Muu tukitoiminta kuuluu palvelua tarjoavalle tai kutsuvalle organisaatiolle.

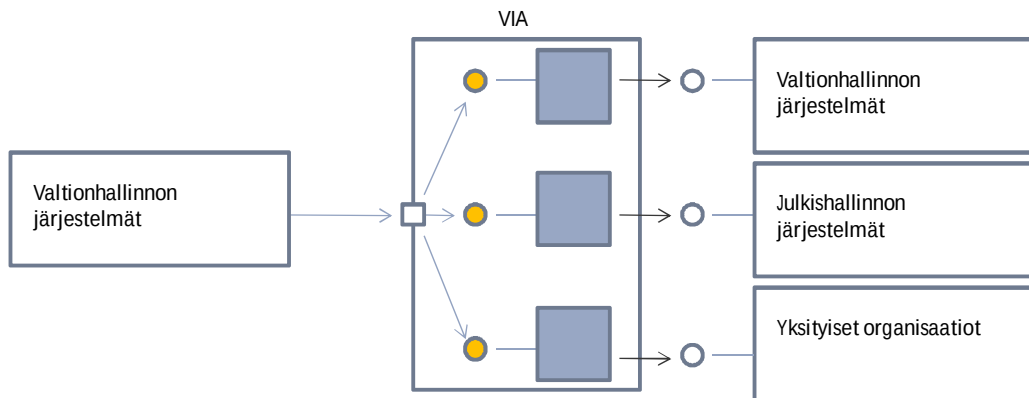


6 Sovellus-sovellus integraatiot

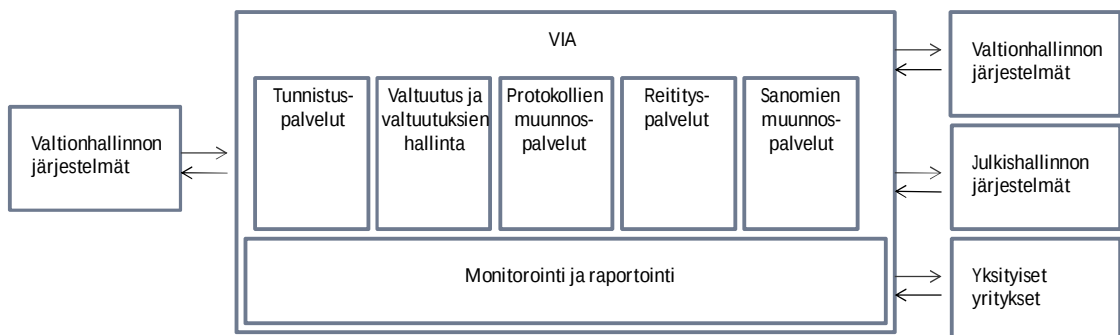
Kaikki VIA:n kautta julkaistut palvelut ovat käytettävissä yhden juuri-URL:n alaisuudesta. Tämä helpottaa palveluiden käyttöönottoa esimerkiksi tietoliikenneavauksien määrän vähenemisenä.



VIA tarjoaa myös valtionhallinnon organisaatioille keskitetyn reitin muiden organisaatioiden tarjoamien palveluiden kutsumiseen.



VIA:n sovellus-sovellus -integraatioihin tarjottavat palvelut on kuvattu alla olevassa kuvassa.



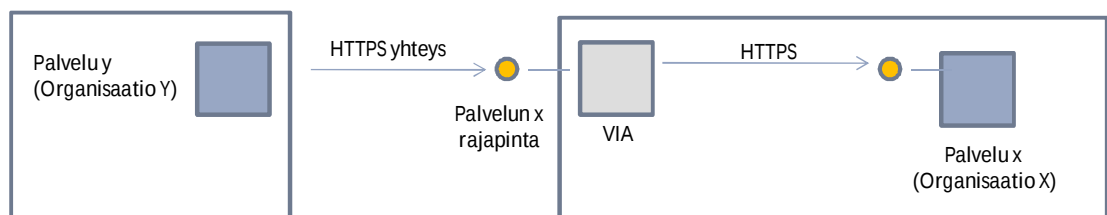


VIA:n tulee tarjota sovellus-sovellus -palvelupyyntöihin esimerkiksi

- Tuki synkronisille kutsuille
- Tuki asynkronisille taustajärjestelmien kutsuille
- Tuki asynkronisille palvelukutsuille (esim. päivittävät operaatiot)
- Tuki asynkroniselle vastauksille
- Toiminnallisuudet tiedostojen välittämiseen pyyntöjen yhteydessä, PERA-määrityksen mukaisesti
- Sanomien muunnospalvelut

6.1 Tunnistus

VIA:n tulee pystyä tunnistamaan palvelukutsut PERA-määrityksen mukaisilla tekniikoilla: HTTPS client -sertifikaateilla sekä sanoman allekirjoituksella. Tunnistuksen jälkeen VIA:n tulee sijoittaa tunnistetun organisaation sekä järjestelmän tunnistetiedot palvelupyyntöön metatietoihin, mikäli tunnistus toteutetaan myös palvelua tarjoavassa organisaatiossa.



Yllä olevassa kuvassa on esitetty palvelupyyntöjen välittäminen VIA:n kautta kutsuttavalle palvelulle. Lähtökohtaisesti viestiliikenne salataan tietoliikennetasolla, käyttäen HTTPS:ää, jolloin pyyntöjen kuljettaminen VIA:n kautta tarvitsee kaksi HTTPS-yhteyttä.

Vasteaikojen optimoimiseksi VIA:n tulee kyetä käyttämään HTTP:n keep alive -toiminnallisuutta SSL/TLS:llä suojatuissa yhteyksissä, koska muuten yhteydenluontien vasteajat aiheuttavat merkittävän vasteaikaongelman palvelupyyntöille.

6.2 Valtuutus ja valtuuksien hallinta

VIA:n tulee tarjota integraatioihin liittyvien valtuutuksien hallinta organisaatio- ja järjestelmätasolla. Tällä tasolla VIA:ssa voidaan toteuttaa myös palvelulle tulevien palvelupyyntöjen auktorisointi. Tarvittaessa VIA välittää tunnistustiedot pyynnön kehystiedoissa palvelua tarjoavalle organisaatiolle, jolloin palvelua tarjoava organisaatio voi toteuttaa tarkemmat valtuutuksien tarkistukset.

6.3 Protokollan muunnospalvelut

VIA tarjoaa palvelut protokollamuunnoksiin palvelukutsuissa, esimerkiksi tiedostopohjainen rajapinta voidaan muuttaa pohjautumaan HTTP-protokollaan. Lisäksi



VIAssa tulee voida tehdä muutoksia protokollaversioiden välillä, jolloin esimerkiksi SOAP 1.2 pohjaiset palvelut voidaan konvertoida SOAP 1.1 pohjaisiksi VIAssa.

VIAN tulee voida muuttaa REST-tyyppiset palvelut SOAP-tyyppisiksi ja toisinpäin, huomioiden myös metatietojen sekä virheiden raportoinnin.

6.4 Sanomien muunnospalvelut

VIA tarjoaa palvelut sanomien formaattien muunnoksiin. Sanomia voidaan muuntaa esimerkiksi XML-muodosta ei-XML-muotoon, ja toisin päin. Tällä voi olla suurta merkistystä aineistojen latauksissa.

Sanomia voidaan muuntaa myös eri XML-muotojen välillä. Tätä voidaan hyödyntää esimerkiksi silloin, kun halutaan tehdä valmisohjelmistojen rajapinnoista PERA-määritysten ja JHS170-suositusten mukaisia palveluita.

VIA suorittaa merkistöjen muunnokset palvelun tarjoajan ja käyttäjän välillä. Jos esimerkiksi palvelun tarjoaja ei kykene tarjoamaan merkistöä, jota käyttäjät tarvitsevat, VIA suorittaa merkistönmuunnoksen.

6.5 Reitityspalvelut

VIA tarjoaa palvelukutsujen reitityksen.

Reititys voi olla staattinen, jolloin tietyn palvelun kutsu välitetään aina tiettyyn kohdeosoitteeseen. Tällöin saavutetaan se hyöty, että kohdeosoitteen muutos merkitsee muutosta ainoastaan VIAssa.

VIAssa tulee voida suorittaa myös ehdollista reititystä, jolloin kutsuttavan palvelun sanoma valitaan sisällön perusteella. Molemmissa vaihtoehdoissa VIAN tulee suorittaa myös kuormantasausta kohdejärjestelmän palvelulle / palveluille. Jos taustajärjestelmän palvelu on saatavissa useasta eri paikasta, VIA:n tulee voida suorittaa kuormanjakoa näiden välillä.

Reititys voi olla myös puhtaasti dynaamista, jolloin palvelun kutsuja voi ilmoittaa VIALle mitä palvelua se haluaa VIAN kutsuvan. Dynaamista reititystä on mahdollista hyödyntää mm. Callback-palvelukutsuissa, joissa palvelun tarjoaja tehdessään Callback-kutsun VIAN kautta ilmoittaa osoitteen, johon kutsu ohjataan.

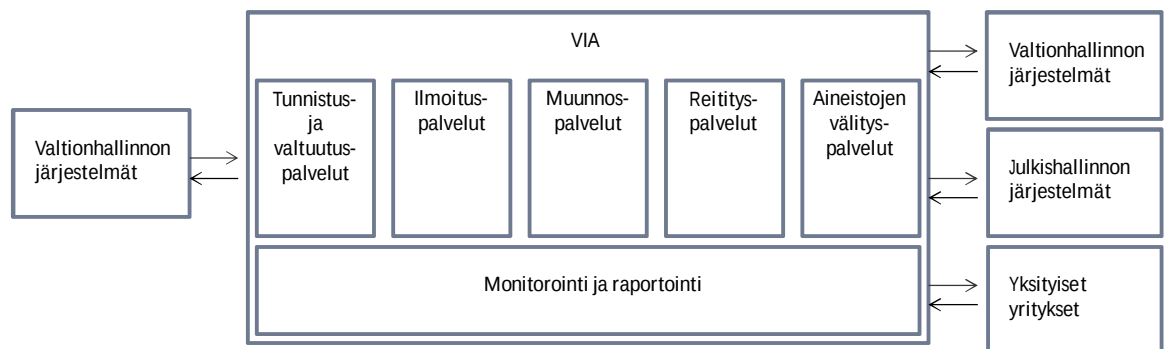
6.6 Monitorointi ja raportointi

VIAN tulee tarjota asiakkailleen monitorointityökalut, joilla voidaan seurata pyyntöjen ja virheiden määrää sekä vasteaikoja. Raporteilta tulee nähdä tiedot palveluittain sekä asiakkaittain. Lisäksi VIAN tulee voida tarjota mahdollisuus sanomatason lokitukseen mikäli asiakkaalla on siihen tarve.



7 Aineistonvälitys

VIAN tulee tarjota aineistonvälityspalvelua, joka tarjoaa aineistojen siirron lisäksi tunnistus-, muunnos-, reititys-, ilmoitus- sekä monitorointi- ja raportointipalvelut. Aineistojen julkaisun tulee olla mahdollista VIAN kautta muille julkishallinnon organisaatioille ja yksityisille yrityksille. Lisäksi aineistojen vastaanoton tulee olla mahdollista eri tyyppisistä organisaatioista, mikäli palvelun tilaaja on valtionhallinnon organisaatio.



Keskitetty aineistonvälitysratkaisu auttaa organisaatioita, jotka julkaisevat samoja aineistoja useille asiakkaille tai joilla on paljon asiakkaita, joiden kanssa siirretään aineistoja. VIAN kautta tarjottavat aineistonvälitysratkaisut näkyvät valtionhallinnon ulkopuolisille organisaatioille yhtenä kokonaisuutena, jolloin tarvittavat tietoliikenneavaukset vähenevät.

VIAN tulee tarjota mahdollisuus myös HTTPS-pohjaiseen aineistonvälitykseen. Tällöin aineisto noudetaan joko suoraan organisaation tarjoamasta HTTPS-palvelusta tai VIAN tarjoamasta välivarastosta, johon aineisto on siirretty esimerkiksi SFTP-pohjaisesti.

7.1 Tunnistus- ja valtuutuspalvelu

VIAN tulee tarjota aineistonvälitykseen tunnistus- ja auktorisointipalvelut mukaan lukien SSH-avaimien hallinnointi.

7.2 Aineistojen siirto

VIAN tulee tarjota aineistojen siirtoon palvelut, joissa yksi aineisto toimitetaan yhdelle tai monistetaan useille asiakkaille. Aineistojen siirto voi pohjautua ratkaisuun, jossa aineistot joko noudetaan määritetystä SFTP-hakemistosta tai tarjotaan paikka, johon aineistot voidaan tallentaa.

VIAN tulisi tarjota aineistojen siirron ajoittamiseen muutama eri vaihtoehto:

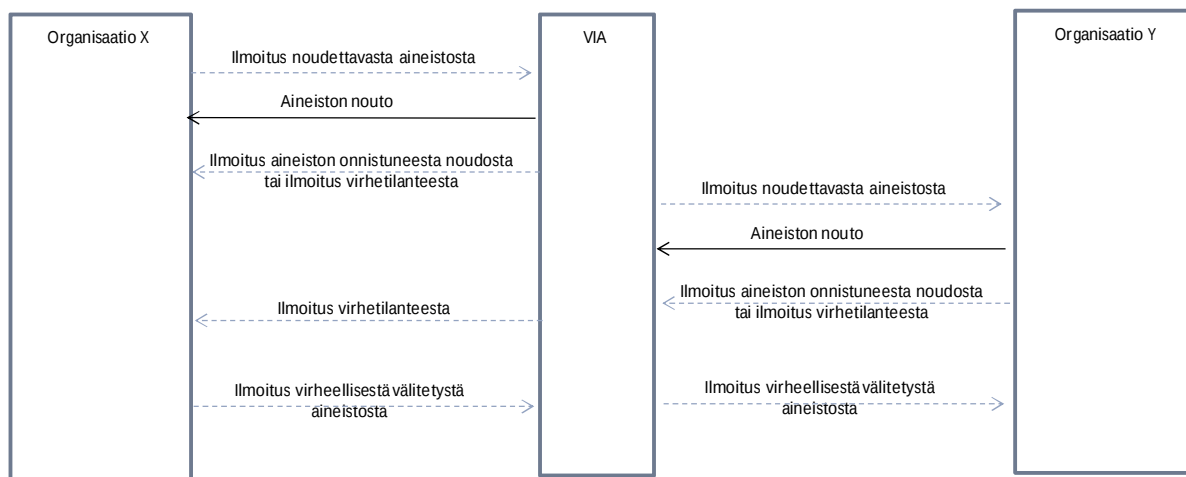
Ajastettu aineistojen siirto	Aineistojen oletetaan olevan tiettyyn aikaan mennessä noudettavissa, jonka jälkeen VIA
------------------------------	--



	siirtää aineistot asiakkaalle / asiakkaille sovittuun aikaan mennessä.
Toimitus aineiston saapumisen jälkeen	VIA seuraa aineiston saapumista määriteltyyn hakemistoon ja toimittaa aineiston välittömästi eteenpäin asiakkaille.
Aineiston toimitus erillisen ilmoituksen jälkeen	Aineiston toimittaja lähettää sovellus-sovellus-yhteydellä VIAlle ilmoituksen aineiston valmiudesta. VIA noutaa aineiston ja välittää sen kohdeorganisaatioille.

7.3 Tiedotuspalvelu

VIAN tulee tarjota aineistovälitykseen toiminnallisuus, jossa aineistojen saapumisista, toimituksista sekä virhetilanteista lähetetään viestit informaatiosta kiinnostuneille osapuolille.



Yllä olevassa kuvassa on esimerkin omaisesti kuvattu kuinka VIA voisi tiedottaa aineistovälityksen osapuolia aineistojen saapumisista, toimituksista, häiriöistä sekä virhetilanteista.

Ilmoituksen tyyppi	vastaanottaja
ilmoitus noudettavasta aineistosta	VIA, Organisaatiot joille aineistot toimitetaan
ilmoitus aineiston onnistuneesta noudosta	Aineiston toimittanut organisaatio
ilmoitus virhetilanteesta	VIA (mikäli lopullinen vastaanottaja havaitsee virheen),



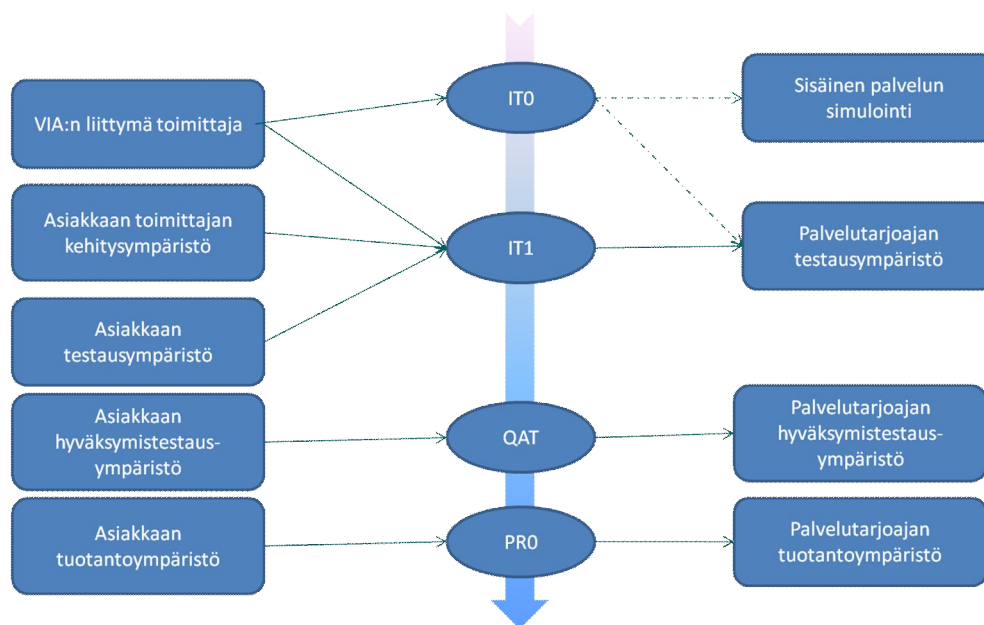
	Aineiston toimittanut organisaatio
ilmoitus häiriöstä	VIA, Aineistoa vastaanottavat organisaatiot
ilmoitus virheellisestä, välitetystä aineistosta	VIA, Aineistoa vastaanottaneet organisaatiot

7.4 Monitorointi ja raportointi

Asiakkaat tarvitsevat tiedot välitetyistä aineistosta, tapahtumien ajanhetkistä sekä onnistumisista ja epäonnistumisista. Tämän takia VIAN aineistonvälityspalvelun tulee tarjota työkalut, joilla asiakkaiden edustajat voivat seurata aineistonvälityksen toimivuutta.

8 Testiympäristöt

VIA tarjoaa asiakkailleen tuotantoympäristöjen lisäksi erilaisia testiympäristöjä. Alla olevassa kuvassa on esitetty eri testiympäristöt ja kuvattu kuinka VIAN testausympäristöjä voidaan käyttää liittymän kehityksessä ja testauksessa.



- ITO kehitysympäristö
 - tarkoitettu VIA:n sisäiseen liittymäkehitykseen ja testaukseen
- IT1 integraatiotestausympäristö
 - suoritetaan VIA:n kehittämien liittymien varsinainen testaus asiakasympäristöä vasten



- kehitys ja testausympäristö asiakkaan toimittajalle
- asiakkaan ensimmäisen asteen testaus
- suurin osa kehitys- ja testaustyöstä suoritetaan täällä
- QAT hyväksymistestausympäristö
 - liittymien hyväksymistestaus – tuotannon kopio
- PRO tuotanto
 - varsinainen tuotantoympäristö

9 Muutoshistoria

Versio	Päiväys	Tekijä	Tarkastaja	Hyväksyjä	Muutoshistoria
1.0	8.12.2011	Jukka Matilainen, Jussi Lattu	Jukka Uusitalo		Viimeistelty versio
0.9	31.5.2011	Jukka Matilainen, Jussi Lattu	Jukka Uusitalo		Luonnosversio lausuntokierrosta varten
0.2	24.11.2010	Jukka Matilainen, Jussi Lattu	Jukka Uusitalo		Luonnosversio julkaistavaksi työryhmän välituloksissa 2010