Infotilaisuus Suomi.fi-palveluväylän uusista ominaisuuksista

ti 27.4.2021 klo 14.00–15.30

DIGI- JA VÄESTÖTIETOVIRASTO

Liittyminen Suomi.fi-palveluväylään

*Palveluväylä on helpoin tapa **yksinkertaistaa organisaatiosi it-arkkitehtuuria tietoturvallisesti**: vähemmän integraatioita, enemmän aikaa kehitykselle. Mitä useampi toimija liittyy käyttäjäksi, sitä suurempi hyöty siitä seuraa Palveluväylän käyttäjille ja loppuasiakkaille.*

Uudistamme käyttöönoton ohjeistusta:

- Käyttöönoton tueksi on nyt tarjolla viisiosainen videosarja Palveluväylään liittymisestä
- Soittolista videoista löytyy suomifi:n YouTube-kanavalta: https://www.youtube.com/watch?v=L1vr1SNR7Ng&list=PL_4wcX5Kd8SGR0bDbg66N25BIO19mMYKP

Nordic Institute for Interoperability Solutions

What's new in X-Road 6.26.0?

PETTERI KIVIMÄKI, CTO @pkivima

Release notes

- The official release notes are available at:
  - https://confluence.niis.org/display/XRDKB/X-Road+v6.26.0+Release+Notes

Support for alternative Java 8 distributions on Ubuntu

- Ubuntu OpenJDK 8 support ends after April 2021.
- Therefore, it is strongly recommended to migrate from the Ubuntu OpenJDK to AdoptOpenJDK which will be supported until 2026.
- Installation guide for Ubuntu has been updated to include AdoptOpenJDK installation.
- Migration instructions for existing installations are available at (**requires version 6.26.0 or later**):
  - https://confluence.niis.org/display/XRDKB/How+to+migrate+Security+Server+and+Central+Server+from+OpenJDK+8+to+AdoptOpenJDK+8
- RHEL versions of the Security Server are not affected and OpenJDK 8 continues to be supported.

Security improvements

- Write special characters to audit log in encoded format.
  - Special characters in the audit log are now displayed in the JSON escaped format.
  - For example: { "user":"xrd**\u0085**user" }
- Add CSRF protection to Security Server's management API's "API keys" endpoint.
  - In previous versions, the API endpoint wasn't vulnerable to CSRF exploits because of existing configuration prevented them. However, without a proper CSRF protection future configuration changes could have exposed the problem.

Enhancements

- Add Subject Alternative Name (SAN) to the Security Server UI certificate details view.
  - For the management REST API users this introduces a new field to the CertificateDetails type.
- Update the Security Server UI local groups view to forbid adding non-printable characters.
- Improve the Security Server UI input validation of REST endpoint “path” fields.

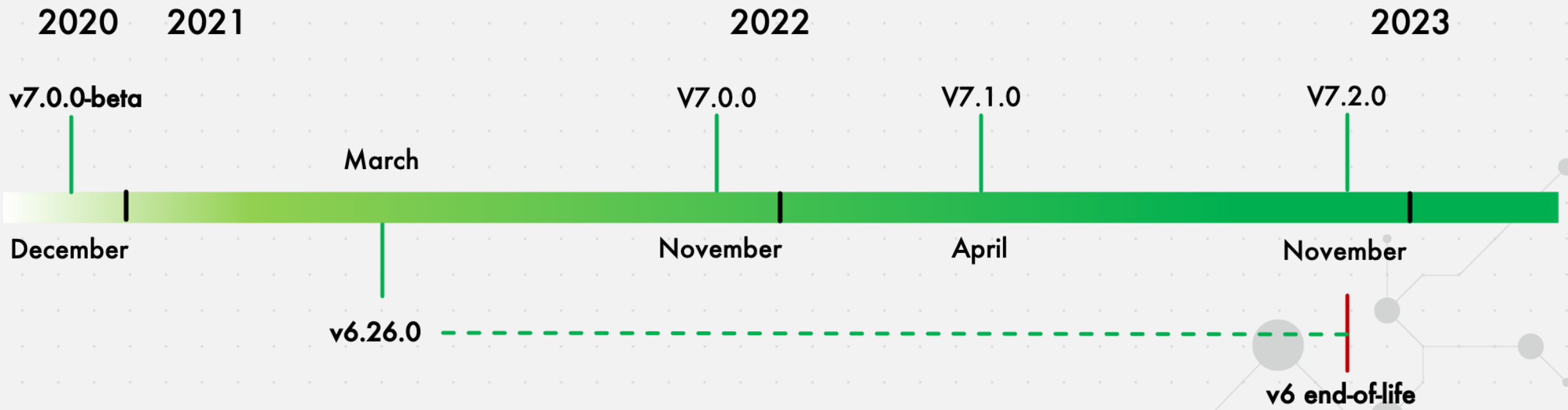
Enhancements

- Update the Security Server clustering documentation to cover Ubuntu 20.04 and RHEL 8 setups.
  - https://github.com/nordic-institute/X-Road/blob/develop/doc/Manuals/LoadBalancing/ig-xlb_x-road_external_load_balancer_installation_guide.md
- Log the Java version being used to run a component at startup. In case the version is not supported by the software a warning is logged.

Bug fixes

- Fix issue causing log file entries being hardcoded to use the UTC timezone. Now the logs default to the server's timezone.
- Fix issue causing the log file "/var/log/xroad/proxy_ui_api_access.log" not being created.
- Fix incorrectly displaying session expiration errors in the Security Server UI when navigating away and back to the server.
- Fix installing xroad-opmonitor packages on a server with no Security Server installed.
- Minor bug fixes to the Security Server UI.

X-Road development roadmap



https://x-road.global/development-roadmap

WWW.NIIS.ORG
WWW.X-ROAD.GLOBAL

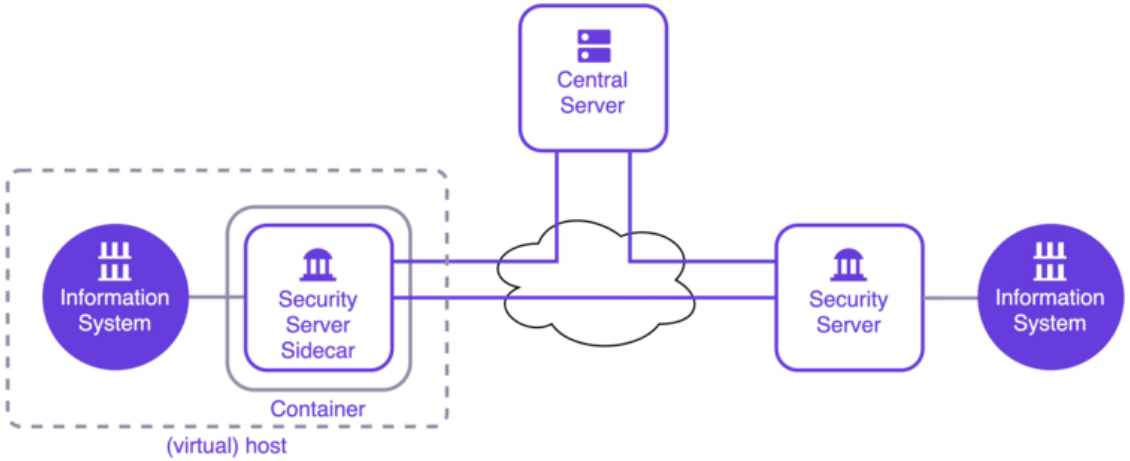
Docker-kontitettu Liityntäpalvelin (Sidecar)

Ilkka Seppälä
Tekninen Projektipäällikkö
Gofore Oyj

ilkka.seppala@gofore.com

Esittely

- Suomi.fi-palveluväylään voi nyt liittyä Docker-kontitetulla liityntäpalvelimella (Sidecar)
- Yksinkertaisimmillaan Sidecar asennetaan samalle palvelimelle asiointipalvelun kanssa
- Sidecar mahdollistaa myös entistä paremman pilven hyödyntämisen



Kontitetun liityntäpalvelimen edut

- ✓Parantaa Palveluväylän kehittäjäkokemusta
- ✓Alentaa kynnystä Palveluväylän käyttöönottoon
- ✓Kustannustehokkaampi tapa liittyä Palveluväylään
- ✓Automaattisesti skaalautuva klusteri pilvessä

Docker Imaget

- **Sidecarin Docker imaget löytyvät Dockerhubista**
- **Yksittäinen liityntäpalvelin Palveluväylän asetuksilla**
  - 6.25.0-fi
  - 6.25.0-slim-fi
- **Klusteroitu liityntäpalvelin Palveluväylän asetuksilla**
  - 6.25.0-primary-fi
  - 6.25.0-secondary-fi
  - 6.25.0-slim-primary-fi
  - 6.25.0-slim-secondary-fi
- **Slim-versiot ovat tarkoitettu ainoastaan palveluiden hyödyntämiseen. Niissä ei ole mukana sanomien lokitusta eikä monitorointiominaisuuksia.**

Asennus

- **Sidecarin tuotantokäyttö on tuettu ainoastaan Linux-alustalla**

```
$ docker run --detach -p <ui port>:4000 -p <http port>:80 -p 5588:5588 \
--network xroad-network -e XROAD_TOKEN_PIN=<token pin> -e XROAD_ADMIN_USER=<admin user> \
-e XROAD_ADMIN_PASSWORD=<admin password> -e XROAD_DB_HOST=<database host> \
-e XROAD_DB_PORT=<database port> -e XROAD_DB_PWD=<database password> \
-e XROAD_LOG_LEVEL=<log level> -e XROAD_CONF_DATABASE_NAME=<database name> \
--name <container name> niis/xroad-security-server-sidecar:6.25.0
```

- **Lisäksi konfiguraatiotiedostot kannattaa tallentaa kontin ulkopuolelle (kts. volume support käyttöoppaassa)**

Käyttöympäristöt

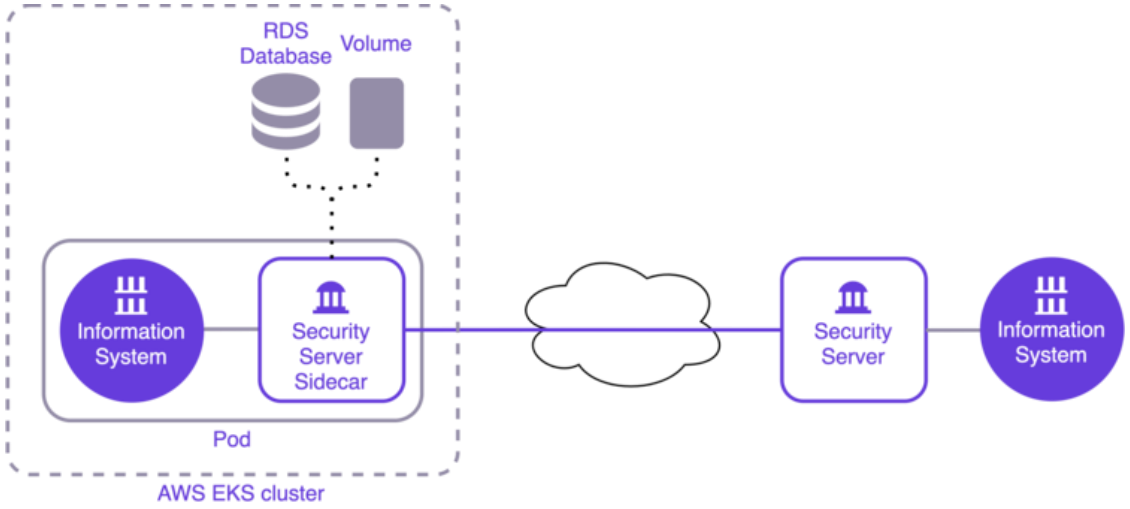
- **Valitse liityntäpalvelimen käyttöympäristö organisaation tarpeiden mukaan. Suositus on ajaa samassa ”kontekstissa” asiointipalvelun kanssa.**
  - Asiointipalvelun Linux-palvelinkone
    - Kevyt vaihtoehto - kontitettu liityntäpalvelin asennetaan samalle koneelle asiointipalvelun kanssa
  - Konesali Suomessa
    - Jos palveluväylän yli välitettävän tiedon tulee pysyä Suomessa, täytyy liityntäpalvelin sijoittaa johonkin Suomessa olevaan konesaliin
  - Pilviympäristö
    - Järeisiin käyttötapauksiin - kun liityntäpalvelimelta vaaditaan vikasietoisuutta, suorituskykyä ja skaalautuvuutta

Pilviympäristö

- **Sidecaria on mahdollista ajaa pilvessä monilla eri tavoilla, mutta olemme keskittyneet tukemaan erityisesti AWS EKS –palvelua**
- **Amazon Elastic Kubernetes Service (EKS) on Kubernetes-palvelu, joka automatisoi tehtäviä liittyen konttien hallintaan**
  - Kuormantasaus
  - Itsekorjautuvuus
  - AWS:n tarjoama alustan ylläpito ja tietoturva

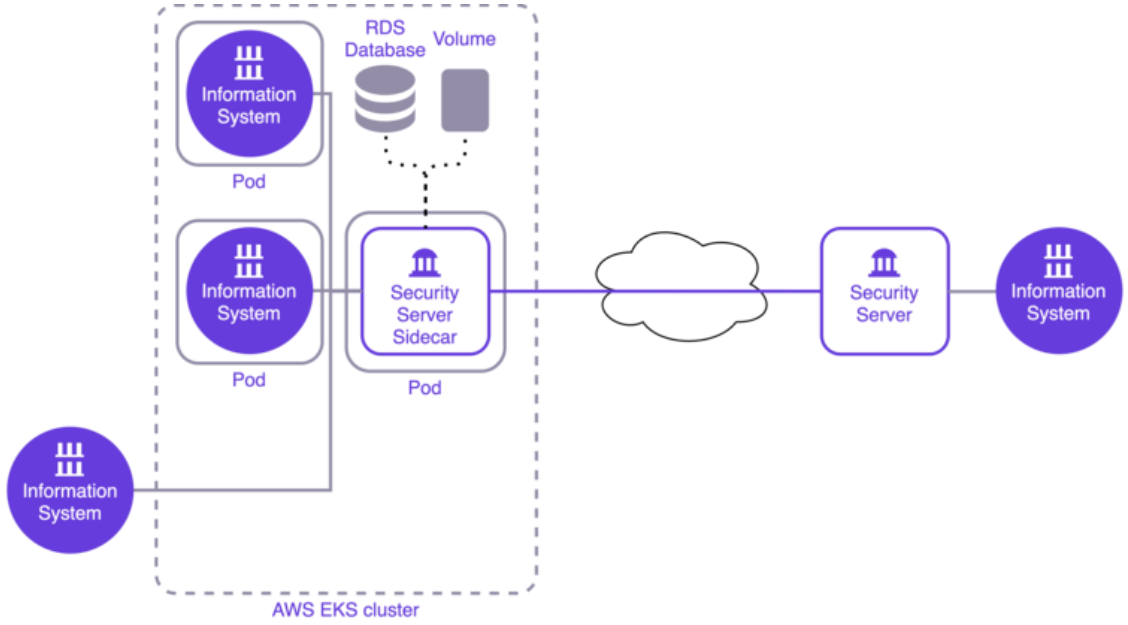
AWS EKS 1/4

- Asiointijärjestelmä- ja Sidecar-kontit samassa podissa
- Konfiguraatio tallennetaan kontin ulkopuolelle, esim. RDS-tietokantaan ja EBS/EFS-volumeen



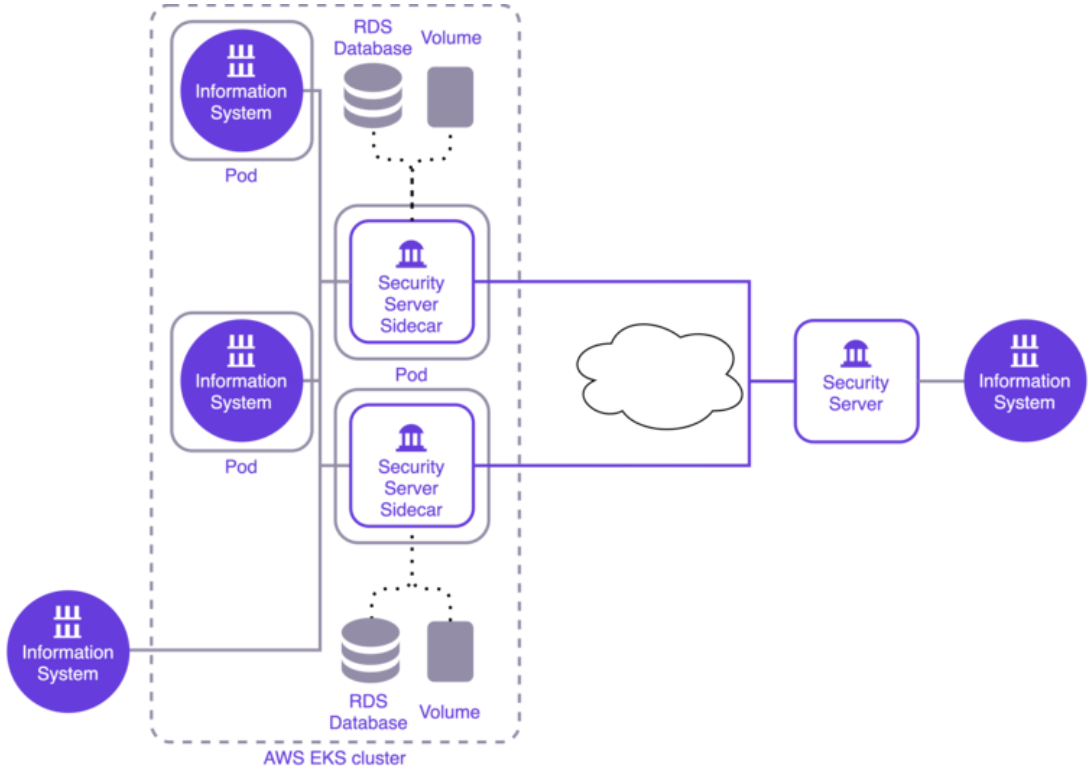
AWS EKS 2/4

- Eri asiointijärjestelmät ja Sidecar omissa podeissaan
- Asiointijärjestelmät jakavat saman liityntäpalvelimen
- Vika Sidecar-kontissa aiheuttaa katkoksen palveluissa



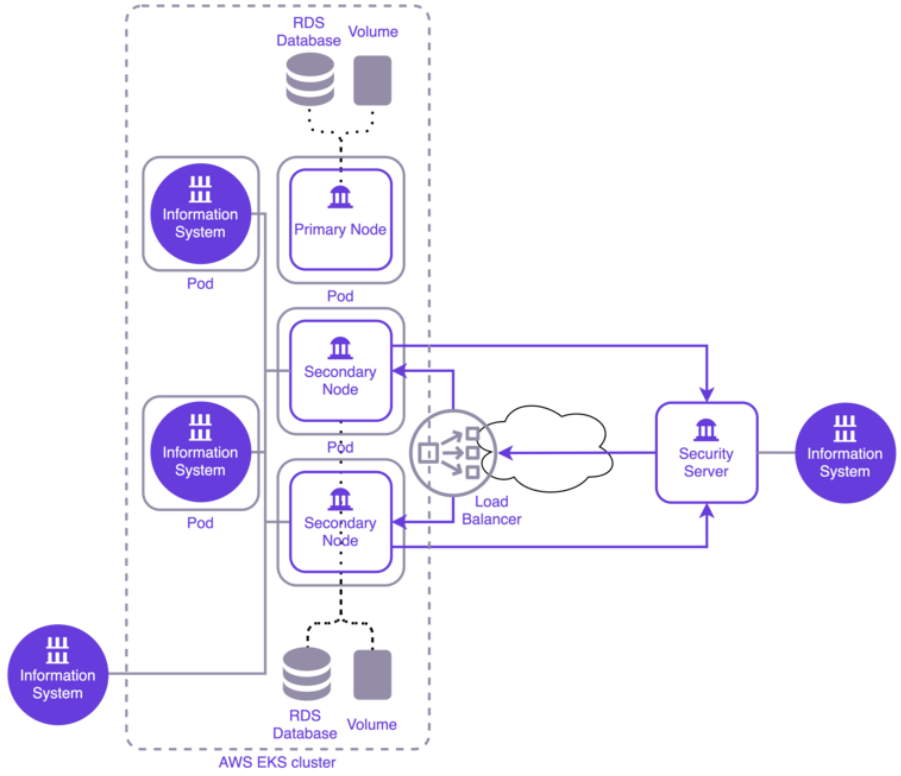
AWS EKS 3/4

- Kaksi Sidecar-konttia tarjovat useampia palveluita vikasietoisessa konfiguraatiossa
- Käyttää X-Roadin sisäänrakennettua kuormantasausta



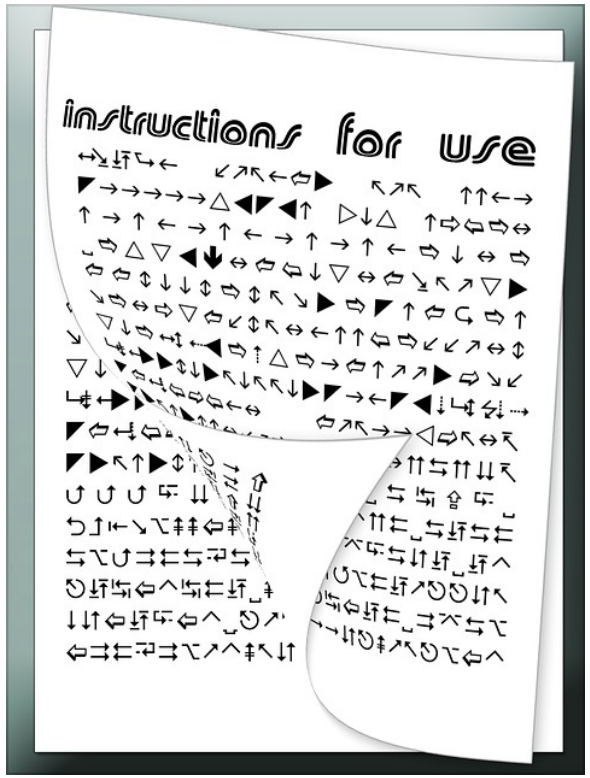
AWS EKS 4/4

- Palveluiden tarjoaminen ulkoisen kuormantasaajan avulla
- Vikasietoisuus ja suorituskyky
- Automaattinen skaalaus



Lisätietoa

- Suomi.fi liityntäpalvelimen käyttöönoton ohjeistus
- Sidecarin lähdekoodi ja käyttöoppaat Githubissa
- NIIS:in blogisarja Sidecarista
- Goforen blogi Sidecarista



Automaation Mahdollistavat Skriptit

Ilkka Seppälä
Tekninen Projektipäällikkö
Gofore Oyj

ilkka.seppala@gofore.com

Taustaa 1/2

- Liityntäpalvelimen konfigurointi on perinteisesti suoritettu sen tarjoamasta käyttöliittymästä
- Liityntäpalvelimen manuaalinen konfigurointi on melko työlästä ja virhealtista
- Liityntäpalvelimen ”infrastruktuurimaisen” luonteen vuoksi automaatiolle sen pystyttämisessä on selvästi kysyntää

Taustaa 2/2

- X-Road 6.24.0 versiossa julkaistiin liityntäpalvelimen API, jonka avulla voi tehdä samat asiat kuin käyttöliittymässä
- API on melko matalalla tasolla ja automaatio suoraan sitä käyttämällä on työlästä
- Tästä lähti ajatus ”työkalupakista”, jonka avulla liityntäpalvelimen konfigurointi olisi mahdollista tehdä helposti ja automatisoidusti

X-Road Toolkit

- X-Road Toolkit on Python-pohjainen työkalu liityntäpalvelimen automaattiseen konfigurointiin
- Julkaistu Python Package Index (PyPI) – pakettina
- Lähdekoodi, asennusohjeet ja käyttöopas löytyvät Githubista

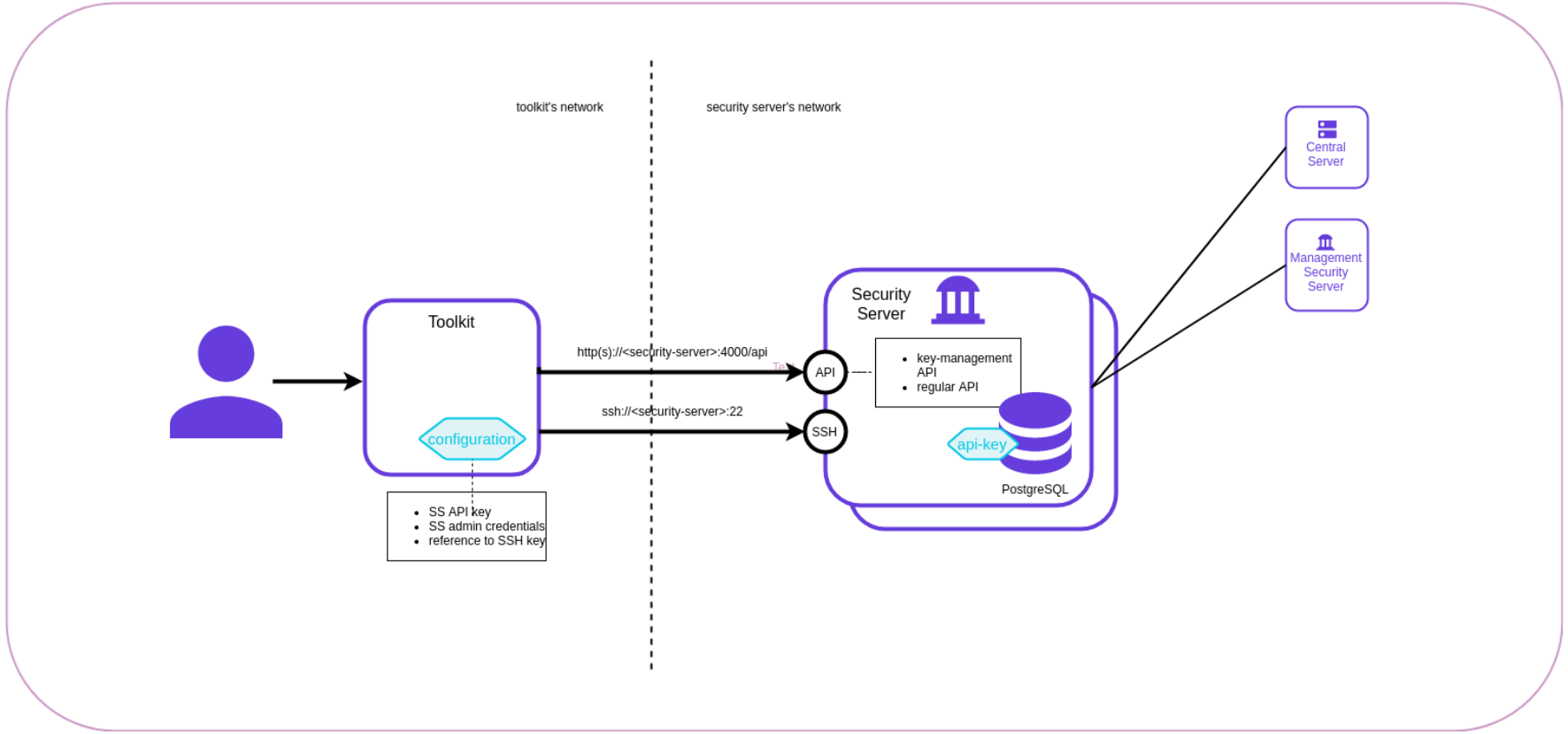
Käyttöönotto

- **Vaatimukset**
  - Python 3.6+, PIP 21.0+
  - Konfiguroitu keskuspalvelin ja keskuspalvelimen liityntäpalvelin
  - (suositus) Keskuspalvelimen asetukset, jotka tukevat automaattisia rekisteröintejä

```
$ pip install --extra-index-url http://xroad-toolkit.s3-website-eu-west-1.amazonaws.com/
xrdsst --trusted-host xroad-toolkit.s3-website-eu-west-1.amazonaws.com
```

- **Asennuksen jälkeen järjestelmässä on käytettävissä komento ’xrdsst’**
- **Toolkit toimii YAML-pohjaisen konfiguraation mukaan**
- **Kohteena voi olla yksi tai useampi liityntäpalvelin**

X-Road Toolkit



Konfiguraatiotiedosto

- **Toolkitin haluttu toiminta speksataan YAML-konfiguraatioon mm.**
  - Liityntäpalvelimien tiedot mm. osoite, viittaukset API-avaimeen ja SSH-tunnuksiin
  - Organisaatiot (member), alijärjestelmät (subsystem), palvelut (service), palveluiden pääsyoikeudet
  - Varmenteisiin tulevat tiedot

```
admin_credentials: <SECURITY_SERVER_CREDENTIALS_OS_ENV_VAR_NAME>
ssh_access:
  user: <SSH_USER_OS_ENV_VAR_NAME>
  private_key: <SSH_PRIVATE_KEY_OS_ENV_VAR_NAME>
security_server:
- api_key: <API_KEY>
  api_key_url: https://localhost:4000/api/v1/api-keys
  admin_credentials: <SECURITY_SERVER_CREDENTIALS_OS_ENV_VAR_NAME>
  configuration_anchor: /path/to/configuration-anchor.xml
  certificates:
    - /path/to/signcert
    - /path/to/authcert
  name: <SECURITY_SERVER_NAME>
  owner_dn_country: <OWNER_DISTINGUISHED_NAME_COUNTRY>
  owner_dn_org: <OWNER_DISTINGUISHED_NAME_ORGANIZATION>
  owner_member_class: <MEMBER_CLASS>
  owner_member_code: <MEMBER_CODE>
  security_server_code: <SERVER_CODE>
  software_token_id: <SOFT_TOKEN_ID>
  software_token_pin: <SOFT_TOKEN_PIN>
  fqdn: <SECURITY_SERVER_EXTERNAL_FQDN>
  url: https://<SECURITY_SERVER_INTERNAL_FQDN_OR_IP>:4000/api/v1
  ssh_user: <SSH_USER_OS_ENV_VAR_NAME>
  ssh_private_key: <SSH_PRIVATE_KEY_OS_ENV_VAR_NAME>
  clients:
    - member_class: <MEMBER_CLASS>
      member_code: <MEMBER_CODE>
```

Komentojen Ajaminen

- Toolkitin konfiguraatioon määritellyt toimenpiteet voidaan ajaa joko kaikki kerralla tai yksitellen
- ’xrdsst apply’ –komento ajaa koko konfiguraation kerralla
- Osia konfiguraatiosta voidaan ajaa yksitellen alikomennoilla esim. ’xrdsst init’ syöttää konfiguraatioankkurin ja alustaa liityntäpalvelimen tiedot

Komentojen ajaminen

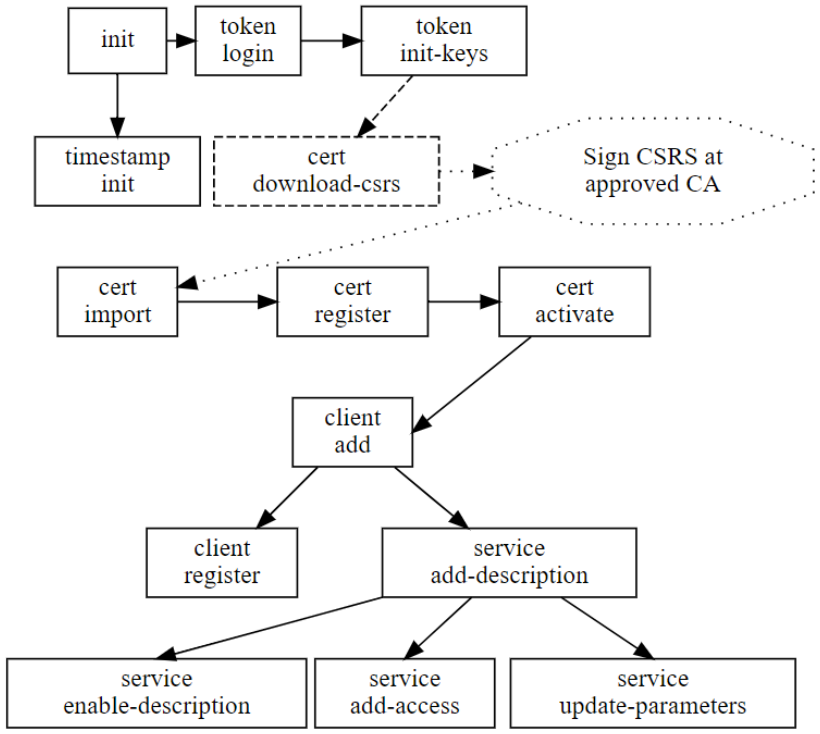
- **’xrdsst status’ näyttää yhteenvedon kohdeliityntäpalvelimien tilasta**

```
$ xrdsst status
```

GLOBAL	SERVER	ROLES	INIT	TSAS	TOKEN	KEYS	CSRS	CERTS
OK (SUCCESS) LAST 131158 0202 NEXT 131258 0202	ss5 VER 6.25.0 DEV:GOV:9876:UNS-SS5	System Administrator Service Administrator Registration Officer Security Officer Securityserver Observer	ANCHOR INITIALIZED CODE INITIALIZED OWNER INITIALIZED TOKEN INITIALIZED	Test TSA	ID 0 softToken-0 STATUS OK LOGIN NO	SIGN (2) AUTH (2) 4 KEYS	AUTH* (1) 1 CSRS	SIGN AUTH
OK (SUCCESS) LAST 131222 0202 NEXT 131322 0202	ss3 VER 6.25.0 DEV:GOV:9876:UNS-SS3	System Administrator Service Administrator Registration Officer Security Officer	ANCHOR INITIALIZED CODE INITIALIZED OWNER INITIALIZED TOKEN INITIALIZED	Test TSA	ID 0 softToken-0 STATUS OK LOGIN NO	SIGN (1) AUTH (1) 2 KEYS	SIGN (1) AUTH (1) 2 CSRS	
FAIL (INTERNAL) LAST 131217 0202 NEXT 131317 0202	ss4 VER 6.25.0	System Administrator Security Officer	TOKEN NOT_INITIALIZED			0 KEYS	0 CSRS	
	ss9	NO ACCESS						

Alikomennot

- Toolkitin ensimmäisessä versiossa on saatavilla komennot, jotka ovat pakollisia suorittaa palvelun pystyttämiseksi
- Jos keskuspalvelimen asetukset tukevat automaattisia rekisteröintejä, niin koko prosessi on mahdollista ajaa kahdessa osassa



Toolkitin Seuraavat Askeleet

Alikomentojoukko laajentuu

Vikasietoisten konfiguraatioiden tukeminen (internal load balancing)

Ulkoisen kuormantasaajan tukeminen (external load balancing)

Usean organisaation (member) niiden alijärjestelmien (subsystem) asentaminen samalle liityntäpalvelimelle

Parannuksia käytettävyyteen, tietoturvaan ja dokumentaatioon

Yhteenveto Palveluväylän uudistuksista

tuotepäällikkö Anssi Ahlberg

DIGI- JA VÄESTÖTIETO-VIRASTO

Helpompi liityntäpalvelimen määrittely

- **X-Road 6.24 hallintarajapinta**
  - Liityntäpalvelimen määrittely ja ylläpitotehtävien automatisoiminen
  - Liityntäpalvelimen etähallinta

- **Kontitettu liityntäpalvelin** skaalautuu useisiin käyttötarpeisiin
  - Konttina oman asiointipalvelun kyljessä Linux-palvelimella
  - AWS kyvykkyydet: Autoscaling: kapasiteetti, redundanssi, kuormansieto

- **Hallintaskriptit** ja muokkausohjeet

→ **Helpompi liityntäpalvelimen määrittely ja ylläpito**

Helpompi palveluiden hyödyntäminen

- **Uudistetut liittymisohjeet** Palveluhallinnassa
  - Hallinnollinen ohjeistus
  - Tekninen ohjeistus
  - Päivitetty ja laajennettu, yksityiskohtaisempi sisältö

- **Hae palvelun käyttölupaa** suoraan Liityntäkatalogissa
  - Palveluntarjoaja voi mahdollistaa käyttöluvan haun suoraan Liityntäkatalogissa
  - Useita toteutusvaihtoehtoja

- **Paremmat palvelukuvaukset** Palveluväylän palveluista
  - Viraston palveluiden kuvaukset päivitetään kesän aikana
  - Mallikuvaus ja ohjeistus muille palveluntarjoajille

→ **Helpompi ja nopeampi palveluiden hyödyntäminen**

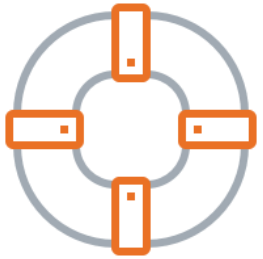
1+2+3+4 = 20

1. Kontitettu liityntäpalvelin
2. Hallintaskriptit
3. X-Road 6.24 hallintarajapinta
4. Päivitetyt ohjeet

=

- Nopeampi, helpompi ja kevyempi väylään liittyminen
- Enemmän vaihtoehtoja toteuttaa liityntäpalvelin
- Väylään liittyminen ja hallinta ostopalveluna
- Mahdollisuus tuottaa räätälöityjä asennuspaketteja asiakkaille, joilla on samanlaisia toistuvia käyttötarpeita (esim. kunnat, sote-sektori)

Haluatko liittyä palveluntarjoajien listalle?



- Keräämme Suomi.fi-palveluhallintaan listaa organisaatioista, jotka tarjoavat Palveluväylän käyttöönoton ja liityntäpalvelinten ulkoistamisen palveluita
- Vaatimuksena
  - **Liityntäpalvelinratkaisuja tarjoavien** täytyy olla rekisteröityneitä Palveluväylään ja Palveluväylän tuotantoympäristössä pitää olla ainakin yksi liityntäpalvelin
  - **Palveluväylän käyttöönottoa tarjoavilla** palveluntarjoajilla täytyy olla ainakin yksi referenssi Palveluväylän käyttöönoton toteutuksesta.

Ota yhteyttä palveluvayla-kayttoonotot@dvv.fi ja kerro organisaatiosi tarjoamista palveluista

Kiitos!

Kaikki kysymykset voi toimittaa myös jälkikäteen osoitteeseen

palveluvayla-kayttoonotot@dvv.fi

DIGI- JA VÄESTÖTIETO-VIRASTO