X-Road technical day
Meeting with Tunduk managers/administrators team

2022-11-03, Кыргыз Республикасы

Toomas Mölder, expert, Estonian e-Governance Academy (eGA)

General suggestions

- Add instance kg-test
- Do - Cluster
- Do - Upgrade
- Policy of HSM

Roadmap to improve Security Server mgmt

Problems:

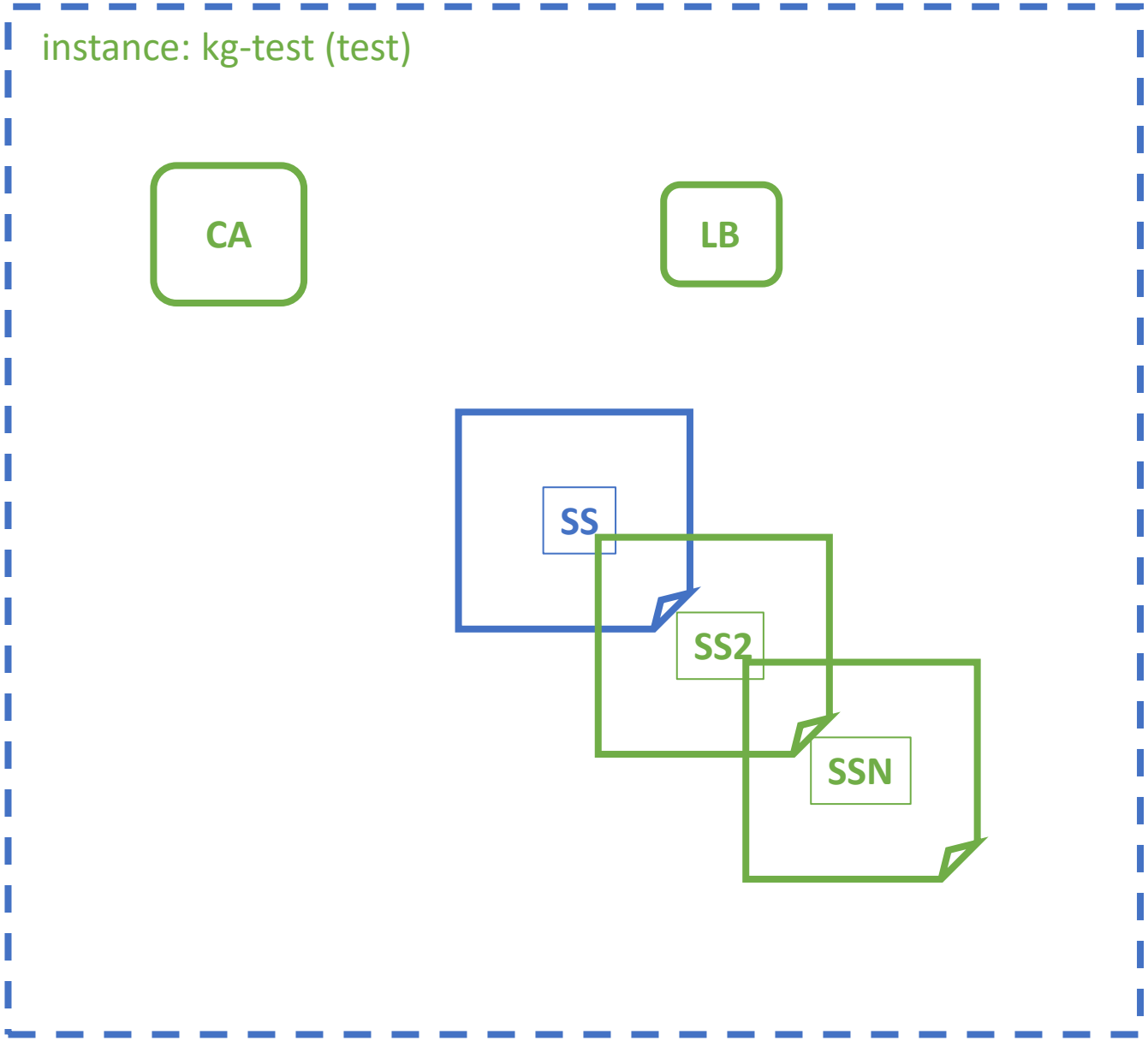
- Old versions of Tunduk (X-Road software)
- Service availability issues

- No test instance, only prod central-server
- No cluster of SS

Steps:

1. Use instance kg-test
2. CA for kg-test
3. New SS in kg-test
    1. upgrade*
    2. cluster, internal** OR
    3. cluster with external load balancer***

4. **DO THE SAME IN PROD!**



Upgrade

- Operating system
  - Upgrade regularly!
  - Ubuntu LTE 18.04 (until EOL april 2023)
  - Move into Ubuntu LTE 20.04
- X-Road Upgrade
  - Repository of Tunduk, own CA policy
  - 6.21 > 6.23
  - 6.23 > 6.24, as of recommended
  - 6.24 > 6.26, mandatory step before v7, seamless database migration
  - 6.26 > 7.1
- RTFM, release notes

Why to upgrade, features of v7

- REST support
- Addin for better management of message.log
- Bugfixes
- More useful update / upgrade
- Features
  - Automated registration, autoapprove
  - New UI
  - API first

wiki.tunduk.kg/doku.php?id=установка_сервера_безопасности

32%D0%
0%B5%D
D0%B7
.%D1%8

Войти

Центр электронного взаимодействия "Тундук"

Найти

Недавние изменения Управление медиафайлами Все страницы

Вы посетили: • установка_сервера_безопасности

установка_сервера_безопасности

Пошаговая инструкция по установке сервера безопасности Тундук

1 Введение

Целевой аудиторией руководства по установке являются системные администраторы Сервера безопасности Тундук ответственные за установку и сопровождение программного обеспечения X-Road. Документ предназначен для читателей с умеренными знаниями администрирования Linux серверов и компьютерных сетей.

2 Установка

2.1 Поддерживаемые платформы

Сервер Безопасности работает под управлением операционной системы Ubuntu Server 18.04 Long-Term Support (LTS) на 64 разрядной платформе. Дистрибутив Сервера Безопасности распространяется в пакетах формата .deb через официальное хранилище которое расположено по адресу https://deb.ordo.gov.kg Программное обеспечение может быть развернуто как на физическом, так и на виртуализированном оборудовании (на данный момент работа ПО была протестирована в виртуальном окружении KVM).

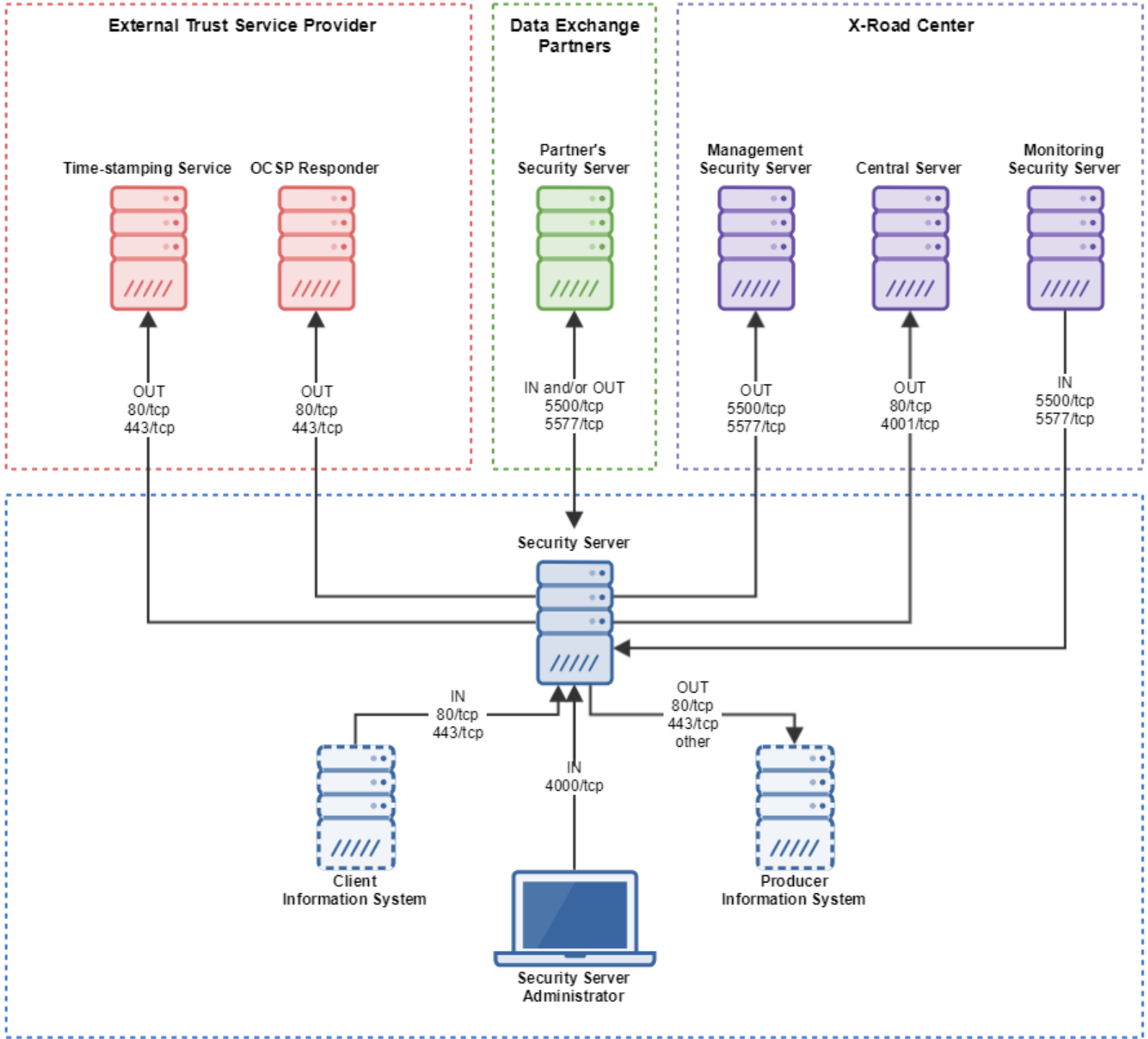
2.2 Справочные данные

Содержание

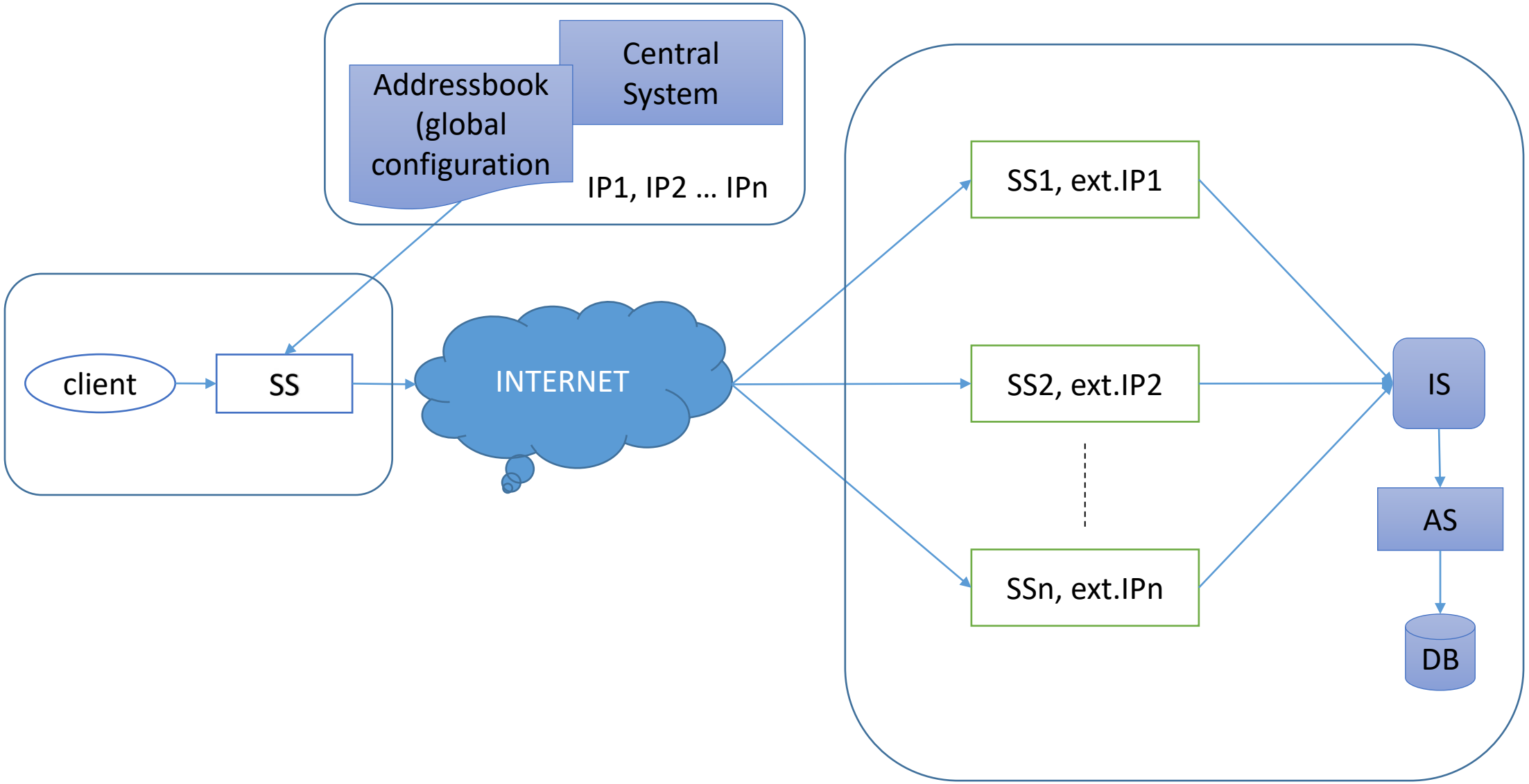
- Пошаговая инструкция по установке сервера безопасности Тундук
  - 1 Введение
  - 2 Установка
    - 2.1 Поддерживаемые платформы
    - 2.2 Справочные данные
    - 2.3 Требования к серверу Безопасности
    - 2.4 Подготовка операционной системы
    - 2.5 Установка программного обеспечения сервера безопасности
    - 2.6 Установить Поддержку аппаратных токенов (Smart-card, USB Token, Hardware Security Module)
    - 2.7 Проверка сервера после установки
  - 3 Первоначальная настройка сервера безопасности
    - 3.1 Предпосылки
    - 3.2 Справочные данные
    - 3.3 Настройка
    - 3.4 Настройка службы

Migration Guide from version 6 to version 7

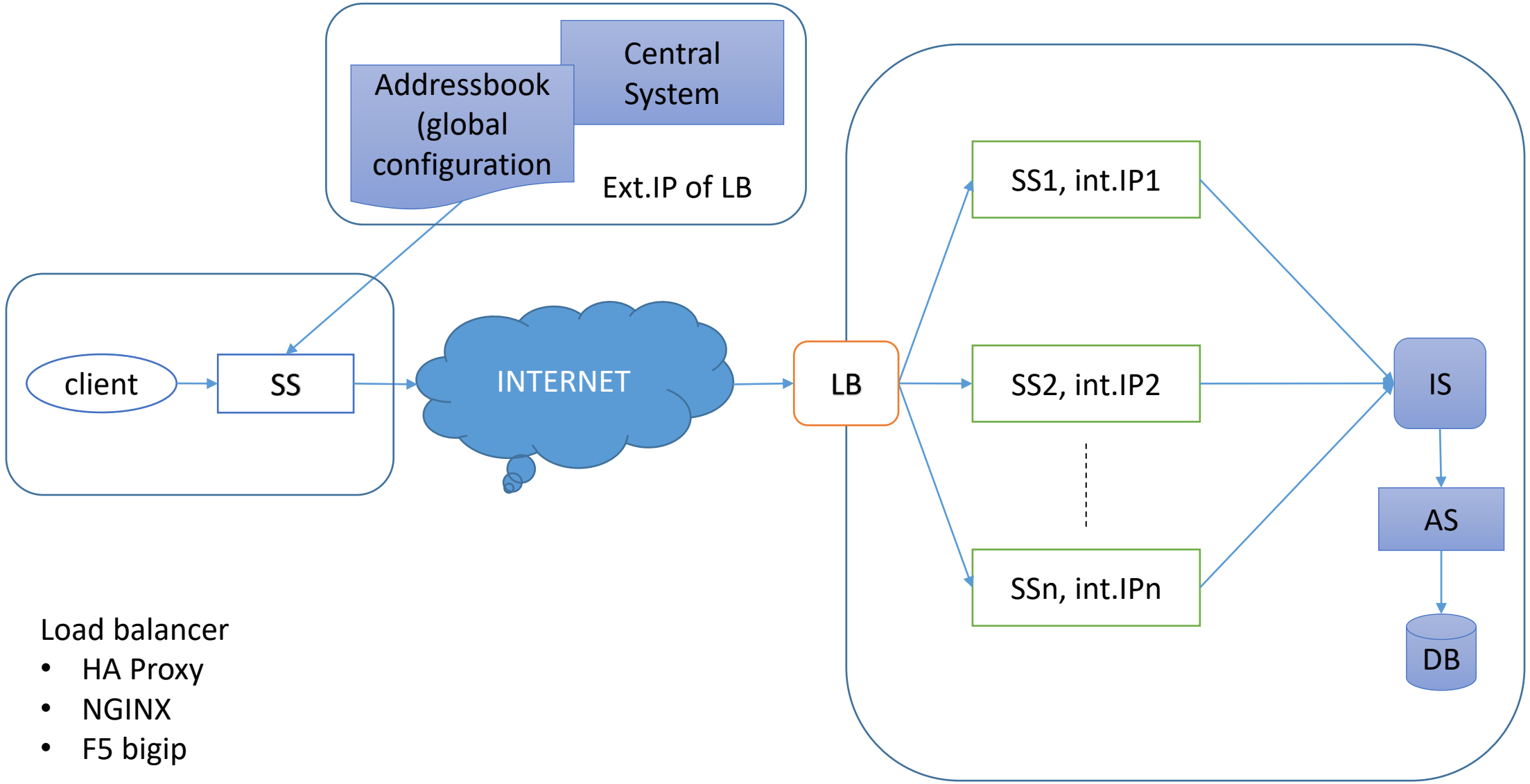
- Specifics might occur when trying to upgrade too old v6, dependent:
  - operating system requirements (Ubuntu version)
  - database migration
  - clustering options
- Please follow directions https://confluence.niis.org/display/XRDKB/Migration+Guide+from+X-Road+6+to+X-Road+7
- EE-specific guidelines (en, might help KG in some aspects) https://abi.ria.ee/xtee/en/turvaserveri-haldus/turvaserveri-uuendamine


External Trust Service Provider
Data Exchange Partners
X-Road Center
Time-stamping Service
OCSP Responder
Partner's Security Server
Management Security Server
Central Server
Monitoring Security Server
OUT 80/tcp 443/tcp
OUT 80/tcp 443/tcp
IN and/or OUT 5500/tcp 5577/tcp
OUT 5500/tcp 5577/tcp
OUT 80/tcp 4001/tcp
IN 5500/tcp 5577/tcp
Security Server
IN 80/tcp 443/tcp
IN 4000/tcp
OUT 80/tcp 443/tcp other
Client Information System
Security Server Administrator
Producer Information System

SS cluster with built-in cluster option



SS cluster with external load balancer



Load balancer

- HA Proxy
- NGINX
- F5 bigip

Certification Authority, CA

- Problems:
  - Hardware Security Module (HSM)
    - Adds security for process but reduces technically
    - Availability, integrity
      - May be not functional after few years
        - Cheap module
        - Not available due to sanctions
      - Requires enter PIN manually after restart / power issues
    - Costly for Members
  - Only one CA, pressure to be fully functional 24/7
- Proposals:
  - Do not require HSM, allow soft-token
  - Allow CA from Infokom and Tunduk
- Certificates for auth and **sign**
  - HSM or software-based
  - From Infokom
- OCSP (Online Certificate Status Protocol)
- TSA (Time-Stamp Authority)

Logs in SS

- /var/log/xroad/…
  - ls -alrt
  - message.log
    - Message.log (.mlog) within Postgre
      - Policy how long to keep
  - signer.log
  - proxy.log
  - tail -f *.log | grep -A5 -B5 „string“
  - trace …
  - Elasticsearch > Kibana

Links to additional documentation

About, NIIS

- This overview includes links to documents available at NIIS repository https://github.com/nordic-institute/X-Road
  - NIIS – Nordic Institute for Interoperability Solutions, https://www.niis.org/
  - NIIS is non-profit association with the mission to ensure the development and strategic management of X-Road® and other cross-border solutions for digital government infrastructure. The republics of Estonia, Finland and Iceland are members of NIIS. NIIS history https://www.niis.org/history

- Every instance, including Estonia makes his own specific package and environment of secure data exchange based on NIIS repository and may attach his own specific documentation and guidelines into that
  - Guidelines for Estonian X-Road (X-tee) members are available at https://www.x-tee.ee/docs/live/xroad/ and https://abi.ria.ee/xtee/en (English version is under construction. Until it's finished, please look the Estonian version)

X-Road Data Exchange Layer

- https://github.com/nordic-institute/X-Road
  - Source code => https://github.com/nordic-institute/X-Road/tree/develop/src
  - Installation
    - Building https://github.com/nordic-institute/X-Road/blob/develop/src/BUILD.md
    - Ansible https://github.com/nordic-institute/X-Road/blob/develop/ansible/README.md
  - Technical documentation (next slide)

Architecture, documentation

- https://github.com/nordic-institute/X-Road/blob/develop/doc/README.md
  - Architecture
  - Protocols
  - Manuals
  - Use cases
  - Data Models

- At the moment, no need to look too seriously into if you do not deal with that:
  - Configuration Proxy
  - Audit and message logs
  - Monitoring
  - Protocol extensions
  - High Availability, External Load Balancer <= still, take a look if you plan it!
  - Testing

Protocol

- https://github.com/nordic-institute/X-Road/blob/develop/doc/README.md#protocols

- **Message Protocol for REST**
- Message Protocol v4.0 (SOAP)
- Transport Protocol (HTTP Headers, Body, Attachment(s))
- Service metadata

X-Road Center, Central Server, management Security Server

- The intended audience are the X-Road **central server administrator(s)** responsible for installing and configuring the X-Road central server software. The documents are intended for readers with a good knowledge of Linux server management, computer networks, and the X-Road functioning principles.

- Documentation
  - Installation Guide
  - User Guide
- Software
- Configuration (RTFM!)

X-Road Member, Security Server

- The intended audience are X-Road **Security server system administrators** responsible for installing and using X-Road software. The document is intended for readers with a moderate knowledge of Linux server management, computer networks, and the X-Road working principles.

- Documentation
  - Installation Guide
  - User Guide
- Software
- Configuration (RTFM!)

X-Road CA

- **Depends on country, instance choice and CA-s available**
- Different options for different instances (dev, test, prod)

- In Estonia - Trust services and their providers https://abi.ria.ee/xtee/en/x-tee-usaldusteenused-ning-nende-pakkujad (in english)
  - **Sign** – e-Seal certificate (sign certificate)
  - **Auth** – x authentication certificate (auth certificate)
  - **OCSP** – certificate validity confirmation service (Online Certificate Status Protocol)
  - **TSA** - time-stamping service
- Two CA-s offer trust services on EE X-tee. With few but key differences.

X-Road addressing, important notes

- All codes are case sensitive! I.e. "kg" <> "KG"
  - Suggested to use lowercase
- Codes must be as short as possible to fit into different UI-s and not to be cutted from right side
- Avoid special symbols in all parts (may become when copy/paste using Win systems)
- Avoid delimiters, single and double quotes, slash, backslash etc (may be problematic while rendering in diferent systems)
- Try to understand meaning of addressing system, include country specific to have it theor.available for federation and cross-border services
  - Good sample: "ee/gov/monitoring/getSecurityServerOperationalData.vx"
  - Bad sample: "my-org_central-server/Commercial/õssõk köl/service-cleanWater"

X-Road addressing, EE sample

- Member
  - Sample: "EE/GOV/70006317", where
  - "EE" is xrdInstance, choices in Estonia: "EE" – "ee-test" – "ee-dev"
  - "GOV" is xrdMemberClass, choices: "GOV" – "COM" – "NGO" – …
  - "70006317" is xrdMemberCode, sample of Estonian State Information System Authority (RIA) registry code in Estonian Business Registry
- Subsystem
  - Member/monitoring
  - "monitoring" is xrdsubsystemCode, ie system, subsystem, choice of member
- Service
  - Subsystem/serviceCode[.serviceVersion]
  - If serviceVersion is used, then it is mandatory to be used by clients as well
  - Sample: "getSecurityServerOperationalData" or "getSecurityServerOperationalData.v1"
- Security Server, optional field block in protocol (TARGETSS, id:objectType="SERVER")
  - Sample: "EE/GOV/70006317/serverCode", where serverCode is choice of admin

Playground

- X-Road playground, a pre-configured X-Road environment for trying out X-Road https://x-road.global/xroad-playground
  - Service provider's Security Server: https://testagess01.playground.x-road.global:4000 (username for the UI is "xrd" and password is "secret“)

Problems

- ~4000 request/response per second => software-based sign cert + cluster
- X Gb per request

- Too much logging, HDD overload => review log policy, rsync to external log-server, more aggressive archive/delete

- ? Service log

- Java version support, LOG4J => upgrade

Contact

- eGA experts, toomas.molder@ega.ee