AUTOMATING OPEN-SOURCE LICENSE COMPLIANCE

Petteri Kivimäki
Twitter: @pkivima
petteri.kivimaki@niis.org

04 March 2024

DIGITAL SOCIETY SOLUTIONS AND CROSS-BORDER COOPERATION

Nordic Institute for Interoperability Solutions

Non-profit association to ensure the development and strategic management of X-Road® and other cross-border solutions for digital government infrastructure.

niis.org

X-ROAD®

Open-source software and ecosystem solution that provides unified and secure data exchange between organisations.

x-road.global

Harmony eDelivery Access

A free and actively maintained open-source component for joining one or more eDelivery policy domains.

edelivery.digital

X-Road® is open-source software and ecosystem solution that provides unified and secure data exchange between organisations.

23

ECOSYSTEMS

DEPLOYED BY GOVERNMENTS OR OTHER ORGANISATIONS

150

COUNTRIES

REPRESENTED IN THE X-ROAD COMMUNITY

3600

MEMBERS

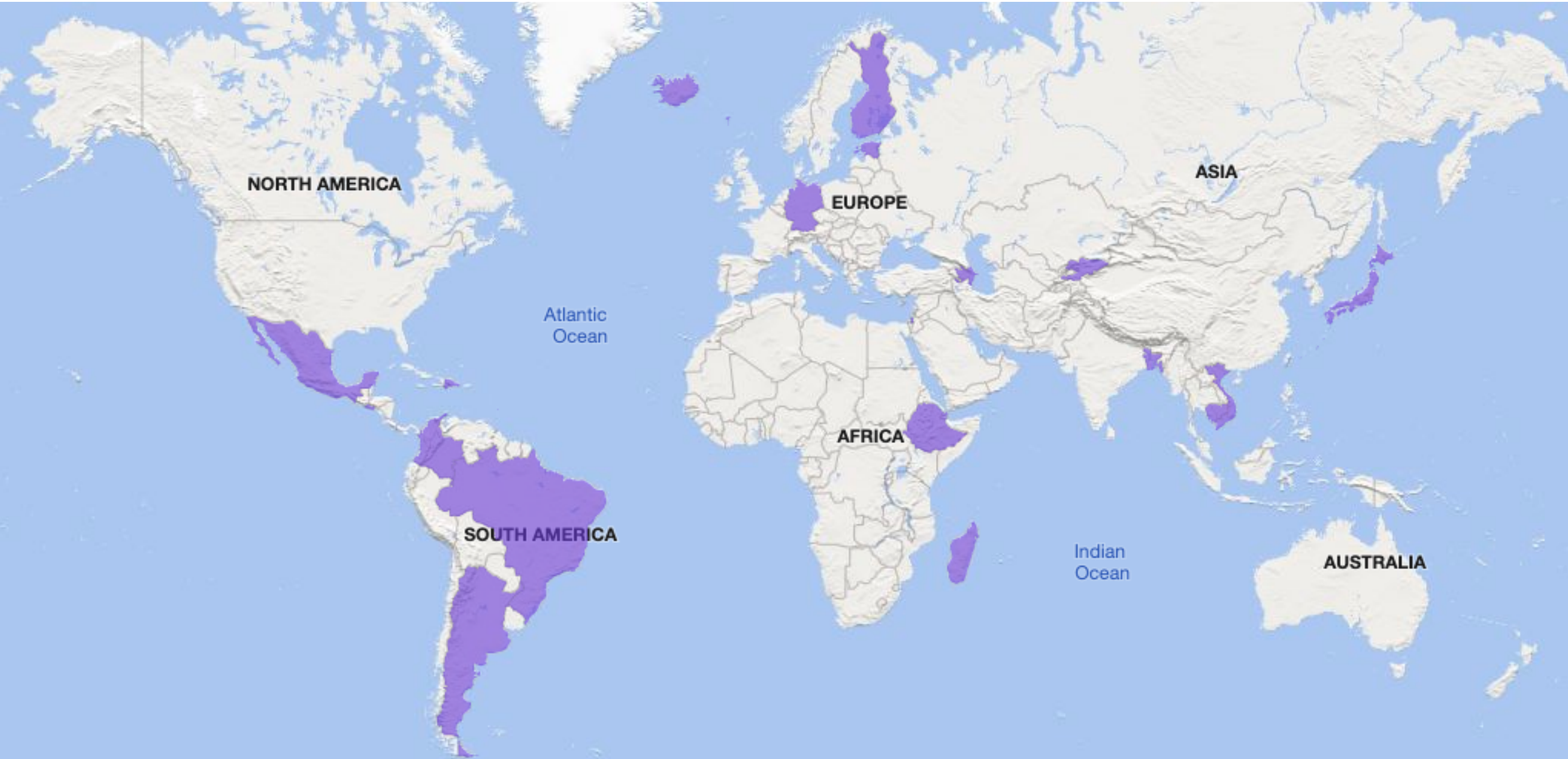
PARTICIPATING IN THE X-ROAD COMMUNITY

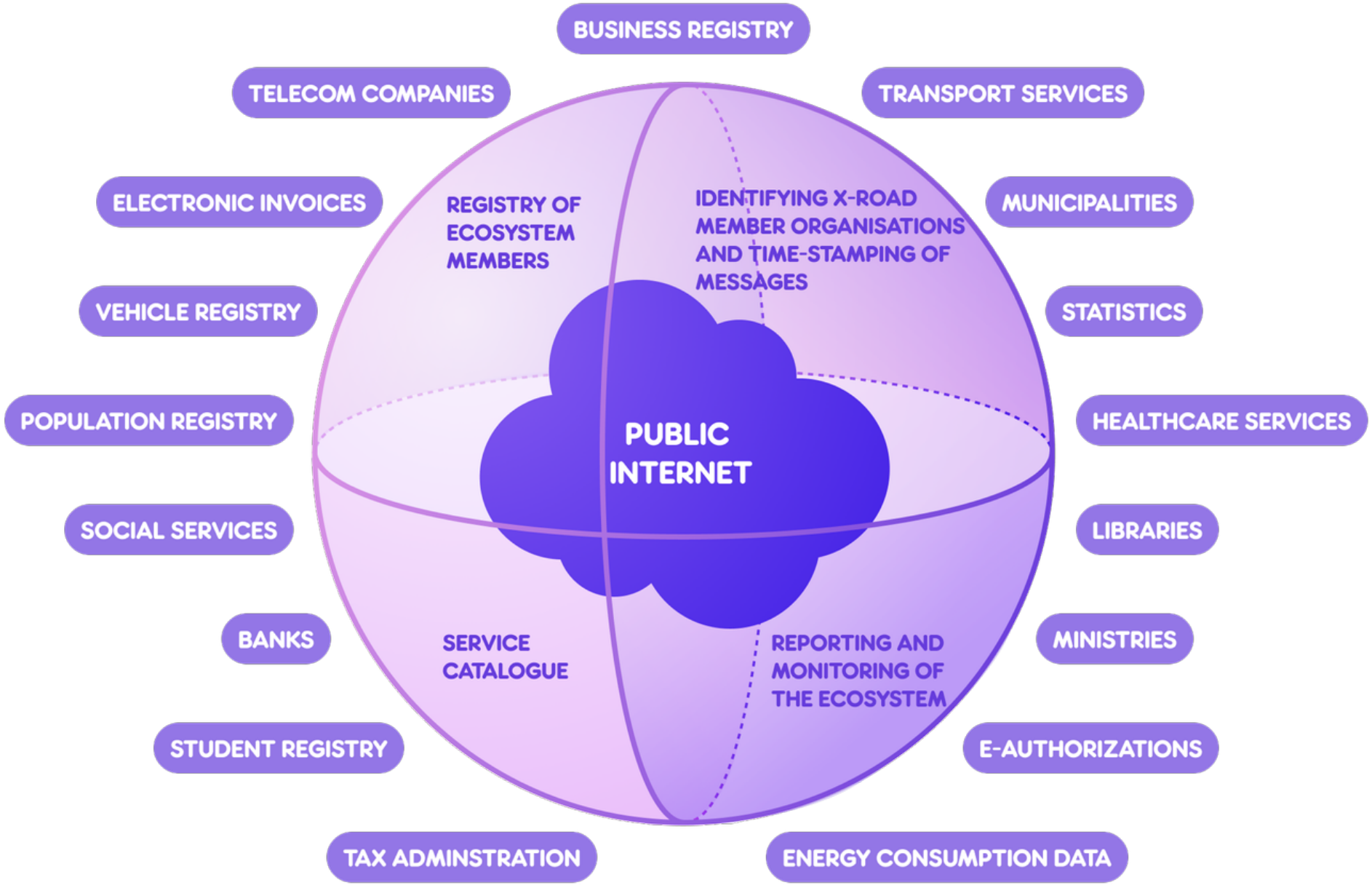
542M

END USERS

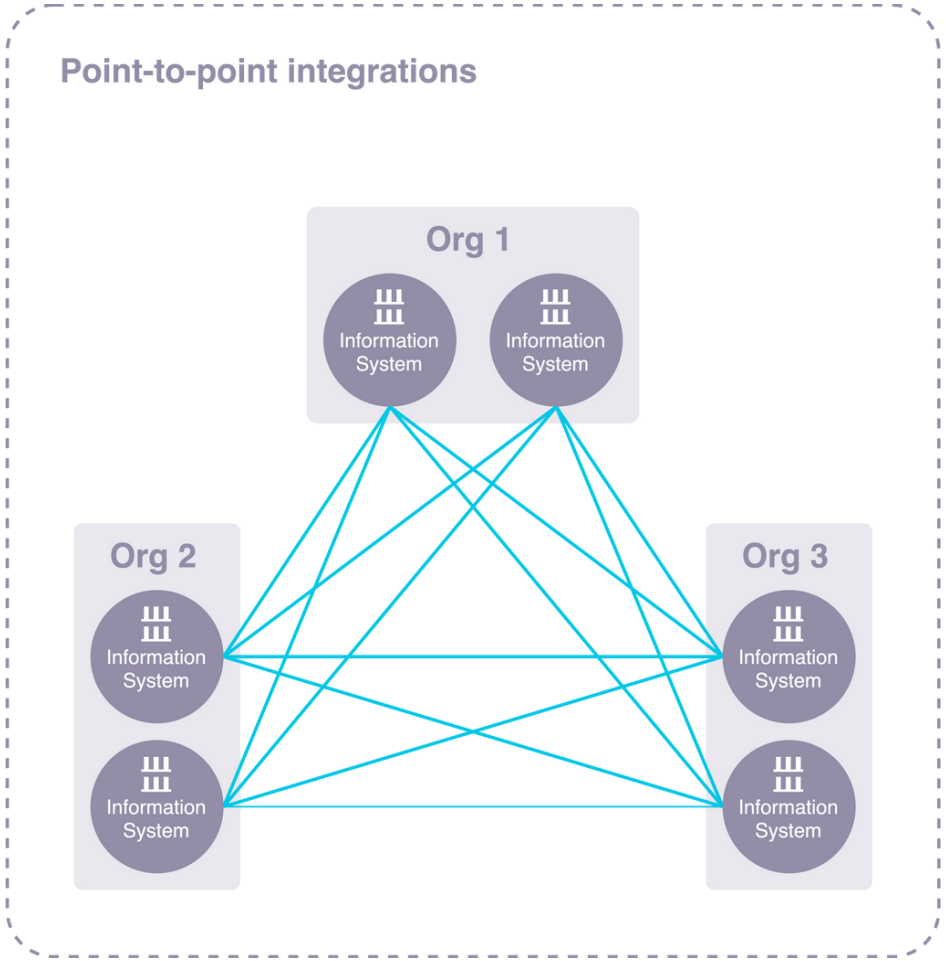
WORLDWIDE

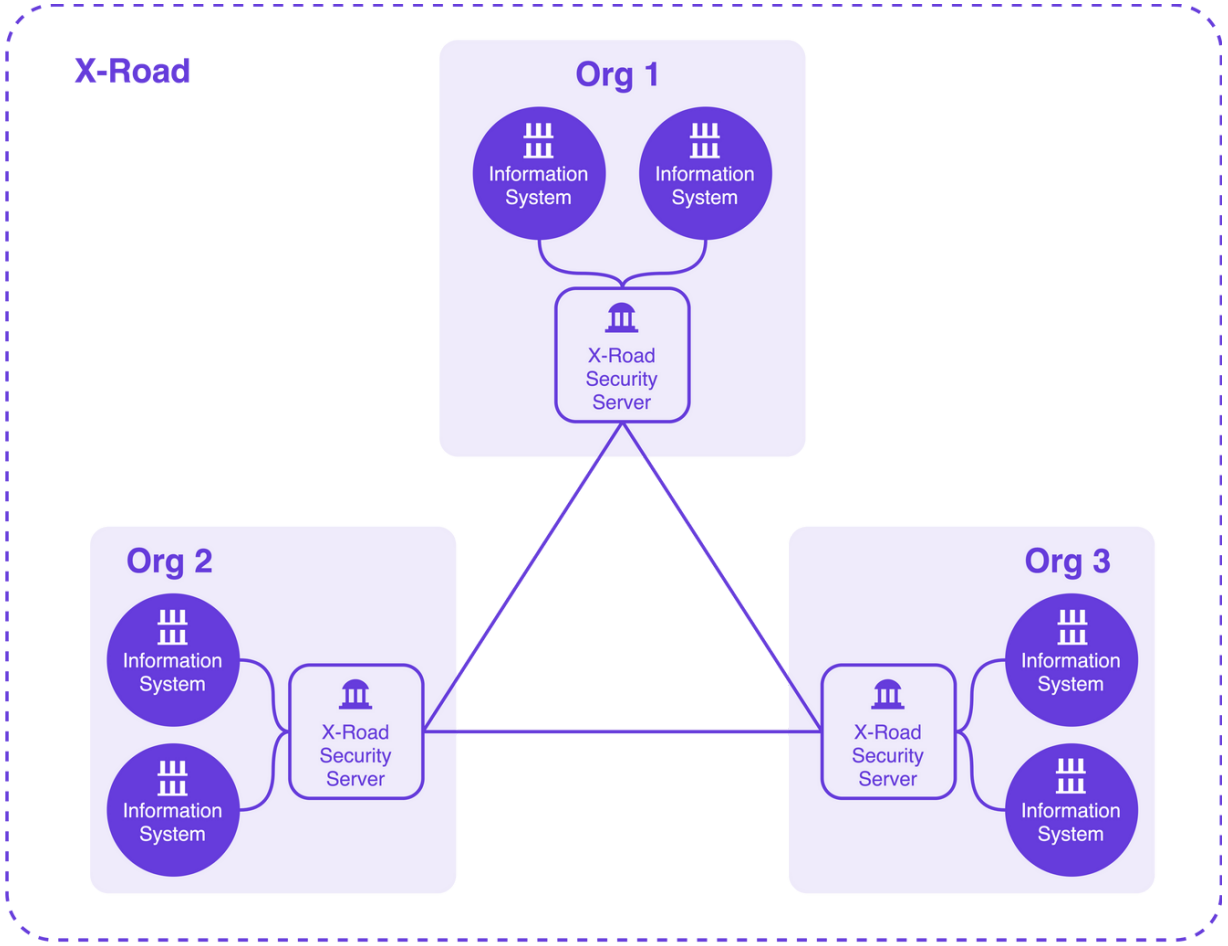
COUNTRIES WITH X-ROAD ECOSYSTEMS



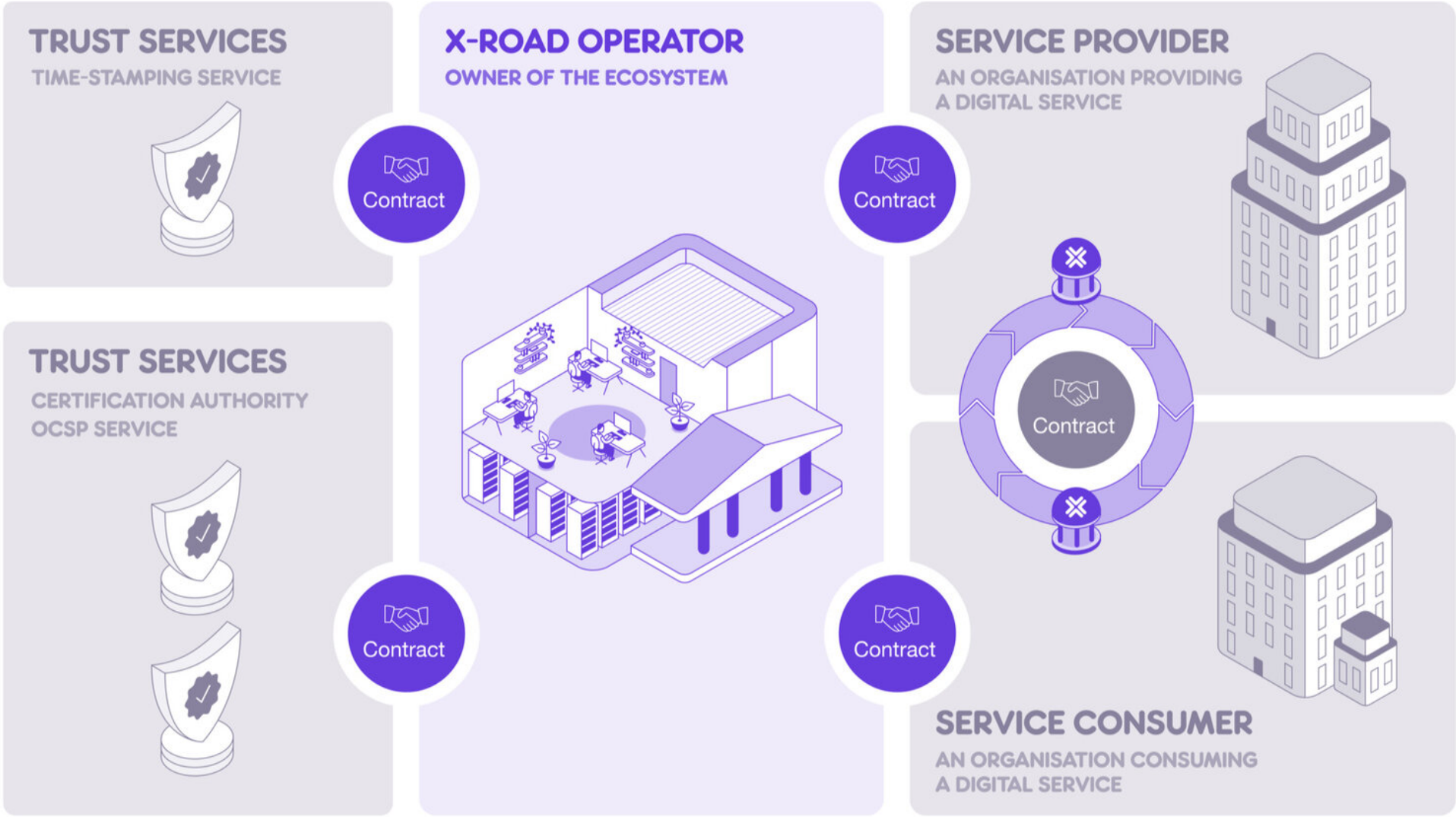

BUSINESS REGISTRY
TELECOM COMPANIES
TRANSPORT SERVICES
ELECTRONIC INVOICES
MUNICIPALITIES
VEHICLE REGISTRY
STATISTICS
POPULATION REGISTRY
HEALTHCARE SERVICES
SOCIAL SERVICES
LIBRARIES
BANKS
MINISTRIES
STUDENT REGISTRY
E-AUTHORIZATIONS
TAX ADMINSTRATION
ENERGY CONSUMPTION DATA
REGISTRY OF ECOSYSTEM MEMBERS
IDENTIFYING X-ROAD MEMBER ORGANISATIONS AND TIME-STAMPING OF MESSAGES
SERVICE CATALOGUE
REPORTING AND MONITORING OF THE ECOSYSTEM
PUBLIC INTERNET

X-ROAD VS POINT-TO-POINT





X-ROAD ECOSYSTEM



NIIS RESPONSIBILITIES REGARDING X-ROAD

- Management, development, verification, and audit of the source code
- Administration of documentation
- Administration of business and technical requirements
- Conducting development
- Developing and implementing principles of licensing and distribution
- Providing second-line support for NIIS members
- International cooperation

NIIS PRODUCT PORTFOLIO

X-Road® (MIT)

- X-Road Metrics (MIT)
- MISP2 (MIT)
- REST Adapter Service (MIT)
- XRd4J (MIT)
- Example Adapter Service (MIT)
- X-Road Test Service (MIT)
- Security Server Sidecar (MIT)
- Security Server Toolkit (MIT)
- X-Road Catalog (MIT)

Harmony eDelivery Access (EUPL 1.2)

NIIS PRODUCT PORTFOLIO

- All the NIIS products use many third-party open-source components that are licensed under various open-source licenses.
  - Tens of direct dependencies.
  - Hundreds of transitive dependencies.
- The products use different technologies and various package management systems.
- Not all the dependencies are managed using package management systems, but also vendored dependencies are used.

OPEN SOURCE COMPLIANCE CHECKS

- Until 2021 the legal qualities of the X-Road's software packages were validated approximately once year using a project-based approach that required a lot of manual work.
  - A tendering process was required each time.
  - List of dependencies to be analysed was combined manually in Excel.
- In 2021, the open source compliance was automated to the largest effective extent by taking into use Open Source Review Toolkit (ORT) and integrating it into the development process and CI pipelines.

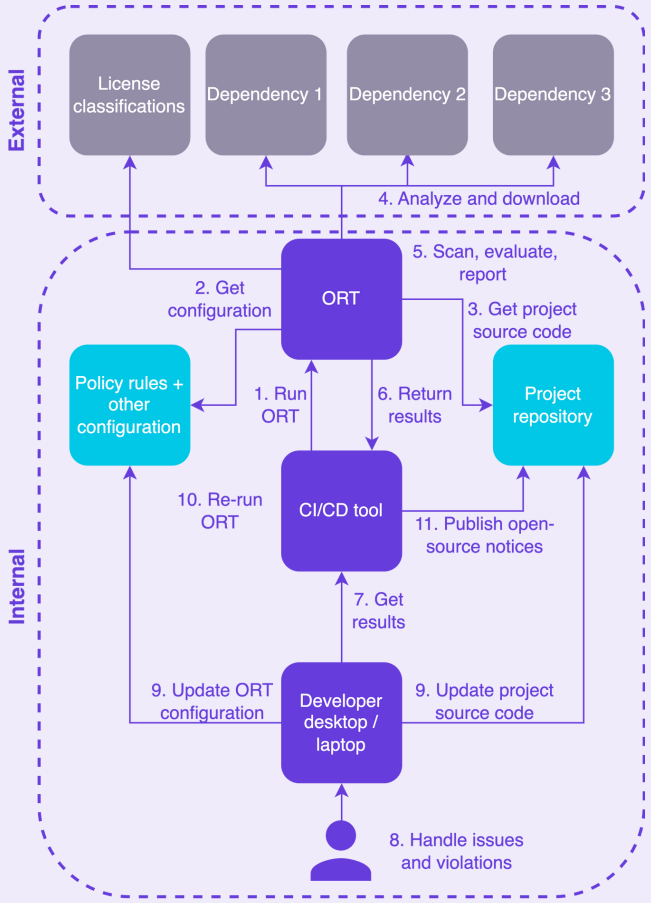
THE ORT IMPLEMENTATION PROJECT

- The ORT implementation project was completed in collaboration with attorneys-at-law HH Partners in May and June in 2021.
- The project included X-Road core and two X-Road extensions.
- The aim of the project was to:
  - Create a written open-source policy description document.
  - Take into use ORT, create necessary configurations and integrate ORT into NIIS's CI process.
  - Provide initial training to NIIS users.

ABOUT ORT

- ORT aims to assist with the tasks that commonly need to be performed in the context of license compliance checks.
- ORT is used to identify dependencies, licenses, copyrights and policy rule violations, and to generate Open-Source notices and Software Bill-of-Materials (SBOMs).
  - Open Source notices include license notices and copyright notices.
- ORT analyzes and scans a project and its dependencies' source code, and evaluates license / copyright findings against customizable policy rules and license classifications.

WORKFLOW



- Run ORT on Jenkins regularly (e.g., once a week).
- Review the results for issues and policy rules violations.
- Download the scan results to your workstation.
- Fix detected issues and policy rule violations locally and update ORT configuration accordingly.
- Re-run ORT on Jenkins to verify the changes.
- Copy generated Open Source notices to the project's source code repository.

EXPERIENCES (1/3)

- Initial configuration requires prior knowledge of ORT.
  - Running ORT with a simple example project is easy, but getting it to work with your own Gradle multi project with 40 000 LoC is not.
- Technical and legal skill profiles combined with open source knowledge are needed during setup and actual use, and they must work in collaboration.
- Finding the right configuration options requires some time and the use of ORT in the target hosting environment.
  - For example, what's the right storage type for scan results (git vs. Artifactory).

EXPERIENCES (2/3)

- Resolving issues and policy rules violations is relatively straightforward when there are existing solutions that can be used as an example.
  - The easiest way to work on the issues is locally – not using the CI/CD tools.
  - Additional tooling (=ORT wrapper scripts) is a great help when working on the issues locally.
- ORT documentation is targeted to developers and technical people.
  - For example, some configuration values must be checked from ORT source code files.

EXPERIENCES (3/3)

- Adding a new project that uses the same outbound license with the already existing projects is straightforward.
  - However, in a big project the number of initial issues may be in hundreds.
- Adding a new project with a new outbound license requires more work – especially if the ORT configuration was initially designed for one outbound license only.
- It’s good to have continuous support available for resolving policy rules violations and technical issues.
  - For example, ORT version upgrades.

OPEN-SOURCE LICENSE COMPLIANCE AS A SERVICE

- In 2024, we have switched from running our own ORT instance to an open-source license compliance service provided by Double Open.
  - Piloting the service with Double Open started in 2023.
- The service is SaaS based and its using ORT under the hood.
  - Existing ORT configuration could be utilized when migrating from our own ORT instance to the SaaS service.
- The service offers analyzing software repositories for the purpose of managing Software Bill-of-Materials (SBOMs), Open-Source license compliance and security vulnerabilities.
- The service covers the required infrastructure, onboarding new projects (technical + legal), resolving technical issues and providing support services, e.g., support in resolving policy issues.
  - The user is responsible for curating / resolving policy issues.

SUMMARY

- ORT has reduced the amount of work related to open-source compliance validation significantly. Also, it has allowed us to:
  - Validate all our products instead of just the main products.
  - Have up-to-date notice files all the time.
- Once ORT has been implemented, it’s relatively easy to scale its use to new products.
  - The easiest way to use ORT is to use it as a service.
- Despite ORT manual work is still needed and it requires both technical and legal skills combined with open-source knowledge.
- ORT alone doesn’t directly cover all the aspects of open-source compliance.
  - For example, making available source code of the dependencies which license requires it.

THOUGHTS? QUESTIONS?