



REPUBLIC OF ESTONIA
MINISTRY OF JUSTICE
AND DIGITAL AFFAIRS

Interoperability and Digital Innovation in the Estonian Land Register

ELRA IMOLA IV Closing Conference

Kadri Laud

Ministry of Justice and Digital Affairs

Brussels, June 4th, 2026

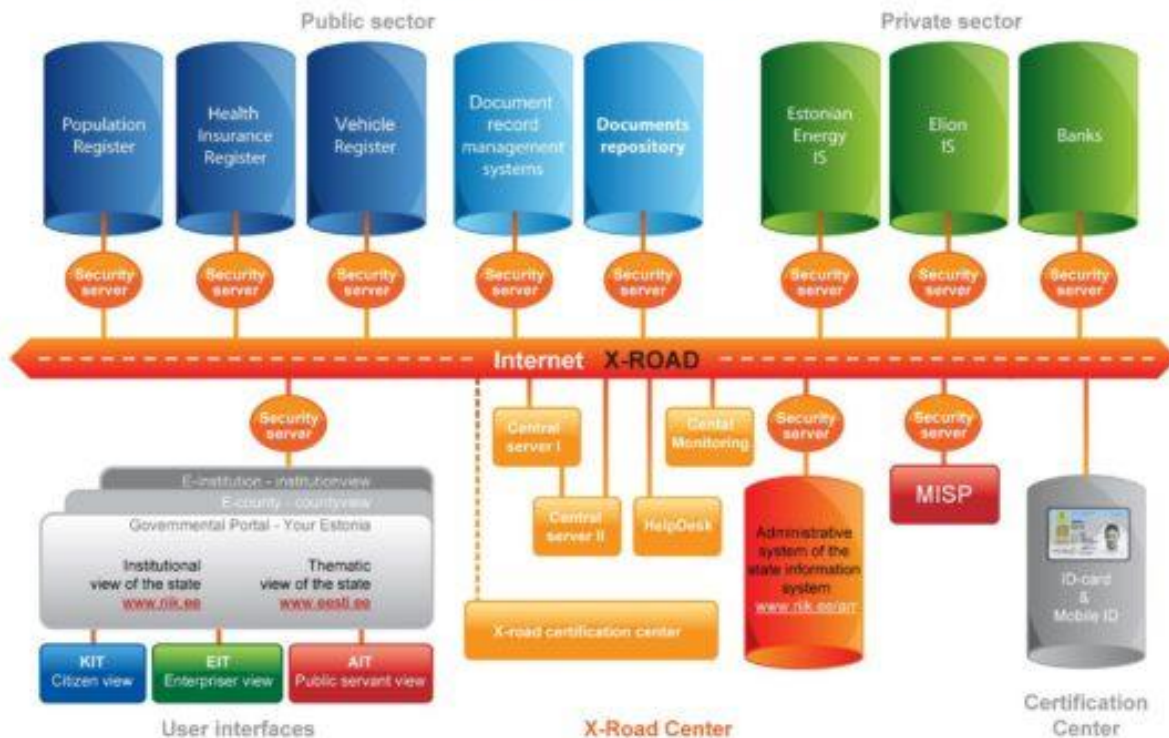


Digital Accessibility & User-Centric Services

- Title-based land register ensuring legal certainty
- Fully digital and accessible online
- Covers all immovable property and real rights
- Legally reliable and trusted data source
- Online access via ID-card / Mobile-ID / Smart-ID
- Self-service portal for property data and documents
- Authorisation and digital document access
- No need to visit public LR office
- Notary-centric System

HOW X-ROAD ENABLES LAND REGISTER DATA EXCHANGE

Estonian information system



Distributed Data Exchange Layer

X-Road connects public and private databases without centralizing data, enabling seamless communication and interoperability.

Standardized Machine-to-Machine Services

X-Road enables automated, structured data exchange and validation improving data quality and reducing human errors.

Security and Trust

All data exchanges via X-Road are encrypted, digitally signed, and logged ensuring traceability and legal reliability.

Automated Land Register Workflows

X-Road supports automation of updating, validating, and synchronizing land register data for efficient governance.

Automated Data Exchange Between Land Register and Cadastre

- Automated “entries” are in practice data exchange between two registers, not traditional legal entries
- Data flows from the cadastre to the land register electronically (e.g. daily synchronization)
- The process replaces the need for a separate application in defined cases

Initiated by cadastre operations, such as:

- subdivision or merger of parcels
- boundary updates
- improvement of spatial data accuracy

Applies mainly to technical and declarative data, including:

- parcel identifiers and area
- boundary changes
- spatial information

No change to substantive property rights

The New Geopolitical Reality and E-State Security

From Transparency to Security

- **Previous focus:** Maximum transparency and unrestricted data availability.
- **Current focus:** Personal safety, national defense, and security.
- **Driver:** Increased cyber risks and the shifted geopolitical landscape.
- **Goal:** To prevent public registries from being abused for malicious intelligence activities and tracking individuals.

Changes in Land Register Personal Data Protection

The Biggest Change – Limitations of Person's Name Searches

- **Restriction of Person-Based Searches**
- **Before:** A query by name or personal code displayed all real estate owned by that individual.
- **Now:** Regular users can no longer perform person-based individual queries.
- **The exceptions:** legal entities under public law and for persons who need land register data to perform public law duties or obligations set out in law.
- Protects critical officials (military personnel, judges, security agency staff) by preventing hostile services from mapping out their residences and assets.






















The Public Principle of the Land Register

- **Property-based search is active:** Data can still be accessed via a specific property.
- **Search criteria:** Address, cadastral code, or register part number.
- **Result:** You can see the actual owner of a property, but *reverse searching* ("all assets of a person") is disabled.

Data Tracker: Control and Transparency for Private Individuals

- In accordance with the GDPR and the Estonian Personal Data Protection Act, a citizen has the right to receive an overview of operations performed with their data.
- Through integration with the national Data Tracker, citizens can now see:
 - who has accessed their data
 - and when this access took place
- Every query related to private property is logged.
- This has two key effects:
 - it increases trust
 - and it discourages unjustified or “curiosity-based” searches
- It also allows suspicious patterns to be identified and addressed.



	 Government Cloud	 Public Cloud
 Users	Public sector, state institutions	Companies, individuals
 Ownership & control	 State-controlled	 Third-party providers (AWS, Azure, Google)
 Data governance	 National control, data sovereignty	 Provider-managed infrastructure
 Security & compliance	 High, strict regulatory standards	 Standardised, depends on provider
 Services	 Core IT services (more limited)	 Wide range (AI, analytics, platforms)
 Scalability	 Controlled scaling	 Highly scalable, global
 Main goal	 Security & compliance	 Flexibility & innovation

Data Embassy



- Estonia's Digital continuity in times of crisis, such as a cyberattack or war
- A need to back up and run critical data and systems outside of Estonian territory
- Own server resources outside the territory of Estonia and under the control of Estonia



REPUBLIC OF ESTONIA
MINISTRY OF JUSTICE
AND DIGITAL AFFAIRS

Thank you!

