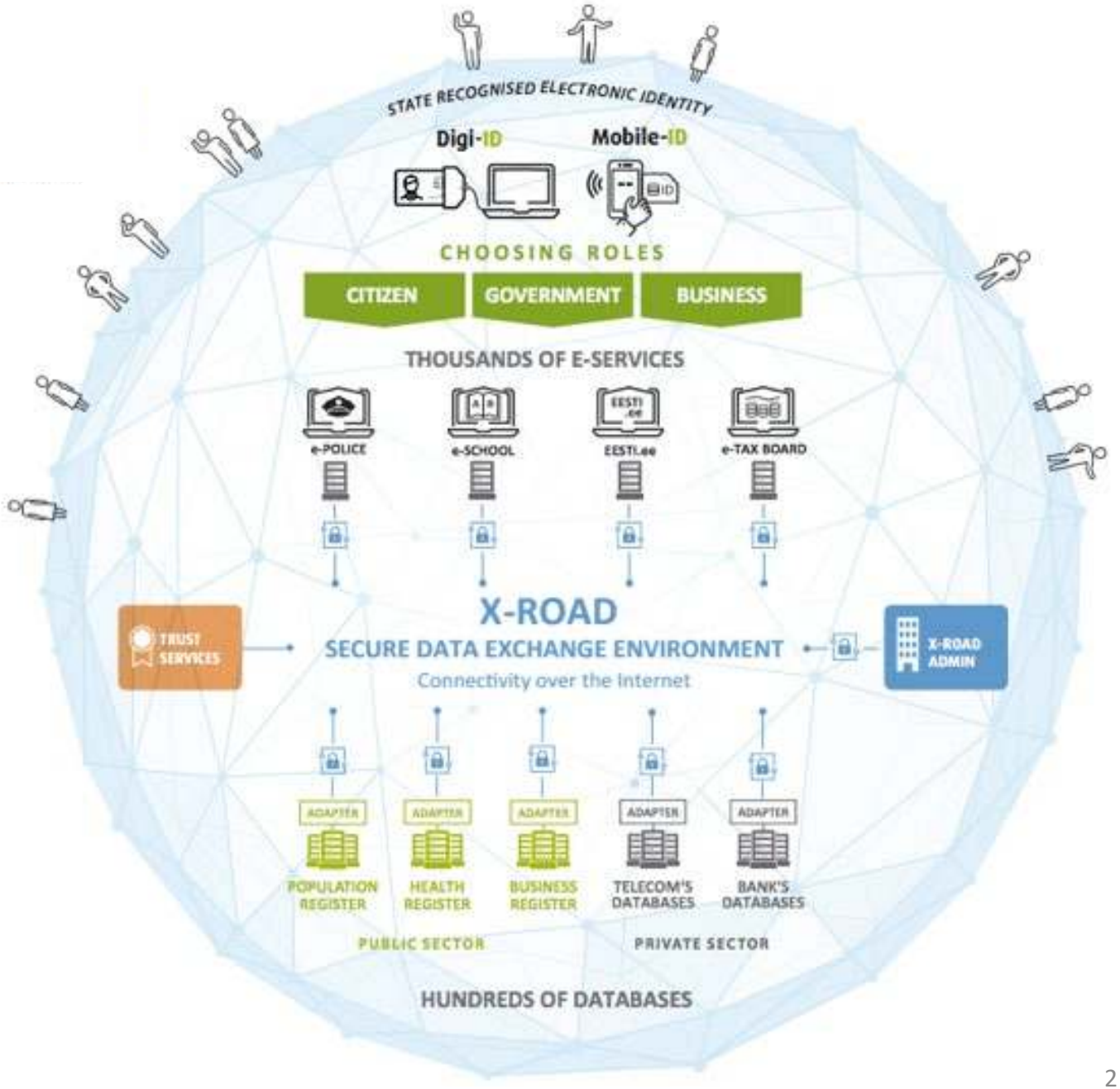
REPUBLIC OF ESTONIA
MINISTRY OF ECONOMIC AFFAIRS AND COMMUNICATIONS

Cloud solutions: public cloud

Raavo Palu
Cyber Security Legal Advisor

Architecture of Estonian National Cyberspace



Protected assets

Data

- publicly accessible information
- restricted (for internal/official use), including personal data
- national and foreign secrets (classified data)

ICT systems

- commercial infrastructure, products and services
- state infrastructure, products and services
- external connections and global Internet

Trend:

towards the public cloud platforms (whether we want it or not)

Challenges (1/2)

The goal is to keep digital data and ICT systems protected – while using (public) cloud, this means solving aspects of:

1. **availability** – services need to be available
2. **integrity** – data needs to be correct
3. **confidentiality** – only authorised access to data
4. **continuity** – services need to be up and running during a disruption
5. **protection** – how third parties protect data and ICT systems

Challenges (2/2)

The goal is to keep digital data and ICT systems protected – while using (public) cloud, this means solving aspects of:

6. monitoring and logging – technical monitoring by CERT-EE
7. data location – EE gov entities are in EE, but larger cloud service providers might/do not store data in EE
8. data protection – rules and requirements of the General Data Protection Regulation (e.g. access to the cryptographic keys)
9. …

Current legislation (1/2)

- Estonian Public Information Act and our national information security standard ISKE allows to move to the public clouds.
- ISKE has divided information that is meant for internal/official use into different data classes:
  - S0 – public information (already cloud eligible), S1-S2 classified information and S3 – secret information;
  - S1 and S2 the cryptographic keys are in the sole possession of Client (GOV).
- additional requirements from the GDPR (e.g. access to cryptographic keys)

		K0	K1	K2	K3
T0	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T1	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T2	S0	M	M	M	H
	S1	M	M	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T3	S0	H	H	H	H
	S1	H	H	H	H
	S2	H	H	H	H
	S3	H	H	H	H

Current legislation (2/2)

Problem:
only 5% of all information is public cloud eligible.

This means:
no motivation and/or real possiblity moving towards cloud

		K0	K1	K2	K3
T0	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T1	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T2	S0	M	M	M	H
	S1	M	M	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T3	S0	H	H	H	H
	S1	H	H	H	H
	S2	H	H	H	H
	S3	H	H	H	H

Solution (1/2)

- ISKE is available until 31.12.2022
- ISKE shall be replaced with Estonian Information Security Standard (E-ITS)
- Draft legislation (regulation of the Government of the Republic) for using of public clouds:
  - expected entry into force: October 2022
  - requirements only for the public sector - listed in Estonian Cybersecurity Act § 3 (4)

Solution (2/2)

- Main requirements of draft legislation according to the draft that was on public consultation in May-June 2022:
  - evaluation the **trustworthiness** of the cloud service provider
  - prohibition to disseminate information meant for official/internal use that is related to maintaining national security to the cloud service provider (**encryption**)
  - duty of the client to use **alternative measures** or ICT systems for cloud systems that are important for the organisational continuity of the client
  - duty to follow specific measures in said regulation that are related the use of cloud computing services and sending or making available **logs** that are related to the use of cloud computing services to CERT-EE (e.g. client-side logs)

NB! said requirements may change due to received feedback

Concept of draft legislation - encryption

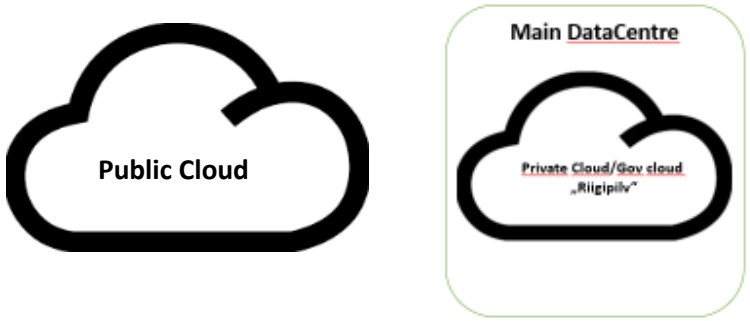
Public Information Act § 35

Entails legal grounds (descriptions) on when information is classified as internal/official use

90% of all information

„Light“ classified information

We encrypt the data with a key controlled by the cloud service provider.



10% of all information

„Hard“ classified information

The cloud service provider cannot decrypt the data (the key is in the sole possession of the customer)

Questions?

REPUBLIC OF ESTONIA
MINISTRY OF ECONOMIC AFFAIRS
AND COMMUNICATIONS

Thank you!

Raavo Palu
Cyber Security Legal Advisor
Department of National Cyber Security
Office of Government Chief Information Officer
raavo.palu@mkm.ee