UNIVERSITY OF TARTU
1632

Digital identity, digital signature and secure data exchange in Estonia

Sten
Aus

Head of Information System Services
EUNIS 2023

ESTONIA

- A small country in northeastern Europe
- 1.3 million inhabitants
- The Republic of Estonia was established in 1918, regained independence in 1991
- Capital: Tallinn
- Area: 45,000 km^2
- Population: 1.3 million
- Official language: Estonian
- English, Russian, Finnish and German are widely spoken
- Member of the EU and NATO since 2004
- Currency: euro (since 2011)

finland
sweden
est
russia
latvia
lithuania
belarus
poland

estonia.ee

INNOVATIVE ESTONIA

- The first country to adopt online voting
- The only country in the world to offer e-residency
- Estonia is a digital society
- World-changing start-ups originate from Estonia: Wise, GrabCAD, Fortumo, Pipedrive, Starship Technologies, and Skype
- Excellent education. According to OECD's PISA results, Estonian basic education is the best in Europe and in the top 8 globally. Our pupils' science, math and reading skills are outranked only by Singapore and Japan

ابتكار
novation
Estonian high-tech companies offe
smart solutions to
complicated prob
شركات التقنيات الفائقة الإستونية
ذكية
كل المعقدة

Start of a successful eID story

Start of eID

- Personal ID code was fundamental (and mandatory) starting point
  - Each person receives a unique unchangeable 11-digit personal identification number from the government
- Physical ID card is mandatory (above 15 of years)
- Mobile-ID, digital ID and Smart-ID are additional layers
  - Mobile-ID (2007) is related to a SIM card (and your phone)
  - Digital ID (2010) is not a valid travel document, but only a digital
  - e-Residency (2014): Anyone can apply!
  - Smart-ID (2017) is related to physical device

Start of eID

- They all relay on Public Key Infrastructure
  - Two keys (protected by two PINs respectively) and two certificates: authentication (1) and signing (2)
  - Electronic identification, electronic signing and secure transfer of sensitive data
- eID is everywhere – in communication with public and private sector
- Authentication by any of the eID means is the same as physical identification
- Signature by any of the eID means is the same as physical signature and it’s eIDAS compatible
- Additional usage (as a client card, bus tickets etc)

Mobile-ID and Smart-ID

- Mobile-ID:
  - Disadvantages: One Mobile-ID per person, related to physical SIM
  - Advantages: always with you, no need to have smart-card reader
  - eSim is now an option!
- Smart-ID:
  - Disadvantages: most-costly ☺
  - Advantages: multiple IDs per person, one ID is related to device

eID security flaws

- 2011: You can use it without PIN code
  - You need a card and can send special command
  - Resolution: 120k cards were replaced
- 2017: keys were generated at producer’s servers, not at the cards (inside chip)
  - Resolution: 74k cards were affected, 12k needed to be replaced
- Both of them were card and/or chip manufacturer’s flaws where standard was not followed appropriately
- UT scientists have always been testing and members of this team (also discovering flaws)

X-Road

- Started in 1998 (pilot), launched 2001 as a Estonian governmental project
- Data Exchange Layer (started with XML) between different government registries
- Used daily between private and public sector
- Mandatory since 2006
- Since 2017 Nordic Institute for Interoperability Solutions for cross-border e-governance solutions
- Over 2B queries at 2022 (2 201 929 119), approx 180M queries per month

Data Exchange

Open standards, open source

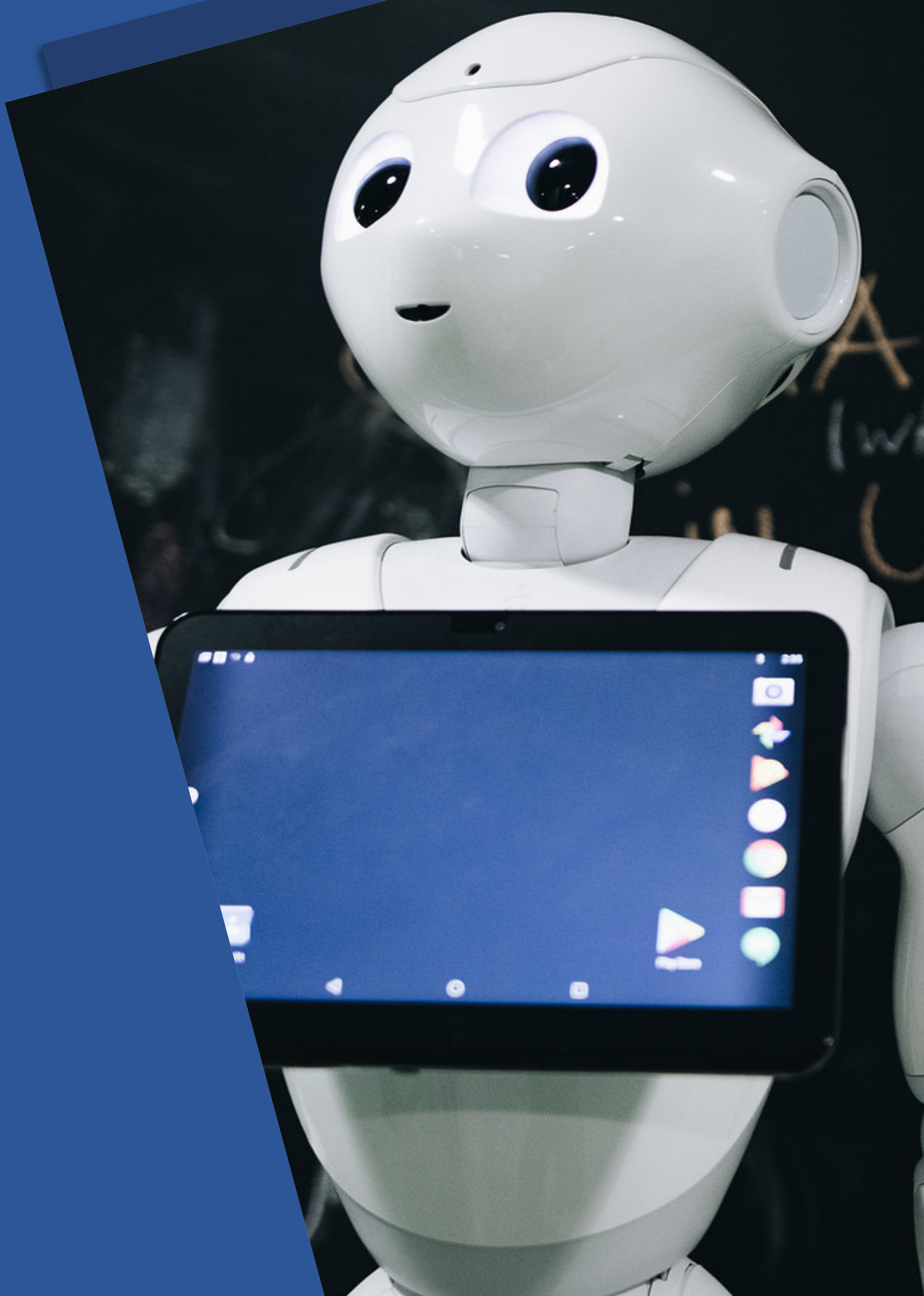
Government holds national registries (such as person registry or study registry)

And every organization can apply to use those registries

Every service provider needs to allow their data(base) usage to a specific client

All requests and responses are signed with corresponding organization certificate

So this means: when I change my name/address, organization can query my data - and I can see that they have queried it!



Data Exchange: everything can be a X-road query

- Doctor writes a prescription
  - I can go to pharmacies and receive my medicine by using my eID
- Police officer stops me and checks for my data/licenses etc
- Document exchange (DHX) in document management systems: I can send from one organization to another a document via DHX, not via e-mail
- Proactive services: when I become a parent, government knows and can already give me child support without my application
- Also possible to use for cross-border communication (for example EST and FIN pharmacies)

Data Exchange: and not a single paper …

- You apply to (any) university and use SAIS:
  - RR: Your personal data (name, ID code, place of residence etc)
  - EHIS: Graduated studies
  - EIS: Your graduation tests / marks / scores
- Let say that you are selected to (any) UNI and SAIS sends your data
  - University SIS: queries your data from SAIS and receives your application
  - You can now start your studies!
  - University SIS sends your information (that you’ve started) to EHIS
- Without any single paper being moved throughout the process!
- Let say that you graduate
  - University SIS sends your data to EHIS again
- And maybe you want to re-apply to another school

And then?

We **actually** sign documents online!

We **actually** (ex)change information and documents online!

We **actually** don’t need to hold “one database to rule them all”

SEE YOU AT THE UNIVERSITY OF TARTU!

Sten Aus (*Head of Information System Service*)
Risto Rahu (*Chief Information Security Officer*)

www ut.ee

✉ info@ut.ee

tartuylikool
tartuuniversity

unitartu
unitartuscience
unitartutiksu