# Estonia

## Context
- Independence from USSR 1991
  - Left them with no infrastructure, no legislation, no economy
- A small country, but with the same needs as a big one
  - Public sector must be small and efficient
- Access to the Internet is enshrined as a right for all people
- The government issues every citizen with an e-mail address
  - Format: firstname.surname@eesti.ee
  - Used for all official communication with the citizen
  - Redirects to the citizen's chosen e-mail provider e.g. gmail
- Extensive 4G network, even in the forests
  - 5G mobile network being planned
- The average citizen needs to transact with government 2.6 times a year
- Use of technology by government saves 2% of GDP

## Demographics
- Population 1.3m
- 80% of families have a PC at home
- 88% of people have broadband at home
- 230 municipalities
- Population of Tallin: 400,000

## e-ID
- Issue
  - Originally issued by banks - now by Police & Border Guard
  - Citizen can collect card at their bank or at Police & Border Guard
  - Police & Border Guard
    - Big hall
      - circa 30 desks
      - photo booths
      - take a number and wait to be called
      - very efficient
      - transactions
  - At birth
    - Done online if parents are married, otherwise offline
    - Currently has to be initiated by parents,but becoming automatic
- Validity
  - 5 years
    - Cards wear out
    - Photo updated
    - New technology on card
      - e.g. stronger encryption
        - Quantum computing might pose a threat one day
- An identity card is compulsory from age 15
  - Optional up until 15th birthday
- Introduction
  - 10% of citizens took up the offer of a two day course on how to use it
  - Project started 1997
  - First cards issued 2002
  - Rollout complete 2006 (1 million cards)
  - Based on technology used at the time in Finland
- Cost
  - €25 for the card, on issue, every 5 years or on replacement of lost/damaged card
  - €5 for card reader
- Security
  - Annual challenge to hack the system
    - €30,000? prize to any successful hacker
  - Public confidence is built by openly notifying the public of any breaches of security, before the media do
  - 6-monthly audit of the system
  - RSA cryptography
  - Contains two sets of cryptographic credentials
    - Straight-through TLS encryption between web browser and web server
    - For digital signing of documents and encryption of sensitive data in documents
- Multi-purpose
  - Driving licence
  - Passport
  - Library card
  - Student card
  - Health insurance card
  - Authentication token
  - Signing of documents
  - Entitled the holder to 30% discount on bus pass initially, but now all public transport is free to Estonian citizens
  - etc.
- Requires a card reader
  - Can be purchased in any computer shop
  - Different types
    - Portable - will fit on a keyring
  - Plugs into USB socket
  - Device drivers automatically download
    - Custom-developed
  - Compatibility
    - Windows
      - Including Windows tablets
    - Mac
  - Incompatibility
    - Smartphones
    - Non-Windows tablets
      - e.g. iPad
- Information held
  - Printed photo
  - Name
  - Identity number
    - These are public knowledge
    - Digits represent various attributes
      - Gender
      - Date of birth
      - Place of birth
    - Replaces social security number
    - Replaces tax number
- Can be provided to businesses as a USB stick
  - e.g. for use on a server
- Firmware on the card needs to be periodically updated
  - Several times a year?
  - Performed remotely
  - If not updated, cards are not usable
- A future version may feature NFC (contactless)

## Mobile-ID
- Useful as an addition to ID card
  - e.g. could be used if card lost or damaged
  - avoids having to have ID card to hand at all times
- Compatible with all GSM mobile phones
  - Not just smartphones
  - Even works on the oldest, most basic models
- Requires special SIM card
  - Extra capacity
  - Extra processing capability (cryptoprocessor)
  - Stores the cryptographic keys
  - Runs an applet
  - Government supervises supply chain to mobile network operators
  - Estonian cards manufactured by Gemalto
    - Almost all other suppliers can supply cards to the equivalent spec
- Establishes trust between the SIM and the citizen's computer through the exchange of one-time PIN numbers
- Secures the communications between the computer and the server through TLS
- Transport mechanism is SMS text messages
  - Reliability
    - As encryption keys get longer, can take up to 4 text messages
    - If one or more message isn't received it will not work
    - Mobile network operator must have sufficient network capacity to avoid SMS message latency
- Used for digital signatures
  - ETSI XAdES standard
- Revenue shared between MNO and certificate authority (government)
  - Per transaction cost
  - Annual projected usage
    - Overage/underage payment
- SIM cards issued face-to-face by MNOs
  - Person issuing the SIM has to perform some identity verification tasks
- A new generation of phones are coming that do not have SIM cards
  - Future version of Mobile-ID may be software-only i.e. AppStore app
  - Currently working to overcome private keys being vulnerable to brute force attack
- Average user uses their Mobile-ID 38 times per month
  - More than E-ID card (25 times per month), because to have a Mobile-ID the citizen first needs to have an E-ID. Only those who have greater need for Mobile-ID pay extra for it.
- Unlike E-ID, Mobile-ID is not used by Estonia in face-to-face transactions
- Cost
  - €10 signup fee
  - €0.60 per month

## Privacy principles
- Citizen owns their own data
- Citizen has the right to see and check their own data
- Data about a child is accessible by their parents, up until the age of 18
- Citizen can decide who else can see their data (e.g. family members)
- All access to data is logged
  - Criminal offence to access personal data without a valid reason
    - Citizen can demand to know the reason for access. Agency has 30? days to provide the information
    - Citizen can appeal to data protection agency
  - Citizen can access the log online
    - Shows date and time and name of agency, but not the name of the officer or the reason
- Estonia is planning to establish "data embassies" in different countries
  - Protects the data in case of future political upheaval e.g. occupation of Estonia by a foreign country, as has happened numerous times in their past

## e-services
- over 3,000 services available online
- i-voting
  - Introduced in 2005
  - Differs from e-voting (which is done using an electronic device in a booth at a polling station)
  - See demo video at https://youtu.be/ILvsmJPaDY8
  - i-voting done completely online, remotely
  - Citizen has to download a small application to their PC
    - Windows, Mac, Linux
  - 30.5% of votes cast in the 2015 election were online
    - Maximum take-up in previous elections was 33%
    - Not higher because many people like to go to the polling station to vote
  - Not just used by young people - biggest segment is people aged over 55
  - Voting takes place over 11 days
    - Pre-election period for online voting only
      - Vote cast electronically can be re-cast at any time during this period
        - Allows anyone who is coerced to vote for a candidate not of their choice to change their vote with nobody knowing
    - Followed by one day when no voting takes place
    - Polling station voting always takes place on a Sunday
  - Can be used while out of the country
    - In 2015, votes were cast from 115 countries, including Jersey
    - Useful if the election takes place when somebody is on holiday or away on business
    - Our host had voted from an Internet cafe while travelling in Australia
- very few offline transactions
  - Marriage
  - Divorce
  - Opening a bank account
  - Buy or sell property
  - Taking out a loan or mortgage
  - Have to be done in front of official
    - Shows not entering transaction under duress
    - could be done online, but should they be?
    - While done face-to-face, still supported by digital i.e. after notary oversees propery sale, the actual exchange is recorded on-screen and both parties sign using their digital ID
  - No paperwork is generated
    - If someone wants a paper copy, they can have one but there is a charge
- Compulsory for businesses to transact online
  - Transactions can still be done offline, but there is a charge to do so
- Electronic signature has the same standing as a 'wet' one
  - Same across all EU member states by law
- Company registry
  - Average time to register a company online is one hour, but it has been done in as little as 18 minutes
- e-Taxation was the first e-service, 16 years ago
  - Introduced before e-identity
  - 98% online
  - Citizens saw the immediate benefit
- e-banking
  - 99.8% of bank transactions take place online
  - Introduced in 1996
    - Originally used a bank-issued identity and password
    - Quickly adopted the government ID scheme after it launched
      - Banks like that it is a government scheme
- e-prescriptions
  - In 2014, 95% of prescriptions were issued electronically
  - Citizen can delegate others to collect a prescription on their behalf
    - Done via a web site, with the citizen authenticating their identity using e-ID or mobile ID
- e-health
  - Introduced in 2008
  - Medical records stored online
- background checks
  - new service recently
- m-parking
  - Every parking area has an ID shown on a sign
  - Driver identifies where they have parked and starts a timer. When they leave the space they stop the timer.
  - Driver is billed monthly in arrears
- e-signatures
  - Browser integration on Windows and Mac
  - Needs certificate authority
    - Government itself could be CA, or can be outsourced
  - Widely used
    - Government
    - Banks
    - Telcos

## XRoad
- Launched in 2001
- Use enshrined in legislation (the Public Information Act)
- Intellectual property owned by Estonian government, but technology available under licence
- Commercial 'of the shelf' version is called UXP (Unified Exchange Platform), available from Cybernetica
- Connects registries and services
- Agreements are made between the agencies that need to exchange information
  - Dictates which data a particular agency can ask for
  - Dictates which data a particular agency may provide
- Stateless
- Generic APIs
- Security layers
  - Supplied as a hardware device
- Integration model
- Transaction logging
  - Every 6 hours the log files are sent from individual 'security servers' to central servers
  - Two staff monitor the system 24/7/365
- Performance
  - Takes two seconds for a request from a police car for a vehicle check, person check etc. to complete
- Version 6 allows cross-border exchange of data

## e-Residency
- Scheme has been running for a year
- Was controversial
- Has been successful
- Interest has been high from overseas
- Run like a government startup
  - Disruptive
- 8,956 e-Residencies issued
  - Ambitious target: 10 million by 2025
- Stripe Atlas recently launched as a means to apply online to set up a new company in jurisdictions worldwide, starting with Delaware
- Development plans
  - Personal
  - Business
  - Service providers (via 'wholesale' API)

## Success factors
- Human factors are critical to success - must include in plans
- There are over 70 countries with smartcard-based citizen ID
  - Mostly used as travel documents
  - Only 7-10 countries using it to full potential
- "Cargo cult" - blindly repeating what worked elsewhere and expecting the same success
- Must have sufficient services available to make having a digital ID worthwhile for the citizen and to make the investment cost-justifiable
- Involve governance people
- Involve policy makers
- Metrics
  - Citizen opinion
  - Take-up
  - Baseline initially
- Involve experienced practitioners, not academics
  - Avoid mistakes made elsewhere
- Cultural differences
- Dealing with the digital divide
  - Training
- Marketing
  - Build awareness
  - Drive uptake
- 24/7/365 support
- Citizen confidence
  - Data integrity
    - Estonian registers use blockchain for timestamping to prove data integrity
      - e.g. succession register
      - e.g. titles
      - e.g. wills
      - e.g. legislation
  - Legislation
  - Regulatory regime
  - Privacy
    - Confidentiality
- Only truly paperless once the whole process is electronic, end-to-end
- User experience
- Kerckhoff's Principle
- Estonian system is 'battle hardened' after an alleged state-sponsored cyber attack in 2007