



Aalto University

Electronic Citizen Identities and Strong Authentication

Sanna Suoranta, Lari Haataja, Tuomas Aura

Department of Computer Science

Aalto University

Finland

21.10.2015
Sanna Suoranta
sanna.suoranta@aalto.fi

Content

- Motivation
- Situation around the world
- Technical solutions
- Usage around the world
- Summary

Motivation

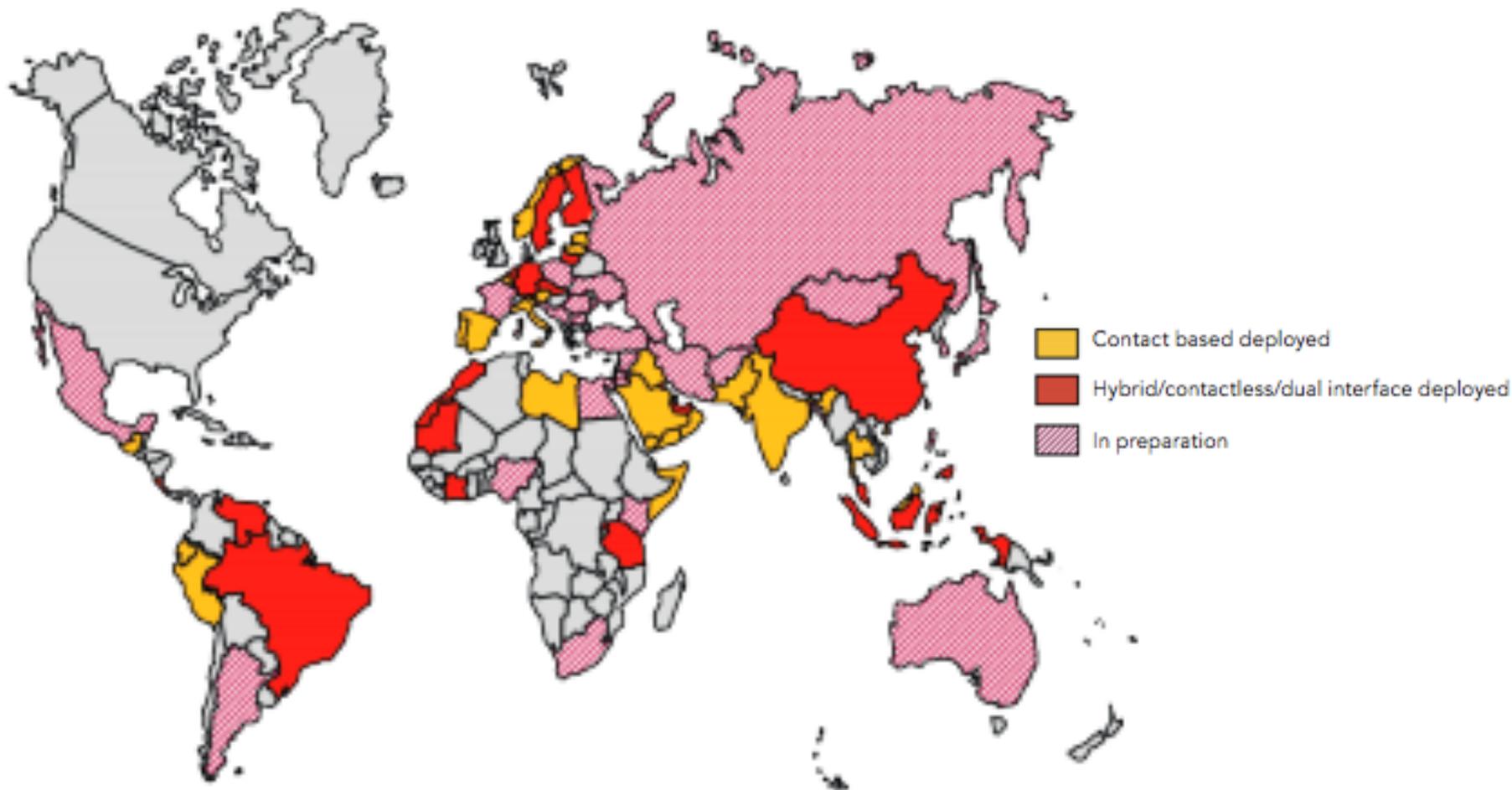
Why is strong citizen authentication interesting?

- OECD claim: lack of mature digital identities delays the development of Internet economy
 - But credit cards are widely used as payment methods without strong citizen authentication
- Citizen id used for bootstrapping of other identities
- Nordic countries as early adopters
 - Finland was the first country with smart cards for strong citizen authentication (1999), but few people use it
 - Estonia provides “electronic id” to anyone and waits this to boost its economic life

Why the survey?

- Background survey for our more technical research

Overview National eID projects



Picture from http://www.nxp.com/documents/leaflet/939775017234_V9.pdf

Strong Citizen Authentication

Two approaches:

- A governmental organization as identity provider
 - Traditional source of identity (birth certificate -> passport)
 - Often used both offline and online
- Outsourced to trusted non-governmental identity providers
 - E.g. banks, post offices, mobile phone operators
 - Already required to verify the customer identity strongly, e.g. “know your customer” rules for banks

Authentication by Smart Cards

- Electronic identity cards with a micro chip
 - Contains e.g. X.509 certificates and biometric information
 - Targeted for both online and offline use
 - Contactless and contact cards
 - Bank cards may also be used in authentication if the bank is the identity provider
 - Banks may also provide card readers to their customers
 - Pros: considered to be uncopyable and tamperproof
 - Cons: requires chip reader or NFC capability
 - Deployed (or soon to be deployed) in many countries:
 - Argentina, Australia, Austria, Belgium, Brazil, China, Estonia, Finland, France, Germany, Indonesia, Italy, Japan, Mexico, Portugal, Russia, South Africa, Spain, Switzerland, Turkey etc
-

Password Authentication

- Some countries use passwords as the authentication method
 - May be combined with another method
 - Pros: familiar and “easy” to use
 - Cons: may be weak, prone to phishing
 - Canada, India, New Zealand, South Korea, Saudi Arabia
- Some banks offer citizen authentication using one-time-passwords
 - Delivered e.g. on paper
 - Pros: banks are considered to be trustworthy
 - Cons: the same credentials used for online bank login, your money at risk
 - Denmark, Finland, Sweden, Lithuania

Authentication with Mobile Phone

- Typically as a part of two-method authentication
 - One-time code sent to the mobile phone
 - New Zealand
- ETSI Mobile Certificate
 - Cryptographic keys stored on the SIM card
 - Used for authentication and digital signatures
 - Australia, Finland, Estonia, Lithuania, Netherlands, Norway, Poland, Slovenia Switzerland, and Turkey
- Pros: trusted communication channel, personal device
- Cons: mobile malware, currently on national level, lack of trust between operators internationally

Other Physical Tokens for Authentication

- USB stick
 - Switzerland (post office as identity provider)
- Pros: most of the computers have the USB port
- Cons: cannot be connected to mobile phones

Usage around the World

- Estimated that 33% of world's population have an electronic identity card in 2009
 - Highest numbers in Estonia: 90% has the card, 24% voted online in 2011 parliament election
 - e.g. in Spain 27% has the card, but only 2% has card reader and 5% have used the card
- Mostly still used offline
- Some countries do not have or have even abandoned their online citizen authentication projects
 - Fear of central database of sensitive information
 - Citizens trust private companies more than the government
 - E.g. United Kingdom, USA

Summary

- Many citizen authentication projects are still early deployment phase
- Technical solutions are quite mature
- Use grows very slowly
 - Support from online services is lacking
 - Cross-border use is small
 - Alternative solutions have already filled the space
- Citizens often concerned about privacy and liberty issues, and sometimes for good reasons