Trusted National Identity Schemes

Coralie MESNARD
Worldwide digital transactions are booming

The number of G2C digital transactions is said to grow 30% by 2020
Citizens expect to exercise choice and control over their data when accessing digital services.

They also expect a convenient and trusted digital journey.
Digital life implies Security concerns
A person is a citizen, an employee, a friend…
Identity is a set of attributes

Your **National Identity** is issued by your government, it *makes you unique* and enables the recognition and distinction from others.
→ to *confer right and duties.*

*Multiple Digital identities*
- a SIM card,
- e-mail addresses,
- aliases on the Internet
- profiles on social networks,
- IP addresses,
- bank account..
→ to *communicate, make business*…
Digital identity is a cornerstone of digital transformational for citizens, businesses, and public administrations

- To declare a birth
- To obtain access to your bank account
- To establish ownership
- To establish who has control
Trusted National Identity scheme
Identity provider a key role in Digital ecosystem

Citizens access securely & easily online services

**Identity Provider** are responsible for:
- authenticating individuals
- (and/or) Federate Services
- (and/or) Verify Identity
- (and/or) Manage Identity on behalf of the relying party.

**Identity Attributes**
- Trust
- Convenience
- Privacy

**Certify Citizens identity**

**Relying party**

**Service Providers – Online Services**
Delegates authentication of an individual to the Identity provider.

**Reduce fraud**
**Increase usage**
**Reduce cost**

**ISSE Conference 2016 - Issy Les Moulineaux France**
Digital Identity providers landscape

Private sector driven

**Model 1** - Self asserted open digital identity frameworks

- **Model 2** - Hybrid models based on multi-identity federated frameworks across identity providers

Public sector driven

**Model 3** – Multi-channels infrastructure digital identity based on national eID schemes

- National Digital Identity schemes
- Identity Validation on eID state

- US
- UK
- Australia

ISSE Conference 2016 - Issy Les Moulineaux France
Model 3 Multi channels infrastructure digital identity based on national eID schemes
Use Case: Estonia
Many private and more than **700 e-services available**

Digital ID is available on **smart card (eID)** as well as **mobile phones (MobileID)**.

1 212 178 Active Cards
Key Metrics

One of most developed digital societies in the world leader in e-Government

× Electronic ID card introduced already back in 2002
× More than 90% of inhabitants possess electronic ID card
× Mobile-ID is „government-managed“ e-Identity.

× 12 mio transactions e-ID per month Inc. ~1.5 mio Mobile-ID transactions
× Number of transactions per month: [Public Online taxes Once a year / Private Mobile banking 2 times/week]
  ✓ 25 for each eID user
  ✓ 38 for each Mobile-ID user

× 99% of bank transfers are digital
× 98% of medicines are prescribed electronically
× 95% of tax declarations are filled digitally
× 85% of students, teachers and parents are using ane-school system
Key success factors

- Almost all public services online with no alternative
  - First country to make internet voting available in national elections - and to allow m-voting
  - 2011 elections: 25% of votes submitted electronically
  - 99% of banking transactions and more than 94% of all tax returns online.

- Very connected country with high broadband coverage and over 1100 free WiFi areas

- Computer Security 2009 & XRoad strategy:
  - Co-operation program between private and public sector
  - Aimed for safe information society in general

- Reader distribution Available at retail stores, Sold by banks or Giveaways in campaigns

- Every citizen clearly identified by a Personal Identity Code (PIC) since 1992

- Standardized national Public Key Infrastructure to bind citizens’ identity to cryptographic keys with digital certificates
National Identity scheme

Certification Centre (AS Sertifitseerimiskeskus) is Estonia’s primary and currently only certification authority (CA), providing certificates for authentication and digital signing. Owned by banks and Mobile Network Operators.

* Certification Centre (AS Sertifitseerimiskeskus) is Estonia’s primary and currently only certification authority (CA), providing certificates for authentication and digital signing. Owned by banks and Mobile Network Operators.

ISSE Conference 2016 - Issy Les Moulineaux France
Use case: Belgium
More than 3 millions citizens public online users

Foundation: federal constitutional monarchy
Population: 11.3 millions
Territory: 30 527 km²
Capital: Brussels
Language: French, Dutch, German
EU membership: since 2004
Currency: Euro
Key Metrics

Public Online Services

- 700 applications & services
- 3.3 millions users (FAS: Federated Authentication Services)
- 2.2 millions eGov profiles (binding with the eID)
- 2 millions transactions/month and, 4 millions during the tax payment period

Authentication Methods

- 60% eID
- 30% token and 10% others
- Mobile Authentication schedule for end 2016

Electronic ID card introduced already back in 2008

>17 years eID cards
12<years<17 kid ID cards

ISSE Conference 2016 - Issy Les Moulineaux France
Trusted National Identity Scheme
Model 2: Hybrid models based on multi-identity federated frameworks across identity providers

BankID in Sweden
Use case: Sweden
BankID is the leading electronic identification in Sweden

BankID is available on smart card as well as mobile phones, iPads and other tablet computers.

BankID is a citizen identification solution that allows companies, banks and governments agencies to authenticate and conclude agreements with individuals over the Internet.

Foundation: Unitary parliamentary
Constitutional monarchy
Population: 9.8 millions
Territory: 450 295 km²
Capital: Stockholm
Language: Swedish
EU membership: since 2004
Currency: Euro
Key Metrics

BankID : Successful private public Partnership

10 banks (consortium BankID) issues BankID services for use by members of the public, authorities and companies:

✓ digital identification guaranteed by the bank issuing the BankID
✓ signing transactions and documents with legal binding within European Union

+80% population [6.5 million people]

2 billion transac/year = 22 transac/citizen/month. [June 16]

The first BankID was issued in 2003.
Key success factors

- A working business model
- Cross industry usage with same user experience
- A dedicated organization that handles all important parts of the infrastructure
- A cost effective and scalable infrastructure where “one size fits all”
- So far it has been free of charge for the users
Ecosystem driven by Banks

Government
Private sector

Bank Consortium

IDP
- Authentication
- Digital Identification
- Signature

ID issuers (DL, eID)

Future

IDP
Federated Identity (2016?)

Public SP

Private SP
Companies, banks…

Citizens

eLegislation board

ISSE Conference 2016 - Issy Les Moulineaux France
Model 4: hybrid models based on verified attributes exchange

Use cases Gov.uk Verify in UK
Use case: UK
Gov.uk Verify: to prove who you are online

Foundation: Unitary parliamentary constitutional monarchy
Population: 64.7 million
Territory: 242,495 km²
Capital: London
Language: English
EU membership: since 2004
Currency: Euro
Key Metrics

Gov.uk Verify launched in April 2016

Main drivers:

Cost reduction.
- The cost of identity services has been estimated in UK in 2014 at £3.3bn
- Federated approaches like Gov.uk Verify is supposed to reduce these costs by 90%

Fraud. (Source CIFAS)
- 41% of all fraud was identity fraud in 2014
- 84% of identity fraud was online

- No use of ID cards nor central database. The user’s identity is verified by a certified company.

- The current main certified companies are Barclays, Digidentity, Experian, SecureIdentity, Post Office, Royal Mail and, CitizenSafe.
Ecosystem
driven by private sector / regulated by government

Government
Private sector

Identity providers
POST OFFICE
BARCLAYS
Royal Mail

Citizens
Gov.uk
HMS Her Majesty Services
Gov.uk verify
GDS Hub
Gov Digital Services
Regulation

Certificates Authority *

Attributes Providers
Bank
MNO
Social Network

Documents issuers
DVL
Passport

Private Service Providers
Liability is key.

- Allocates risk among participants
- Enforces obligations of participants
- Punishes non-compliance and compensate injured parties

Potential concerns

Identity Provider
- Incorrectly identifying or authenticating a user
- Failing to verify or revoke a credential
- Failing to protect a user’s personal data

Relying Party
- Relying on a false identity credential
- Failing to protect a user’s personal data

User Providing false identity data
- If someone else uses the user’s credential
Sources of duties

- Laws or regulations (public law)
  - per countries such as Gov.uk Verify
  - per region for cross border transactions such as eIDAS for Europe or PAA.net, ASEAN SW in Asia

- Contracts among the parties (private law)
  - such as Facebook, Google

Concerns

- Lack of international legal framework for data protection and data flow
- Lack of uniform standards
- Intensifying cyber-security concerns
  - Data localization/sovereignty
  - Extraterritorial law enforcement
Thank you

Coralie Mesnard  
coralie.mesnard@gemalto.com  
Innovation Digital Identity manager  
mob: +33 676 095 670