3rd Generation eIDs

EVOLUTION BEYOND NATIONAL CREDENTIALS

EJ CONSULTANTS
2020

The National Identity Card

- Government Owned
- No Embedded Chip
- Printed Data on surface
  - Facial Biometric
  - Name
  - Date of Birth
- T1 form factor polymer card
- Off-line use only

1st Generation eID Schemes

- Government Owned
- Embedded Chip
  - Contact/contactless interface
  - ICAO Applet
  - 2 or 3 digital certificates
- Printed Data on surface
  - Facial Biometric
  - Name
  - Date of Birth
- T1 form factor polymer card
- On-line or off-line use

1st Generation eID Schemes

Used for:

- eGovernment access
- ICAO Travel Document
- Digital signing via contact interface with digital certificate (EU Qualified)
- Authentication for private applications with limited liability

1st Generation eID Architecture

2nd Generation eID Schemes

- On-line use only
- Mainly Public / Private Partnerships
- PKI stored centrally
- Released by a One-Time Password device or mobile app
- Multiple authentication methods with ‘platform-less’ options

Example:

NEM ID

2nd Generation eID Schemes

- No travel document
- Cannot be used for ad-hoc off-line digital signing
- Server form and on-line digital signing
- Uses existing registration processes via banks, telco operators and local government
- Simple to use
- Fast deployment
- Low-support costs

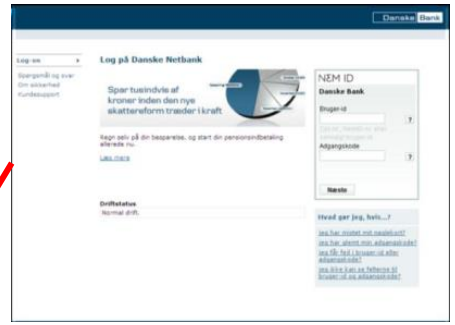
It’s low cost to implement, fast to deploy, and light to support, but with no off-line capability and cannot be used as an ID card

2nd Generation eID Architecture

Private Sector provides Identity Assurance

Central server stores keys

User is logged in



One Time Password authenticates and instructs to release keys

Key Features

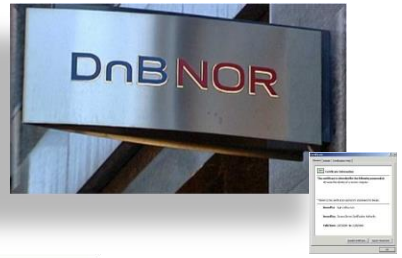
Ethics

- Minimum Data Disclosure
- User Centric Permission (and revocation)
- Usage Governance and remedy management

Technology

- Privacy enhancing
- Security Assurance

3rd Generation eID – EcoSystem

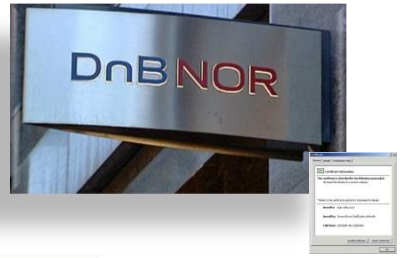


A multitude of brands providing credentials – “Derived eIDs”

3rd Generation eID – EcoSystem

Telefónica

ZURICH



McDonald's

Carrefour

e·on | UK

NEM ID

Mixed with existing government issued credentials to provide multiple overlapping Trust Frameworks

What are the Benefits?

eID Card may already be distributed

- Travel Document
- Offline ID Card

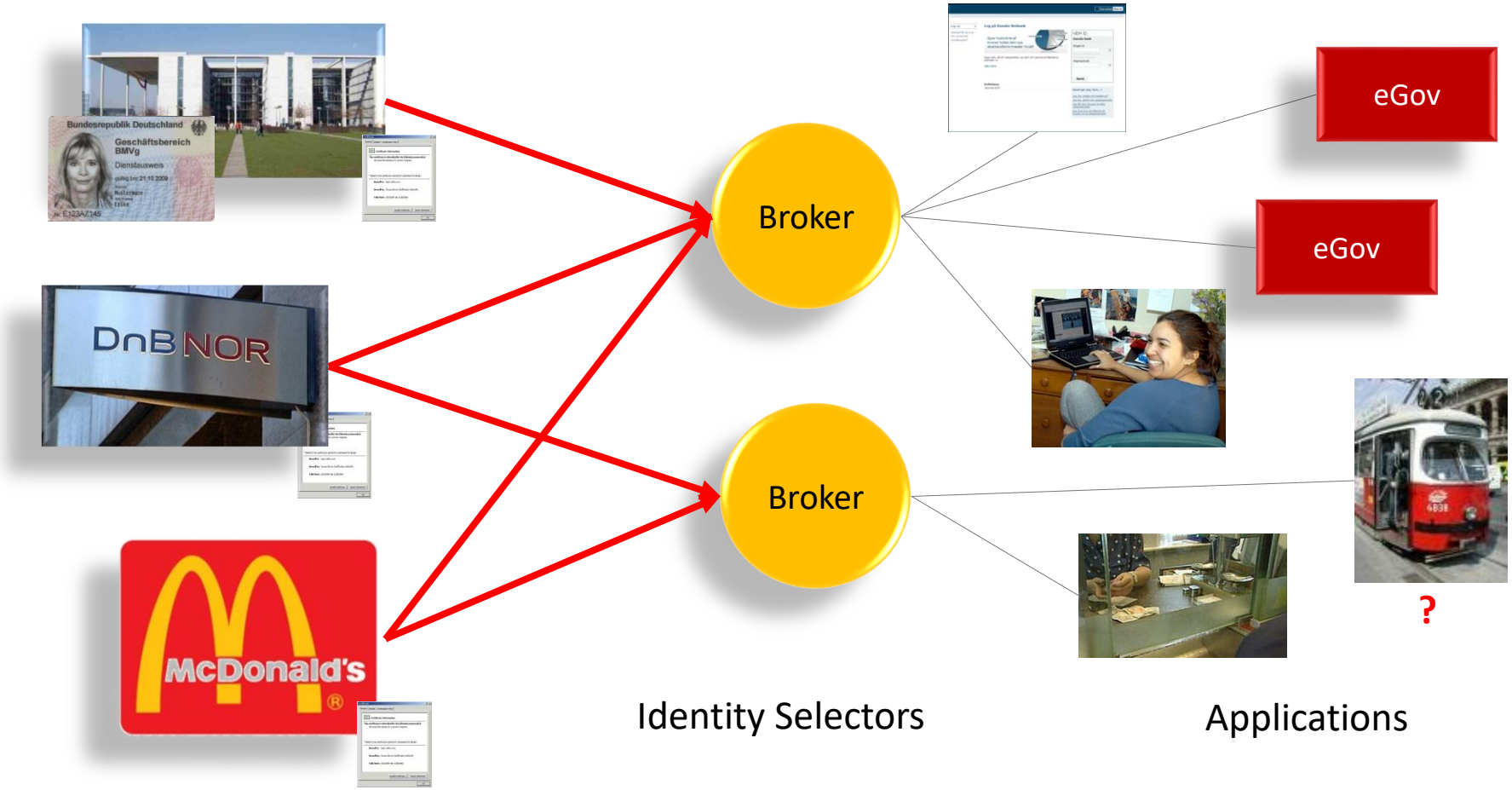
Operational risk can be reduced by identities being anchored to a government credential

Legislation may restrict or prevent the use of national eIDs for private sector use, but could permit the use of derived eIDs

Places transactions into the contractual domain, with opportunities for commercial terms and conditions, and enabling the use of mobile eIDs

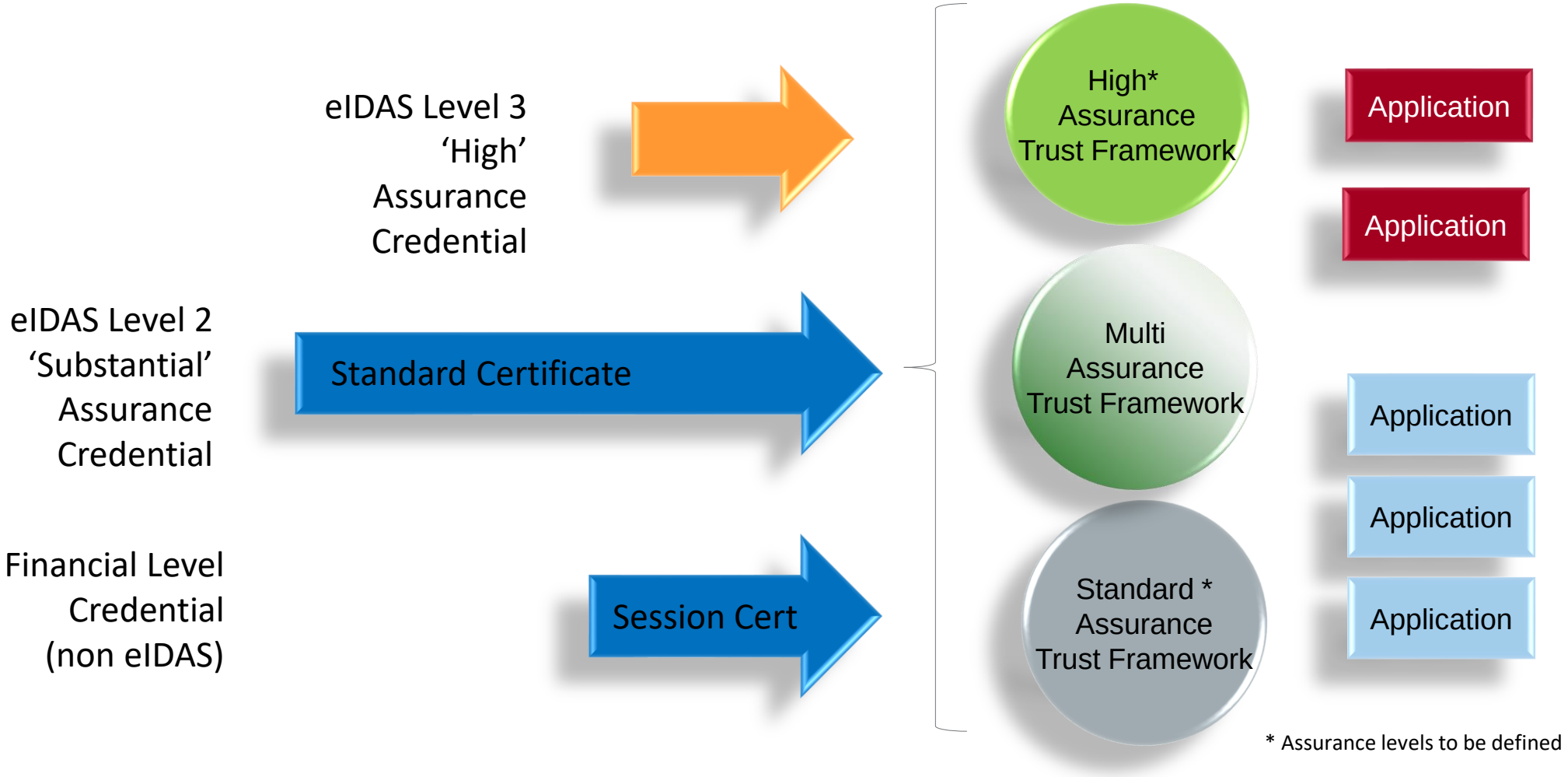
- Can use common infrastructure investment
- Reduces cost of on-boarding and KYC by using the government eID as a breeder document

3rd Generation eID Architecture



eID as a Federated multi–tier Architecture

3rd Generation eID Assurance Levels – Multiple Trust Frameworks



Why is this better?

Government eID Card can be used as breeder document

- Government acceptance of private eID service signed by citizen using eID Card
  - Trust flows through Government credential
  - Improves cost of offsetting risk by Identity Service Providers (IdSP) and relying parties

Familiar branding encourages uptake

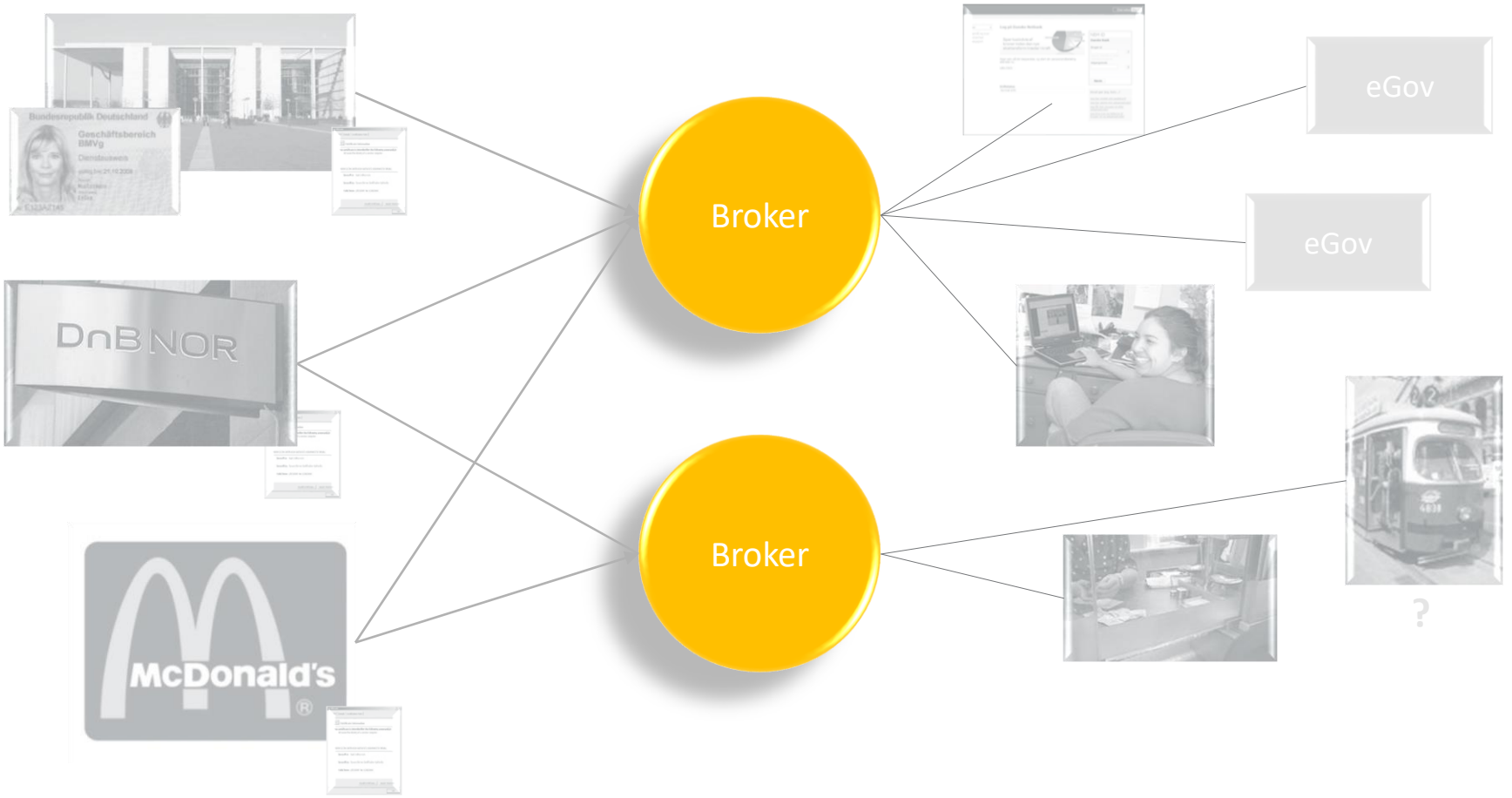
Increased trust

- Ability to ‘spread’ segments of identity across multiple service providers – membership of many trust frameworks
- Less direct connection to government in day-to-day use

However…..

- The cost of establishing an IdSP is high

3rd Generation eID Architecture



The Role of Brokers in a Federated multi–tier Architecture

Brokers - Additional Roles

Preserve data integrity, security and separation both up and down tiers

Mediate Assurance Levels, Minimum Information Datasets

Potential to perform auditing and logging at request of the relying party application and agreement of individual

Provide anti-fraud protection similar to credit-card transaction monitoring

Accept routing interfaces and trust paths for overlapping frameworks and cross-border requests (example: eIDAS)

Brokers - Ownership

Need to have ownership

- Independent of Identity Service Providers
- Independent of Relying Parties

Will require bilateral agreements with all relying parties and IDSPs if they require

- SLAs
- Liabilities
- Compliance

Strong regulation required for higher assurance roles

Attributes and Attributes Management

Public Sector ‘Owned’ - Primary

- Social Security
- Driving Licence
- Medical reference number
- VAT
- Passport

Privately owned - Secondary

- Biometrics
- Personal Preferences
- Bank details
- Medical Data
- ……..

Example of Use - Primary Attributes

Level n Assurance

Example of Use – Step-up Levels of Assurance

Level n Assurance

Level n + 1 Assurance

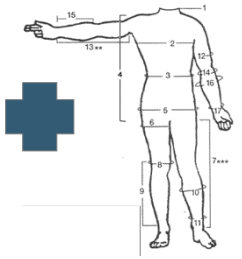
Example of Use - Secondary Attributes

Step 1

Enquire

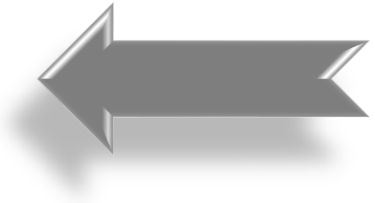
Step 2

Order and send attributes



Step 3

Fulfil



Attribute Management

As authentication becomes accepted, the use of attributes and ‘mandates’ will be seen as desirable:

- Who will be responsible for managing these mandates?
  - Government owned Attribute Provider
  - Citizen owned Attribute Provider
- How and when will mandates be certified for accuracy?
- How and when will mandates be validated for timeliness?
- What are the rules which govern the release?
  - Who determines what is needed?
  - Choice of automatic mandate or prompt
  - Minimal disclosure
- How will anonymous credentials be incorporated?
- Should they be incorporated via the IdSPs or provided directly?
  - Is there any conflict of interest?

Uses for Attributes

Establishing Identity Credentials

- ‘Primary’ type attributes
- High Assurance
- Critical for ecosystem integrity

Supplementing Identity Credentials

- ‘Secondary’ Type Attributes
- Providing Service Providers with data
- Additional Authentication

Business Models & Revenues

From Government savings and benefits

- Movement to “e-only” Government
  - Front desk outsourced for marginalised citizens
- Many statistics available demonstrating advantages

From Private Sector

- Reduction in identity risk
  - Compliance
  - Fraud
- Reduced costs
  - Process automation
  - Error reduction

“New Business” and paradigms

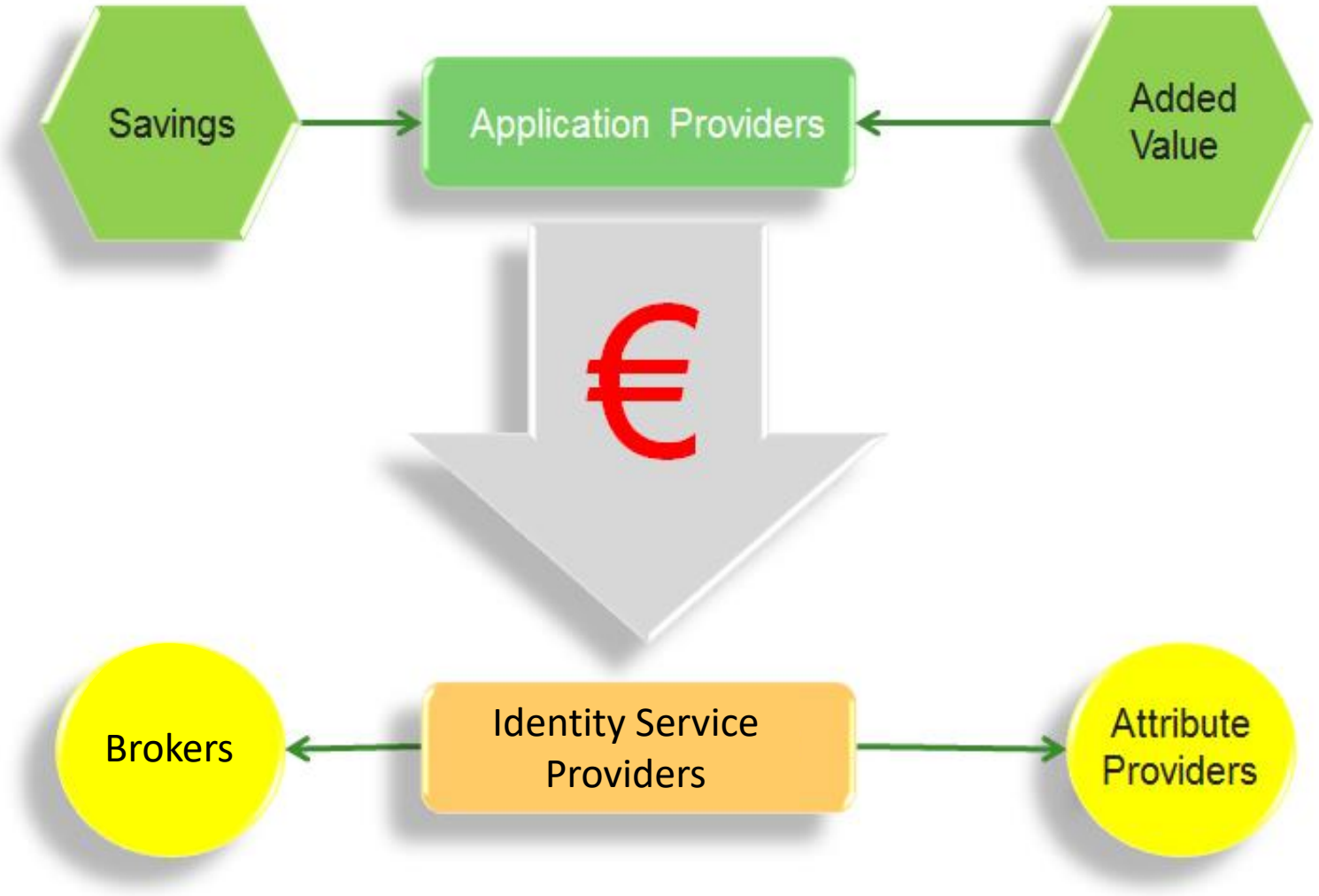
Example: Digitisation of Contract Application

- Service consisting of a signing and workflow service is used in conjunction with eIDs to digitally process bank loan application

	Application	Guarantee	Contract	Terms & Conditions
Applicant	X		x	x
Advisor	X	x		x
Manager	X	x	x	
Guarantor		x	x	x

- Traditionally this process can take over one month in time to complete and require over 70 sheets of paper.
- Real examples have shown savings in excess of €50 per application and each bank may process many thousands of applications per week.
- For the case of 10,000 applications per month, the saving to a bank is worth approximately €6 million per year.

eID Revenue - Flows

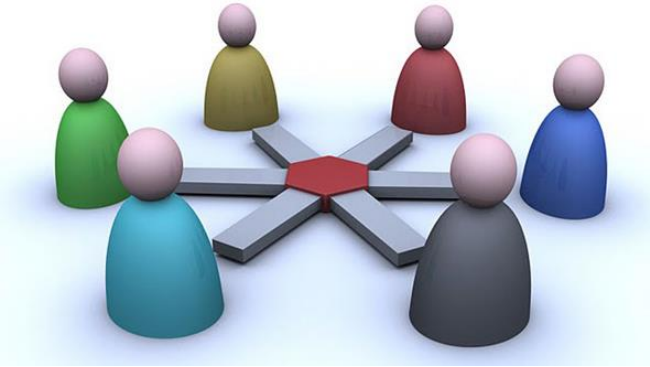


Common Governance

Technical Interoperability
- Assurance Levels for different applications
- Protocols, schemas, profiles

Commercial Interoperability
- Trust Schemes
- Revenue flows
- Liability

Exception Management
- Complaint Resolution
- Regulatory Compliance
- Redress
- Recovery



Roles for Standards

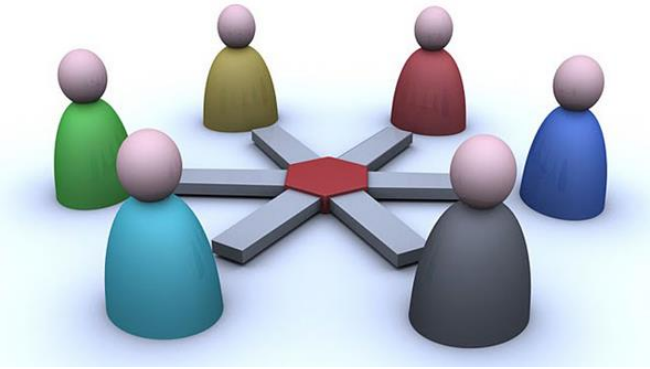
Large number of complex interactions
- Many cross-border

Essential that those interactions are standardised

Roles and duties need to be clearly understood by all players

Governance needs to be established against clearly defined actions

Much of the environment has yet to be defined



Current EU trend towards eIDs

Problems with State issuance of eID credentials

- State programs always have long delays
- Liability
- Need to maintain state/citizen separation

Advantages of private organisations

- Agility, innovation and drive
- Risk reduction
- Promotes citizen choice and opt-in
- Capability for branding
- Multi applications

Measurement of Success….

Jon Shamah

jshamah@ejconsultants.eu

+44 7813-111290