3rd Generation EID: Digital Identity for Widespread National Use and the Opportunities for Revenues

The drive towards a Single European Digital Market has brought the inconsistencies in the performances and models of digital identity across the EU Member States into focus. **A new consensus between early adopters and those yet to deploy fully digital identity schemes has led to a convergence in the understanding of what can be successful and embraced by the Citizen.**

This convergence of understanding takes the key components and best-practice from the existing models and combines them into a new environment. Crucially, existing investments are not sacrificed and are re-used making evolution much more politically acceptable. Another feature is the incorporation of privately operated schemes as well as the recent concept of Attribute Providers to extend the use of digital identities to fully transactional information exchanges, which are in the control of the citizen rather than the Service Provider. This involves a shift in the way of thinking by Governments, but one which has already started to take place. This new model is able to be federated across Member States and is able to move towards achieving the Single European Digital Market goal.

This paper presents a very high levelled view as to how this new model is formed, can evolve from existing schemes and might be successfully exploited within a revenue-generating business model.
1. Introduction

Digital Identity has matured over the last 10 years with the majority of developed countries having introduced identity-cards incorporating smartcard chip technology as part of their strategy of reducing Citizen-to-Government costs of communications, providing an electronic travel document and occasionally providing capability to legally sign documents electronically.

However, these smart identity cards have not been highly successful and their uptake by the general population has not been as high as expected and hoped. There have been some fundamental errors in this ‘1st Generation’ of eIDs, which have led to this failure and that need to be understood and addressed before a successful ‘Digital Identity Revolution’ occurs. Moreover, the potential roles of the Private Sector, and especially the Telco Operators and Carriers must be clearly understood before the full benefits of the venture are realised.

2. The Issue of Ownership - The Differences between Digital Identity Using National EID Cards and eID’s

National eID Cards are not strictly eIDs, and there has been considerable confusion by both Governments and Citizens as to the very nature of National eIdentity Cards.

National eID Cards tend to be funded by Governments. They are intended to act as an internal analogue to the Passport, providing a trusted form of visual identification for law-enforcement agencies, border control and other interactions between the citizen and the Government. These cards typically have an electronic passport component as proscribed by the International Civil Aviation Organisation (ICAO) (International Civil Aviation Organisation (ICAO), 2010), and have, when inspected visually, the same details of the card holder printed on the surface of the card as the ones contained in the normal passport.

An eID, on the other hand, is not necessarily smartcard based and has an entirely different purpose and function.

The eID is usually not owned by Government. It is a purely online identity and has the primary purpose of projecting an individual (not always a citizen) into the digital world. As such, the benefits of such eIDs are limited and cannot fulfil the role of passport or that of visual identification.

This confusion has led to a lack of enthusiasm of citizens to embrace the concept of digital identity and in extreme cases, such as in the UK, has led to the absolute failure of National eID programs and significant political costs. In this case, the confusion was propagated by incoherent and mixed messages regarding usage and benefits of National eIDs.

3. 1st Generation EID

National eID Cards can be considered as the ‘1st Generation eIDs’ and were originally conceived amidst the confusion described above.
They typically consist of a standard smartcard with a ‘T1’ form factor (International Civil Aviation Organisation (ICAO), 2010) (a passport booklet is ‘T3’) with printed information (Face Biometrics, Name, Date of Birth) on the surface and two or three digital certificates carried in the embedded processor chip. These are accessed via a contact interface to provide digital signing capability. When an ICAO electronic passport application is included, a proximity interface is needed to be included as well as a Machine Readable Zone (MRZ).

Typical Key Features of 1st Generation eIDs

- Online or offline use
- eGovernment access
- ICAO travel document
- Digital signing via contact interface with digital certificate (EU qualified)
- Authentication for private applications with limited or no liability

The smartcard functionality of these identity cards is intended to reduce identification errors and fraud in these interactions and to provide the capability to automate the transactions either across the internet or as part of a face-to-face transaction. In most cases, the total number of these interactions per person is small \(^1\) and the benefits in the use of these cards are all addressed to the Government.

4. 2\(^\text{nd}\) Generation EID

Pure digital identities, existing only electronically can be considered as ‘2\(^\text{nd}\) Generation eID’ schemes. These credentials are intended solely for use on the Internet and only serve the function of projecting an individual into the digital domain. As such, they do not require an ID card or any other carrier, but can and should make use of some physical authentication mechanism such as a One-Time Password\(^2\).

---

1 For example on average in Austria, typically 2-3 uses per year per citizen.
2 A One-Time-Password is a unique code generated specifically for a single authentication of the recipient. It is usually sent via a different communication channel (i.e. mobile phone or custom device) or a number are pre-generated and issued in advance and randomly selected for use.
This evolution of eID can fulfil government requirements for electronic transactions with citizens and retains those financial benefits, but does not provide offline use such as the one provided by the ICAO electronic passport or police identification. However, there are significant advantages compared to the 1st Generation eIDs such as simplicity in use and a much lower cost for production, distribution and support.

These credentials are based on centrally managed PKI credentials released by the individual owner using a one-time password or another authentication mechanism. The main implementations of these eIDs are in Nordic countries where the banking system is responsible for the eID schemes - sometimes independently or in conjunction with the Government - but in both cases taking advantage of banking enrolment and verification procedures. Given the fact though that the credential is stored on a central server, it is difficult to use eIDs to digitally sign ad-hoc documents, although standard forms can be signed using server-based services. Additionally it is difficult to absolutely encrypt documents on the individual’s desktop using the credential as the keys are located on the server.

Typical Key Features of 2nd Generation eIDs
- Online use only
- Mainly bank or private sector owned
- Private keys stored centrally
- Released by a one-time password device
- Multiple authentication methods with ‘platform-less’ client
- Not a travel document
- Cannot be used for ad-hoc digital signing (only server form signing)
- Desktop encryption is not possible using the credential

2nd Generation eIDs in Norway and Denmark, operated by the Nordic banking consortia, NETS 3, and a similar system operated by Swedish banks, are highly successful. In those countries, eID usage

---

3 NETS Norway AS [http://www.nets.eu](http://www.nets.eu)
exceeds 10 million transactions per week which averages at approximately 2 transactions per citizen per week. This is significantly higher per citizen than in any other country and their use is already firmly embedded in society.

5. 3rd Generation EID - The Best of Both Worlds

It is unrealistic to expect governments who have invested large sums of money and political will to change tracks and withdraw a national identity credential in favour of a new technology. However, emulating the success of 2nd Generation eID schemes, especially in Nordic countries, is attractive to all governments who have experienced only marginal success with their own programs.

5.1 Identity Providers

3rd Generation eID addresses this problem and extends the concept. It is essentially an ecosystem of multiple identity providers providing credentials for use both within the public and private sector, but critically utilising and relying on Government eID Cards as initial ‘breeder’4 documents assuring the enrolment is ‘tethered’ to the existing national identity. These new credentials will essentially build on both 1st and 2nd Generation eID techniques and benefits but will be able to be issued by a wide range of identity providers utilising the quality of the breeder documents. The National eID Card will still be the credential used for law enforcement and border control, but the eID will be used for digital transactions.

This combination also addresses Governments’ reluctance to share a credential with any private sector application and conversely the hesitation of any private sector application to be associated with any governmental organisation, especially considering public perceptions of privacy etc.

5.2 Hubs

The large number of private sector Identity Providers presents some unique problems and opportunities.

• a large variation in quality may be expected;
• integration between the many identity providers and applications will be complex;
• general privacy and security issues;
• many identity providers can operate in the same scheme (‘federation’) and may be differentiated, not only by quality of enrolment but also via brand confidence. In fact, the brand reputation may well be the deciding factor in the individual’s choice or ID Provider.

---

4 A breeder document is a Trusted source document that underpins the identity of the applicant for enrolment. It is typically a government issued document or one that has been issued by a government certified entity.
Therefore there is a need for intermediary hubs, (sometimes called ‘identity brokers’) between the many identity providers and applications providing common interfaces and standards in a form of 3-tier architecture.

Hubs have a critical role to play in this architecture. They form the basis of imposing the scheme’s governance and standards as well as mediating between assurance levels and liabilities from within the scheme and externally from sources such as STORK 5 (Secure Identity Across Borders Linked).

The Hubs must be independent of both application providers and identity providers but do need to be highly regulated with strong Service Level Agreements, governance and integrity in order to act as truly Trusted Third Parties as well as pathways for linking to other eID schemes cross-border.

5.2.1 Attributes

<table>
<thead>
<tr>
<th>Role of Hubs in 3rd Generation Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Maintain standards-based interfaces for all components of the architecture</td>
</tr>
<tr>
<td>• Preserve data integrity, security and privacy both up and down tiers</td>
</tr>
<tr>
<td>• Mediate between Assurance Levels</td>
</tr>
<tr>
<td>• Perform auditing and logging at request of the relying application and agreement of individual</td>
</tr>
<tr>
<td>• Provide anti-fraud protection similar to credit-card transaction monitoring</td>
</tr>
<tr>
<td>• Provide assurance to individuals that data is only retained for agreed lengths of time</td>
</tr>
<tr>
<td>• Accept routing interfaces and trust paths for inter-hub and cross-border requests from sources such as STORK</td>
</tr>
</tbody>
</table>

One of the benefits of a strong identity ecosystem is the ability to securely present additional attributes of the individual to an application provider. These could range from the applications provider’s internal reference number - if a relationship has already been established - or preferences and characteristics which are essential for the completion of a transaction. An example could be: Preferences for car-hire, together with driving licence and payment details.

5 STORK (Secure Identity Across Borders Linked), www.eid-stork.eu
The management of attributes, their authentication and certification is beyond the scope of this document, but their application in 3rd Generation eID schemes can be achieved using technologies already in development such as IBM’s IDEMIX (IBM Switzerland, 2012) and Microsoft’s U-Prove (Microsoft, 2012). Attribute Providers must remain separate from other service providers, conform to minimum disclosure best practices and user-centric control of distribution.

5.3 Early Implementations of 3rd Generations EIDs

3rd Generation eIDs schemes are beginning to be implemented by the earlier eID adopters as they realise the costs and timelines regarding their existing National eID Card deployments. Both Estonia and Austria, amongst the earliest adopters of eIDs, have begun to offer server-centric eIDs to citizens in conjunction with existing card-based eIDs and using those as breeders for the enrolment. Other countries are looking to telcos and banks to provide mobile-based eIDs as alternatives to the existing national eID cards.

6. EU Cross-Border Operations

As described earlier, the Hub provides a Trusted Third-Party middle layer for mediating between Identity Providers and Applications. An identity provider may not even need to be located within the same country as the eID scheme, but nonetheless must conform to, and meet the standards in force of the eID scheme in which it wishes to participate.

Scalable models for achieving this and providing conformance to appropriate Data Protection legislation can be based on Large Scale Pilots already under test in the EU under STORK. These STORK protocols could easily be integrated within the 3rd Generation tier architecture.

At present, STORK provides a technical structure for the interoperability of eIDs across Member State boundaries typically via a series of proxies, and ensures the citizen permissions, the transfer of data and the authentication. This methodology can also be used to bridge different eID schemes between hubs. The hubs could then mediate between Levels of Assurance.

7. International Programs and Collaboration

The concept of 3rd Generation eIDs within the Seamless European Digital Market being linked to non EU schemes, such as NSTIC (The White House, 2009), in the USA is now being actively considered and investigated in the European Commission’s SSEDIC 6 Thematic Consultation Network.

8. Opportunities for Profits in 3rd Generation EIDs

How can organisations address opportunities in this market?

Opportunities arising from 3rd Generation eIDs derive from delivering capacity, services or applications. Given the fact that functionality is clearly delineated within each tier of the architecture, it is possible to visualise potential roles with greater clarity.

1. Identity Provider

---

2. Application Provider
3. Attribute Provider
4. Hub Operator

8.1 Identity Provider

It is clear that mobile telecommunication providers have strong customer loyalty and brand strength from a high level of market penetration. Other sectors that might have competitive positions are banks and retail brands, although new entrants such as social media and other organisations may be able to enter this market via the white-labelling of services from the primary providers.

Indirect benefits include adding long term added value to existing clients and attracting new clients to the brand.

8.2 Application Provider

Organisations that depend on eID Application Providers will probably be operating in existing business sectors or eGovernment and will be able to reduce costs and improve added value services through the use of identities that are trusted and do not need to be established for each and every instance of use.

These savings and added value services will generate the revenues needed to fuel the eID architecture. Savings can be substantial in a fully developed 3rd Generation eID scheme.

8.3 Attribute Provider

Attribute providers may well grow up as a completely new business sector, with roots in existing financial information aggregators such as Experian but now being controlled by the end user rather than traditionally by business clients. However their role will require very high levels of trust and governance.

8.4 Hub Operators

Hubs form the core components of the 3rd Generation eID scheme and impose the governance and standards for the scheme to operate correctly. Operation of hubs could be undertaken by government or industry institutions.

7 Experian: www.experian.com
9. Example of Revenue Opportunity

A single example of the savings possible using a 3rd Generation eID scheme is that of the granting of a bank loan application using the ‘TrustSolutions’ signing service from NETS.

In this case there are a number of documents required to complete the application:

- Application
- Guarantor
- Contract
- Terms and conditions

Additionally there are a number of different signatures needed:

- Applicant
- Bank Advisor
- Bank Manager
- Guarantor

These signatures need to be applied in a certain order and from different individuals who may have to have their identities validated for compliance.
Table 1: Signature & document example for loan application

<table>
<thead>
<tr>
<th></th>
<th>Application</th>
<th>Guarantee</th>
<th>Contract</th>
<th>Terms &amp; Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicant</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advisor</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manager</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Guarantor</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

This process can take over one month in time to complete and require over 70 sheets of paper, much of which will be needed to be posted. In this case real examples have shown savings in excess of €50 per application and each large bank may process many thousands of applications per week. For the case of 10,000 applications per month, the equivalent annual saving is approx. €6 million. With a 50% savings split, this would generate an annual revenue to the Identity Provider of €3 million.

10. Conclusions

3rd Generation eID is a natural evolution from the early and current schemes seen throughout Europe. As early adopters are realising the advantages, more eID schemes will evolve to the new paradigm, maintaining and using the existing investments as part of the advanced solution.

Revenues can be realised from existing improvements in process and new added value services. Additional organisations will emerge providing identity and attribute services to the individual as well as Trusted Third Party infrastructure and operations.

It is likely that early movers will establish strong footholds in the market and organisations in the sectors that have a natural fit to the opportunities stand not only to gain financially but to enhance their position within the community as a whole, making 'sticky' and loyal customers.

11. References


Authors

Jon Shamah
EJ CONSULTANTS
jshamah@ejconsultants.co.uk
http://www.epractice.eu/en/people/14869