e-Identity – monetization and interoperability

Marc Sel

PwC

marc.sel@pwc.be

Abstract

This article discusses different ways to approach the value of identity. It attempts to modelise the economic value of identity, and to demonstrate the added value of making use of government provided identities.

1 Context

The value of identity means different things to different people at different times. In a world where Internet-based dematerialisation continues to increase, concepts such as identity, authentication and integrity are among the key safeguards against mis-use scenarios such as money-stealing, misappropriation and identity theft. Unfortunately, most countries have a unique and not necessarily interoperable approach to electronic identity.

However, where an electronic identity is available and sufficiently reliable, it can be used to the benefit of the Public and Private Sector alike.

2 Problem and analysis

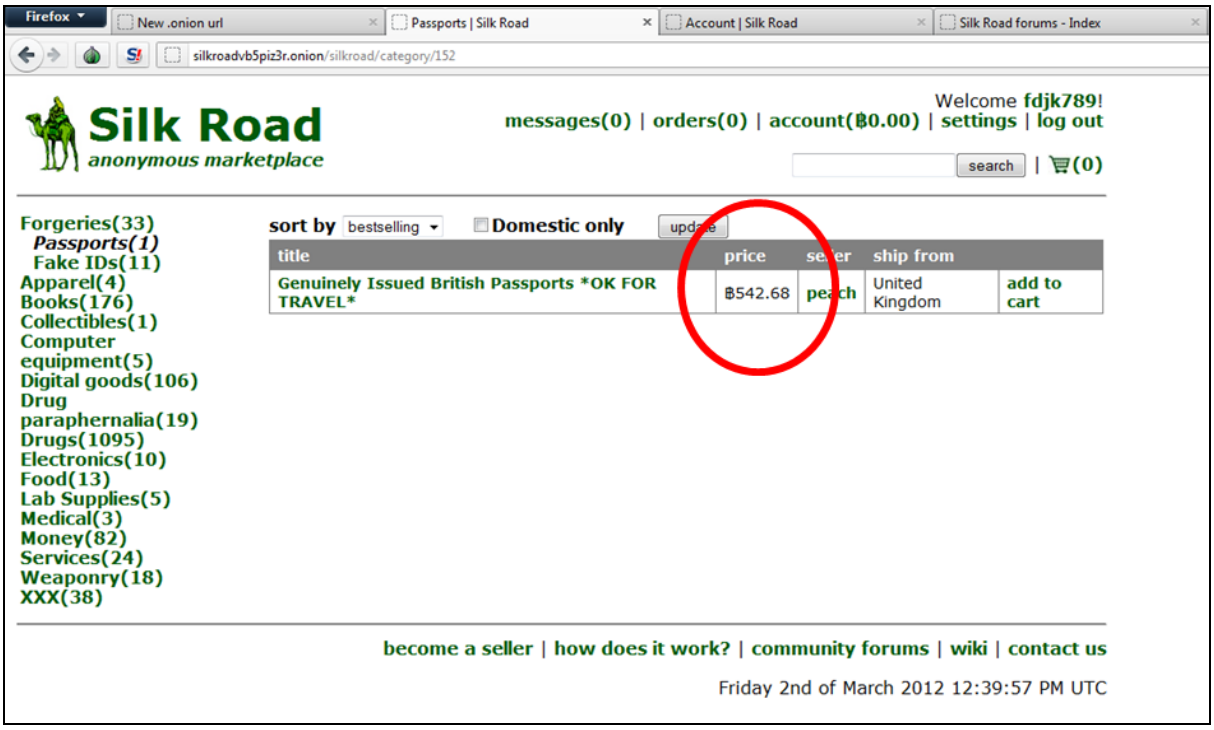
2.1 A short description of the problem

Countries are free to choose how they manage their citizen's identity. As a consequence, their area quite diverging approaches in use worldwide. Solutions range from regulation-driven (such as the EU) to rather market driven (such as the identity elements in the M-PESA mobile payment ecosystem, popular in Africa, driven from KYC[1] regulations), and mixed approaches such as in the current US/UK situations. Other market-driven solutions include those from e.g. Microsoft, Facebook and Google.

It can be observed that markets require various and different forms of trust for execution of transaction. It can equally be observed that in a Public Service context, for allocation of benefits to citizens, trust is also a key element to make sure the money reaches the right individual, and is spent as intended.

Calculating the value of an identity is a complex subject that we will not attempt to here. However, we performed a search on alternative ways for this valuation. One particular source of information is the Silk Road market place on the TOR network [TOR].

[1] KYC: Know Your Customer



Silk Road
anonymous marketplace

Welcome fdjk789!
messages(0) | orders(0) | account(฿0.00) | settings | log out

| (0)

Forgeries(33)
Passports(1)
Fake IDs(11)
Apparel(4)
Books(176)
Collectibles(1)
Computer equipment(5)
Digital goods(106)
Drug paraphernalia(19)
Drugs(1095)
Electronics(10)
Food(13)
Lab Supplies(5)
Medical(3)
Money(82)
Services(24)
Weaponry(18)
XXX(38)

sort by bestselling □ Domestic only

title	price	seller	ship from	
Genuinely Issued British Passports *OK FOR TRAVEL*	฿542.68	peach	United Kingdom	add to cart

become a seller | how does it work? | community forums | wiki | contact us

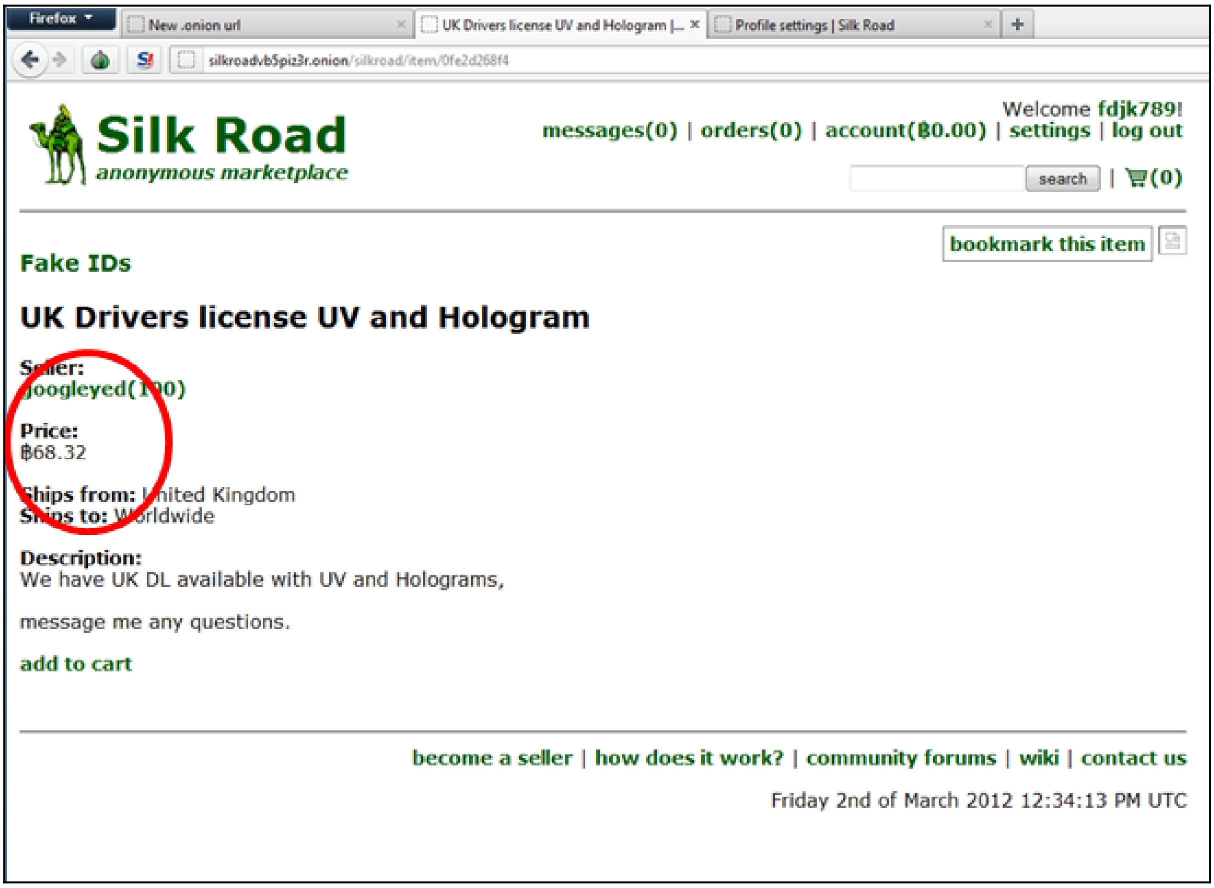
Friday 2nd of March 2012 12:39:57 PM UTC

Fig. 1: Screenshot of Silk Road market place on TOR offering UK passports

As you can see from the screenshot taken in March 2012, the passports are quoted in Bitcoins, for a value of 542,68 Bitcoins each. With an exchange rate quoted around 5 € to a Bitcoin (averages as published by Mt.Gox Bitcoin Exchange[MTGOX], figures taken in March 2012), this amounts to approximately 2710 € for a UK passport.

In case you are not familiar with it, the Bitcoin ecosystem was initiated by Satoshi Nakamoto, a Japanese cryptographer. It is one of the cryptography-based digital currencies that enables instant payments from wallet-to-wallet, anonymously. It uses peer-to-peer technology to operate with no central authority and is a prime illustration of using cryptography in a P2P setting to explore new ways for anonymous payments, at low cost. It is extensively used in communities such as those based on TOR. Bitcoins are generated by mining, which is actually the processes of finding hashes which start with a long string of zeros. This imposes a workload for the mining process, which guarantees that coins cannot be created just like that. Over time, foreign exchanges have appeared that exchange Bitcoins against the Euro and the Dollar. Bitcoin wallets are available cross-platform, and its acceptance is on the rise.

As a short visit to the Silk Road market place will learn, what is on offer is not necessarily legal. It can be observed on the screenshot in Figure 1 that the category "Drugs" has the highest number of entries. Also, but not visible from the screenshot, is that some of the offerings in the category "Services" are rather appaling.


Firefox
New .onion url
UK Drivers license UV and Hologram |...
Profile settings | Silk Road
silkroadvb5piz3r.onion/silkroad/item/0fe2d268f4
Silk Road
anonymous marketplace
Welcome fdjk789!
messages(0) | orders(0) | account(฿0.00) | settings | log out
search | (0)
bookmark this item
become a seller | how does it work? | community forums | wiki | contact us

Fake IDs

UK Drivers license UV and Hologram

Seller:
googleyed(100)

Price:
฿68.32

Ships from: United Kingdom
Ships to: Worldwide

Description:
We have UK DL available with UV and Holograms,

message me any questions.

add to cart

Friday 2nd of March 2012 12:34:13 PM UTC

Fig. 2: Screenshot of Silk Road market place on TOR offering UK driver license

In case you prefer a cheaper identity credential, UK Driver licenses are on sale as well. Using the same exchange rate as before this amounts to approximately 350 € for a UK Drivers license. The seller claims this is including the security features such as printed on paper supposed to be sufficiently deceiving with regard to ultra-violet security patterns, and incorporating the hologram. Obviously such a Driver license can be used as bootstrap to obtain stronger credentials such as a passport or an identity card.

While this information is in no way conclusive, we consider it indicative that there is a e-market for fake identities, and it allows us to form an idea with regard to prices.

2.2 Where the Facebook id-approach falls short

Another interesting alternative to construct identity comes from Facebook. You may like or dislike it, but its success cannot be denied. While Facebook has interesting characteristics, the identies it generates are dificult to deploy in an eGovernment or eBusiness context (unless explicitly corroborated with an independent identity verification). Consider the following questions that seem to relate to identity, and how answers to them could be generated or derived from the social graph.

What was the make of your first car? *Pictures of it are online*.

What was the name of your first pet? *My friends know my new dog is my first*.

What is your mother’s maiden name? *I'm friends with my mother, who lists this so she can catch up with old school friends*.

What was the name of your first school? *Facebook asks for this.*

What is your favourite food? *I've probably posted a picture of it, or commented on it.*

What was your first job? *Facebook and Linked-in like to record this*. *The same applies for the name of the first company I worked for.*

Which country did you visit on your first overseas holiday? *See my timeline and you'll know.*

What is your father's middle name? *If I'm friends with my father, who put his full name online, you'll see.*

What is your preferred musical genre, artist, album? *See all the music I posted onto Facebook or other social media.*

So deriving an identity claim should be based on something significantly stronger than just knowing the answers to these questions. Nevertheless, use cases can be envisioned that allow Facebook identification/authentication if there would be a way to bootstrap the Facebook identities from a stronger credential.

2.3 United Kingdom

System cost estimates in the UK

Please note that the following statements are only based on public domain information from public documents and from the Internet.

Originally, studies suggested that costs for an identity system for the United Kingdom could be as much as **£12 billion to £18 billion**. The reliability of these studies has been challenged by the Government which disputed some of the assumptions used in the calculations such as the need to retake biometric information every 5 years. Tony McNulty, Home Office minister responsible for the scheme, responded by saying a "ceiling" on costs would be announced in October 2005.

After the general election the Home Office stated that it would cost **£500+ million a year to run** the scheme.

In May 2007 the Home Office forecast a cost rise to £5.3 billion, a figure revised in November 2007 to £5.612bn.Subsequently, the Government abandoned plans for a single new computer system to run the national identity card scheme. Instead of a single system, information will be held on three existing, separate databases.

Citizen direct costs

For citizens, an estimate from the Home Office placed the cost of a 10-year passport and ID card package at £85, while after the 2005 general election in May 2005 they issued a revised figure of over £93, and announced that a **"standalone" ID card would cost £30.**

2.4 United States of America

The USA has been very active in establishing large scale PKI's as well as PKI-bridges. They have equally been issuing PIV (personal identification verification) technology including smart cards (such as the CAC – the Common Access Card). However, all of this was mainly in a military or homeland security context. With regard to the approach for the citizen, the landscape is more complex, and typically based on the Social Security Number and the Driving License. The Obama administration launched the „National Strategy for Trusted Identities in Cyberspace" (NSTIC).

We quote from this document:

QUOTE

The Federal Government will support the private sector's development and adoption of the Identity Ecosystem through activities such as: convening technology and policy standardization workshops, building consensus, establishing public policy frameworks, participating in international fora, funding research, supporting pilots, and initiating education and awareness efforts

The Federal Government will partner with the private sector and participate in the development of the Identity Ecosystem Framework to ensure that it establishes a sufficient baseline of interoperability, security, and privacy

The Federal Government's role in this area is to help ensure the outcome; the private sector is better suited to ascertaining the means of achieving that outcome This participation will also enable the Federal Government to advocate for and protect individuals Among the actions that the Federal Government must undertake, privacy is the most important for individuals; as such the Federal Government will ensure that the FIPPs are effectively incorporated into the Identity Ecosystem Framework

UNQUOTE

As such it is our interpretation that the main investment will not be made by the US Government, but this is rather left to the private sector.

2.5 Belgium

Belgium, albeit a small contry, invested significantly in electronic identities to improve the service level offered by the Public Service to the Citizens. Following cost figures are derived from public documents.

On the CAPEX side, the government allocated the card contract to the private sector company Zetes. The contract was allocated in 2002, for a total value of approximately 65 million € for 10 million eID cards, delivery over 5 years (source: Zetes prospectus 2005). The Certification Authority contract was allocated to Belgacom, the incumbent operator, who passed it on to Certipost (part of the incumbent national telecom operator at that time, today part of the Belgian Post "bpost"). We have not identified cost information in this respect.

The following OPEX elements could be identified from public sources. Statutory employees were made available for 3 years, free of charge, to the municipalities by Belgacom (the incumbent telecom operator), NMBS (national railroad operator), De Post, BIAC and Belgocontrol. This to facilitate the first wave of enrolment and card delivery.

Furthermore, the National Register (RRN) allocated a budget of approximately 7 million € per year for the eID (source: the official State Gazette – "Begroting"). And FEDICT (Federal ICT department) allocated an annual eID budget around 2 million € annually as follows:

	2004	**2005**	**2006**	**2007**	**2008**	**2009**	**...**
FEDICT budget eID	976.330	2.410.000	1.912.000	3.533.000	1.903.000	1.850.000	

Fig. 3: FEDICT eID budget (source: FEDICT annual reports)

Depending on further assumptions made, one could estimate the total project cost of implementing the BeID around 200 – 250 million €. An official audit report by the State Auditor (Rekenhof/Cour des Comptes/Court of Audit) is expected this year, and will most likely provide more accurate and detailed figures on the actual eID cost.

Nevertheless, we assume that the figures will be of another order of magnitude than those put forward for the UK eID.

Obviously, this is a model where there is a relatively high degree of trust placed in the State's role in the eID ecosystem. We argue that this is a cost effective way to address the State's own identity-related problems in its "business" processes, and that it may be relevant for the Private Sector to "piggyback" on such investment made with taxpayers money.

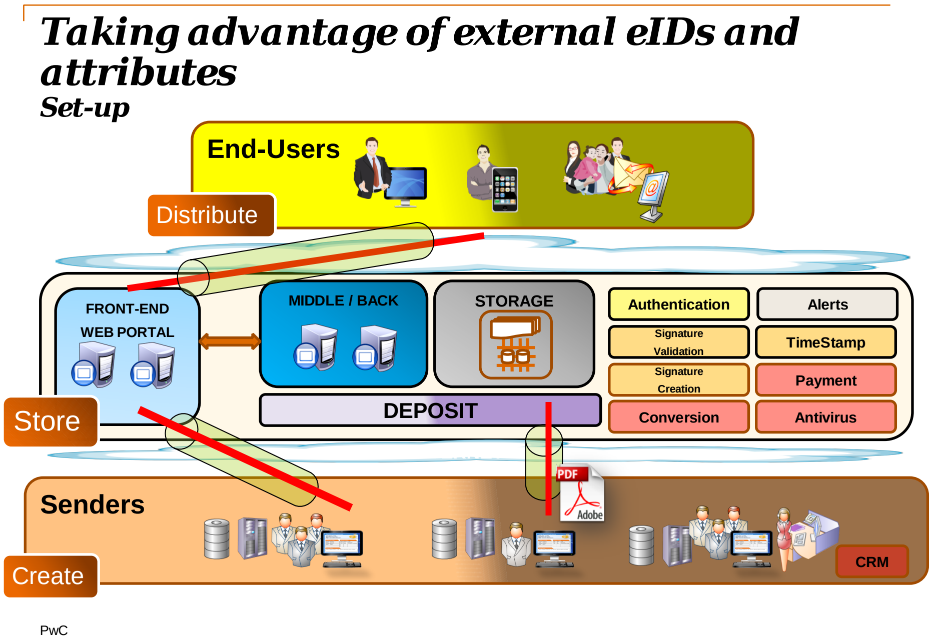
3 Taking advantage of eID

3.1 Business idea

Consider an electronic document delivery platform, to serve stakeholders from different industries, who decided to pool resources to develop a competitive edge. Such a platform would typically be open to parties that contribute a relevant volume in eDD (electronic Document Delivery. The partner model allows to capture *"Economies of Scale"*, with cost saving for everybody involved. Such a model should preferably start from end users' "Use Cases" rather than technical solutions, and should be "low entry" for end users.

3.2 Functional architecture

The functional architecture of such an eDD platform can be summarised as:



Taking advantage of external eIDs and attributes

Set-up

PwC

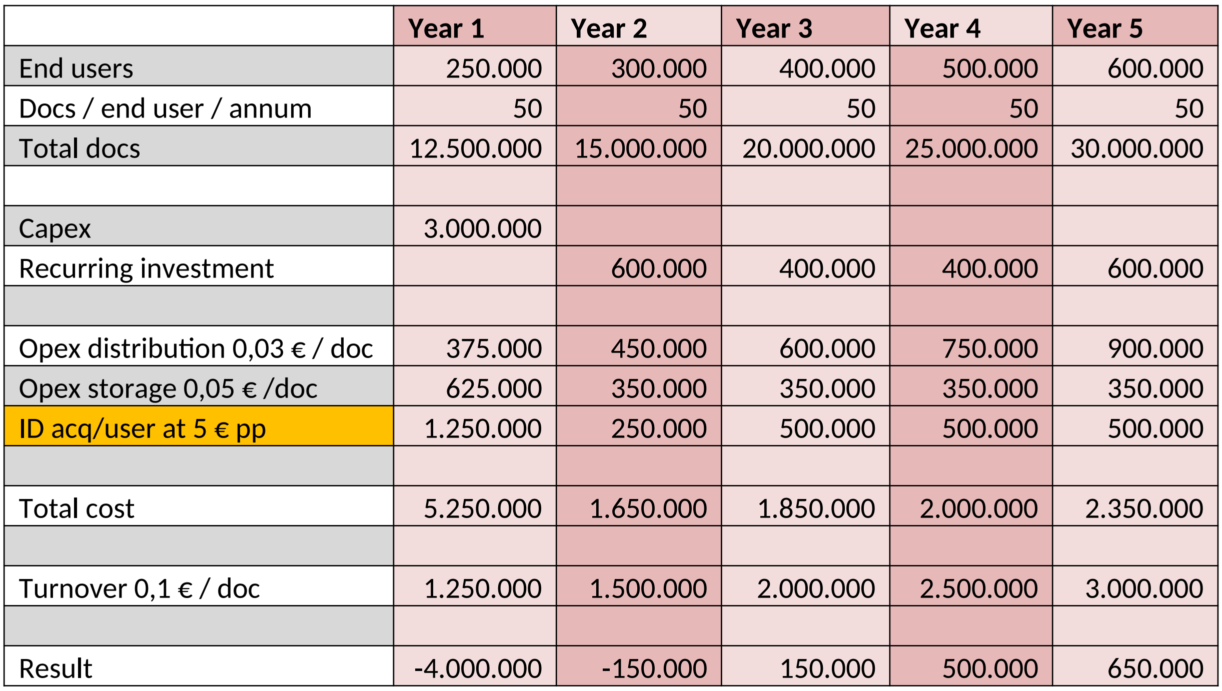
Fig. 4: Electronic Document Delivery set-up

It is not difficult to imagine security requirements for such an eDD. These should include the „usual suspects“, such as User Data Protection (access control, data authentication, data integrity, …), Privacy (Anonymity, Unlinkability, …), Identification and Authentication (user identification, …), Cryptography (key management, …), Communication (Non-repudiation of origin and receipt, …), Protection of the platform itself (availability, confidentiality, …), Resource Utilisation (fault tolerance, resource allocation, …), Security Management (roles, responsibilities, …), Security Audit (event selection , storage, analysis and reporting, …) and many more. Obviously, IAS functionality (Identification, Authentication, and Signature) would be a foundational element.

3.3 Business perspective

For such an eDD, the business model could be “document based”, i.e. using on a charge calculation based on volume. A partner in the hypothetical eDD system would have a financial participation, with Capex (-) and Dividends (+). He would experience an operational effect of both Ristorno’s (+) and Costsaving (+). The eDD operator would have his own Capex, containing his expenditure for service establishment as well as any recurring investments. He would have his Opex, consisting of Turnover (+), Cost (-) and Ristorno’s paid (-).

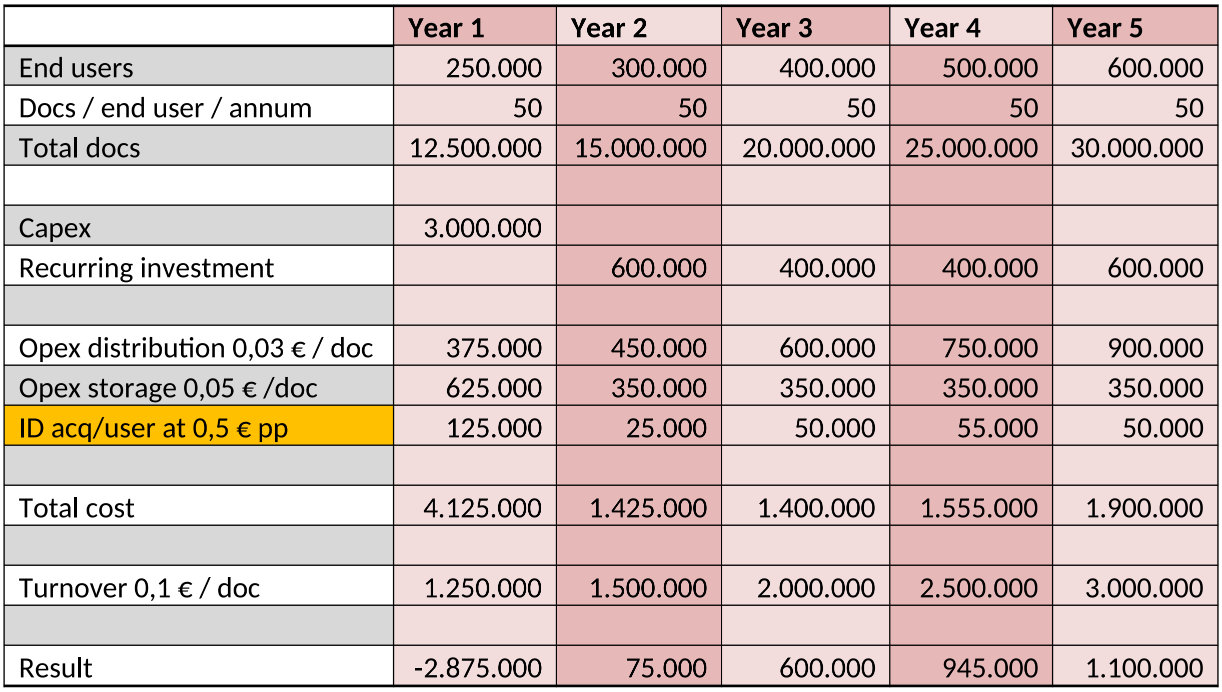
In case no government eID is available to the eDD platform, the acquisition of the identity of a user would have to be organised (invitation, enrolment, verification, ...). We estimated this at 5 € per person. A simplified income statement would then look as follows:



	Year 1	Year 2	Year 3	Year 4	Year 5
End users	250.000	300.000	400.000	500.000	600.000
Docs / end user / annum	50	50	50	50	50
Total docs	12.500.000	15.000.000	20.000.000	25.000.000	30.000.000
Capex	3.000.000				
Recurring investment		600.000	400.000	400.000	600.000
Opex distribution 0,03 € / doc	375.000	450.000	600.000	750.000	900.000
Opex storage 0,05 € /doc	625.000	350.000	350.000	350.000	350.000
ID acq/user at 5 € pp	1.250.000	250.000	500.000	500.000	500.000
Total cost	5.250.000	1.650.000	1.850.000	2.000.000	2.350.000
Turnover 0,1 € / doc	1.250.000	1.500.000	2.000.000	2.500.000	3.000.000
Result	-4.000.000	-150.000	150.000	500.000	650.000

Table 1: Electronic Document Delivery cost estimates without eID

In case a government eID is available to the eDD platform, the acquisition of the identity of a user can be limited to online verification of the eID. We estimated this at 0,5 € per person. A simplified income statement would then look as follows:



	Year 1	Year 2	Year 3	Year 4	Year 5
End users	250.000	300.000	400.000	500.000	600.000
Docs / end user / annum	50	50	50	50	50
Total docs	12.500.000	15.000.000	20.000.000	25.000.000	30.000.000
Capex	3.000.000				
Recurring investment		600.000	400.000	400.000	600.000
Opex distribution 0,03 € / doc	375.000	450.000	600.000	750.000	900.000
Opex storage 0,05 € /doc	625.000	350.000	350.000	350.000	350.000
ID acq/user at 0,5 € pp	125.000	25.000	50.000	55.000	50.000
Total cost	4.125.000	1.425.000	1.400.000	1.555.000	1.900.000
Turnover 0,1 € / doc	1.250.000	1.500.000	2.000.000	2.500.000	3.000.000
Result	-2.875.000	75.000	600.000	945.000	1.100.000

Table 2: Electronic Document Delivery cost estimates with eID

Even for a small scale hypothetical eDD platform such as presented here, and using the approximate figures as per table 1 and 2 above, the positive impact on the result can be appreciated.

4 The new EU Trust Services regulation

1.1 The regulation

The new draft EU regulation on electronic Trust Services[2] [EUTRUST] was proposed on June 4, 2012. It reflects the EC's objective of "Boosting trust on the Internet". It merges two Digital Agenda *Key Actions*, key action 3 on eSignature Directive revision, and key action 16 on the decision on eIdentification mutual recognition across the EU. It aims to cover mutual recognition and acceptance of e-identification across borders, eSignature interoperability and usability, and the cross-border dimension of ancillary trusted services such as time stamping, signature archiving, e-seals, registered documents delivery, e-documents. The rationale for proposing this new regulation can be found in the Commission's Impact Assessment [EUIA]. Among the arguments developed there are the existing problems of market fragmentation and lack of confidence in electronic services. If this would remain or worsen, and its negative economic impact would become more significant, then investments cannot be optimally monetised, efficient electronic processes cannot replace paper alternatives, and cross border trade might be hampered. This would harm the development of the Digital Single Market, and in extension, of a European Citizenship. Therefore it is required to boost the trust on the Internet. Taking into account the lessons learnt from the preceding Directive on Electronic Signatures, the Commission opted for the Regulation as a mechanism of choice.

1.2 Semantic aspects

One particular element of the eIAS ecosystem that we feel should be addressed more strongly is its semantic aspect. We observe that today there are at least three main "vocabularies" that compete and overlap. There is the regulatory vocabulary, geared towards "legal effect". Then there is the technical vocabulary, geared towards "functionality/technical interoperability". And finally there is the conformity assessment/certification vocabulary, geared towards "trust", and with a recent convergence towards the ISO CASCO vocabulary.

The regulatory vocabulary describes terms such as Qualified Certificate, Advanced, Electronic, and Digital Signature, and the Notified Identity.

The technical vocabulary includes the RSA PKCS standards, S/MIME, IETF CMS, the W3C/IETF XMLDSIG, the ETSI TS 101 733 CAdES, TS 101 903 XAdES, TS 102 778 PAdES standards and the new M460 vocabulary.

The conformity assessment/certification vocabulary defines terms such as "Certified", "Conform", "Accredited", "Included in the TLIST" and related.

However, we think it would be beneficial from many perspectives, including economic and interoperability, to start addressing these semantic aspects.

[2] Originally referred to as eIAS - Identification, Authentication and Signatures

5 Conclusion

Smart governments can help both themselves and the private sector to build an identity foundation that benefits everybody. This is slowly making its way into the (federated) identity and access control applications. Hopefully this will continue to go beyond identity, and will go deeper towards mutual recognition/interoperability of authentication, and authorization/mandates/attributes

The new IAS regulation on Trust Services has a broad ground to cover, hopefully it will be well received by the Member States. At the level of the EU, the new regulation will bring a new impetus to public and private sector usage of electronic services, and will allow us to improve our competitiveness while balancing privacy and socio-economic aspects. This would facilitate systems that rely on trustworthy eIAS solutions for the benefits of everyone.

We estimate there will be a need to cooperate/coexist with the de-facto approaches where companies allow customers to login via Social Network, eg after confirmation that a particular Social Network account maps to a stronger identity. We expect to see interesting attacks on such schemes.

Finally, the semantic aspects of signatures and all related areas should also be addressed, probably better sooner than later ....

References

[EUIA] Commission Staff Working Paper, Impact Assessment Accompanying the proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market {COM(2012) 238}{SWD(2012) 136}

[EUTRUST] The proposal for a "Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market" of 4 June 2012.

[IASPRJ] The EC DG Information Society IAS study: http://www.iasproject.eu/

[MTGOX] The MT. Gox bitcoin exchange, https://mtgox.com

[TOR] The Onion Router network, https://www.torproject.org

Index

Identity, electronic identity, identity fraud, bitcoins.