Visitor report eYou in the EU

Connecting consumers in a digital world

Date
27 juni 2016

Classification
Publiek

Author
Esther Makaay

Page
1/4

Contact
T +31 (0)26 352 5500
support@sidn.nl
www.sidn.nl

Offices
Meander 501
6825 MD Arnhem
The Netherlands

Mailing address
PO Box 5022
6802 EA Arnhem
The Netherlands

Through participation in IDnext, SIDN was involved in this event that was organised as part of the activities surrounding the Dutch EU Presidency. We have produced a short report on the event, because we feel that the topics addressed are of interest to a much wider audience than the policy-developers and decision-makers who attended.

European eIDAS programme

The programme focused on European national eID developments and the progress of the eIDAS project. Representatives of various countries, such as Austria, Belgium, Spain, Estonia and the United Kingdom shared their experiences with implementation of eIDAS.
Member states can voluntarily submit their national eID schemes for recognition in eIDAS. Thirteen member states have announced they will do so before 2018 and ten more are working towards that goal. From September 2018, cross-border recognition of eID becomes mandatory for public administrations offering services that require online authentication.

Digital single market

The overarching theme for the day was the European aspiration for a 'digital single market': no sinecure with twenty-eight member states, each with its own approach and ideas. A digital single market has to be based on trust: in technology and systems, but most of all in the agreements that need to be made (and enforced!). eIDAS is a unique project, providing international legal interoperability.
Considered in a wider perspective, the programme offered a lot of scope for supporting, alternative and disruptive developments from the private sector.

Martijn Kaag from Connectis is a fervent believer that federation is the way to go when creating true global solutions for a single digital market: reusable identities allowing for real-time cross-border secure transactions of any type. Through an overview of the history of federation (from X.500 and MS Passport through Kim Cameron's Seven Laws of Identity to current large-scale implementations such as OpenID, SURFConext and eRecognition), he showed that technology and standards have

matured. The missing link now is now being provides by eIDAS: the first legally binding framework for cross-border identification and authentication.
However, eIDAS has not yet been implemented. In order to boost adoption and support the realisation of this much anticipated development, Connectis is working with the Dutch Ministry of Economic Affairs on the 'eIDAS 2018' project. This project aims to connect seventy municipalities (providing more than a thousand online services) to more than twenty-five online identity providers through eIDAS.

Like the Netherlands, France has yet to adopt a national eID scheme. So, how can digital transactions be performed and electronic signatures applied without a government-issued eID? You take what's available and make it work! With a small team, a limited budget and time constraints, Charles-Henri Menseau did just that. He showed the gathering what had been achieved: a demo of AliceM.
All you need is an NFC-equipped phone and a physical identity document with an RFID chip (such as most European ePassports). AliceM creates an ID on the phone through a secure enrolment process that you can then use for all sorts of electronic transactions.
The demo is so impressive that the French government is now investing in further developments and implementations. Maybe other European countries would be interested as well?

TrustTester

TNO research has shown that one of the hurdles for an eID scheme is data exchange: many data sources are reluctant to provide access to their information or to release attributes to third parties. Strict data protection regulations need to be complied with, and providing access can devalue the data. There are also concerns about validation and attribute content guarantees. As a way around those problems, TNO came up with a concept based on ***not*** exchanging data: TrustTester
TrustTester is a scheme that allows for secure (and auditable) validation of data without disclosing the data to other parties in the scheme (it's a 'zero-knowledge' solution where no party involved learns anything that they don't already know or aren't told by their users). TNO is currently working on a pilot for mortgage offers with the Dutch Tax and Income Authority and a major bank. Users can state their income at the bank and get a validation of their statement without any personal data or income data being exchanged. SIDN is involved in this initiative.

Data overload

Watson Ambassador Nicky Hekster from IBM has a very personal motive for working on innovation in healthcare services: what's more important than people's health? This was easily demonstrated by asking the audience to stand and then to sit down again if anyone close to them had diabetes, cardiovascular disease or cancer. It wasn't long before everyone was back in their seats again.
The healthcare industry faces data overload. As well as the growing amount of academic, clinical and genetic data, people are collecting terabytes of information through wearables and health apps.

Capturing and using all the data enables new insights into populations and individualised care. Watson Health Cloud, based on the Watson Cognitive Technology Platform, makes this possible. Watson understands natural language, reasons and evaluates, learns and adapts, understands and engages an individual and it can process 800 million A4 pages per second. Watson came to the attention of the public by winning the American gameshow Jeopardy (where the answers are given, and the players have to come up with the related question), ahead of the best human players.

The Watson Health Cloud integrates and enriches data and content contributed by ecosystem partners, enabling evidence-based analysis and insights to be gained, while providing for data-stewardship on privacy and security.
Amongst the first examples of services based on this platform are a personal diabetes coach on the smartphone that predicts hypoglycaemic events three hours in advance (state of the art is 0.5 hours) and a platform that helps asthma patients with respirator usage by combining real-time inhaler use and lung function monitoring.

Privacy centre stage

In all these developments, security and privacy stand centre stage. In one of the break-out sessions, a solid basis was provided on those subjects.

Jaap-Henk Hoepman (Director of the Privacy and Identity Lab, etc) presented a practical approach to designing for *not collecting* personal data. Research by Radboud University offers a very elegant model featuring eight privacy design strategies.
Data-oriented strategies:

- Minimisation (collect data on fewer people or fewer attributes per person)
- Separation (store data in separated locations or databases)
- Aggregation (use generic data on groups of individuals)
- Hiding (encrypt data, use access controls)

Process-oriented strategies:

- Inform (data subjects should know when data is processed)
- Control (data subjects should have control over when and how data is processed)
- Demonstrate (verifiable compliance with policies, rules and regulations)
- Enforce (have a privacy policy and enforce it)

The impact of these strategies was practically illustrated through various examples of how alternative approaches would work out for social networks, cloud storage and eID solutions.
Hoepman stressed the importance of honest design: design systems that work as advertised, and don't surprise or harm you (afterwards).

Strong authentication

Jens Bender from BSI asked an intriguing question: *what do we mean when we say 'strong authentication'*?
European and governmental directives and regulations mention trust and security, but the wording is very implicit on how they should be achieved. In technology, we talk about 'strong authentication' and currently this is simply translated into two-factor authentication.
Jens made an analysis of the different types of authentication factor (possession, knowledge and biometrics) and the various aspects that are relevant to those types. For example, whether a factor is used in symmetrical authentication (e.g. where a password is known locally by the user and also stored remotely in a provider's system) and how revocation can be performed.

His recommendations:

- When authentication factors are combined (as in two-factor authentication), the different strengths of each factor should be utilised.
- The two factors should not both be susceptible to the same kind of attack.
- Revocation is a strict requirement, preferably independent of a service provider.
- It should be apparent to the user if the resources used have been compromised.
- And of course we should avoid 'privacy hot spots'.

People-based trust

In her closing keynote speech, Benita Matofska presented another perspective on trust: people-based trust.
Matofska is founder of The People Who Share: a social enterprise that helps people and companies discover and access the Sharing Economy, a system built around the sharing of all kinds of resources. And it's big: the growth of the Sharing Economy is valued at $15 billion in its first seven years, exceeding the combined growth of Facebook, Google and Yahoo ($11 billion). There are over 9000 platforms, apps and projects and it's impacting every sector: private, public, charitable and social. Already 28 per cent of the global adult population is involved and the proportion is predicted to double over the next year.
However, trust is the biggest barrier to sharing. That creates a need for, and is driving the rise of, people-based trust technology. Examples include Veridu (global identity verification based on your digital footprint) and HooYu (a peer-to-peer identity confirmation service). It is important such new technologies are encouraged: in the future, our cities will need to accommodate 70 per cent more people. The need to share resources has never been greater. Therefore we need to transform our cities into smart, sharing cities.
Trust technology enables us to safely connect strangers and enable the sharing of idle assets, transforming our cities and our economy at large.

eYOU in the EU was immediately followed by the conference Trust in the Digital World on 15 and 16 June, allowing for further and more in-depth debate of the subjects described.