New Digital Security Models

Discussion Paper

National IT and Telecom Agency
Ministry of Science
Technology and Innovation

New Digital Security Models
Discussion Paper

Published by:
The National IT and Telecom Agency

The National IT and
Telecom Agency
Holsteinsgade 63
DK-2100 Copenhagen Ø

Tel: 3545 0000
Fax: 3545 0010

ISBN (internet): 978-87-92572-46-2

Printet by:

Impression:
ISBN:

>

New Digital Security Models

Discussion Paper

The National IT and Telecom Agency

August 2011

Contents >

1. Introduction 5

2. Background – the social Internet 7

3. Objectives for a new way of thinking security 10

4. Privacy-by-Design 11

5. Security-by-Design 12

6. Description of the security model 13
   - 6.1 Traditional (federated) security model 13
   - 6.2 Traditional credentials 14
   - 6.3 From identification to identity 15
   - 6.4 Attribute-based credentials 17
   - 6.5 Virtual identities and transaction isolation 22
   - 6.6 Data in the cloud 24

7. Workshop cases 26
   - 7.1 Workshop case A: Reporting income for sperm donors 26
   - 7.2 Workshop case B: Electronic job application for teacher 29

8. Other examples 32

9. Relation to existing (Danish) public sector identity solutions 34
   - 9.1 Interaction with the users 35

10. Perspectives in relation to interoperability and innovation in the long term 37

11. Summary and discussion 39
   - 11.1 Summary 39
   - 11.2 Future or existing technology? 39
   - 11.3 Discussion 40
   - 11.4 Questions on Digitalisér.dk 41

12. Terminology 43

13. References 46

1. Introduction

>

Due to the extensive digitalisation of the public sector, as well as the private sector, the challenge of providing security and protecting privacy in IT-solutions is increasing. The traditional perception of IT-security is to protect systems by surrounding them by massive walls – e.g. perimeter security or the walled-fortress metaphor. This perception is, however, out-dated. It is necessary to integrate security and privacy into the design of the solution (preventive action) as opposed to perceive it as an addition (curative action) to the developed business solution. At the same time there is a need to include interoperability in the model because security requirements change over time and because many, parallel solutions need to work together to foster competition and innovation.

The traditional perception of security is challenged by e.g. cloud computing with data no longer being located within the organisation or in the data centre of a classic out sourcing company – physical control of data is no longer sufficient as a means to provide against misconduct. Through cloud computing, public authorities can benefit enormously in terms of flexibility and cost savings in IT-operations. But before this can be utilized in all aspects, a series of questions on handling of sensitive data in cloud-based solutions must be addressed.

For example, in many areas it is uncertain how existing laws and regulations concerning protection of information privacy are to be interpreted and used in cloud solutions. This is partly because there is no precedence in the area and partly because the existing laws and regulations have been formulated prior to cloud computing and, therefore, do not take the special circumstances within this area into account. Handling of user consent with traditional models is often complicated and not well-suited to express rights or ensure they are respected – in cloud solutions the problem is even worse.

The idea, that data is located in a particular server room in the basement, is challenged when data is moved around in large server centrals throughout the world and when data and applications are shared between many different organisations when using virtualisation (multi tenancy). Security models which to a higher degree can prevent inappropriate use of data are needed. Thus, it is necessary to supplement and develop the existing security models by new ones more capable of facing today’s challenges – both in terms of known types of solutions, but also open to new types of solutions.

This discussion paper provides an initial recommendation for how to create such a further development.

Target audience
This discussion paper is addressing those who are interested in digital security design. However, it is especially addressing decision-makers and IT-responsible in the private business sector and in public authorities.

>

About the discussion paper
The discussion paper is inspired by two workshops held by the Danish National IT- and Telecom Agency (NITA) in the autumn of 2010 with a number of interested parties. Stephan J. Engberg from Priway facilitated the workshops and presented a number of visions and concepts (including Security by Design) and formulated those workshop cases the participants were to work with. For more information reference is made to [PRIW].

The main focus of the debate at the two workshops was how to design digital security models compliant with modern requirements. The discussions produced a variety of interesting thoughts and ideas, which form the basis for this publication.

The discussion paper first presents the background and motivates the need for new security models. Then a suggestion for a new security model is described. The description is concluded by an outline of perspectives and a discussion of challenges. Lastly, the central terminology is defined.

2. Background – the social Internet

>

Throughout the past ten years the Internet has developed from being an information container to an interactive platform which is becoming increasingly valuable when users share, create and communicate with each other. It is often the users' interactions that create value on the Internet. Wikipedia, YouTube and Facebook are examples of social Internet services, which would be worthless if their users did not write articles, upload videos, debate viewpoints and wrote personal anecdotes.

The development from a static Internet towards a more dynamic net of social services is called Web 2.0. This term illustrates that the Internet has become a catalyst for a sharing and participation culture, which in some areas has overtaken the reality existing in traditional digital service and security solutions.

The emergence of the social Internet has intensified the expectations for digital services in general. What demands do the "digital natives" set for public digital services, when they are used to being involved with Facebook, YouTube,

The digital natives
A digital native is a person who is born after the prevalence of the digital technologies and who, therefore, is very confident with digital appliances and services. The digital natives have grown up with mobile phones, computers and Internet, but to them, technology is just something that has to work. They find that technology is most interesting as a social tool.

The user-generated and social Internet is together with the digital natives currently transforming the way people communicate with each other. At the same time this situation creates whole new expectations for the digital solutions presented to us in terms of user-friendliness, simplicity and interaction between several systems. The more interaction and cooperation across systems, the more challenges present themselves in traditional security models based on the notion of guarding ones systems by as massive walls as possible – e.g. perimeter security. Therefore, we must develop security models able to take e.g. interaction between several systems into account.

Taking the digital natives as starting point, one might ask the question whether e.g. the first generation of ESDH-systems[1] in the public administration matches the use of digital services a person born after 1990 normally practices.

[1] ESDH is the Danish abbreviation for Electronic Case- and Document Management

Another consequence of the Internet having become social is that more and more data about the users is created – data such as status updates on Facebook, Google searches, and who, when, and where the last login on the Danish citizen portal Borger.dk took place. We constantly leave digital fingerprints on the Internet. And often, we are not even aware of it. Finally, to an even lesser degree do we realise who use this information and for what purpose. Therefore, there is a massive and increasing challenge in securing the users' privacy in the digital world.

Companies face a series of challenges when wanting to exploit Web 2.0 and cloud computing. The current security models are not always adequate to resolve these challenges. The fact is that a company can no longer alone protect its systems by building the earlier described massive walls. Thus, the perimeter may be opened, when the employees move outside the company's internal systems. For example it is not all companies that have a security policy on smartphones. When employees start checking and sending mails via their smartphones it generates a hole in the company's perimeter. The same is the case when employees start exchanging documents in Google Docs instead of using the company's own systems or if the employees start using various social services in combination with the company's own systems.

Therefore, a strong perimeter is no longer a sufficient basis for an adequate security level. To comply with this development it is necessary to supplement the existing security models with new ones.

This discussion paper will not deal with resolving all of the above mentioned challenges. The new security models sketched in the following sections only present some of the solutions in the form of building blocks and design principles.

For example, privacy in connection with communication channels is not treated – for example it might be possible to profile users based on their IP-addresses if mechanisms preventing this are not employed. The aim of this paper is not to present complete production-ready solutions – but instead to show the readers via illustrative examples that things can be done in new ways. At full-scale implementation there are, naturally, a series of other aspects that need to be attended to – for example user-friendliness, revocation, renewal etc.

How is control over data secured?
There are two general approaches in terms of securing data located in a cloud (outside the individual company or authority's direct physical control):

- **Assurance-based security**: via the contract with the cloud supplier and by independent audits assuring that the supplier observes appropriate organisational and technical security arrangements.
- **Preventive security**: via Security-by-Design the security is implemented in the system from the beginning in a way such that there is far less dependence on the service providers own security (including the cloud supplier).

>

This discussion paper only deals with the preventive security in form of Security-by-Design. NITA is also working on advancing Assurance-based security. However, this will not be treated in this paper.

3. Objectives for a new way of thinking security

>

In this section, the principles and properties that have been used as for a new security paradigm will be described. These requirements are based on the desire for a balanced security with strong privacy protection, flexible processes that can adapt to new demands as well as the possibility of moving data into the cloud. The below listed points comprise the objectives for the security model described in the following sections:

1. There must be security for all parties of a transaction – the owners of the solution as well as its users.
2. Users must have the possibility to control what data is being provided to what solutions and further be able to control whether their data in different solutions can be interconnected.
3. Stored information about the user is not to be ascribed directly to their physical identity unless it is strictly necessary and negotiated. Therefore, virtual identities/pseudonyms rather than identified keys such as social security numbers are to be used.
4. The users' data is not to be linkable even if more external parties work together on extracting more information than the user explicitly has approved.
5. Service providers must be guaranteed that they only receive valid user-information and that the information relates to the user providing it.
6. In those situations requiring it, it must be possible to establish mechanisms which ensure the user's responsibility. An example is the so-called proof of liability that makes it is possible to identify a user who does not follow the playing rules e.g. by attempting to commit fraud. The responsibility mechanisms must not compromise of security in the vast majority of non-fraudulent transactions.
7. A security model must wherever possible be arranged so that the consequences of security breech in one system or for one user are limited to the local context – and, thus, does not scale to other systems or other users. This is especially important in connection with cloud solutions.
8. Generally, all transactions shall be isolated and it shall be secured that the controls are not *just* outside the cloud but "client-side" by the user.
9. The design should when possible follow the notion that many different stakeholders might have different knowledge about a transaction (fine grained) and use different technologies (semantic interoperability) while keeping the control client-side.

4. Privacy-by-Design

>

The above-mentioned objectives and principles for the security model are compliant with the concept of "Privacy-by-Design" (PbD)[2], which e.g. is described by the Canadian Information and Privacy Commissioner Ann Cavoukian in the 1990's.

The general notion of PbD is that business processes, IT systems, and infrastructure from the beginning must be designed to prevent breach of the citizen's privacy – e.g. a pro-active as opposed to re-active approach. It is often seen that privacy is implemented as a kludge of procedures and controls contrived on an already established system, in which privacy has not been a design parameter from the beginning.

Privacy must be attained without users doing anything explicit. The principles must be incorporated in the systems from the beginning – that is before any information is collected.

PbD is user-centric in the sense that the users have control of their data.

Privacy is not to be seen as an opposition to security (for the owner of the solution). On the contrary, the essential point is that the two properties can be attained at the same time. In other words, security has to be established for all parties – i.e. several parties' interests must be carefully balanced against each other.

The following sections will present a security model utilizing attribute-based credentials[3], transaction isolation and purpose-specific keys, which technologically are able to support PbD in the design of IT systems. The architecture e.g. enables:

- That only the necessary information about the user is disclosed.
- That disclosure is done under the user's control.
- That the users may perform transactions under a virtual identity – including not being identified unless strictly necessary.

These possibilities allow system designers to consider what information is being released where, and to what extend it is to be linked to the user's physical identity – in contrary to traditional security models where these building blocks are not always available and where designing systems complying with PbD principles often is difficult.

[2] http://www.privacybydesign.ca

[3] These are also referred to as "Attribute-based credentials" in other contexts.

5. Security-by-Design

>

One of the challenges of PbD has been the focus on risk from one stakeholder's point of view – typically that of the user.

Therefore, this discussion paper takes a step further by introducing a concept we call Security-by-Design (SbD)[4]. This concept illustrates how to take responsibility for the entire transaction with more stakeholders involved. The objective is not anonymity which could optimize privacy – or surveillance, which would do the exact opposite. Instead, a careful balance between the two extremes must be found for each individual system through careful security design using the building blocks and principles we describe.

The objective is to become operationally able to design with security balances that are compliant with the concrete business transaction, and simultaneously designing digital processes that can adapt to the individual user's needs, and at the same time complying with the increasing security requirements of cloud, Internet of Things and the increasing integration of IT systems – altogether circumstances requiring innovation of the perception of security.

The central element in the new perception of security is to move away from identification-based security, by eliminating identification as much as possible, and skip directly to those aspects or properties, that needs validated, without creating security problems caused by the assumption of identification. In other words, we move from an identification paradigm to a validation paradigm. Later in this discussion paper it is shown how to logically segment identity in different logical security aspects, which are better covered without creating vulnerabilities. For example the security objective "Responsibility" does not require the user to be identified to the counterpart. Instead the user can act under a virtual identity and simultaneously demonstrate proof that he can be identified under specific conditions (e.g. using identity escrow techniques).

Another mechanism could be e.g. when a patient provides data for a cloud-system where the doctor – but not the cloud-system – can link the data to a specific patient. In such case the trust relationship between patient and the doctor is equal but both parties are less vulnerable to the cloud-system. Correspondingly, cloud-services can be established without the vulnerabilities provided through accumulation and use of personally identifiable information.

SbD is a further development and operationalisation of PbD. By new cryptographic mechanisms and conscious system design, SbD creates value while simultaneously preventing a variety of security issues.

[4] The concept Security-by-Design as described here is primarily developed by Stephan J. Engberg.

6. Description of the security model

>

In the following, the general principles and building blocks of a new security model are presented which make it possible to realize the above-mentioned objectives. First, the challenges of traditional credentials in connection with the user's security and privacy are described. After that, the principles for attribute-based credentials and transaction isolation are described as a solution to these problems, which simultaneously reaches a high level of security to all parties.

At first sight, the described properties may seem unachievable – e.g. it might seem a paradox that security for all parties can be achieved at the same time. Nonetheless the described properties are realisable by using known technology based on advanced cryptography – and this technology is available on the market.

This paper does not go into details about the underlying cryptography. Instead, the description is kept on a general, application-orientated, and technology-neutral level that allows communication to a broader audience.

6.1 Traditional (federated) security model

A security model, often used when users employ several different services, is the federated security model. In the federated security model, the user must present digital credentials to access Service Providers, while the issuing of credentials is performed by an external, trusted party – i.e. an Identity Provider. When a user for example uses the Danish citizen portal borger.dk, he needs to log in via the Government issued credential NemID[5], while DanID (which is the CA used by the Danish government) issues NemID independent of the citizen portal.

A (digital) credential is a collection of data related to a user, issued by an external party, which a user can present (or partly present) in order to gain access to an IT system. In the physical world credentials are somewhat equivalent to a holder-certificate enabling the holder to act e.g. in terms of a written authority. Within the security terminology these are often called "certificates", "tokens", "assertions" or "tickets".

The federated security model operates with following three types of actors:

- *An issuer* of credentials – e.g. an authority or an application that has stored data about a user – including so-called attribute-services. This is a third party trusted by other service providers in terms of attesting certain attributes about user – e.g. the Danish centralised Civil Registration System attests a users age or sex, the National Board of

[5] The citizen uses his NemID to login on the Single Sign-On solution NemLog-in, which the gives access to borger.dk using the OIOSAML protocol.

Health attests that a user is an authorized doctor, and a college of education attests that a user has passed his or her exam. In traditional models this role is performed by Certificate Authorities (PKI), Identity Providers (SAML) or a Security Token Service (WS-*) that attests the user's identity and/or attributes. But in the new security model the role will to a larger extend be performed by applications or attribute-services that has stored data about the user, but where the credential does *not* identify the user.

- *A service provider* who provides a service/application to the users and gives access to functionalities and data based on presented credentials. This may for instance be a digital self-service application from a public authority such as the Danish Citizen Portal borger.dk. This role is often called "relying party" or "verifier" as validation of the user's presented credentials is involved.
- *The user* receiving credentials from the issuer employs a service provider's services by presenting credentials. This role is also called "prover" because this concerns proving (ownership of) credentials.

The federated security model is illustrated in the figure below:

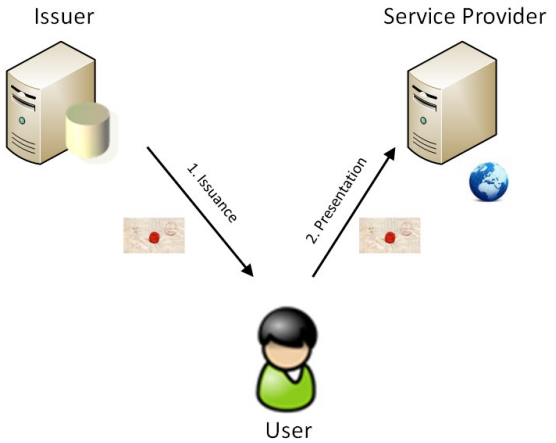

Figure 1: Basic principles for the model

6.2 Traditional credentials

The above-described principles for a federated security model comprising users, issuers of credentials and service providers are very widespread. Below are a few (Danish) examples of traditional credentials:

- DanID acts as issuer of OCES certificates for Danish citizens, employees and companies. certificate., The certificate is a credential that the user presents to service providers (together with a proof of knowledge about the related private key) in order to be authenticated. An OCES person-certificate contains a PID-number (Person ID number), which is directly linked to the person's identifier in Danish centralized Civil Registration System (which is called a CPR number).

- When using the Danish public sector owned identity provider for single sign-on called NemLog-in, a SAML Assertion is issued. A SAML Assertion may be (and often is) attached to the user's identity via a "CPR number-attribute" but may also contain a persistent pseudonym.

Traditional X.509 certificates and SAML Assertions have a number of strong security features, but they do also present a number of potential challenges to the user in the ways they are typically used:

- The explicit connection to the user's physical identity forces the user to become identified to the service provider.
- Certificates contain unique keys allowing the user's actions across services to be coupled. Furthermore, when a certificate is presented, all attributes are revealed – regardless of whether the receiver requires them or not.
- The weakness of SAML Assertions (or rather, the protocols) is, that even when assertions only contain pseudonyms and only are used once (transient pseudonyms), the issuer has knowledge about the coupling between the user's identity and his pseudonyms. Moreover, the issuer will be able to follow what services the user employs as well as when he does so. Furthermore, the issuer (or criminals wanting to steal his signature-key) will be able to issue assertions without the user's involvement and, thereby, impersonate the user to all service providers.
- Security breaches may affect many stakeholders at the same time – particularly breach at the identity providers may escalate.
- When users are identified, and data is easily interconnected without the involvement of the user, pressure for using and combining data in new ways may appear – which is not necessarily approved by the users.

The above-mentioned challenges are traditionally dealt with by setting high security-demands for development and operation of IT systems containing sensitive data (e.g. PII), which prevents misconduct by third parties (e.g. hacker attacks). These high demands may lead to significant cost increases for development, operation and system administration as well as hinder usage of cloud computing. Furthermore, the systems are subject to personal data regulations, which, apart from the strictly security related demands, also imposes limitations on permitted usage of data.

6.3 From identification to identity

As described in the introduction, it is advisable to move from a simple one-dimensional perception of identity (all is packed into a single digital key or credential) to a flexible and nuanced identity model where different security-considerations are dealt with by specific mechanisms.

In the traditional one-dimensional perception of identity and security there is a tendency to reduce identity to identification (how well is the user identified to the system?). Hence, the perception is fundamentally that a given identity can

be looked up in other systems in order to establish authorisations, retrieving and recognising data by one and the same mechanism. Arguably, this approach leads to two essential challenges:

- Security is locked in a fragile model accumulating vulnerabilities (e.g. scalable attacks and data protection issues).
- The IT systems are being locked and "spaghetti hard-coded" in all directions causing increasing instability and makes maintenance and upgrading more expensive.

The traditional one-dimensional perception of identity may comprise the risk of more expensive, yet, poorer solutions and poorer security. This means, furthermore, that the marginal value invested drops.

In the new perception of identity and security, identity is broken down into logically separate components each of which can be made:

- Interoperable (compared and substituted – e.g. upgraded algorithms).
- Concrete (semantically compared to operationally formulated policies or requirements, which thereby becomes supervisory as an alternative to plug-on security).
- Limited (non-invasive and purpose-specific, so that security does not amount to a choice between evils).

Central logical components for an identity are:

- Authentication / recognition – those mechanisms, used for verifying that a user is the same as in an earlier transaction, and which, as a rule, uses beforehand agreed mechanisms controlled by the user (holder certificates, user AD password, keys etc.).
- Responsible / conditional identification – those optional mechanisms used to hold the counterpart responsible should he not comply with agreements or legislation.
- Communication – those communication channels, encryption keys, algorithms etc. requested by the user for the specific transaction.
- Integrity – those security mechanisms used for verifying that a third party has not taken over the user's role.
- Credentials, which may be divided into two types – positive if they are beneficial to the user (such as an acquired academic degree or citizenship) or negative if they are detrimental to the user (such as an exclusion or prison sentence).

The positive credentials are verifiable, positive statements about the user, i.e. will always be a third party's verified truth. These may for example be:

- Identification (an encrypted message for a doctor containing a Digitally Signed message).

>

- Holder certificates (tickets, money, assets).
- Authorisations (proofs of belonging to a group of persons, who are authorised to a perform action – e.g. doctor, administrator or power of procuration).

The negative credentials are verifiable, negative statements about the user, i.e. will always be a third party's verified truth. These may for example be:

- Exclusion.
- Convicted/punished for.
- Defaulter.

A problem concerning negative credentials is that the user may have an interest in not showing them, whereby they are easiest proven as being positive credential (I am *not* excluded, I *still* have access, I am *not* convicted, I *have* credit facility/drawing right, etc.)

The task of breaking down, structuring and standardising the identity elements and simultaneously establishing standards for evaluating, comparing and upgrading security is far from completed – as with all market areas under development, it is a "moving target" where local focus on best value is necessary.

6.4 Attribute-based credentials

A central element in the new security model is the so-called attribute-based credentials[6]. Attribute-based credentials may be thought of as a digital equivalent to recognised, attribute-based credentials in the physical world such as bus tickets, coins, ballots, etc. All these have built-in security mechanisms preventing fraud – but allows the holder not to be identified in the usage situation. Attribute-based credentials have a number of similarities to traditional security credentials, such as X.509 certificates, SAML Assertions or Kerberos tickets:

Similarities:

1. They contain a collection of attributes with information about the holder (user) of the credential. Attributes might for instance describe the holder's birth date, membership of a group (such as "Danish citizen", "authorised doctor", "student at Copenhagen University", etc.).

[6] Note that these are sometimes called "Attribute-based credentials" in other contexts.

2. The credential cannot be forged or changed as it is protected by the issuer's digital signature, which is validated by the recipient – and they are, as traditional credentials, based on cryptography – resistant to replay and phishing attacks because they are bound to a secret key, which only the user possesses.
3. They may be blocked (revoked) and have an expiry date.
4. They may only be used with a private (secret) key, which alone is known to the holder. This provides a strong binding to the holder. The secret key (or parts thereof) may be protected by tamper-resistant smart cards.

The attribute-based credentials separate themselves from traditional credentials by also containing the following features:

1. Normally, they do not contain any information that directly reveals the holder's identity – e.g. they do not contain CPR numbers etc[7]. Instead, the attribute-based credential will be used together with a virtual identity (pseudonym), which is detached from the physical person. A virtual identity, therefore, is a digital substitute (real subset) for the physical person – just as when writers in the physical world publish texts under a pseudonym instead of using their physical identity. A substantial difference is that, in the digital world, it is possible to use many different identities to keep different transactions separate.
2. An attribute-based credential presented at a service provider is not traceable back to the issuing process. Even the issuer of the credential cannot, after the issuing process on the individual credential, tell to whom it has been issued, even though the holder was known at the time when it was issued (see figure 2 below). This corresponds for example to a ballot at an election: the ballot does not reveal who has used it, even though the individual was known when the ballot was issued.
3. A holder may use *different* attribute-based credentials at different service providers without the possibility to determine that it was the same user (see figure 3 below). This prevents e.g. two service providers from interconnecting the information that they have each registered about the holder based on information from attribute-based credentials.
4. An attribute-based credential is technically not sent to the service provider, but is presented via a protocol, where the user proves it to contain certain attributes with certain values.

[7] In such case the user is not to reveal these attributes during the presentation of the credential (cf. "*selective disclosure*" in point 5 below), if he wishes not to be identified.

>

5. The user has in the dialogue with the service provider complete control of what attributes from the credential to reveal (see figure 4 below). For example, he may choose to reveal one attribute about his sex, and yet, keep another attribute with his birth date secret. This is called “selective disclosure”.
6. One can build in mechanisms ensuring that attribute-based credentials are only used a certain number of times - e.g. electronic cash ensuring that a digital note is only used once.
7. It is possible to sign data with the private key belonging to an attribute-based credential, and thereby attain the same properties as by a traditional digital signature (including integrity and non-repudiation).
8. It is possible for a user to send encrypted data to a service provider, and subsequently prove properties about them, without revealing the content (so-called verifiable encryption). The user might for example send his identity encrypted under a third party key, which the service provider does not possess, but at the same time prove to the service provider, that it is in fact the correct identity that has been sent. Thereby, the service provider has insurance of getting the user’s true identity decrypted by the third party (identity escrow) – for example in the event of fraudulence in the transaction. Note, that this is a very simplified example of responsibility-proof, which serves as an illustration of the mechanism.

The above mentioned features show that there are substantial differences between traditional and attribute-based credentials. One might say, that X.509 certificates (traditional credentials) are traceable per design, and obligatorily display all attributes, while attribute-based credentials are non-traceable per design, and provides user control of what attributes to present.

>

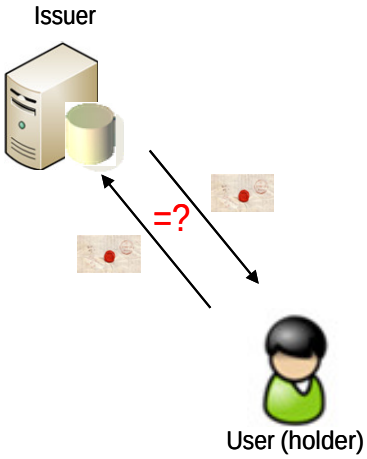

Figure 2: A credential not traceable even to the issuer

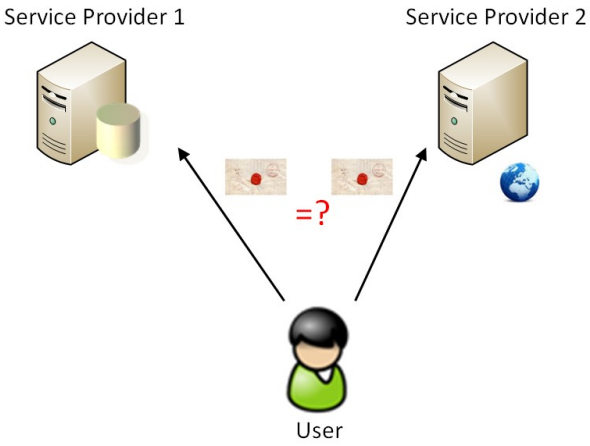

Figure 3: The user cannot be traced across service providers

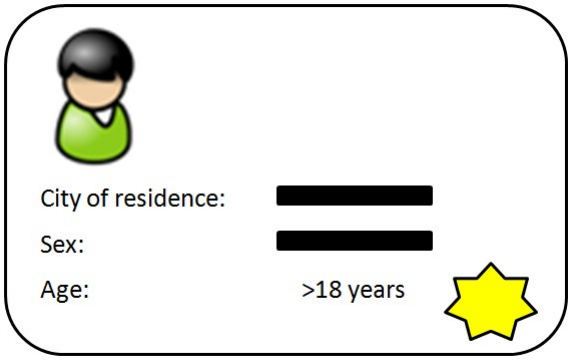

Figure 4: Selective disclosure of attributes from credential

The issuer will normally authenticate the user before issuing an attribute-based credential, but not necessary to identify the user (e.g. establishing CPR number) – and in many situations it is not desirable. For example, an attribute-based credential can be issued on the basis of another attribute-based credential

>

from another issuer or by a pseudonym. For example, the credential may inform that the person with the pseudonym “1234abcd” has a master’s degree in medicine from the University of Copenhagen, and the holder, by using the credential to the receiver, must prove knowledge of a given secret key (proof key/holder-of-key).

Examples of known realisations of attribute-based credentials are the so-called “U-Prove Tokens” from Microsoft [UPCS] and “Identity Mixer Anonymous Attribute-based credentials” from IBM [IDMX2]. Note, that these operate with an Identity-Provider centric model, and that this paper is concerned with a broader perspective.

Note also, that when attribute-based credentials are used, the issuer and service provider do not exchange user-data directly – this is done via the user and is subject to the user’s control. Practically, the user must possess an agent/client[8] facilitating the usage of attribute-based credentials.

[8] The client may be a combination of hardware and software – or e.g. strictly software based. An example of a client is Microsoft Windows CardSpace or a citizen-card.

>

How secure are attribute-based credentials?
The theory behind attribute-based credentials relies on advanced cryptographic techniques, by which (under appropriate assumptions) it is possible to prove mathematically, that a number of alleged properties including unlinkability and untraceability are achieved.

Examples of the underlying cryptographic techniques are so-called “blinded signatures”, “secret sharing” and “zero knowledge protocols”. For details about the mathematical theory, reference is made to [BRA], [UPCS] and [IDMX2] (see also references in chapter 12).

As always there has to be made technical compromises when a mathematical model is employed into the real world – and made usable by ordinary citizens. These compromises may produce weaknesses not existing in the strictly mathematical model. An example can be the traceability of an attribute-based credential: if an issuer chooses to include an expiry date as an attribute in the credential, which has a fine-grained value (e.g. time of issuing by an accuracy of milliseconds), it may be practically possible to correlate credentials to the time of issuance and confine the possible user-identities to a limited set. Another example is when the issuing of an attribute-based credential is time-related to the usage in an application (just-in-time issuance). Here the issuer and the service provider could work together in identifying the users based on the temporal correlation. Both of these examples are characterised by the practical use of attribute-based credential in an inadequate manner leaking information via so-called side-channels.

Such problems are all *practical* implementation problems which have *practical* solutions: Thus faults and deficiencies can be corrected by providing new and better implementations. This is in contrast to those models forming the basis for traditional credentials such as X.509 certificates. Here, all implementations will inherit the earlier mentioned problems related to close coupling with the user’s physical identity, traceability via unique keys re-used across service providers, and possibility for a third party to impersonate the user.

6.5 Virtual identities and transaction isolation

By introducing the new security models a switch from an identification-based paradigm to a validation-oriented paradigm takes place. This means, that instead of all applications identifying the users and coupling local data to the identity (e.g. CPR number), data is coupled to virtual identities (pseudonyms), which are subject to validation (i.e. the user can prove that he represents a pseudonym via a secret key).

The interconnection between virtual identities and data may be done at different levels of granularity:

>

- The user chooses a new virtual identity for each transaction. This provides total isolation of the user's transactions and a service provider is not able to tell whether two transactions belong to the same or to different users.
- The user chooses same virtual identity for more transactions by the same service provider. Thereby, the service provider can maintain user history – e.g. an online film distributor can learn the user's preferences at a case-by-case basis (without knowing the user's real identity).
- A user can punish bad service provider behaviour by closing an old virtual identity and create a new. The service is the same for the user but the service provider loses control and a customer which can have a strong effect.
- No matter how many personally identifiable data that exist in other databases, a user can perform his next transaction without negative consequences of previously submitted data. The systems are forced to adapt to the user.

Using these principles, the user can accumulate completely isolated *islands* of profile-information attached to different virtual identities by different service providers. However, as mentioned before, (should the usage render it necessary) responsibility-mechanisms may be implemented revealing the physical person behind a virtual identity under predefined circumstances (e.g. identity escrow).

>

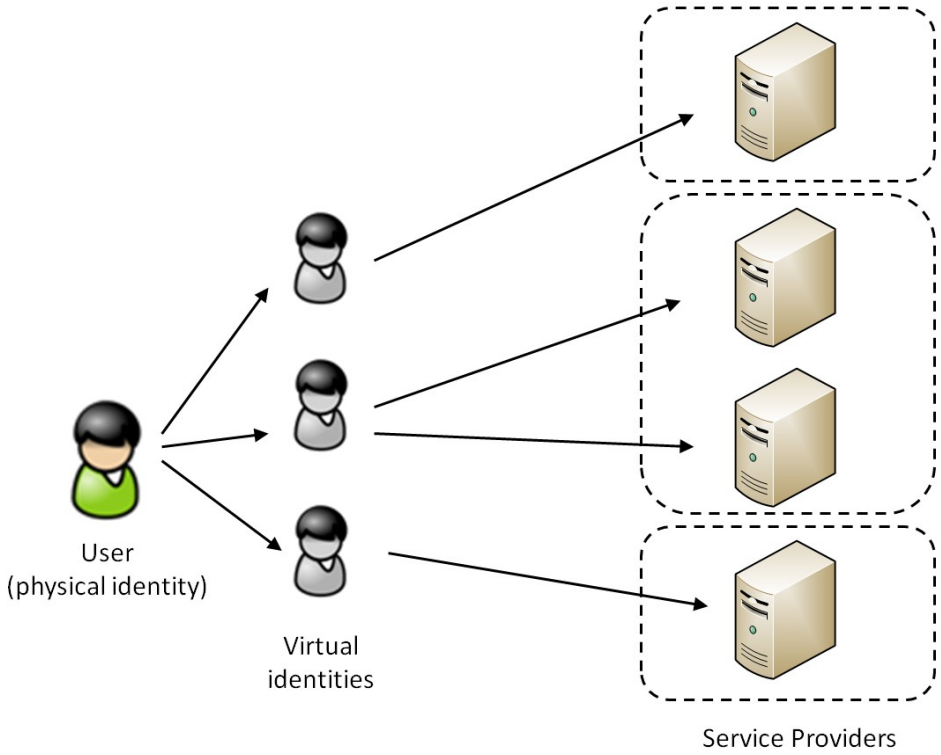

Figure 5: Use of virtual identities for separating user data at the service providers

If a user already has an existing profile with a service provider, he may even choose to attach a virtual identity to it by authenticating traditionally (e.g. by stating the username and password attached to his profile) and in the same session present a new credential. Thereby, a service provider can couple the profile to the virtual identity by the credential and spare the user from having to employ the traditional credential. This technique is often called “account linking” and may be interesting in a transition-phase from traditional models to new models.

6.6 Data in the cloud

It is often stated that traditional security models, based on the paradigm of perimeter-security, are not adequate for moving personal data (or personally identifiable information) to the cloud due to the increased risks and loss of control.

By designing applications in a new way including usage of attribute-based credentials, user data attached to the virtual identities and transaction isolations, the risk barriers can be broken. By a sensible design of the security model the consequences of compromising applications and data are minimal – and do not scale out of control. If the application and its data are compromised, they will not be linkable to physical persons, but only to virtual identities and data will be confined to local transactions and may not be linked to other data restricting the consequences to the local context. Thus, the need to protect data

and the relating costs are reduced dramatically. Note that these advantages are attained without having to trust or be dependent on the cloud supplier.

A central problem which is solved is how to secure backups. If compromise of the system doesn’t scale because all keys and PII are isolated and revokeable, focus can be placed on the recovery in the backup procedures:

- Data in backups are not sensitive because they are locked to context, and there are therefore no issues with deleting or protecting PII in backups as is often the case in traditional systems.
- A user can validate a new key before an identity is resumed from a backup in the event of a system recovery due to successful hacker attack.

A fictitious example with sensitive (but not person identifiable) data in the cloud is described below in workshop case A.

7. Workshop cases

>

In this chapter, two practical cases[9] are described. These cases were examined on workshops held by NITA in 2010. The two cases are fictitious examples illustrating realistic situations where security to all parties and data in cloud can be achieved through employment of the new security model, e.g. by avoiding using personally identifiable data in the cloud.

7.1 Workshop case A: Reporting income for sperm donors

On the first workshop, a case aimed at illustrating how a realistic problem containing obvious requirement for anonymity is solved, yet, maintaining security for all parties involved.

Problem

The sperm bank Cryos pay their donors in cash, who, for obvious reasons, do not want the rest of the world to know about their relation to Cryos. Meanwhile, the Central Danish Tax Administration (SKAT) requires that Cryos reports the issued capitations via their e-income system using the donors' social security numbers (CPR number). SKAT's requirement is made to ensure that income tax is paid properly. Cryos' donors are thereby registered centrally by SKAT, and the reported monthly capitation-size reveals the frequency of the donor's contributions. This causes a conflict with the wish for anonymity of the donors.

The workshop participants were assigned the task to figure out whether they could ensure, that the reporting of data to tax authorities could be done without providing SKAT with knowledge on the source of the income. .

Solution 1

The first (simple) solution proposed was that SKAT establishes an IT system where persons can report taxable income via their CPR number and then receive a non-identifying ticket that can be used once (an attribute-based credential with a virtual identity), wherein the reported income appears. E.g. this could be a web application provided by SKAT where the citizen can login using digital signature (in order to secure that a report is not made on others' CPR numbers). After logging in, the issued virtual "tax-ticket" is downloaded to a local client, from which it may be transferred to the employer later on.

A sperm donor may then, by presenting the virtual tax-ticket to the sperm bank, receive cash corresponding to the value stated in the ticket. The ticket is designed so that the donor may only use it once – otherwise his identity is released and the recipient will be able to observe any repeated use.

[9] The two cases and different solutions were presented by Priway.

>

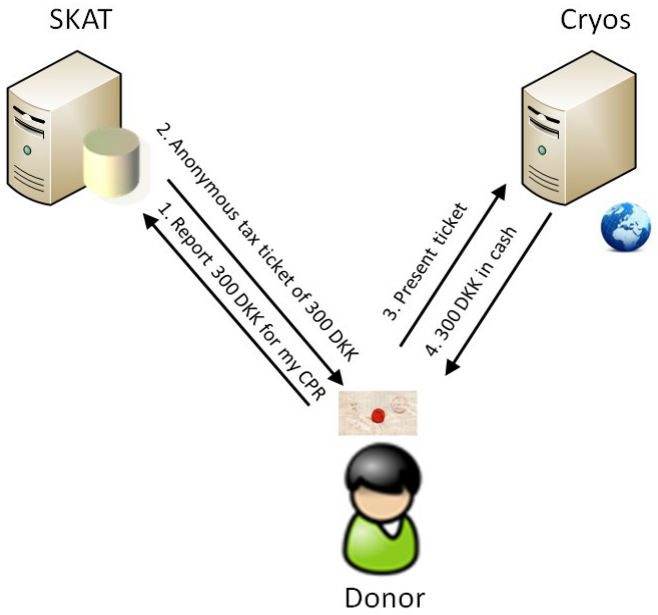

Figure 6: Report of tax data without identification

In case of an audit the sperm bank is able to, by presenting the received tickets (issued by SKAT), document (also to a third party such as an accountant) that tax reports have been made for all issued capitations – without SKAT or others knowing the identity of the sperm donors. Thereby, both security (correct reporting of data to tax authorities) and the donors' privacy to SKAT is achieved.

Solution 2
The above solution solves some of the problems related to keeping the sperm donors' identity secret from SKAT. But the solution also has unsolved challenges:

- SKAT's income report application cannot be hosted the cloud because income-data is linked to CPR numbers in the current model. Therefore, compromising SKAT's application would, in worst-case scenario, result in publication of all Danish citizens' income.
- If a person loses his NemID others may commit identity-theft and report taxes on his CPR number. If a hacker launches an assault on DanID's central servers, he might, in worst-case scenario, be able to make tax reports for the entire population or extract all persons' incomes. Thereby, a security breach in NemID or DanID escalates onto SKAT.

In order to meet these challenges, the first, simple solution design may be changed by SKAT, so that reporting tax is not linked to CPR numbers but to virtual identities instead. Each citizen, thereby, has a "virtual tax-account", to

which he may report tax-income at SKAT if he proves ownership of a secret key attached to the virtual identity and only possessed by the citizen. SKAT will then potentially be able to move their tax report application and data onto the cloud because the data no longer is personally identifiable. The issuing of attribute-based credentials, after reporting of data to tax authorities, is unchanged from the simple solution.

Furthermore, it should be ensured that citizens can only create one virtual tax-account, e.g. in an attempt to circumvent progressive taxation, and due to other reasons, SKAT may need to know the physical identity behind each virtual identity. By creating a new application (which is not run from the cloud), used by each citizen to create a virtual tax-account, this problem can be solved. When creating the tax account, the citizen could use his digital signature in order to identify himself by social security number, and initially connect to the virtual identity and secret key – after that, the social security number is no longer used. SKAT can store the relation between social security number and virtual tax-account in a local database[10], which is not in the cloud. After that, all authentication of the citizen, related to providing data to tax authorities in the cloud, will be done via the citizen's secret key and not his digital signature[11].

In that way the following properties are ensured:

- SKAT makes sure that there is only one tax-account for each social security number.
- Nobody, apart from the citizen, will be able to make reports in the name of the citizen (the reports require signing of the secret key only known to the citizen). Not even DanID (CA) or a hacker, having compromised DanID, will be able to do so – they will only be able to create a new, empty, virtual tax-account if the citizen does not already have one.
- If the database in the cloud containing tax reports is compromised, the hacker will not be able to relate the virtual identities to physical persons. Thereby, data is not very attractive for an attack.
- SKAT can issue a digital proof (an attribute-based credential) for the citizen, proving that he has created a tax-account. Subsequently, this can be used to prove to other service providers that he is "costumer" of SKAT which can in turn be used to grant access to other services.

[10] This database becomes single point of failure. In turn it is not used on a daily basis but only when creating new tax-payers in the system.

[11] Such a model would for electronic patient journals isolate knowledge on the link between a social security number and the virtual identity at the user's own bdoctor.

>

The above-described model requires that a citizen is not able to transfer his credentials or virtual identities/secret keys to others – e.g. parents trying to report income on their children's virtual tax-accounts to avoid higher rate tax. There are a number of different methods to prevent this, which will not be elaborated here. In the Cryos-case, a solution would be to bind the virtual tax-tickets to a tamper-resistant smart card with biometric authentication, which belongs to the donor. Then the donor could, by physical presence, prove that he possesses the card and subsequently transfer the tax-ticket to Cryos. Another technique to prevent transfer is, that the issuer can embed secrets (e.g. electronic cash, passwords, credit card numbers or personal information), which are sensitive to the user, into the private key. As the secrets have to be presented, in order to use the private key, the user cannot transfer the token to another user without also having to transfer the secret.

7.2 Workshop case B: Electronic job application for teacher

Problem
The other workshop case dealt with how security can be designed in a situation with electronic applications for a teacher job – e.g. through an electronic job-portal in the cloud. The focus of the case was on the early stage of the application process, where the primary sorting of the applicants is performed using a number of objective criteria while keeping the applicant's physical identity secret.

The applicants must e.g. be able to present following documentation:

- Documentation for education (diploma from a recognised educational institution).
- Proof of supplementary training (course diploma).
- Proof of not having been sentenced for paedophilia (part of criminal record).
- Number of years of experience as teacher.
- References or recommendations from earlier hiring.
- Current salary.

The wish for protecting the applicants' identity serves several purposes, including:

- It protects the applicants from discrimination in terms of race, age, sex, etc.
- Nepotism is avoided.
- It ensures those applicants, employed elsewhere, that their current employer or colleagues will not know that they are applying for a new position.

>

Solution
At the workshop various solution models were discussed. However, in this paper, only one is presented. This suggestion is based on the idea that a number of institutions establish IT systems, which can issue authoritative documents (e.g. diplomas) as attribute-based credentials, containing only a virtual identity. I.e. teacher colleges may issue electronic diplomas, the criminal register may issue electronic criminal records, the providers of training programmes may issue digital course diplomas, and employers may issue electronic proof of hiring, acquired salary or recommendations. Each of these issued document-types could be based on the user being authenticated e.g. by a digital signature to ensure that proofs were only issued for the right person – or, more ideally, they could be based on having virtual identities attached to secret keys, which then could be used for authentication.

A potential applicant would be able to create an application in a job-portal, without being identified, and then upload the electronic credentials documenting the required information. The documents are digitally signed by the issuer's certificate, and thereby, the applicant will be able to prove that the documents have been issued by recognized institutions. At the same time, the documents, when they are issued (or via a selective disclosure of attributes), can be limited to their purpose restricting the revealed information to what is necessary. An example is criminal records where there is no need to inform about speeding tickets etc. as the receiver only requires information about whether the person has been sentenced for paedophilia.

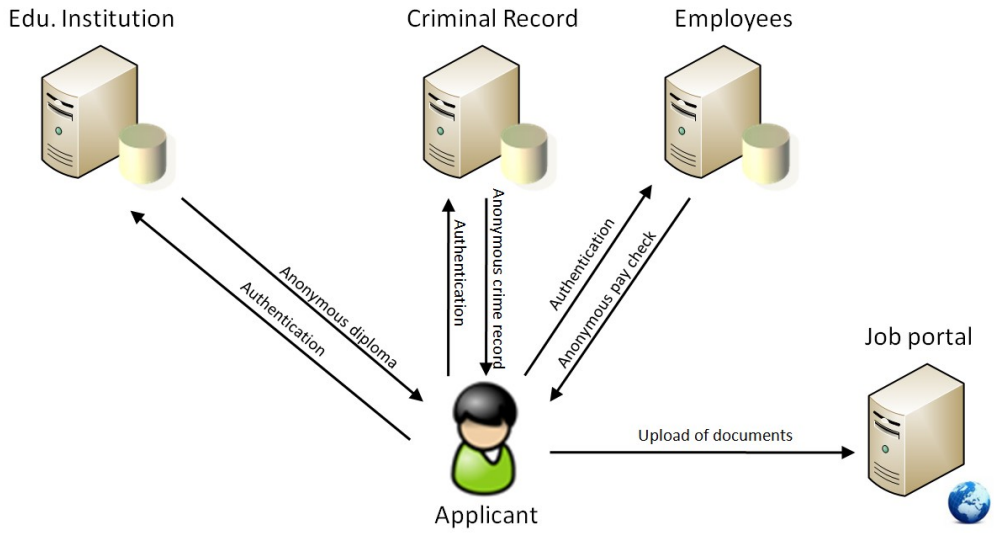

Figure 7: Non-identifying application

Another perspective in the case is that the portal, after evaluation of the applicant, may issue a proof (in form of an attribute-based credential) to the

applicant, that he has applied for a job and indicate his status in the application process. By such a proof, the applicant can document to others that he is applying for jobs and that these are relevant (e.g. that he passes the first primary sorting) – which e.g. could serve as documentation in relation to unemployment benefit.

At the workshop it was discussed that not all documents are suited for being non-identifying. For example, a job-reference describing that the person has been employed in a given period performing a given function, might narrow down the number of possible candidates to such an extent that a person's identity may be revealed. Another example is that by a non-identifying reference, it might be difficult to contact an earlier employer to arrange a conversation about the person's qualifications. Finally, references may include "unstructured prose" making it impossible to (mechanically) remove identifying information.

These challenges were not considered to hinder the case from being solved through above-described principles. A practical solution might be to run the application process in several steps. The first steps involve the introductory screening of the applicants, where formal requirements are met without identification of the applicant (and in the cloud). The later steps involve (partial) identification of the applicants in relation to evaluation of references and personal conversations with the candidates. The system should, in this context, be designed so that the opening of identifying documents later in the process does not happen in the cloud solution – e.g. the documents are encrypted under a secret key only accessible to members of the review panel.

8. Other examples

>

In this section, some other examples of how the security model can be employed are described in form of a number of cases. The descriptions are relatively short as the examples are based on the principles introduced in the two previous cases.

Case: Feedback for teachers after completing a course

Problem
A university wants to provide students with the opportunity of giving feedback on their courses and teachers via their student portal. This has to happen without the students being identified to ensure the students that their feedback will not result in retaliatory measures. At the same time, it has to be ensured that only students having followed a course will be able to give feedback and that the students only give feedback once.

Solution
The university creates two systems. In one of the systems the students receive an attribute-based credential with a virtual identity, and in the other system they use the attribute-based credential and the virtual identity to give feedback. The first system authenticates the student (e.g. based on a digital signature) and issues a non-identifying single-use ticket with an attribute informing what course the student has participated in. Simultaneously, it is registered that the student has received such a ticket preventing the student from receiving more tickets (for that particular course). In the other system, where feedback is given, the ticket is validated. Here, a check is performed via the course-attribute, ensuring that the ticket is valid and has not been used before. It is, however, not possible to derive from the credentials who gives the feedback – even if the two systems were operating together in collusion. In practical implementations one would additionally have to address timing attacks, where issuance of tokens and submitting of feedback are linked because of their temporal correlation.

Case: Electronic auctions / tender
Another variation of the two previous cases is electronic auctions or tenders. The first part consists of establishing a registration system where participants are identified and approved (pre-qualified) to make bids. Hereafter, they will get an attribute-based credential to use in the system receiving the bids. It is even possible to sign the stated bid by a private key attached to the credential in order to achieve non-repudiation.

Case: Access to scientific articles

Problem
A university subscribes to scientific journals, which can be read online. The wish is to give access to registered students and teachers, but the issuer of the publication is not to know who reads what articles – only that the reading is done legally.

>

Solution
The university establishes a system, which can issue an attribute-based credential to students and teachers including an attribute revealing access to read publications from a certain issuer. The issuer is then able to validate the attribute-based credential and thereby give access to the articles – without being able to track who reads what. At the same time, the issuer may register how many different users from a given university are accessing the issuer's articles, in order to make a comparison to the university's subscription, where the price could be dependent on the number of users.

Reference is made to a case concerning invitation of loan offers in the following chapter.

Case: A dating service

Problem
A dating service[12] requires knowledge about the users' age and sex, in order to prevent the users from providing false information in their profiles. E.g. persons under 16 years of age or persons who create profiles of false age and sex for fun are to be banned. At the same time the users' identities are not to be registered because this would discourage many persons from using the service as their actions can be traced to their identity.

Solution
The dating service is expanded, so that it allows login using attribute-based credentials containing the two attributes of age and sex. For issuing the credentials, an existing service, or a service developed by the dating service, which e.g. based on login with NemID, may derive the value of the attributes and issue a credential with this information. Thereby, the users can provide the dating service as little information as possible and at the same time have insurance that their activities are not traced to any other digital online activities.

A more advanced expansion of the dating service could be exclusion of users if they behave against the service's ethical guidelines – still without knowing the users. This could be achieved if the users prove that they are not on the list of excluded users – still without revealing their identity – and in such a way that the users cannot just switch virtual identity if they are excluded.

[12] The website www.love.dk e.g. allows the users to login via NemID.

9. Relation to existing (Danish) public sector identity solutions >

The described security model may be thought of as a natural further development of existing standards, architectures and solutions within the Danish public sector for user identity, single sign-on and access management such as the NemID, the OIOSAML and the OIODWS profiles as well as the NemLogin and KFOBS solutions. Therefore, the notion is that of evolution instead of a revolution.

As described earlier, the model is fundamentally a federated model where users are given access to services by presenting credentials (security tokens) issued by a third party. The primary difference is that of a new kind of credential/security token, which allows the user not to be identified. For example, existing Security Token Services[13] can further developed so that they become able to issue attribute-based credentials.

Another resemblance is that the user often has to be authenticated before a credential can be issued. In such case, the digital signature/NemID may be used in the same way as the NemLogin solution is currently being used. The interaction between the existing user management solutions and new elements with attribute-based credential is illustrated in the figure below.

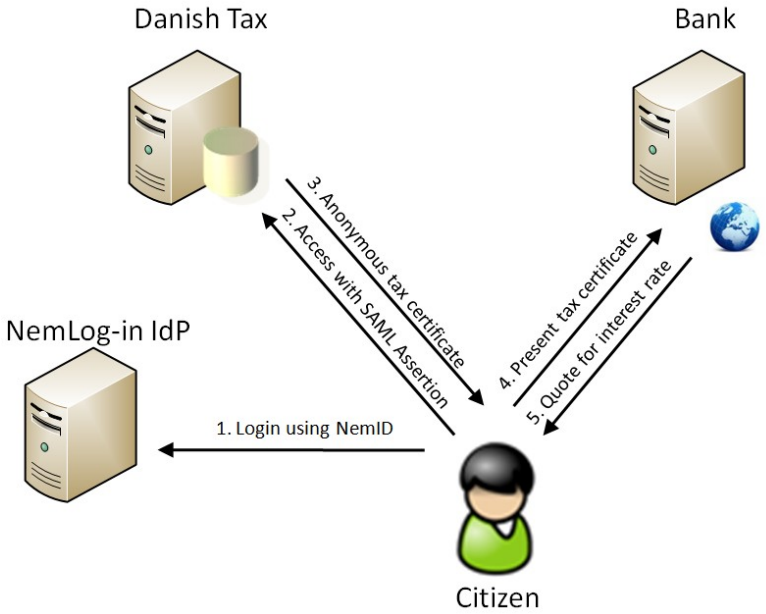

Figure 8: Interaction with existing solutions

[13] The KFOBS solution (KFOBS is the Danish abbreviation of consolidated, common public user management solution) establishes a Security Token according to the OIOWDS profiles for identity based web services, and is prepared for the support of attribute-based credentials.

The figure illustrates a user, who wants a loan offer from a (unfamiliar) bank, but does not wish to become identified, before having reviewed the offer and decided to accept it. This case could be solved if the user logs in on the existing NemLog-in solution using his NemID and then gains access to SKAT's solutions, which can issue an attribute-based credential (attached to a virtual identity) with the user's income information as well as his current debt to public institutions. The user will then be able to present the credential to the bank as basis for calculating the interest rate on the loan. By verifying SKAT's signature on the credential, the bank will be able to verify the information but not transfer it to the user's identity. Thereby the existing user management solutions have been combined with the new model. The case may also be implemented without attribute-based credentials, but hardly comprising the same security for the user (pseudonymity) or the bank (authentic data about tax and income for the actual user).

Also, there are a number of differences in relation to existing technologies and solutions, including that service providers and issuers will never communicate directly to each other. The SAML protocols are, therefore, not compatible with the model (a SAML IdP implies knowledge of the service provider's identity) where WS-Trust, as mentioned, is applicable. Finally, the user-centric model implies existance of dedicated clients for the users supporting this form of interaction whereas current user management solutions only require a standard web browser.

Public authorities may deal with this by exposing user data in both traditional ways and via services, which may issue attribute-based credentials. This provides the users with the opportunity of choosing the new privacy-friendly forms as clients bceome available and the demand increases. Modern applications may be designed and developed to be independent on how data about the user flows to the system – so-called "claims aware" applications, by delegating these concerns to infrastructure components that can evolve over time. Thereby the applications are prepared for the new types of credentials and do not require re-programming.

9.1 Interaction with the users

The proposed security model makes it possible to design applications giving the users control over their data. This requires, however, that the users actively participate and that the user-interaction is effective, intelligible, and user-friendly to the group of intended users. Imaginably, in a number of situations a part of the users do not want – or have enough knowledge – to participate actively in orchestration of credentials and identities. In such case it is relevant to design the application so it allows the user to choose. Some users may, fundamentally, trust public and private companies (e.g. banks) to treat their data securely, and are, therefore, not interested in being given the choice.

The new security models do not necessarily force the users to do anything different from the way they currently use it solutions. The essence is that the new security paradigms, in contrast to the traditional security models, provide

>

the user with liberty of choice in relation to when to become actively involved in the orchestration of identities and credentials.

10. Perspectives in relation to interoperability and innovation in the long term >

In the description of the new security models this paper's focus point has been how security in a transaction can be achieved simultaneously for all parties. Additionally, the described security model may enable cloud computing. However, there are a number of additional desirable properties in a new security model. These properties have also been dealt with on the two workshops, which have been the foundation for this discussion paper. Here, we will draw special attention to the aspects of *interoperability* and the opportunity for *need-driven innovation*.

Interoperability
Generally, interoperability means that a security model should be open to future introduction of new elements and the ability for these to interact and co-exist with existing solutions. This might for example be introduction of new types of credentials, communication channels, clients etc. Support of interoperability, thereby, has a direct correlation to a company's opportunity to be innovative.

A concrete example might be that a self service solution should not be strictly tied together with Danish credentials. Incorporated into the system design should be the opportunity for citizens of other EU countries to use their local credentials access the self service solution as long as these credentials meet the application's security requirements and the necessary information is present. This form of interoperability is more ambitious than the traditional understanding of the concept where software suppliers may implement a technical standard (e.g. GSM) so that their products are interoperable but contain large parts of "hard coding" in relation to the standard – so-called "plug" compatibility.

A more ambitious form of interoperability may be model-driven or at the semantic level by use of ontologies where an application e.g. expresses its needs in form of an explicit policy enabling other software at "run-time" to read the policy and dynamically try to comply with it. This is simply the well-known architectural principles "loose coupling" and "late binding" taken to their widest extent. Practically this means that open systems should be listening and telling what they need instead of dictating it.

Need-driven innovation
By need-driven innovation, the users dynamically control flow of data and interaction between systems through their needs and requirements. This requires that systems are flexible and interoperable in order to be able to adjust to the current situation. If the systems, on the contrary, are rigid and lock the users without choice, there is no possibility of achieving the wanted dynamics and innovation.

The aim of the need-driven innovation is to achieve synergies, reuse of solution elements, facilitate competition and improve productivity and quality in the solutions. Furthermore, future costs are reduced because further development

>

of the system is facilitated, and thus, removing the need for re-building new solutions.

From an economical perspective, there is sound reason for designing systems, which are to a greater extend able to take interoperability and need-driven innovation into account.

11. Summary and discussion

>

11.1 Summary

Due to the changing nature of the Internet and the fact that the perimeter as security concept is vastly challenged it is necessary to evolve traditional security models in order to meet future requirements.

This paper has described how security models can meet these challenges by adopting the following principles:

- Provide security for all parties in a transaction (including users).
- De-couple user data from users' physical identity.
- Utilize attribute-based credentials and transaction isolation.
- Move from an identification-oriented paradigm towards a validation-orientated paradigm.

If these principles are built into the design of applications it will in many cases be possible to use cloud computing without significant risks[14], even though sensitive data are involved. If the application and its data are compromised they will not be linkable to physical persons but only virtual identities. Data will only have meaning for local transactions and can, therefore, not be connected to other data. Thereby the consequences of compromising data are confined to the local context. It is worth noticing that these advantages are attained without dependence on the cloud supplier.

Subsequently a number of practical cases have been described. Altogether they illustrate how the above-mentioned principles can be used when designing security models specific applications.

Finally, it has been described how the new security models can be seen as further development of existing standards, architectures and solutions within the Danish public sector.

11.2 Future or existing technology?

Even though the models described in this paper might seem advanced at first, the basic mechanisms are already implemented in commercial products and the first pilot projects have already been successfully run.

As an example, the company Fraunhofer FOKUS, that created the German eID-system, has run a pilot where German citizens via attribute-based credentials[15] are able to participate in opinion polls anonymously but at the same time via the German eID card prove their eligibility as voters (adult as

[14] In this context, loss of confidentiality is the primary concern and not loss of availability or integrity.

[15] UProve technology.

well as resident the city to which to poll is relevant). For details about the particular pilot project reference is made to [EPAR] and the website: http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/eid.aspx

New applications today should be organised flexibly in order to support future credentials without having to rewrite them from scratch. Instead the management of identity and credentials should be confined to a separate identity layer or component, which may be expanded according to new requirements – without affecting the functionality of the application.

11.3 Discussion

There are a number of questions associated with the new security model described in this paper. We will touch upon some of them in this section, where we also invite to further debate on the Digitaliser.dk web site[16].

New solutions possible

The new security models make it possible to create new solutions which were not possible with a traditional approach – especially solutions where identification of users is not desirable. For example, the models provides opportunity for receiving anonymous loan offers from financial institutions – that is, without *providing* the financial institute more information about oneself than needed in relation to the loan application in question. This model enables a system design, where only information about relevant economic conditions will be provided to the loan application.

The technology may also be used for a number of other new solutions, which we have not yet thought of. We invite ideas to such solutions to be submitted and discussed on Digitalisér.dk.

Democracy and social responsibility

Protection of privacy is too often being attempted as an add-on to a solution after it has been built. By following the principles of Privacy-by-Design and Security-by-Design these aspects shall be part of the system design from the beginning. The question is why, in a democratic society, the possibility of protection of privacy is sometimes not considered even by government institutions?

The future development is relevant to bear in mind if mechanisms for dealing with privacy protection are not used. This problem is significant taking the

[16] www.digitaliser.dk is a social network and tool for development, knowledge sharing and a forum for the digitisation of Denmark. The literal translation is Digitise.dk. Digitaliser.dk is both a formal central repository of information on data interchange standards and a big open digital playground - a creative space for everyone involved in digitising the public sector.

growing amount of data on the Internet as well as the increasing technological opportunities for automatically collecting data into account.

It is also relevant to consider what kind of data private companies can collect from our activities on the Internet. What are the incentives for a private company to increase privacy protection? One argument might be that it is cheaper to protect few or non-sensitive data than to protect many and sensitive data. On the other hand, business models of a number of companies are built upon collecting as much information about their users as possible, and then combine it in different ways. The debate about privacy rights has increased in recent years and Internet users have started to set higher demands and request solutions that can meet these. Imaginably, companies will to a larger degree secure privacy to demonstrate social responsibility – or see it as a competitive parameter differentiating them from competitors. Finally, there may be a number of applications, which users simply will refuse if they do not trust their privacy to be respected.

The work on the new security models seemingly includes more perspectives and potentials stretching beyond the security area and which are relevant to discuss further.

11.4 Questions on Digitalisér.dk

The below listed questions will be discussed on Digitalisér.dk, where there will also be opportunity for discussing other positions:

1. Are the new security models in fact better?

- Is there a need for further developing digital security models in the direction sketched in this paper?
- Are the security models described in this paper secure and flexible enough?

2. How do we get to the new model – what challenges are there?

- What practical challenges are there by initiating new security models?
- What attitude needs to be changed to commence the new security models?

3. Where is it possible to implement the new model easily?

- Can any of the principles presented in this paper be implemented on a smaller scale?
- In what areas will it be relevant to use the new security models?
- How are applications designed so that they are prepared for the new security models?

4. What do the new security models require from the users?

- The new security models may in some cases require that the users (or rather the users' clients) administer a number of keys and credentials

>

for different services. Are the requirements for the users' competencies to high to interact with the application as well as making choices? The new models also require that the users actively decide on what information the user wants to provide the different services with. Is this something the average user will find interesting?

5. What solutions do you imagine?

We hope that you will contribute your thoughts by following this link (digitliser.dk is primarily a Danish website, but you can contribute in English:

http://digitaliser.dk/resource/896495

12. Terminology

>

Privacy
Privacy concerns the right for a private sphere in connection to ones actions both public and private, in physical rooms, on the telephone and on the Internet. Privacy may be thought of as protection against different forms of risk – e.g. the risk of loss of control over personal information. For more definitions reference is made for [OVG].

In the held workshops the term privacy was perceived as security from a single person's view (the user/citizen) – see [PRIW]. A decisive target of the new security models is to attain a balance where security for more or all parties (so-called *multiparty security*).

Issuer (of credentials)
An issuer of credentials is a trusted third party who is trusted by others in terms of certifying certain attributes about users – e.g. a person's age or that a person is an authorized doctor.

Service provider
An organisation providing a digital service or application to users and provides access to functions and data based on presented credentials. This might for example be a digital self-service solution by a public authority. This role is often called "relying party" or "verifier" due to the inclusion of validation of the user's presented credentials.

Identity
Identity is a technical presentation of a legal person in a given context.

Virtual identity (pseudonym)
A virtual identity is a digital substitute of the physical person – analogically to when authors in the physical world publish writings under a pseudonym. Virtual identities are often used for making a balance between anonymity and identification – the user is not identified to the service providers (potential loss of user's security) nor is the user completely anonymous (potential loss of responsibility or the service provider's security). Both (total identification and total anonymity) comprise the term but in most situations none of them are desirable.

Identification
Identification is a process where a person's physical identity is established – e.g. via a CPR number.

>

Authentication
Authentication is a process whereby a user is recognized. Certain authentication mechanisms identify the user directly (e.g. an OCES digital signature) while others only produce a technical key (virtual identity). Authentication often occurs at presentation of a credential[17] (see below).

Credential
Credentials are collections of data related to a user. It is typically issued by a trusted third party and presented by a user (or parts of) with the goal of gaining access to an IT system. Examples of traditional credentials are X.509 certificates, SAML Assertions and user-id + password.

Attributed-based credential
An attributed-based credential is a credential that does not identify the user but instead comprises a virtual identity (pseudonym). For this reason they are sometimes called Anonymous Credentials. It is not traceable to the issuing process and the user has direct control of what attributes from the credential are released.

Transaction isolation
Transaction isolation is the principle that a user's data is isolated to a specific context. Thereby they cannot be linked to other data or actions of the same user. The isolation may be done between different service providers or within the same service provider. As an example of the latter, the transaction isolation can be used on a job application portal (reference is made to the description earlier in this document). Here the portal cannot deduce that the same user applies for more jobs, as the user's applications are isolated transactions. Transaction isolation is e.g. achieved as the user uses different virtual identities for different transactions and uses attribute-based credentials, which do not contain any correlation handles enabling linkage. Note that even though the service providers cannot link isolated transactions the user may prove (e.g. using private keys) that a set of isolated transactions all derive from him.

(SAML) Assertion
A SAML assertion is a traditional credential in XML format. A SAML assertion is typically digitally signed by the issuer and contains attributes about the user (e.g. CPR numbers or persistent pseudonyms) and authentication events (e.g. that the user logged on by digital signature at 12:56 o'clock). For details about OIOSAML reference is made to

[17] Practically, authentication is most often done by proving knowledge of a secret (a private key), which is linked to the credential (e.g. via a public key).

>

http://digitaliser.dk/resource/524480 and for details about the SAML standard reference is made to http://docs.oasis-open.org/security/saml

13. References

>

[BRA] ”Rethinking Public Key Infrastructures and Digital Certificates – Building in Privacy”, Stefan A. Brands, MIT Press.

[UPCS] “U-Prove Cryptographic Specification V1.0”, Stefan Brands og Christian Paquin, Microsoft Corporation.

[IDMX1] “A Quick Introduction to Anonymous Credentials ”, Gregory Neven, IBM Zürich Research Laboratory.

[IDMX2] “Specification of the Identity Mixer Cryptographic Library”, Jan Camenish, IBM Zürich Research Laboratory.

[UPROV1] “U-Prove Technology Overview”, Stefan Brands, Microsoft Corporation.

[UPROV2] “U-Prove CTP White Paper”, Christian Paquin og Greg Thompson, Microsoft Corporation.

[OVG] ”De overvågede”, DI & Forbrugerrådet.

[EPAR] “eParticipation Scenario Reference Guide”, Microsoft Corporation.

[PRIW1] “Without PETs, democracy and markets won’t work”, Stephan J. Engberg, Priway.

http://ec.europa.eu/justice/news/events/workshop_pets_2009/presentations/ENGBERG_Stephan.pdf

[PRIW2] “A World without PETs”, Stephan Engberg, Priway.
http://danskprivacynet.files.wordpress.com/2008/08/a20world20without20pets20v2.pdf

<