# Privacy Protection Goals and Their Implications for eID Systems

Harald Zwingelberg, Marit Hansen

# Privacy Protection Goals and Their Implications for eID Systems

Harald Zwingelberg[1], Marit Hansen[1]

[1] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Holstenstr. 98, 24103 Kiel, Germany
{hzwingelberg, marit.hansen}@datenschutzzentrum.de

**Abstract.**[1] Protection goals such as confidentiality, integrity and availability have proved to be successful in evaluating information security risks and choosing appropriate safeguards. The recently developed privacy-specific protection goals unlinkability, transparency and intervenability complement these classic goals and thereby provide cornerstones to define requirements concerning information security as well as privacy and to assess solutions. This text focuses on the application of the three new protection goals to eID systems such as government-issued electronic identity cards in different settings.

**Keywords:** Privacy Protection Goals, Electronic Identity, eID Systems, Identities Management.

## 1 Introduction

Currently many nations throughout the globe are working on electronic identity (eID) systems. An important component in an eID system is the eID card or another hardware or software token that usually is assigned to one citizen. These government-issued eID tokens are meant to replace a national identity card or to provide a means for online and offline identification in one or more specific sectors, e.g., the health sector, the social security sector or the employment sector.

eID systems have a huge influence on the extent of the citizen's possibility to manage their privacy and identities [1]: An eID token often may function as an "official" identification document towards public entities as it is issued by the government on the basis of a law and well-defined processes. Alternatively, eIDs may be issued by private entities, which are considered trustworthy like banks (as this is the case in Sweden [2]). eID and traditional ID systems accompany the citizens throughout their full lifetime, and the usage of these systems is often not based on the individual's consent, but may well be mandatory for every citizen – be it on basis of a legal requirement or factual necessity. Many use cases for eIDs are not restricted to

[1] The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257782 for the project Attribute-based Credentials for Trust (ABC4Trust) as part of the "ICT Trust and Security Research" theme.

the citizen-to-government relationship. eIDs are likely to be used in other contexts as well, e.g., in a customer-to-business setting, possibly in peer-to-peer scenarios or in (other) identity management systems. All these properties show the need for a privacy-respecting design of eID systems right from the planning phase to provide comprehensive support to individuals. In this text we assess relevant parts of eID concepts and implementations by specifically applying the protection goals "unlinkability", "transparency" and "intervenability" that have recently been proposed on the national [3][4][5] and international level ([6], p. 482 et seq.) to strengthen the privacy perspective by supplementing the classic information security protection goals "confidentiality", "integrity" and "availability".

The text is organised as follows: The protection goals and their usage are explained in Section 2. Section 3 deals with specific examples from the European eID landscape that illustrate how privacy protection goals aid the privacy assessment and could have improved the design. In Section 4, we deploy the privacy protection goals to several use cases throughout the lifecycle of an eID system. The results are summarised in Section 5.

## 2 Protection Goals for Information Security and Privacy

Since some decades, protection goals have been playing an important role in assessing information security regarding concepts or implementations of data processing systems and supporting the choice of the appropriate technical or organisational safeguards for each use case. The classic triad of confidentiality, integrity and availability – already used in the early 1980s – has remained unchanged in decades of debates whether these protection goals should be changed or supplemented [7]: **Confidentiality** means that an unauthorised access to information or systems is prevented. **Integrity** means that information or systems are protected from unauthorised or improper modifications. **Availability** means that information or systems are available when needed.

Although in some areas an extended set of information security protection goals is being used (e.g., [8]), most proposals for primarily addressing privacy characteristics have not found a wider audience (e.g., [7] and [9]). When the Common Criteria became an international standard (ISO/IEC 15408) for computer security certification in 1999, they contained already a section on describing a "Privacy Class" that consists of descriptions of the four families "Anonymity", "Pseudonymity", "Unlinkability" and "Unobservability" (Version 2.1 from 1999: [10], Version 3.1 from 2009: [11]). However, this Privacy Class is in practice not established on the same level as a protection goal comparable to the classic triad. Since 2009, an extension of the classic triad by three privacy-specific protection goals is being discussed. At first having started among a few researchers and the German data protection commissioners' community [3][4], then with lawmakers which resulted in some adoptions of the terms in national or regional data protection law [5], and meanwhile on the international level as a contribution to ISO's privacy reference architecture [6].

The new privacy-specific protection goals complement the ones existing for information security by adding the central privacy aspects from the legal and privacy

sphere. The privacy protection goals unlinkability, transparency and intervenability are defined as follows [6]:

**Unlinkability** means that all data processing is operated in such a way that the privacy-relevant data are unlinkable to any other set of privacy-relevant data outside of the domain, or at least that the implementation of such linking would require disproportionate efforts for the entity establishing such linkage. Unlinkability is the key element for data minimisation [12] because it encompasses all kinds of separating data from persons, e.g., by means of anonymisation, pseudonymisation, erasure or simply not having the data at all. In addition, it aims at separating different data sets, e.g., if they belong to different purposes, and thereby supports the principle of purpose binding. Further, separation of powers is related to unlinkability. Unlinkability in this wide definition comprises the criteria from the Privacy Class in the Common Criteria (anonymity, pseudonymity, unlinkability (in a stricter definition) and even unobservability in the sense that any observation of another party cannot be linked to the action or non-action of a user). The overarching objective of this protection goal is to minimise risks to the misuse of the privacy-relevant data and to prohibit or restrict profiling spanning across contexts and potentially violating the purpose limitations related to the data.

**Transparency** means that all parties involved in any privacy-relevant data processing can comprehend the legal, technical, and organisational conditions setting the scope for this processing – before, during and after the processing takes place. Examples for such a setting could be the comprehensibility of regulatory measures such as laws, contracts, or privacy policies, as well as the comprehensibility of used technologies, of organisational processes and responsibilities, of the data flow, data location, ways of transmission, further data recipients, and of potential risks to privacy. All these parties should know the risks and have sufficient information on potential countermeasures as well as on their usage and their limitations. This information should be given before the processing takes place (ex-ante transparency) which is in particular necessary if data subjects are being asked for consent or if data controllers want to decide on the usage of a specific system. But also subsequent to the processing, transparency on what exactly happened is important so that all parties can keep track of the actual processing (ex-post transparency).

**Intervenability** means that the parties involved in any privacy-relevant data processing, including the individual whose personal data are processed, have the possibility to intervene, where necessary. The objective is to offer corrective measures and counterbalances in processes. For individuals, intervenability comprises the data subject's rights to rectification and erasure or the right to file a claim or to raise a dispute in order to achieve remedy when undesired effects have occurred. For data controllers, intervenability allows them to have efficient means to control their data processors as well as the respective IT systems to prevent undesired effects. Examples for such means may be the ability to stop a running process to avoid further harm or allow investigation, to ensure secure erasure of data including data items stored on backup media, and manually overruling of automated decisions or applying breaking glass policies.

**Extending the widely known CIA model with privacy protection goals** offers benefits for the communication between the usual groups of practitioners involved in planning, evaluating, and operating systems processing personal data: Experts in

information security are accustomed to deal with protection goals. The same is true for lawyers: The concept of goals that partly or completely conflict each other is daily business in legal practice, for instance in form of conflicting legal interests or in the interpretation of rules considering goals outlined by, e.g., basic rights. We therefore believe that applying privacy protection goals to ICT systems can aid the communication between the involved experts.

It is important to stress that any application of protection goals does not tackle the basic question of lawfulness. On the one hand, the legal basis, e.g., specific statutory provisions or consent of the data subject, has to be identified when designing an IT system or an application. On the other hand, together with the risk analysis for the specific use case, the applicable regulations set the conditions and the level of how important the respective protection goals are for a specific setting. For instance think of statistics on energy consumption in different regions: As long as the energy consumption is not linkable to specific persons or households, the data may be considered not to be personal data, and therefore confidentiality may not be required, but integrity and availability. There might still be demands of unlinkability (to avoid that personal or non-public data are being linked to the public data), transparency (to understand what is happening) and intervenability (to intervene if necessary, e.g., if social sorting may be based on the region). However, in some countries it is regulated that fine-grained statistical energy data must not be disclosed to foreign countries – not because of privacy issues, but because from the data it may be derived whether preparations for war are being made. This law may call for more confidentiality, i.e., no disclosure, or for less integrity, i.e., disclosure only after having added some fuzziness to the data.

The protection goals are to some extent complementary to each other: For instance, confidentiality against unauthorised parties may be regarded as "guaranteed non-availability" concerning these parties. While unlinkability calls for the separation of knowledge, full transparency would require that the different sets of information can be linked together – again, for authorised parties this linkage should be possible, but excluded for unauthorised parties. Or full integrity of an archive that aims at completeness means that it must not (or cannot) be manipulated, but this would also exclude the possibility to intervene, e.g., if privacy-relevant data had to be erased from the archive. In case conflicts arise, the objective is to find suitable balances and choose appropriate mitigation techniques to implement this balance. Identifying and understanding such conflicts are a prerequisite for the development of adequate and balanced solutions. The protection goals are complementing and overlapping each other while putting emphasis on specific aspects depending on the issue at stake.

To take full effect, protection goals must be applied to a specific use case as the conflicts result from the individual particularities [13]. If legal requirements strengthen one specific protection goal in a certain use case, one or more of the other goals will likely be less relevant to the use case allowing to consider this relation for the balancing of safeguards, even if this is not a zero-sum game.

The set of six protection goals can be applied both on the information itself and on the processes – throughout all technical layers. For each, the perspective of all involved parties, e.g., the data controller, the individual or a third party, should be adopted to figure out different objectives that have to be considered. Privacy protection goals help to structure risks and to define which safeguards to apply. The

extended set of protection goals also allows for the expression of mismatches and conflicts of different goals. This will support and guide the process of balancing the safeguards dealing with them when designing, operating and improving the ICT systems to comply with information security and privacy goals alike. For each use case, individual balances and implementations have to be determined, dependent on, e.g., the sensitivity of data, the attacker model, legacy issues from already existing components of the information system, and last but not least, legal obligations.

In this text, our elaborations are based on the following understanding:

Existing eID systems vary by type of issuer from governmentally issued travel and ID documents to privately issued IDs and format between smartcards and software certificates (Denmark, Sweden) [14]. For this analysis we regard **"eID"** as including all documents and tokens that allow electronic identification. Being aware of the ongoing efforts in the EC Member States to develop, introduce or roll out national eIDs and the European efforts to develop a more harmonised and interoperable eID landscape[2], our examples will focus on this development.

The **holder** of an eID is the person to whom the ID was issued. This will usually be a natural person endowed with data subject rights. While in some states eIDs might be issued also to other entities including authorities and legal persons, such business or public entities will be referred to as **service providers** and **authorities** respectively.

Legal terminology is used consistent with Art. 2 of Directive 95/46/EC.

## 3 Examples From the European eID Landscape

Within the European Union, several eID systems have already been conceptualised and implemented. The central purpose of the systems is to allow authentication and identification of the holder towards third parties. Thus, they are actually not intended to achieve unlinkability; instead, the link to the holder and often also to other usages of the eID has to be maintained so far needed for the purpose of authentication or identification. Nevertheless, profiling and merging of information that is spread over several databases should be prevented. While name and date of birth are often sufficient for merging databases, this is made easier by the deployment of unique identifiers (UID) across these databases. Therefore, UIDs should be deployed restrictively and in a most privacy-respecting way. This shows that the unlinkability protection goal is the most interesting one to discuss with respect to different use cases and functionalities of eIDs.

In the various eID systems throughout Europe, the Member States took different approaches regarding the deployment of UIDs. For instance, in currently deployed eID systems the Swedish [2] and Estonian [15] eIDs include the pre-existing national personal identification code, which is widely used in relation to public authorities and private entities alike. In addition to the latent danger of profiling, such a system of completely linkable IDs used across different domains poses higher risks in case of identity fraud because several areas of life are directly affected. Finland and Denmark have avoided the use of their personal identity number by introducing a derived non-

[2] E.g., by funding projects like STORK https://www.eid-stork.eu/ and SSEDIC http://www.eid-ssedic.eu/.

descriptive number with the eID. Similarly, in Spain the identification number introduced with the eID is allocated to each citizen and was taken up by public and private bodies [16]. Germany has so far relinquished the use of unique identifiers or person identification numbers across domains.[3] The German eID merely contains the serial number of the card.

The deployment of a unique identifier is completely contradicting the idea of unlinkability as introduced above. The sensitivity of unique identifiers is also acknowledged by Art. 8 para. 7 of Directive 95/46/EC that demands that Member States determine the conditions under which a national identification number or any other identifier of general application may be processed. Admittedly, the use of UIDs might be acceptable for some specific purposes such as entries in databases of public entities if required by law. However, it is debated if a freely given informed consent should be required whenever using the UID in relation to private entities. If here eIDs for authentication or identification are being used, the possibility of doing that without automatically transferring the UID as well should be granted.

The need-to-know principle, allowing only such processing that is necessary for a given use case, is reflected in the privacy principles as part of **unlinkability**. In these cases, the amount and quality of personal data transferred should be minimised which is in line with the data minimisation principle spelled out in Art. 5 and Recital 30 as well as Art. 23 of the recently published draft of the European General Data Protection Regulation [17]. Consequently, anonymous – or alternatively pseudonymous – usage should be allowed whenever possible. Many use cases only require the verification of the holder's age or domicile, and thus eID systems could offer a reliable way to prove these attributes without giving away personal information that is not needed. Whenever a re-identification is sufficient, pseudonyms derived from the key in the eID could be used. While some eID systems that are based on classical cryptographic solutions always transfer the complete certificate (for Estonia see [15]), the German eID allows particularly for methods of anonymous and pseudonymous authentication. The next step would be to provide for certificates that allow to verify only specific attributes and to selectively disclose information from the certificate – transparent to and possibly even fine-granularly controlled by the eID holder. To keep anonymity up as long as possible, it is also imaginable to use private credentials where the true identity could be revealed by a third party in predefined case where this is considered necessary. Privacy-enhancing Attribute-Based Credentials[4] (Privacy-ABCs) as being implemented and made available in IBM's Identity Mixer and Microsoft's U-Prove technologies could enable such selective disclosure by cryptographic methods and allow the disclosure of the identity where previously agreed.

---

[3] However, the increased use of the personalised German tax ID introduced in 2008 recently raised concerns of the German Federal Commissioner for Data Protection, online: http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2011/28_SteuerID.html?nn=408908.

[4] The Project ABC4Trust is currently elaborating on an interoperable use of Idemix and U-Prove certificates and is deploying both technologies in two pilots, cf. http://www.abc4trust.eu/.

## 4 Use Cases for Designing Privacy-Respecting eID Systems

In October 2010, the International Conference of Data Protection and Privacy Commissioners agreed to a resolution to recognise Privacy by Design (PbD) and to encourage the adoption of its general principles [18]. These require inter alia that privacy should be dealt with proactively which implies to embed privacy into the design (for instance sketched in [19] basing on Common Criteria) and to have privacy-respecting default settings for all processes. PbD also requires watching the whole lifecycle of an ICT system. "Data protection by design" and "data protection by default" are also demanded by Art. 23 and Recital 61 of the draft European General Data Protection Regulation [17].

In the following use cases, we deploy the privacy protection goals to show how they can aid in the design of privacy-respecting eID systems. The order of the exemplarily chosen use cases follows the lifecycle of eID systems: test and launch of the eID system (4.1), deployment phase in which the system is running with a focus on identification and anonymous / pseudonymous authentication (4.2), as well as selected aspects of identity management, change management and the termination of the eID system (4.3-4.6). After briefly outlining each use case, we take the perspective of each protection goal to spell out requirements or consequences. Note that we put the focus on privacy and basic rights, thereby hardly touching other possible requirements from business interests or national security considerations.

### 4.1 Testing and Launching the eID System

In system engineering, different phases of testing have different requirements. It is characteristic for early phases of development that the protection goals are not that important since reliability of the system is not expected as long as it is in a test mode. For instance, availability is not crucial, yet, but it will be as soon as the system starts running in production mode. Similarly, without the sufficient level of integrity the system would not pass the test. Obviously, the lack of reliability in the early stages means that personal or otherwise sensitive data must not be processed which is demanded by the data minimisation principle, or more general, by the unlinkability protection goal. As long as these data are not processed, confidentiality is barely an issue, or only if trade secrets may be concerned. For testing and debugging purposes, typically more data will be logged than later when the functionality tests have been passed. Tracking down errors and removing them often requires linkage between different processes. Before the system is released for use with personal data, components that provide unintended unlinkability have to be removed. Transparency is very important to understand how the system behaves. System documentation and privacy policies should be drafted at latest during this phase. The system will undergo several changes, so intervenability for the developers is necessary. Existing documentation has to be adapted to changes done to the system.

In theory, the not-so-reliable test mode and the fully reliable production mode are distinct. However, when launching complex eID systems with real users, it has turned out that the practical usage reveals further problems that have to be tackled. Even here there may be possibilities for omitting personal, e.g., by employing anonymised or

pseudonymised data. When real users and their personal data are involved, the requirements for the system's reliability increase. This has effects on the demands concerning confidentiality, integrity and availability as well as unlinkability (data minimisation as far as possible and purpose binding, also for the data that is needed to evaluate the system and track down errors), transparency (ex-ante and ex-post transparency for users, e.g., the data subject right to access) and intervenability (e.g., the data subject rights to rectification, blocking or erasure as well as the possibility to withdraw given consent have to be supported; the user has to be able to issue a complaint if something goes wrong; it must be possible to correct unlawful or unsecure processes).

### 4.2 Use Cases for Identification, Anonymous or Pseudonymous Authentication

**Online identification** towards public and private entities is probably the central use case for eIDs. This use case only refers to natural persons identifying towards companies and authorities and not towards other natural persons. The latter would require further considerations, which are beyond the scope of this paper, e.g., to which extent another user might become data controller who is obliged to ensure information security and consequently might be held liable for a security breach.

While identification means that the holder of the eID provides information that clearly identifies her, authentication can be done with less information or even anonymously, e.g., by providing proof that one lives in a municipality for getting access to the online resources of the municipalities' library or proving to be of a certain age. Here **anonymous authentication** is sufficient.

Other use cases are based on **pseudonymous authentication**, e.g., if different pseudonyms are used for different contexts or purposes. Therefore, modern eID systems should aid the holder with user-centric methods for managing their partial identities, in particular by allowing the deployment of pseudonyms. (For general information on pseudonymous transaction and partial identities, please refer to [12]. For legal requirements regarding user-controlled identity management in the light of the lifelong aspects see [20]).

In any case, holders must be able to know who is processing which data for which purposes. For collection of personal data **mutual authentication** should be mandatory requiring from service providers to identify themselves towards the holder with their identity, purposes of the collection and further information according to Art. 10 of Directive 95/46/EC.[5]

With conventional cryptographic means, it was the easiest way to deploy a public key infrastructure and to issue certificates including the identifying information (e.g., X.509). Usually these certificates do not allow for anonymous proofs or selective disclosure. The project ABC4Trust[6] is researching on Privacy-ABCs that allow for both – anonymous proofs and selective disclosure of only the necessary attributes

[5] This feature has been implemented in the German eID by requiring that the service provider sends an access certificate with its identity information before access to personal data stored on the eID is permitted.

[6] http://www.abc4trust.eu/

certified within a credential. Deploying Privacy-ABCs allows for keeping integrity up while providing unlinkability and confidentiality.

In addition, Privacy-ABCs can reveal the holder's identity in predefined cases. Pseudonymous authentication tokens[7] should be directly derivable from the eID to avoid the need of contacting a central party. Revealing the holder's identity should be possible without the necessity of giving the holder's personal data in clear text to a third party. Both requirements are fulfilled by capabilities of Privacy-ABCs: selective disclosure and inspection (for details see [21]).

For all protection goals, general requirements concerning the use cases are sketched in the following:

- Confidentiality: Naturally, all personal data available have to be protected against unauthorised access. This does not only cover the identity information, but also other information such as traffic data that should be protected against third parties monitoring the communication. In addition, the holder's personal data must not be revealed before the service provider or authority has identified itself providing its privacy policy and the holder has agreed to the transfer. For a potential holder-to-holder communication, identification should take place at the same time and only contain the personal data necessary.
- Integrity: When dealing with official eIDs, the parties must not be able to provide false information. If a pseudonym is provided, this nature must be clear to the receiving party. For the party relying on the authentication, it is important that only authorised persons can successfully claim to be holder of the pseudonym. All attributes proven by the parties must be true according to issuing entity.
  Note that here is a tension between integrity and intervenability: Many service providers (often outside Europe) ask for personal data that are not necessary for the specific purpose. Users have become used to cope with that by giving incorrect data because otherwise they would not be able to get the service. However, eIDs may prevent this possibility of users to intervene before disclosing correct data. A solution could be to regulate the ways how service providers can get eID information, which is the case with the German eID: For reading eID information from a holder's eID card, the service provider has to use a certificate which is only issued after a governmental authority has checked that the data are necessary for the stated purpose.
- Availability: The system must be reliable and available for transactions. If this is implemented in a way so that a central server can be omitted, this could allow point-to-point authentication.
- Unlinkability: Identification, anonymous and pseudonymous authentication differ in which data the holder reveals. In general, because of the data minimisation and the need-to-know principles it should be possible for a holder to authenticate only with the information actually necessary to achieve the purpose (see [22] which data are necessary for a series of use cases). This includes proof of attributes (age within a certain age rage) and selective disclosure (e.g., only providing city of

[7] The term "authentication token" refers to the certificate derived from the master credential to be sent to the relying party. Such tokens only hold the chosen data and not necessarily the complete information stored on the credential issued by the certification authority. The derived token still preserves a valid signature of the issuer.

living or a first name). In scenarios where identification is necessary, the identifying data (name, address, birth date) have to be linked to the holder. For anonymous authentication, no identifying information should be linkable for other parties than the holder herself. For pseudonymous authentication, e.g., for re-identification and replacing classical password log-in, the holder must be able to provide a proof that she is the entity that has acted under the same pseudonym in the past (implemented in the German eID as long as the eID token does not change, cf. [20]). These pseudonyms must be linkable with each other, meaning the previous transaction, but not with any other attribute value from the eID. For some use cases, pseudonyms are required where the identity can be revealed under specific strictly and previously defined conditions (e.g., criminal prosecution, non-performance of contractual obligations, emergency situations).

Apart from this, third parties should not be able to get insight or to learn about which parties are interacting. Therefore, central trusted third parties or ID servers should be omitted or constructed in a way that these are unable to link transactions or to find out who communicates with whom.

Unique identifiers (UIDs), e.g., serial numbers or identifiers used in other spheres already (social security number), allow linking across databases of different controllers and this is hardly necessary for a most purposes with a single service provider involved. To prevent profiling and merging of information spread over several databases, UIDs must not be a mandatory part of the identification using an eID.

- Transparency: The holder of the eID must be able to check which data are to be transferred for which purposes before transmitting them (cf. [23], p. 78 et seq. where a transparency-compliant dialogue for sending personal data is proposed). The information that should be provided by service providers is listed in Art. 10 of Directive 95/46/EC; for the area of electronic commerce see also Art. 5 sec. 1 of Directive 2000/31/EC. The holder must be able to read and understand the privacy policy of the receiving party. She should know about the consequences depending on the result of the identification process (e.g., in case of a positive or negative match). The holder must be able to control the data before transmission to check that only the identity information, pseudonym or set of attributes desired for this particular relation or transaction are sent to the recipient. Further, she should have a convenient possibility to exercise her right to access.
- Intervenability: The holder should be able to intervene if she believes that the process of identification or authentication has not yielded the correct result or leads to an unfair decision. In case the identity behind the holder's pseudonym has been revealed, she should be able to check whether the conditions for that have been met and whether the result is correct.

### 4.3 History Function – Overview of Past Transactions

Holders of eIDs should be able to see who processes which personal data for which purposes also at a later time. Such a history function as part of a user-controlled identity management has been introduced, e.g., as data track [24] and proposed for the user client of the German eID for future deployment ([25], p. 32). The history

function provides **transparency** and supports **intervenability,** as the holder would have the required information about data controllers including the contact information that must be provided at hand.

Note that the history function poses two main challenges: an information security challenge because it contains sensitive information on the holder's activities in a single place, and a privacy challenge because in case of holder-to-holder communication, the personal data of other natural persons may be processed and their privacy rights may be concerned. Here the right to rectification or erasure of a communication partner (his possibility to intervene) may collide with the desire of the holder to fully keep track (her wish for integrity).

- Confidentiality: Only the holder of the eID should be able to read the entries of the history database that should be stored under her control, e.g., on the eID token or by the client software, well protected against attacks, e.g., by malware.
- Integrity: The entries must not be modified by unauthorised parties, i.e., they should be correct and complete unless the holder decides otherwise (e.g., to delete old entries).
- Availability: For a working eID system, the history function is not crucial. However, the holder can only work with the history function if it is available. For the entries, local backups must be possible.
- Unlinkability: While the communication partners of the holder should not be able to link separate communications that were conducted under different pseudonyms, the history function should provide one view for the holder on past communications. For risk minimisation, the holder may wish to separate entries from different context (e.g., for the workspace and for the private space), especially if she cannot exclude that other parties may have access to the entries.
- Transparency: The holder should know about the history function and how it processes the data. She should also understand the risk if other parties could read or manipulate the entries. The holder has to be aware of her responsibility to establish sufficient safeguards.
- Intervenability: Holders must be able to fully deactivate the history function or to delete entries. In case the holder is being forced to give, other parties access to the history function or to provide print-outs, plausible deniability or artificially blurring the data could be necessary (affecting integrity).

### 4.4 Right of Access and Rectification

Holders should be able to access their data stored on the eID token. If data have changed, e.g., address information due to moving or the last name due to marriage, a possibility must be foreseen to rectify this information.

- Confidentiality: Information stored on the eID token should be protected from unsolicited access.
- Integrity: Editing identifying personal data (name, address) on the eID should be restricted to the issuing entity. If the change includes the change of the issuing entity, e.g., as a change of address also may change the competent municipality, the last competent authority must at least be notified or "release" the eID for change by the new authority.

- Availability: The holder must be able to access the data on her token anytime with her client software. The rectification must be available in due time.
- Unlinkability: For exercising the rights of access and rectification, the holder has to prove that she is authorised, i.e., that there is the link between the holder and the eID. An identification of the holder is not always required by the given purpose; instead, a more data minimising way, e.g., by anonymous or pseudonymous authentication with selected attributes, may be sufficient.
- Transparency: The right of access is a manifestation of the transparency principle. The holder has to understand which processes are necessary to exercise the right of access, regardless whether this is directly possibly by putting the eID token in a reading device or whether the involvement of an authority is necessary. Similarly, the holder has to know how to rectify data and what this may mean in the further communication with other parties, e.g., whether the rectified information will automatically be transferred to others or not.
- Intervenability: The right of rectification is a manifestation of intervenability. Usually rectification means to correct and update data, but there may be use cases where erasure or blurring some information could make sense.

### 4.5 Revocation and Renewal of eID Credentials

Seeing the importance of lifelong privacy planning must include the whole lifecycle of an eID. On a smaller level, also the revocation of the credential or a derived pseudonymous authentication token must be looked at.

- Confidentiality: Information whether a credential is revoked must only become known to authorised persons. This includes anyone to whom the credential is presented for authentication to verify that the credential has not been revoked. Public lists of revoked credentials should be avoided.
- Integrity: If additional data may exist (partial identities, history function), the holder must be able to create a secure backup on a device under her control and to migrate the data so that it functions with a new credential as well. The holder must not be able to use a revoked credential.
- Availability: A revocation must be performed within a guaranteed timeframe. The duration for a replacement credential must be proportional to its importance in daily life. The process of revocation must be well defined and tested. Established partial identities must be available under reissued credentials.
- Unlinkability: Where the system is finally terminated, data should be deleted and thus completely unlinkable. However, the user should be able to establish a link between the old and the new credential to maintain partial identities. This requires that the holder can prove under the new credential that she is the same person that acted under a particular credential that has been revoked. Moreover, revocation must not lead to linkability of credentials or derived pseudonymous authentication tokens. Information that is processed or stored to enable the investigation of potentially wrongful revocations must be separated from other data so that no additional linkability is being provided.
- Transparency: The revocation process must be publicly documented in the privacy policy or terms of use. This should include the information on how to act and

whom to contact in case of a lost or compromised eID. For each revocation, it has to be logged who triggered it when, and potentially the reason for revoking the eID should also be documented. Relying parties must be able to verify the validity of an eID.

- Intervenability: Revocation is a form of intervenability. The intervenability requirements depend on who can trigger the revocation and who is affected by it. For a holder-triggered revocation, the holder must be given a sufficient means to react in time, e.g., by a revocation secret to trigger the process. Further, a single point of contact to ask for help should be installed. If other parties can trigger the revocation, the holder has to be able to determine whether the revocation was wrongfully conducted; if this is the case, a remedy has to be provided.

### 4.6 Termination or Major Changes in the eID Lifecycle

Considering the whole lifecycle includes the termination of the process as a whole, e.g., switching to another system of IDs or major changes such as a rollout of a new version of the eID tokens.

- Confidentiality: All personal data have to stay protected against unauthorised access even in the migration process. This also comprises the databases that have served the old eID infrastructure and that are not used anymore. Therefore, once the data have been successfully migrated to the follow-up system, national register etc., they should be deleted.
- Integrity: Integrity is important for the full termination or migration process that has to be invoked only by entitled entities. In particular, it is required insofar as the process of securely storing the data until final deletion must be secured from unsolicited access or changes.
- Availability: The process of termination as such must be defined. There must not be a time where neither the old nor the new system work. In the follow-up system the user should be enabled to maintain established partial identities.
- Unlinkability: When the old eID system is finally terminated, the data should be deleted und thus made completely unlinkable. However, the holder should be able to establish a link between the old and the new eID to maintain established partial identities. She should be able to prove under the new eID system that she is the same person that acted under a particular eID in the old system.
- Transparency: The termination and/or migration must be documented and the documentation should be publicly available upon request. However, it does not need to be part of the privacy policy in daily use.
- Intervenability: All changes in the eID lifecycle are in itself manifestations of intervenability. Entitled entities must be able to trigger the termination of the lifecycle. Holders that believe that something went wrong in a migration process must be able to issue a complaint. In case of errors that affect holders (e.g., if identities get lost), a remedy has to be provided in due time.

## 5 Conclusion

As presented in this text, privacy protection goals can be deployed to assess the privacy criteria of eID systems. For the ongoing development of national eIDs and the movement towards interoperability among European eIDs, privacy protection goals can generate awareness for privacy issues and animate deliberations on balancing the interests of all parties involved.

Future research should cover the relation between the privacy protection goals and other methods to structure privacy-relevant requirements: This encompasses both very specific regulation in different jurisdictions and high-level principles as being laid down in the "OECD Guidelines on the Protection of Privacy and Transborder Flows" or the "Fair Information Practices". It should be discussed how the essence of the privacy protection goals could be put more prominently into such regulations or guidelines. In addition, research should be invested on the process of balancing the protection goals and the different interests in the evolving information society – here a well-documented and comprehensible risk analysis and risk management will become important concepts for policy makers. By no means, risk analysis and risk management should supersede data protection regulation; in particular, risk management methods such as insuring oneself against a risk cannot shift the legal accountability. Still the protection goals have the potential to guide lawmakers because especially unlinkability, transparency and intervenability are overarching principles to achieve a fair and controllable use of information technology. For data controllers and designers of information technology systems, the protection goals can help to develop systems that do not have undesired effects to individuals or to society.

Specifically for national or for planned European eID systems, the approach of applying not only traditional information security protection goals, but also the objectives of unlinkability, transparency and intervenabability for all processes in their lifecycle is one example for the mandatory undertaking of privacy and technology assessment.

**Acknowledgments.** The authors kindly thank Prof. Simone Fischer-Hübner and the anonymous reviewers for their detailed review comments and their valuable input to improve this contribution.

## References

1. Dobias, J., Hansen, M., Köpsell, S., Raguse, M., Roosendaal, A., Pfitzmann, A., Steinbrecher, S., Storf, K., Zwingelberg, H.: Identity and Privacy Issues Throughout Life. Chapter 4 in: Camenisch, J., Fischer-Hübner, S., Rannenberg, K. (eds.) Privacy and Identity Management for Life, pp. 87–110. Springer, Berlin (2011)
2. Grönlund, Å: Electronic identity management in Sweden: governance of a market approach. Identity in the Information Society, Volume 3, Issue 1, 195–211 (2010), doi:10.1007/s12394-010-0043-1
3. Rost, M., Pfitzmann, A.: Datenschutz-Schutzziele – revisited. DuD, Vol. 33, No. 12, 353–358 (2009)

4. Rost, M., Bock, K.: Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen. DuD, Vol. 35, No. 1, 30–35 (2011)
5. Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz - LDSG -). Version after the last change that has been published in: Gesetz- und Verordnungsblatt für Schleswig-Holstein (GVOBl. SH 2012, No. 2, pp. 78–82), https://www.datenschutzzentrum.de/gesetze/ldsg.html (2012)
6. Hedbom, H., Schallaböck, J., Wenning, R., Hansen, M.: Contributions to Standardisation. In: Camenisch, J., Fischer-Hübner, S., Rannenberg, K. (eds.) Privacy and Identity Management for Life, pp. 479–492. Springer, Berlin (2011)
7. Federrath, H., Pfitzmann, A.: Gliederung und Systematisierung von Schutzzielen in IT-Systemen. DuD, Vol. 24, No. 12, 704–710 (2000)
8. Parker, D.B.: Toward a New Framework for Information Security. In: Bosworth, S., Kabay, M.E. (eds.) The Computer Security Handbook (4th ed.). John Wiley & Sons, New York, NY (2002), online: http://www.computersecurityhandbook.com/csh4/chapter5.html
9. Wolf, G., Pfitzmann, A.: Properties of protection goals and their integration into a user interface. Computer Networks, Vol. 32, No. 6, 685–700 (2000)
10. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 2.1, CCIMB-99-032 (1999), online: http://www.commoncriteriaportal.org/files/ccfiles/ccpart2v21.pdf
11. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 3, CCMB-2009-07-002 (2009), online: http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf
12. Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, (2010), online: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml
13. Rost, M.: Datenschutz in 3D – Daten, Prozesse und Schutzziele in einem Modell. DuD, Vol. 35, No. 5, 351–355 (2011)
14. Kubicek, H., Noack, T.: Different countries-different paths extended comparison of the introduction of eIDs in eight European countries. Identity in the Information Society, Volume 3, Issue 1, 235–245 (2010), online: doi: 10.1007/s12394-010-0063-x
15. Martens, T.: Electronic identity management in Estonia between market and state governance. Identity in the Information Society, Volume 3, Issue 1, 213–233 (2010), online: doi:10.1007/s12394-010-0044-0
16. Heichlinger, A., Gallego, P.: A new e-ID card and online authentication in Spain. Identity in the Information Society, Volume 3, Issue 1, 43–64 (2010), online: doi:10.1007/s12394-010-0041-3
17. European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final. Brussels, 25.01.2012 (2012), online: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
18. Cavoukian, A. et al.: Privacy by Design Resolution, 32nd International Conference of Data Protection and Privacy Commissioners, 27-29 October 2010, Jerusalem, Israel (2010), online: http://www.ipc.on.ca/site_documents/pbd-resolution.pdf
19. Skinner, G., Chang, E.: PP-SDLC – The privacy protecting systems development life cycle. In: Milutinovic, V. (ed.) Proceedings of the IPSI Conference (2005), online: http://www.scientificcommons.org/8096648
20. Storf, K., Hansen M., Raguse M. (eds.): Requirements and concepts for identity management throughout life. PrimeLife Deliverable H1.3.5, Zürich (2009), online: http://www.primelife.eu/images/stories/deliverables/h1.3.5-requirements_and_concepts_for_idm_throughout_life-public.pdf

21. Krontiris, I. (ed.): Architecture for Attribute-based Credential Technologies – Version 1. ABC4Trust Deliverable D2.1, Frankfurt/Main (2011), online: https://abc4trust.eu/index.php/pub/107-d21architecturev1
22. Zwingelberg, H.: Necessary Processing of Personal Data: The Need-to-Know Principle and Processing Data from the New German Identity Card. In: Fischer-Hübner, S., Duquenoy, P. Hansen, M. et al. (eds.) Privacy and Identity Management for Life, pp. 151–163. Springer, Berlin (2011), online: doi:10.1007/978-3-642-20769-3_13
23. Fischer-Hübner, S., Zwingelberg, H. (eds.): UI Prototypes: Policy Administration and Presentation – Version 2. PrimeLife Deliverable D4.3.2, Zürich (2010), online: http://www.primelife.eu/results/documents/115-432d.
24. Wästlund, E., Fischer-Hübner, S. (eds.): End User Transparency Tools: UI Prototypes. PrimeLife Deliverable D4.2.2, Zürich (2010), online: http://www.primelife.eu/results/documents/113-422d
25. Hasso-Plattner-Institut für Softwaresystemtechnik: Vom Client zur App – Ideenkatalog zur Gestaltung der Software zum Einsatz des neuen Personalausweises, Berlin (2011), online: http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Begleitstudien/Studie_Usability_Volltext.html