Risk Analysis of Identity Management Approaches Employing Privacy Protection Goals

Marit Hansen

Risk Analysis of Identity Management Approaches Employing Privacy Protection Goals – Position Paper

Marit Hansen

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Germany
marit.hansen@privacyresearch.eu

Abstract. This position paper introduces the approach of privacy protection goals for risk analysis in identity management. It pleads for taking into account external factors such as the data collection via other applications or upcoming legal legislation.

Keywords: Identity Management, Privacy Protection Goals.

1 Protection goals for information security and privacy

For decades, professionals in information technology have been working with the so-called classic triad of the protection goals “confidentiality”, “integrity” and “availability” to assess security properties and risks of information systems. Since 2009, an extended set of protection goals has been proposed that also consider the privacy perspective, and thereby better reflect the interests of the individual whose personal data are being processed [1,2]: In addition to the classic three security protection goals, three complementing privacy protection goals have been introduced:

- “unlinkability”: Unlinkability ensures that privacy-relevant data cannot be linked across privacy domains or used for a different purpose than originally intended. Thereby it addresses both the legal principles of data minimization and purpose binding.
- “transparency”: Transparency ensures that all privacy-relevant data processing including the legal, technical and organizational setting can be understood and reconstructed. Transparency is the precondition for all kind of user decision, e.g. for giving consent.
- “intervenability”: Intervenability ensures that data subjects, operators and supervisory authorities can intervene in all privacy-relevant data processing. Its objective is the application of corrective measures and counterbalances where necessary. The data subject’s rights to rectification or erasure are an example for intervenability.

Since beginning of 2012 the State Data Protection Act Schleswig-Holstein, Germany demands that data controllers take into account the three security protection goals as well as the three privacy protection goals (Art. 5 par. 1 LDSG S-H). They have also been taken up in the draft report of the European Parliament on the European Data Protection Regulation [3].

2 Identity management and privacy protection goals

The six protection goals are not independent from each other. Working with protection goals means to identify how far each of the goals should be implemented and to find a suitable balance between those goals, taking into account the interests of all parties involved. Privacy-enhancing and user-controlled identity management has usually strong requirements concerning the protection of personal data against unwanted linkage across domains or contexts [4]. However, unlike an anonymizing system that aims at full unlinkability, several interactions with the same communication partner should in many cases be linkable for the parties participating in the communication (not for potential observers) which has effect on the choice and (re-)use of pseudonyms. Transparency (beforehand and afterwards) is important for users to understand what the data processing is about, e.g. to enable them to select which attribute values to disclose. In case a relying party asks for information that is not appropriate for the given purpose, users must be able to intervene, i.e. to stop a transaction, to limit the disclosure or to send a complaint.

Note that the protection goals are not only meaningful for designing information and communication technology systems, but can also be used to check organizational procedures or legal regulations.

3 Considering external factors, too

For analyzing risks concerning the desired level of guarantees per protection goal, the system scope should not be too narrow. For instance, even photos that have not been biometrically optimized such as in the ePassport pose the growing risk of being linked across domains and contexts because of the big collections via social networks or search engines and the available technologies of biometric matching.

Another huge risk for all European identity management may be caused by the regulation on electronic identification and trust services for electronic transactions (eID Regulation) in case it is passed in the draft version that was presented by the European Commission in June 2012 [5]. The proposed regulation aims at removing barriers in the internal market for electronic interactions. Each Member State may notify an electronic identification scheme that it accepts to access public online services. All Member States must accept the foreign notified schemes. The draft eID Regulation demands that each Member State sets up at least one national online authentication service for their notified eID schemes that is available for relying parties requesting to check the link to a user authenticating with the eID. This online authentication service is liable for the unambiguity of the link to a citizen. On the ground of “technology neutrality” Member States must not impose any specific technical requirements (e.g. obtaining hardware or software) on relying parties.

As elaborated in [6], such a regulation would likely lead to several risks to the user's privacy:

- The need for one always available online authentication service probably means that centralized services would be given preference.
- Liability for the unambiguity of the link between the eID and the citizen would prevent anonymous authentication.
- The liability also would make it necessary for the services to store logfiles on the individual transactions to prove that they did it right. These logfiles – containing the information of users and relying parties involved in cross-border authentication – would have to be retained for as long as authentication result may be challenged.
- eID systems that provide selective disclosure of attributes are not foreseen in the proposed regulation. Such systems would require that relying parties install at least some software which the draft regulation negates.

All in all, the protection goal unlinkability is severely violated by these risks. The other two privacy protection goals, transparency and intervenability, are less addressed in the draft regulation and depend on the implementation. However, in particular the part on liability would have to be clarified concerning transparency and intervenability. It is necessary to amend the eID Regulation so that privacy-enhancing identity management solutions can be used or are even made mandatory for cross-border authentication. Best practice approaches can help to stop a race to the bottom concerning the level of implemented privacy.

References

1. Rost, M., Pfitzmann, A.: Datenschutz-Schutzziele – revisited. Datenschutz und Datensicherheit (DuD) 33(12), 353–358 (2009)
2. Hansen, M.: Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals. In: Camenisch, J. et al. (eds.): Privacy and Identity 2011, IFIP AICT 375, pp. 14–31. IFIP International Federation for Information Processing (2012)
3. Albrecht, J.P. (Rapporteur): Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs, 17.12.2012, http://www.europarl.europa.eu/sides/getDoc.do?language=EN&reference=PE501.927 (2012)
4. Zwingelberg, H., Hansen, M.: Privacy Protection Goals and Their Implication for eID Systems. In: Camenisch, J. et al. (eds.): Privacy and Identity 2011, IFIP AICT 375, pp. 245–260. IFIP International Federation for Information Processing (2012)
5. European Commission: Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. COM(2012) 238/2, Brussels, 04.06.2012, http://ec.europa.eu/information_society/policy/esignature/docs/regulation/com_2012_2038_en.pdf (2012)
6. ABC4Trust: Privacy-ABCs and the eID Regulation. Position Paper. https://abc4trust.eu/ (2013)