

Authorization Architectures for Privacy-Respecting Surveillance

Ulrich Flegel and Michael Meier

University of Dortmund, D-44221 Dortmund, Germany
{ulrich.flegel|michael.meier}@udo.edu

Abstract. Even more than in our physical world, in our digital world we need systems that meet the security objective of service providers and users in equal measure. This paper investigates the requirements of secure authorizations with respect to accountability and privacy in the context of surveillance for misuse detection during service utilization. We develop a model of system architectures for secure and privacy-respecting authorizations that allows to derive and compare the properties of available technology. It is shown how the model maps to existing authorization architectures.

Keywords: Architecture, authorization, privacy, pseudonym, surveillance, misuse detection, intrusion detection.

1 From Physical to Digital: A Short Visit to the Zoo

Many safeguards in the digital world mimic safeguards in the physical world. The reason probably is that safeguards are necessary, if the actors do not trust each other. However, at the end of the day, trust is usually anchored in the physical world. Using an example it is shown how we deal with trust in the physical world. In the following, we describe the case of a student who wants to visit the zoo. In the example the zoo serves as a service provider offering free admission to students. Non-students might feel tempted to defraud the zoo by pretending to be a student in order to obtain free admission. Hence, the personnel at the zoo ticket booth is instructed not to trust statements that customers make about their own property as a *student*. For customers it is thus insufficient claiming to be a *student*, also because the ticket booth personnel cannot verify the statement without considering supporting documents. Instead, it is required to show a valid student ID. The student ID is used as a certified property statement that assigns the name of the subject of the statement to the property *student*. At the ticket booth a certified property statement is accepted, if it is a student ID, as a matter of policy the issuing university is trusted to generate useful property statements, the person on the picture visually matches the presenting person, the student ID has not yet expired and looks “genuine”.

If the student ID is accepted at the ticket booth, the presenting person is authorized to pass the zoo entrance. The presenting person receives the service-specific property *authorized for zoo entrance*. Therefore customers that are *authorized for zoo entrance* receive an admission ticket at the ticket booth. The

ticket is accepted at the zoo entrance, if the stated ticket booth is trusted to issue tickets only to persons that are *authorized for zoo entrance*, the ticket number looks “plausible”, the ticket authorizes to pass the zoo entrance, it has not yet expired and looks “genuine”.

If the admission ticket is accepted at the zoo entrance, the student may enter the zoo. Right in the front is a sign that specifies behavior that is by policy prohibited in the zoo. Most notably, it is prohibited to tease the monkeys, since they may take revenge using banana peel projectiles. Thus, for the time being, the zoo trusts that the visitors stick to the rules. At critical areas (at the monkey house) the zoo may put a guard in place. The guard observes the behavior of the visitors and reacts, if he detects a violation of the zoo policy.

This paper presents a model for authorization architectures and criteria for deriving and comparing generic high-level properties of existing privacy-enhancing technologies when applied to surveillance for misuse detection. The model and criteria are developed in four steps:

- Generalizing the hybrid PKI model of Biskup and Karabulut [1] by abstracting from PKI-specific technology an architecture model for secure authorizations is developed, which primarily meets the security interests of service providers (see Sect. 2).
- Our previous work on pseudonyms [2] is generalized for the model to solve the privacy problems created by surveillance data, thereby enabling lawful misuse detection. What distinguishes our pseudonym approach from related work is the integrated notion of technical purpose binding for pseudonym disclosure (see Sect. 3).
- Combining the model from Sect. 2 with pseudonyms results in an architecture model for secure and privacy-respecting authorizations (see Sect. 4).
- Given the model, criteria are developed to derive and compare generic high-level properties of privacy-respecting authorization architectures (see Sect. 5). It is shown how the model can be applied to existing privacy-enhancing technologies (see Sect. 6).

The proposed model is compared to existing models in Sect. 7 and the paper concludes in Sect. 8 with a summary of the contributions.

2 An Architecture Model for Authorizations

Based on the assumption that services do not generally trust in property statements that users make on their own behalf, authorization architectures rather rely on property statements that are responsibly certified by agents trusted by the service. In the proposed model individuals, computers and other players in a distributed IT system are denoted as *entities*. A *principal* is a bit string that is unique within its scope of application and it is associated with an entity to serve as its surrogate. An entity can enjoy *properties*, which in turn may be used in conditions in authorization policies, and are taken into account during the trust evaluation.

The terms *certification* and *certificate* in the model denote the process and the result, respectively, when a responsible agent certifies a statement about rather *entity-specific* than *service-specific* properties in its role as a *certifier*. In Sect. 1 the student ID is a certificate, which expresses the certified statement about the entity-specific property *student*.

In the model the term *authorization* denotes the process and the result, when a responsible agent certifies a statement about *service-specific* properties in its role as an *authorizer*. In Sect. 1 the zoo admission ticket is an authorization, which expresses the certified statement about the service-specific property *authorized for zoo entrance*.

A *responsible agent* (cf. the university or the zoo ticket booth in Sect. 1) verifies that a *subject* entity enjoys certain properties and certifies a statement under one of his own principals, such that the statement assigns a principal of the subject to property attributes that correspond to the verified properties of the subject. The association of the subject principal with the presenting entity is verifiable by means of authentication data. A property statement also contains verifiable data concerning the validity of the statement, where the data can only be generated by the responsible agent and practically cannot be counterfeited. Note that certified property statements come in different forms, such as static documents (e.g. certificates [1]) or as traces of interactive protocols (e.g. anonymous credentials [3]).

Property statements comprise the following *components* (see Fig. 1): A principal of the *responsible agent* for the trust evaluation, parameters for checking the *validity*, *authenticity* parameters for authenticating the presenting entity, a set of *attributes* expressing the subject properties and being evaluated for the access decision, and the *subject* principal, which is used for linking property statements while processing service requests.

The components of certified property statements primarily support security objectives of the service providers. Accordingly the fat light grey frames in Fig. 2 enclose the system components where the service-related security objectives are enforced and which must not be controlled by the user. In Fig. 2 the solid arrows indicate the flow of certified or verified property statements.¹ In the text the arrows are referenced by their identifiers (here: ‘A1’ to ‘C2’).

The players in the basic model in Fig. 2 are the user-side management, a certifier, an authorizer and a service. As an example, in *Kerberos* [4] they can be mapped to the client, the *authentication server*, the *ticket granting server*, and the service. The authorization for the utilization of a service can be broken down into the following three phases: 1) The user has his relevant properties certified (see ‘A1’, ‘A2’ and ‘A3’ in Fig. 2). 2) Presenting his relevant certificates the user is authorized for the utilization of the service (see ‘B1’, ‘B2’ and ‘B3’ in Fig. 2). 3) Presenting the authorization the user can utilize the service (see ‘C1’ and ‘C2’ in Fig. 2). The management is controlled by the user. It interacts with other players, and based on the policy of the user, and aiming at satisfying the

¹ We assume that the service answer does not include statements about the properties enjoyed by the user. Hence, the service answers are not shown in the model.

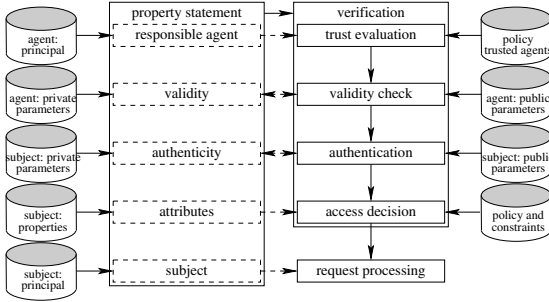


Fig. 1. Verification of property statements

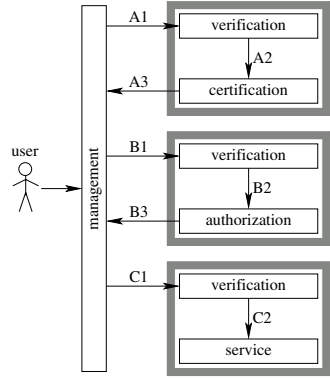


Fig. 2. Basic model

requirements of the service or responsible agent (see the policies in Fig. 1), it chooses property statements and information that are suitable for the respective interaction. There are slightly different variants of the basic model reflecting shortcuts that existing authorization architectures take [5].

3 Pseudonyms with Technical Purpose Binding of Disclosure

As described in Sect. 2 the access decision for service utilization is based on certified property statements including a subject principal. While processing a service request for a subject, in the system occur events that are triggered by the step-wise computation of the answer to the request, where these events usually are linked to the subject principal. That is, system events are accountable, usually with the objective of accounting detected misuse to the perpetrator. The working principle of surveillance technology for misuse detection is based on analyzing relevant system events manifested in *audit data* (cf. guard in Sect. 1). Appropriately responding to detected misuse, i.e. locking out some user or filtering source IP addresses, requires that the manifestation of the misuse in the audit data be accountable.

When collecting and processing audit data the obvious conflict between the individual user’s interest in privacy and the overall security objective accountability can be solved by using *pseudonyms* in the audit data instead of subject principals. In the sense of *multilateral security* [6] a fair solution can be achieved by distinguishing the normal case (no accountability) and the exceptional case (accountability can be established) by controlling the external knowledge about (parts of) the *pseudonym mapping*. We discuss the legal foundation of such a solution elsewhere [5] and define a *pseudonym* as a principal that does not allow the identification of the assigned entity, based on the definitions of Pfitzmann and Hansen for *unlinkability* and *anonymity* [7]. Further concepts of

pseudonymization, *pseudonym mapping*, *pseudonym disclosure* and *reidentification* building on the aforementioned definitions are used intuitively here and defined in more detail elsewhere [5].

The *controlled disclosure* of pseudonyms is the controlled ability to make pseudonymized objects accountable again. This ability is controlled by enforcing who can use the pseudonymity mapping. The entity which manages the pseudonym mapping is responsible for performing reidentification for legal purposes of authorized entities only. We say that pseudonym disclosure is subject to *purpose binding*, if it is granted only for some a priori specified purpose, e.g. responding to detected misuse. If the responsible handling is conferred to a person, the reidentification is subject to *organizational purpose binding*. Since this person needs to manually perform the purpose binding, pseudonym disclosure may be delayed and not be sufficiently fast for a timely misuse response. Alternatively the purpose of pseudonym disclosure can already be incorporated during pseudonym generation. The pseudonymized audit data is automatically supplemented with certain information that neutralizes the protection of the pseudonym mapping under certain conditions. The purpose of pseudonym disclosure determines under what conditions the protection becomes ineffective, and (parts of) the pseudonym mapping can be used for reidentification. The pseudonyms can be disclosed only if these conditions are met. If the protection of the pseudonym mapping is customized for the disclosure conditions, such that it cannot be circumvented – e.g. by means of cryptography [2], the pseudonyms are subject to disclosure with *technical purpose binding*. The advantages of technical purpose binding will become apparent in the context of the architecture model in Sect. 4.

4 An Architecture Model for Privacy-Respecting Authorizations

In many cases person-identifying IDs are not necessary to verify certified property statements and to provide a service [8]. If for a given application IDs are not necessary, property statements and their references can be pseudonymized by replacing the subject principal with a pseudonym. As an example, the German act on digital signatures already allows for pseudonymous certificates (§7 Sect. 1-3 SigG [9]). In the example from Sect. 1 the admission ticket to the zoo does not need to contain the name of the ticket owner. Instead, it has a unique ticket number, which can be interpreted as a pseudonym of the ticket owner in the context of the zoo service.

On the one hand, the agent now is additionally responsible to the interest of accountability of the recipients of the property statement, for disclosing pseudonyms in accord with his pre-engaged policy to specific entities for specific purposes only. On the other hand, the agent is also responsible to the interest of the subject entity in pseudonymity, for protecting the pseudonym mapping and adhering to the declared policy w.r.t. pseudonym disclosure and linkability.

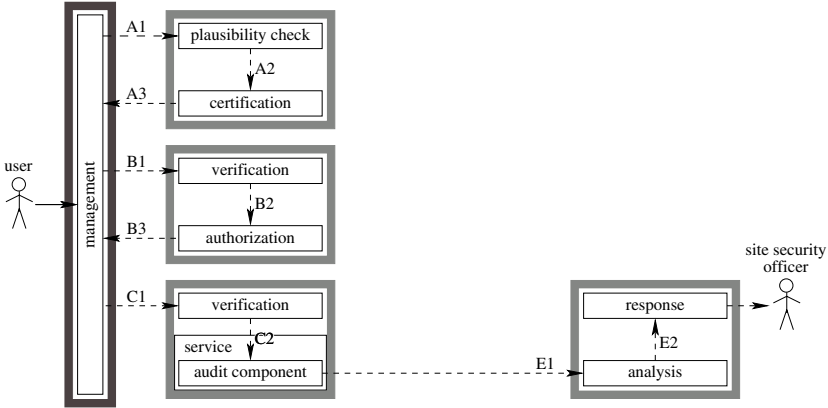


Fig. 3. Unilateral security: management anonymizes

In the following, the basic model from Fig. 2 is extended with the *site security officer* (SSO) of the service provider, who, by means of audit data, observes and analyzes the behavior of the service users, and if necessary, conducts appropriate response (see Fig. 3). The audit data is collected by the *audit component* of the service and is conveyed to the *analysis* component of the SSO (see ‘E1’ in Fig. 3). According to the *purpose of analysis*, i.e. purpose of processing, the analysis component generates *event reports* and provides them to the *response* component (see ‘E2’ in Fig. 3). The response component reacts on the event reports, for example by informing the SSO and by suggesting appropriate action. An event report can comprise an *analysis context*, which is a sub-set of the audit data. For this text we consider an intrusion detection system (IDS) as an instance of the described additional components, where the purpose of processing of the analysis component is the detection of misuse scenarios² that are caused by the service users.

Fig. 3 to Fig. 6 depict the privacy-respecting versions of the basic model (cf. Fig. 2), where user IDs are pseudonymized before they can be observed by the SSO in the audit data. The graphical elements in the figures call for some explanation. The *solid arrows* indicate the flow of accountable and certified or evidenced property statements. The *dashed arrows* indicate the flow of anonymous or pseudonymous property statements. The *dotted arrows* indicate the flow of the pseudonym mapping. Each *fat grey frame* indicates the control requirement of a certain entity w.r.t. the framed components. An entity B must not control the components implementing the interest I_A of another entity A , which is in conflict with the interest I_B of B . The *dark grey frames* represent the user’s interest in pseudonymity. Conversely, the *light grey frames* represent the SSO’s interest in accountability. Finally, the *black boxes* together implement a

² Models of misuse scenarios are activity patterns that are known to the IDS, i.e., here we consider so-called misuse detection, but not so-called anomaly detection.

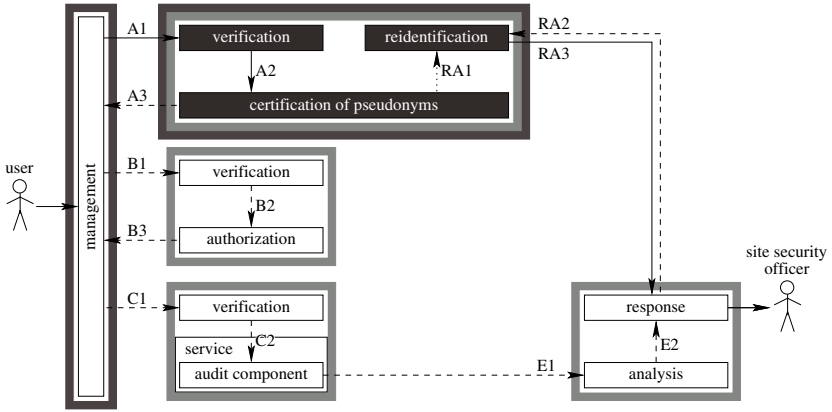


Fig. 4. Multilateral security: certification of pseudonyms

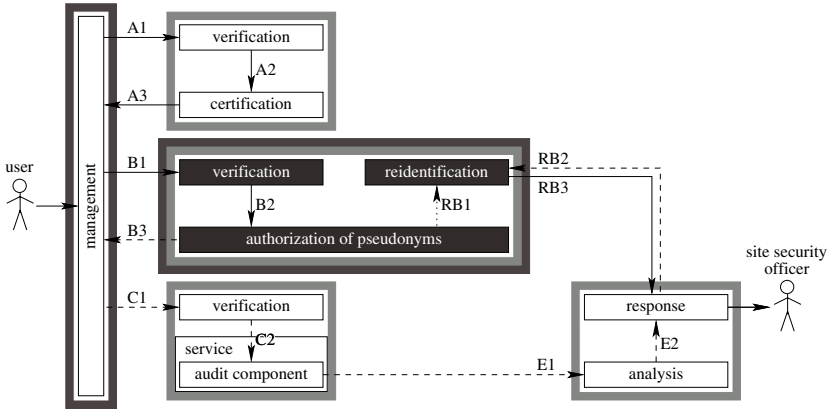


Fig. 5. Multilateral security: authorization of pseudonyms

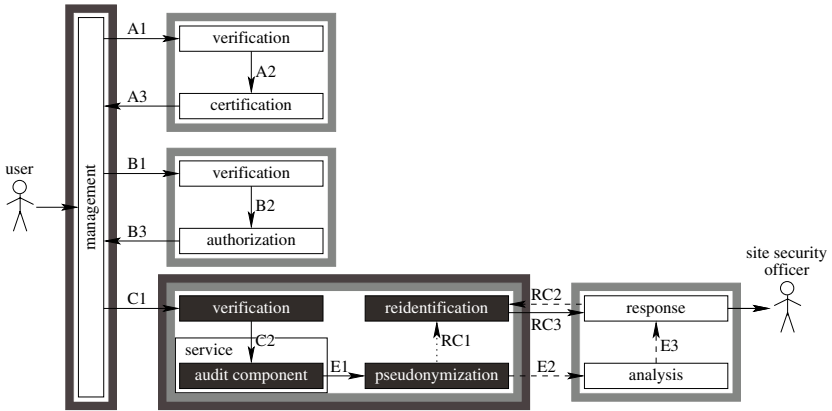


Fig. 6. Multilateral security: pseudonymization of audit data

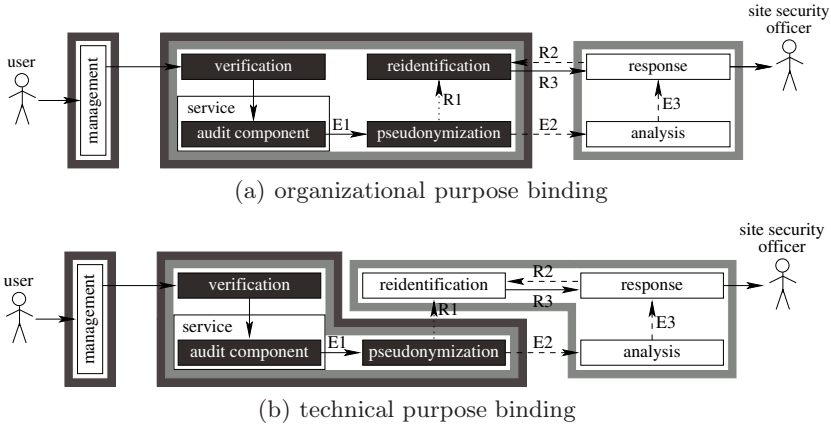


Fig. 7. Purpose binding of controlled pseudonym disclosure

function of multilateral security. Note that they are surrounded by a dark as well as by a light grey frame, i.e., the interests (pseudonymity and accountability) are clashing and need to be balanced.

A unilaterally secure architecture can be built in favor of anonymity. In such an architecture the certifier does not verify that the subject component provided by the user contains an ID which actually identifies the user (see plausibility check in Fig. 3).³ The user’s management component can then choose arbitrary pseudonyms for the property statement and the corresponding pseudonym mapping is also controlled by the user’s management component. The SSO would have to rely on the user to disclose his pseudonyms, i.e. dependable accountability is not possible.

Architectures providing multilateral security take conflicting interests into account [6], such that the entities, who pursue the conflicting interests, should not be able to control the objects of interest, i.e. the pseudonyms in the property statements. Instead, for multilateral security the pseudonym mapping could be controlled by one or more agents, which the users and the SSO need to trust (see Fig. 4 to Fig. 6). The presented architectures can also be adapted to the variants mentioned in Sect. 2 [5].

The architectures depicted in Fig. 4 to Fig. 6 only make use of pseudonyms with disclosure subject to organizational purpose binding. Fig. 7 shows for the architecture with audit data pseudonymization at the service layer,⁴ how the control requirements can be relaxed by using technical purpose binding for pseudonym disclosure, instead of organizational purpose binding.

For technical purpose binding the pseudonym mapping is provided to the re-identifier in a protected form (see ‘R1’ in Fig. 7b). Additionally the pseudonymous audit data is supplemented with information needed to neutralize the protection

³ Note, that this is actually the case for many web-based services on the Internet.

⁴ Technical purpose binding is also possible in the certification and authorization layers of the model, but yields varying benefit (see Sect. 5).

of the pseudonym mapping (see ‘E2’ in Fig. 7b). Due to the nature of the protection of the pseudonym mapping, reidentification is only possible in accordance with the a priori defined purpose of controlled pseudonym disclosure. As a result, the user does not need to trust the entity any more, which controls the reidentification component. Hence, the SSO may control the reidentification component and may disclose pseudonyms in a timely and autonomous fashion, as soon as the respective purpose permits.

5 Comparing Architectures

Fig. 3 to Fig. 6 depict the different phases or layers where pseudonyms can be introduced in the model, such that the analysis component works only on pseudonymized audit data. Introducing pseudonyms in a given layer or phase has specific benefits and disadvantages, which are investigated in the following and summarized in Table 1.

Table 1. Summary of architecture properties, grouped by relation to the issues of trust, security and cost of deployment. Each criterion can be ‘√’=met, ‘-’=not met, or ‘%’=irrelevant in the given context.

property criteria	pseudonymizing entity			
	management	certifier	authorizer	service
multilateral security	-	√	√	√
independence of service	√	√	-	-
dependable attributes	-	√	√	%
technical purpose binding	-	-	√	√
verifiability of pseudonyms b.a.	√	√	√	-
independence of user	-	-	-	√
independence of infrastructure	√	-	-	√

In the model can *multilateral security* only be supported by entities which do not pursue one of the conflicting interests that they are supposed to balance.

Even if an entity does not itself pursue a certain security objective, the organization it is affiliated with and which it depends on still can pursue a certain security objective. Due to the dependence on an organization, the entity’s activity could be biased in favor of the organization’s interests. In the physical world, one hopes to avoid the problem of biased decision-making by conceding an elected person a secure position within the organization, such that he can make decisions that are in conflict with the organization he depends on, without thereby threatening his own employment (see *independence of service* in Table 1). As an example, such a position has been created by the German labor law for the works council and by the German privacy law for the privacy commissioner.

Depending on which entity responsibly certifies a pseudonymous property statement, can the evaluating party rely on the statement, i.e. that the respective entity or person actually enjoys the certified properties. From the perspective of

the service provider an agent, which pursues the security objectives of the service provider, can be trusted to provide *dependable attributes* in property statements.

While in Sect. 4 *technical purpose binding* of pseudonym disclosure is described for audit data, in principle it can also be realized for the authorizer. Considering technical purpose binding for the certifier, one has to bear in mind that a given certificate is used to acquire authorizations for various services with various purposes for processing and for audit data analysis. The pseudonyms and the respective technical purpose binding would have to support all of these anticipated purposes for disclosure as well as linkability. This would come along with a massive erosion of the pseudonymity of the respective certificates, such that it seems inappropriate to realize technical purpose binding for pseudonymizing certifiers.

As long as pseudonyms are introduced before the service access phase, the service can verify the pseudonymous authorization and the properties of the pseudonyms (see *verifiability of pseudonyms b.a.* in Table 1). Service requests with invalid pseudonyms can be detected by the service’s verification component and can be rejected to avoid losses.

If the pseudonymization does not rely on a software component that is controlled or operated by the user, the pseudonymization is said to be *independent of the user*. On the one hand, this leaves the user out of the control loop, and he can independently take additional measures. On the other hand, the service provider is anyway obliged to comply with the privacy law and cannot shift this obligation to the users [5]. Moreover, a software component, which needs to be made available to the user, generates additional cost.

The architectures based on certificates and authorizations require trustworthy agents for certification and authorization, respectively. The effort for establishing such an infrastructure must not be underestimated. Independence of infrastructure therefore is in the interest of a quick and cost-efficient deployment of anonymity or pseudonymity.

6 Mapping Existing Architectures to the Model

In the following, for each of the pseudonymizing entities in Table 1, exemplary privacy-enhancing technologies (PETs) are mapped to the model proposed in Sect. 4. The selection does not claim to give a comprehensive or representative survey over PETs. Rather the intention is to give an impression how the model can be used to classify PETs in the context of authorization.⁵

6.1 Architectures with Pseudonymizing Management

Identity management components installed on the user’s personal device (e.g. personal digital assistant, PDA) assists the user with creating and selecting his partial identities or identity profiles, which contain property statements.

⁵ The selection intentionally does not cover all possibilities for acting pseudonymously or anonymously, for example anonymous publishing, anonymous elections, anonymous auctions, anonymous (peer-to-peer) file-sharing, Private Information Retrieval (PIR) and its applications are not considered.

Instead of locating this functionality on the user device, it can also be located at one or more third parties, also denoted as *infomediaries*, which the user trusts [10], such as Proxymate a.k.a. Lucent Personalized Web Assistant (LPWA) [11, 12].

Property statements to be sent out are selected, e.g. using P3P, by matching the security requirements and the privacy policy of the given recipient to the privacy requirements tied to the partial identities defined by the user, while considering the actual situation in which the user acts [12, 13]. In analogy to the trust evaluation carried out by the recipients of property statements, the user's management component evaluates the trust w.r.t. the recipient's privacy policy, before selecting and sending a property statement.

6.2 Architectures with Pseudonymizing Certifier

To effectively provide anonymous communication in distributed systems, personally identifying data must be avoided in all layers of the OSI reference model. Hence, anonymous services in the application layer require additional services that provide for anonymous communication. Secure anonymous communication services may also support conditional anonymity [14]. As an example, Mix systems distribute the trust, which the user needs to invest, over several autonomous parties. There are various implementations of Mix systems: Onion Routing/TOR, Hordes, Freedom Network, JAP, Babel and Mixmaster-Remailer. Crowds and Cypherpunk-Remailer are based on similar concepts. Simpler systems, which do not distribute the necessary trust, are or were for example Anonymizer.com, Anonymouse and Anon.penet.fi. Surveys of these technologies have been published by several authors [15, 16, 17, 18, 19].

Anonymous or pseudonymous credentials are introduced as anonymous or pseudonymous property statements in Sect. 4. The literature offers various approaches for implementation [20, 21, 22, 23, 24, 3, 25].

Verifying anonymous or pseudonymous property statements comprises anonymously or pseudonymously authenticating the presenting party (see authenticity component in Sect. 2). There are several proposals for authentication technology subject to controlled identity disclosure [26, 27, 28], or at least with strong mechanisms to discourage the unauthorized sharing of pseudonyms with other users [29]. Anonymous authentication is frequently realized using group signatures.

Fair electronic offline cash usually provides for controlled identity disclosure subject to technical purpose binding in the case that someone spends a given electronic coin more than once (commonly denoted as *double spending*) [17, 30, 31, 32, 33, 34].

For the privacy-enhanced intrusion detection system ANIDA the *Kerberos authentication server* was conceptually extended to use pseudonyms with controlled disclosure subject to organizational purpose binding [35].

6.3 Architectures with Pseudonymizing Authorizer

Anonymous credentials, coins and anonymous authentication may also be employed for authorizers (cf. Sect. 6.2). We give only two examples. Based on the

fair electronic coins of Chaum et al. [36] Internet dial-in users can anonymously log-in to dial-in access points of their Internet providers [37]. A similar approach was proposed as a payment system for wireless LAN Hotspots [38].

Serial transactions can be authorized in a completely unlinkable fashion by extending the validity of one-show credentials at each use for the following transaction only [39].

Büschkes and Kesdogan also proposed a second approach to privacy-enhanced intrusion detection, where the *Kerberos ticket granting server* is complemented with a multilaterally secure Mix [35].

6.4 Architectures with Pseudonymizing Service

In the following is only personal data considered that has already been collected by a service in the form of audit data for misuse detection. When considering service-side anonymization or pseudonymization, it is useful to keep the criteria summarized in Table 1 in mind. To be able to react timely on detected misuse, a timely pseudonym disclosure is desirable, preferably without the need to involve third parties. This can be realized using technical purpose binding of pseudonym disclosure. Also, the solution should be practical and independent from users and expensive infrastructures. As shown in Table 1 these requirements can only be simultaneously met at the service layer. In the following, approaches for anonymization or pseudonymization of audit data at the service layer are summarized.

In her seminal work on *Intrusion Detection and Avoidance* (IDA) Fischer-Hübner proposed the concept of misuse detection using pseudonymized audit data [40, 41]. The concept of pseudonymized audit data for misuse detection is used by Sobirey, showing that it is workable with operational intrusion detection systems. The IDA concepts have been integrated with the fully working IDS *Adaptive Intrusion Detection* (AID) [42]. Lundin developed a simple pseudonymizer for the audit data of an operational firewall, to be able to legally use the pseudonymized audit data for intrusion detection experiments [43]. Rieck developed the pseudonymizer *bsmpseu* to pseudonymize Solaris BSM audit data, which was used for intrusion detection experiments. We introduced an approach for pseudonymizing audit data for misuse detection in a multilaterally secure way, where the controlled pseudonym disclosure and pseudonym linkability are subject to technical purpose binding [2].

Further approaches to pseudonymizing audit data are known for web server log files that are aggregated for statistical purposes, e.g. [44], and for network traffic traces, which need to be shared for research purposes, e.g. [45].

7 Related Work

Other approaches or models have been proposed to describe anonymous or pseudonymous authorizations. In the following they are briefly outlined and mapped to our model.

The Dutch privacy authority *Registratiekamer* together with the information and privacy commissioner of Ontario, Canada, developed a model for information systems with a focus on privacy [8]. Based on this model, the authorization process, including the respective audit data, is described in analogy to the architecture, where the service holds the property statements, such that no further responsible agents are needed and the service needs not to verify the validity of the property statements [5]. Accordingly, the users merely obtain references to the statements about their properties. A so-called *Identity Protector* can be placed at several locations in the model. The Identity Protector acts as a pseudonymizing entity which separates components where user IDs are known from components, where merely the respective pseudonyms are processed. For each proposed placement of the Identity Protector the resulting architecture is described by van Rossum et al. [8], however without distinguishing the respective properties and specifying the control requirements. The Identity Protector corresponds to the management component in our model, when implemented near the user, i.e., in between of the user representation and the service. It corresponds to the certifier or authorizer when implemented as a third party between the user representation and the service. Finally, the Identity Protector corresponds to an audit data pseudonymizer, when implemented between the service representation and the audit data.

Alamäki et al. define various functional components (*Profile Broker*, *Identity Broker*, *Authenticator*) that are required for architectures for anonymous or pseudonymous authorizations [46], however without distinguishing the respective properties and specifying the control requirements. Identity Brokers are defined as entities which introduce pseudonyms, and Profile Brokers are user profile access points, where user profiles correspond to the attributes of property statements in our model. Profile Brokers can be complemented with Contract Brokers, which verifiably negotiate the mutual requirements of users and services w.r.t. disclosure of user profiles. In our model these brokers may be part of the user-side management component.⁶ Alternatively the Identity Broker may reside at the certifier or authorizer.⁷ Alamäki et al. define Authenticators as entities which provide for the authentication of users, which corresponds to the authentication part of the verification boxes in our model (see Fig. 1).

A recent approach describes *Privacy-enhancing Identity Management* (PIM) [12], where the user decides on his discretion, who can get which of his personal data, and where the user can separate his activity in different spheres, such that different addressees of his activity may have a different view of the partial identities (personae) of the user. PIM comprises the applications, the middleware and the communication infrastructure [12]. At the application layer the identity manager of the user (cf. management in our model) and the service provider (cf. service in our model) negotiate the requirements for partial identities (represented by property statements in our model). Beyond anonymous authorizations this approach also addresses e-commerce and e-government. Therefore,

⁶ Trusted Mobile Terminal in Alamäki et al. [46].

⁷ Physical Separation of Identity and Profile in Alamäki et al. [46].

PIM leverages not only pseudonymizing certifiers and authorizers (see anonymous credentials and authorizations in Sect. 6.2 and Sect. 6.3, respectively) and an infrastructure for anonymous communication (see Sect. 6.2), but also requires additional mediators or trustees for the digital exchange of goods, settling of liabilities, electronic payment (see Sect. 6.2), and finally, the delivery of physical goods in the physical world.

The above mapping shows that wrt. pseudonymous authorization existing models are subsumed by our model, while our model additionally provides advice concerning control requirements and suitability wrt. various high-level properties of authorization architectures.

8 Conclusion

In this paper we present an architecture model for secure and privacy-respecting authorizations. By generalizing the hybrid PKI model of Biskup and Karabulut [1] we firstly develop an architecture model for secure authorizations, which subsequently is extended for pseudonymity. The resulting model is more comprehensive than existing models.

With a focus on surveillance for misuse detection we identify suitable architectures and control requirements for pseudonymous authorization. Moreover, we provide criteria to determine and compare the properties of these architectures. The contribution to the area of privacy-respecting authorizations is threefold:

- The model provides a systematic view on architectures for secure and privacy-respecting authorizations, as well as on their generic high-level properties.
- Starting from a set of required properties it allows to compare and select suitable architectures, either for designing authorization systems from scratch, or to guide product selection.
- For each architecture the control requirements are made explicit, such that they can be taken into account during design, or can be used to verify the appropriateness of control conditions in products.

References

- [1] Biskup, J., Karabulut, Y.: A hybrid PKI model with an application for secure meditation. In: Sheno, S. (ed.) Proceedings of the 16th Annual IFIP WG 11.3 Working Conference on Data and Application Security, Cambridge, England, July 2002, pp. 271–282. Kluwer, Dordrecht (2002)
- [2] Flegel, U.: Pseudonymizing Unix log files. In: Davida, G.I., Frankel, Y., Rees, O. (eds.) *InfraSec 2002*. LNCS, vol. 2437, pp. 162–179. Springer, Heidelberg (2002)
- [3] Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Pfitzmann, B. (ed.) *EUROCRYPT 2001*. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
- [4] Gollmann, D.: 10.2.1: Kerberos. In: *Computer Security*, pp. 168–171. John Wiley & Sons, Inc, West Sussex (1999)

- [5] Flegel, U.: Pseudonymizing Audit Data for Privacy Respecting Misuse Detection. PhD thesis, University of Dortmund, Dept. of Computer Science (January 2006)
- [6] Pfitzmann, A.: Multilateral security: Enabling technologies and their evaluation. In: Wilhelm, R. (ed.) Informatics. LNCS, vol. 2000, pp. 50–62. Springer, Heidelberg (2001)
- [7] Pfitzmann, A., Hansen, M.: Anonymity, unlinkability, unobservability, pseudonymity, and identity management - a consolidated proposal for terminology (May 2006) dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.28.pdf
- [8] van Rossum, H., Gardeniers, H., Borking, J., et al.: Privacy-enhancing technologies: The path to anonymity, vol. ii, Technical report, Registratiekamer Netherlands and Information and Privacy Commissioner Ontario, Canada, Achtergrondstudies en Verkenningen 5B, Rijswijk, Netherlands (August 1995)
- [9] Bundestag, D.D.: Gesetz über Rahmenbedingungen für elektronische Signaturen (SIGG) (in German). Bundesgesetzblatt, Teil I(1) (January 2005) 2, http://bundesrecht.juris.de/bundesrecht/sigg_2001/
- [10] Gabber, E., Gibbons, P.B., Kristol, D.M., Matias, Y., Mayer, A.: On secure and pseudonymous client-relationships with multiple servers. ACM Transactions on Information and System Security 2(3), 390–415 (1999)
- [11] Cranor, L.F.: Agents of choice: Tools that facilitate notice and choice about web site data practices. In: Proceedings of the 21st International Conference on Privacy and Personal Data Protection, Hong Kong SAR, China, September 1999, pp. 19–25 (1999)
- [12] Clauß, S., Köhntopp, M.: Identity management and its support of multilateral security. Computer Networks 37(2), 205–219 (2001)
- [13] Köhntopp, M., Berthold, O.: Identity management based on P3P. In: Federrath, H. (ed.) Designing Privacy Enhancing Technologies. LNCS, vol. 2009, pp. 141–160. Springer, Heidelberg (2001)
- [14] Köpsell, S., Wendolsky, R., Federrath, H.: Revocable anonymity. In: Müller, G. (ed.) ETRICS 2006. LNCS, vol. 3995, pp. 206–220. Springer, Heidelberg (2006)
- [15] Federrath, H.: Privacy enhanced technologies: Methods – markets – misuse. In: Katsikas, S.K., Lopez, J., Pernul, G. (eds.) TrustBus 2005. LNCS, vol. 3592, pp. 1–9. Springer, Heidelberg (2005)
- [16] Fischer-Hübner, S.: IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms. LNCS, vol. 1958. Springer, Heidelberg (2001)
- [17] Seys, S., Díaz, C., De Win, B., Naessens, V., Goemans, C., Claessens, J., Moreau, W., De Decker, B., Dumortier, J., Preneel, B.: Anonymity and privacy in electronic services (APES) Deliverable 2 – Requirement study of different applications. Technical report, K. U. Leuven (May 2001)
- [18] Goldberg, I.: Privacy-enhancing technologies for the internet, II: Five years later. In: Dingledine, R., Syverson, P.F. (eds.) PET 2002. LNCS, vol. 2482, pp. 1–12. Springer, Heidelberg (2003)
- [19] Goldberg, I., Wagner, D., Brewer, E.: Privacy enhancing technologies for the internet. In: Proceedings of the COMPCON'97, San Jose, California, USA, February 1997, IEEE (1997) <http://www.cs.berkeley.edu/daw/privacy-compon97-www/privacy-html.html>
- [20] Chaum, D.: Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms. In: Seberry, J., Pieprzyk, J.P. (eds.) AUSCRYPT 1990. LNCS, vol. 453, pp. 246–264. Springer, Heidelberg (1990)

- [21] Van Herreweghen, E.: Secure anonymous signature-based transactions. In: Goos, G., Hartmanis, J., van Leeuwen, J. (eds.) ESORICS 2000. LNCS, vol. 1895, pp. 55–71. Springer, Heidelberg (2000)
- [22] Brands, S.A.: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge, Massachusetts, USA (2000)
- [23] Glenn, A., Goldberg, I., L egar e, F., Stiglic, A.: A description of protocols for private credentials (October 2001) <http://eprint.iacr.org/2001>
- [24] Stubblebine, S.G., Syverson, P.F.: Authentic attributes with fine-grained anonymity protection. In: Frankel, Y. (ed.) FC 2000. LNCS, vol. 1962, pp. 276–294. Springer, Heidelberg (2001)
- [25] Lysyanskaya, A., Rivest, R.L., Sahai, A., Wolf, S.: Pseudonym systems. In: Heys, H.M., Adams, C.M. (eds.) SAC 1999. LNCS, vol. 1758, pp. 184–199. Springer, Heidelberg (2000)
- [26] Schechter, S., Parnell, T., Hartemink, A.: Anonymous authentication of membership in dynamic groups. In: Franklin, M.K. (ed.) FC 1999. LNCS, vol. 1648, pp. 184–195. Springer, Heidelberg (1999)
- [27] Gritzalis, D., Moulinos, K., Iliadis, J., Lambrinouidakis, C., Xarhoulakos, S.: Pythia: Towards anonymity in authentication. In: Dupuy, M., Paradinas, P. (eds.) Proceedings of the IFIP TC11 16th International Conference on Information Security (Sec’01), Paris, France, IFIP, June 2001, pp. 1–17. Kluwer Academic Publishers, Dordrecht (2001)
- [28] Hirose, S., Yoshida, S.: A user authentication scheme with identity and location privacy. In: Varadharajan, V., Mu, Y. (eds.) ACISP 2001. LNCS, vol. 2119, pp. 235–246. Springer, Heidelberg (2001)
- [29] Handley, B.: Resource-efficient anonymous group identification. In: Frankel, Y. (ed.) FC 2000. LNCS, vol. 1962, pp. 295–312. Springer, Heidelberg (2001)
- [30] Davida, G., Frankel, Y., Tsiounis, Y., Yung, M.: Anonymity control in e-cash systems. In: Hirschfeld, R. (ed.) FC 1997. LNCS, vol. 1318, pp. 1–16. Springer, Heidelberg (1997)
- [31] Camenisch, J., Maurer, U., Stadler, M.: Digital payment systems with passive anonymity-revoking trustees. In: Martella, G., Kurth, H., Montolivo, E., Bertino, E. (eds.) ESORICS 96. LNCS, vol. 1146, pp. 33–43. Springer, Heidelberg (1996)
- [32] Claessens, J., Preneel, B., Vandewalle, J.: Anonymity controlled electronic payment systems. In: Proceedings of the 20th Symposium on Information Theory in the Benelux, Haasrode, Belgium, May 1999, pp. 109–116 (1999)
- [33] Pointcheval, D.: Self-scrambling anonymizers. In: Frankel, Y. (ed.) FC 2000. LNCS, vol. 1962, pp. 259–275. Springer, Heidelberg (2001)
- [34] Nakanishi, T., Haruna, N., Sugiyama, Y.: Unlinkable electronic coupon protocol with anonymity control. In: Zheng, Y., Mambo, M. (eds.) ISW 1999. LNCS, vol. 1729, pp. 37–46. Springer, Heidelberg (1999)
- [35] B uschkes, R., Kesdogan, D.: Privacy enhanced intrusion detection. In: M uller, G., Rannenber, K. (eds.) Multilateral Security in Communications. Information Security, pp. 187–204. Addison Wesley, Reading (1999)
- [36] Chaum, D., Fiat, A., Naor, M.: Untraceable electronic cash. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 319–327. Springer, Heidelberg (1990)
- [37] Chan, Y.Y.: On privacy issues of internet access services via proxy servers. In: Baumgart, R. (ed.) CQRE (Secure) ’99. LNCS, vol. 1740, pp. 183–191. Springer, Heidelberg (1999)
- [38] Gro , S., Lein, S., Steinbrecher, S.: A multilateral secure payment system for wireless LAN hotspots. In: Katsikas, S.K., Lopez, J., Pernul, G. (eds.) TrustBus 2005. LNCS, vol. 3592, pp. 80–89. Springer, Heidelberg (2005)

- [39] Stubblebine, S.G., Syverson, P.F., Goldschlag, D.M.: Unlinkable serial transactions: Protocols and applications. *ACM Transactions on Information and System Security* 2(4), 354–389 (1999)
- [40] Fischer-Hübner, S., Brunnstein, K.: Opportunities and risks of intrusion detection expert systems. In: *Proceedings of the International IFIP-GI-Conference Opportunities and Risks of Artificial Intelligence Systems (ORAIS'89)*, July 1989, Hamburg, Germany, IFIP (1989)
- [41] IDA (Intrusion Detection and Avoidance System): Ein einbruchsentdeckendes und einbruchsvermeidendes System (in German). Reihe Informatik. Shaker (1993)
- [42] Sobirey, M., Richter, B., König, H.: The intrusion detection system AID – Architecture and experiences in automated audit trail analysis. In: Horster, P. (ed.) *Proceedings of the IFIP TC6/TC11 International Conference on Communications and Multimedia Security*, Essen, Germany, IFIP, September 1996, pp. 278–290. Chapman & Hall, London (1996)
- [43] Lundin, E., Jonsson, E.: Anomaly-based intrusion detection: privacy concerns and other problems. *Computer Networks* 34(4), 623–640 (2000)
- [44] Eckert, C., Pircher, A.: Internet anonymity: Problems and solutions. In: Dupuy, M., Paradinas, P. (eds.) *Proceedings of the IFIP TC11 16th International Conference on Information Security (Sec'01)*, Paris, France, IFIP, June 2001, pp. 35–50. Kluwer Academic Publishers, Dordrecht (2001)
- [45] Pang, R., Paxson, V.: A high-level programming environment for packet trace anonymization and transformation. In: *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Karlsruhe, Germany, ACM SIGCOMM, August 2003, pp. 339–351. ACM Press, New York (2003)
- [46] Alamäki, T., Björksen, M., Dornbach, P., Gripenberg, C., Gyórbíró, N., Márton, G., Németh, Z., Skyttä, T., Tarkiainen, M.: Privacy enhancing service architectures. In: Dingledine, R., Syverson, P.F. (eds.) *PET 2002. LNCS*, vol. 2482, pp. 99–109. Springer, Heidelberg (2003)