Computing and Informatics, Vol. 26, 2007, 105–121

BASIC PROPERTIES OF THE PERSONA MODEL

Radovan Semančík

nLight, s. r. o.
Súľovská 34
812 05 Bratislava, Slovakia
e-mail: semancik@nlight.eu

Manuscript received 12 May 2005; revised 1 February 2006
Communicated by Clark Thomborson

Abstract. This document proposes a terminology and a model for representation of user data in information systems in the form of "persona" objects. It provides the mechanisms for evaluation how the personae relate to real-world subjects or to each other. A mechanism how to evaluate some anonymity and identity properties is proposed. This paper also describes the linking of personae by the use of shared identifiers. The local, global, persistent and transient personal linking types are considered. The model is used to describe persona linking in the different practical technologies as the example of model applicability.

Keywords: Persona, identity, anonymity

1 INTRODUCTION

The interaction with computer system is an important part of our lives. The computers frequently store and use data that describe characteristics of physical persons. Yet only a few attempts had been made to provide a model that would help understand implications of personal data processing.

This paper provides a basic structure of a model that may provide insight into some of the areas that touch personal data. Some concepts in the problem area are understood only intuitively and this work attempts to provide more formalized definitions as well as putting these concepts in broader perspective.

The document describes interaction between two worlds: the *physical world* where all the tangible objects and subjects exist and the *digital world* where intangible software components interact.

2 PERSONA MODEL

The digital identity systems are focused on the properties of entities that interact in the digital world. While "native" digital entities (e.g. software components) may interact in the digital world directly, physical entities are limited only to indirect interaction. A physical entity interacts with digital entities through digital proxies, usually in the form of user terminal equipment and software. These proxy entities form a digital representation of a physical entity whose characteristics are not directly accessible to the digital world.

2.1 Persona

Persons acting as users of computer systems (physical entities) are represented in the digital world by data structures. The computer systems that are interacting with physical users have limited capabilities of determining the user characteristics directly, therefore the data structures that represent users are in common case assembled from the data entered by the users themselves. This data is seldom directly verified, although in some cases personally-identifying information about a subject is collected and stored by a third party such as a certification authority. Third party may also verify the data and make the information about this verification available in the digital world. In any event the data stored by any computer system forms only a partial representation of physical user's characteristics.

The data structure maintained in the computer system is in most cases an incomplete and possibly unreliable representation of a physical user. The data structure may not even be unique: the physical user may create a similar data structure in the same or different computer system. The user may also create several distinct data structures to represent different roles or personalities for different purposes (Figure 1).

We will use the term *Subject* for the physical user and the term *Persona* to represent the virtual data structure maintained in the computer system that is related to the physical entity:

Lemma 1 (Subject)**.** Subject is a physical person that can interact with the computer system.

Lemma 2 (Persona)**.** Persona is a (digital) data structure that represents some aspects of (physical) subject, group of subjects, or computer program. The aspects are represented as a collection of attributes with (possibly multiple) machine-readable values.

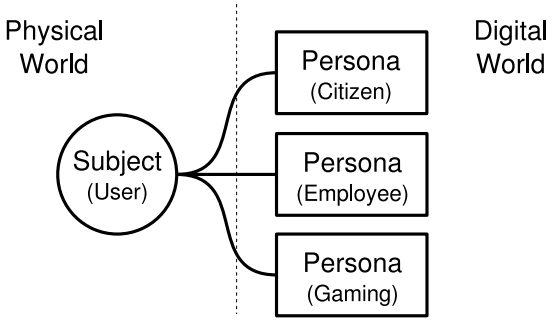

Fig. 1. User and the personae

The correspondence of the persona attributes with the characteristics of the physical subject may vary. One extreme situation may be a government-created persona to represent subject as a citizen, while the correctness of the persona attributes is verified by the official authorities. On the other end of the spectrum may be a persona created for the purpose of a computer game that will represent completely fictional character. The completeness of persona data may vary as well. Some systems will maintain only minimum information needed for correct operation, to conform with privacy legislation. Other systems may gather rather rich data records.

The persona may represent broader spectrum of entities than just physical computer users. It may also represent a physical person who never interacted with any computer system or may represent a fictional character. The persona may even represent a group of physical persons with common characteristics (e.g. a company), but in that case the group of persons is considered to be a single subject for the purpose of this paper.

The lifetime of personae may be different. Some personae will exist for a relatively long time, while other personae exist only for a limited time span. Therefore we distinguish two types of personae:

Lemma 3 (Persistent Persona)**.** Persistent persona is a persona that exists for an extended period of time. The persona data will be usually stored persistently in a computer system, such as on reliable file system or in a database. The persona must usually be explicitly deleted to end its existence. A user account in an operating system is an example of persistent persona. Persistent personae will be denoted by solid-line rectangles in this article. An example of a persistent persona is provided in Figure 2.

Lemma 4 (Transient Persona)**.** Transient persona is a persona that exists for a limited period of time. The persona data may be stored in computer systems in non-permanent memory, may be cached, etc. The transient personae usually automatically expire after a specified time. A user session in a web application is

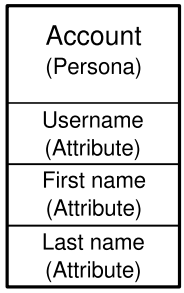

Fig. 2. Persistent Persona

an example of transient persona. Transient personae will be denoted by dashed-line rectangles on following figures.

There is no strict definition of persistence and transience of a persona, it depends heavily on the observer's point of view. The distinction is provided here only to introduce some idea of time dependencies into the model, because the model does not reflect the flow of time in any other way.

2.2 Anonymity and Identity

The persona usually originates as an entity describing one natural person (subject). But after the original creation, the link between the persona (digital entity) and subject (physical entity) may not be apparent. In privacy-enhancing applications the inability to distinguish a subject given a persona may even be crucial requirement. According to this, a mechanism is needed that will allow evaluation of relations between personae and subjects. The following paragraphs provide means that can be used for this purpose.

Lemma 5 (World Set)**.** World set is a set of all possible subjects, denoted as follows:

$$W = \{S_1, S_2, S_3, \ldots, S_n\}. \tag{1}$$

In the broadest possible model the world set will contain all subjects that can, even with negligible probability, describe any possible persona. This definition of a world set would be greatly impractical. In the practical model applications the world set would be chosen with respect to some baseline knowledge base. For example if we know that the personae in our system represent only living natural persons, we can choose the world set that contains all living natural persons. If our implementation allows only Internet-based access and thus our personae describe only the people that can access the Internet, we can choose the world set to include natural persons that are Internet users only.

Lemma 6 (Identity Probability)**.** Identity probability is a (Bayesian) probability that a given persona describes a given subject, denoted

$$i_{P,S}$$

where P is a persona and S is a subject.

Identity probability of 0 means that persona P cannot describe subject S. Identity probability of 1 means that the observer is sure that the persona describes the subject. The values between 0 and 1 may be interpreted as different degrees of belief that the persona describes the subject.

The identity probability value, as well as all other probabilistic metrics defined in the document, are subjective to a specific observer and depend on his/her knowledge. Different observers may assign different values to identity probabilities. The following statements are only expected to hold for a specific observer.

While persona describes exactly one subject (by definition), the sum of identity probabilities for specific persona and all subjects in the world set must be 1. The following holds:

$$\sum_{k=1}^{n} i_{P,S_k} = 1. \tag{2}$$

We can define a random variable I_P with the world set W as the collection of source states and with individual probabilities being equal to identity probabilities of a single persona:

$$P(I_P = S) = i_{P,S}, \forall S \in W. \tag{3}$$

The random variable I_P represents possible subjects that the persona P may describe.

Lemma 7 (Anonymity Set)**.** Given a specific persona, anonymity set (denoted AS_P) is a set of all possible subjects from the world set for which holds that the identity probability of the persona and the subject is greater that zero. Can be denoted as

$$AS_P = S : S \in W \wedge i_{P,S} > 0. \tag{4}$$

In other words, anonymity set is a set of all possible subjects that the persona may describe. In contrast to the world set, the anonymity set is based on identity probability and therefore is subjective to the observer. This definition of anonymity set is a probabilistic extension of the definition used by Pfitzmann and Khntopp [1].

Lemma 8 (Anonymity Ratio)**.** Anonymity ratio of a persona with respect to world set and observer describes the relative uncertainty in persona correspondence to a subject, defined as

$$ar(P) = \frac{H(I_P)}{H_{max}} \tag{5}$$

where $H(I_P)$ is an entropy [2] of random variable I_P, defined as

$$H(I_P) = -\sum_{k=1}^{n} i_{P,S_k} \log_2(i_{P,S_k}) \tag{6}$$

and H_max is a maximum entropy for a random variable with n states, that is

$$H_{max} = \log_2(n) \tag{7}$$

Anonymity ratio of 1 means total anonymity: the persona may describe any subject from the world set with equal probability. The anonymity ratio will be 1 if the observer cannot in any way distinguish the subject that the persona describes (the probability distribution of random variable I_P is uniform).

Anonymity ratio of 0 means no anonymity: The persona describes a single specific subject. The anonymity ratio will be 0 if the observer is sure that the persona describes a specific subject.

Lemma 9 (Identity Ratio)**.** Identity ratio of a persona with respect to world set is a probabilistic inverse of the anonymity ratio, defined as

$$ir(P) = 1 - ar(P) \tag{8}$$

The identity ratio describes the degree of observer's belief that persona P describes some specific subject. Identity ratio of 0 means no identity: the observer cannot infer any useful information about the subject that the persona describes. Identity ratio 1 means total identity: the observer is sure about the subject that the persona describes.

Exact anonymity ratio and identity ratio values may be very difficult (if even possible at all) to compute in the practice. Only the estimated values of these metrics can usually be determined. In a common case, it will be beyond the power of any observer to gather up-to-date information about all subjects in the world set. As such data is required for identity probability computation, the anonymity and identity ratios should be seen as theoretical (and subjective) values that can only be estimated in practice.

2.3 Analogy and Heterology

While anonymity and identity cannot be easily determined in computer applications, we may use other metrics that can be computed in computer environment and may provide estimations of anonymity and identity. The following paragraphs provide description of analogy and heterology relations and analogy probability value that may be used to approximate anonymity and identity in practical scenarios.

Lemma 10 (Analogy)**.** The personae are analogous if and only if the observer believes that they describe the same subject.

Analogous personae describe the same subject. These may be two accounts in different systems that belong to the same user or two database records describing the same person.

Note that the persona attributes for the analogous personae may have different values. For example one persona will provide the subject's office phone number as

a point-of-contact and another may provide his mobile phone number. Also note that it may not be necessary to identify the subject to resolve the analogy of personae – it may be apparent that the personae describe the same subject without actually knowing which specific subject they describe.

The analogy defined in this deterministic manner may not be very useful in practice. Computers usually cannot reliably distinguish if two personae are analogous, but they may provide estimation on how likely it is that the personae describe the same subject. For this reason we define the probabilistic version of analogy:

Lemma 11 (Analogy)**.** Analogy probability is a (Bayesian) probability that two personae are analogous, denoted

$$l_{P_1,P_2}$$

where P_1 and P_2 are personae.

Analogy probability can be seen as a degree of observer's belief that two personae describe the same subject. For example if two personae share the same values of first name and last name attributes, the observer may believe that these personae describe the same subject with 60% probability. Therefore the analogy probability of these personae would be 0.6.

Lemma 12 (Heterology)**.** The personae are heterologous if and only if they describe different subjects.

Heterology has features similar to analogy. For example, two personae may have the same attribute values, but yet may be heterologous (e.g. if the personae have only sex, age and city attributes) and it may not be necessary to identify the subjects to resolve heterology of personae.

Lemma 13 (Heterology Probability)**.** Heterology probability is a (Bayesian) probability that two personae are heterologous, denoted

$$h_{P_1,P_2}$$

where P_1 and P_2 are personae.

Heterology probability can be seen as a degree of observer's belief that two personae describe different subjects. For example if two personae have different values for first name and last name attributes, the observer may believe that the personae describe different subject with 90% probability. Therefore the heterology probability of these personae would be 0.9.

Two personae can only describe the same subject or two different subjects. Therefore it follows that

$$l_{P_1,P_2} + h_{P_1,P_2} = 1 \tag{9}$$

Figure 3 shows an example of anonymity, identity, analogy and heterology applied to simple structure of two subjects and several personae. The thin arrows denote data origin. For example, persona P_3 originated as a (partial) copy of P_2, that

in turn originated as a (partial) description of subject S_1 characteristics. The thick arrows denote anonymity/identity, analogy and heterology relations. For example personae P_1 and P_2 are analogous, because they describe the same subject S_1. Also the personae P_1 and P_3 are analogous. Note that it is neither required to determine relation between P_1 and S_1 nor relation between P_2 and S_1 to evaluate the analogy.

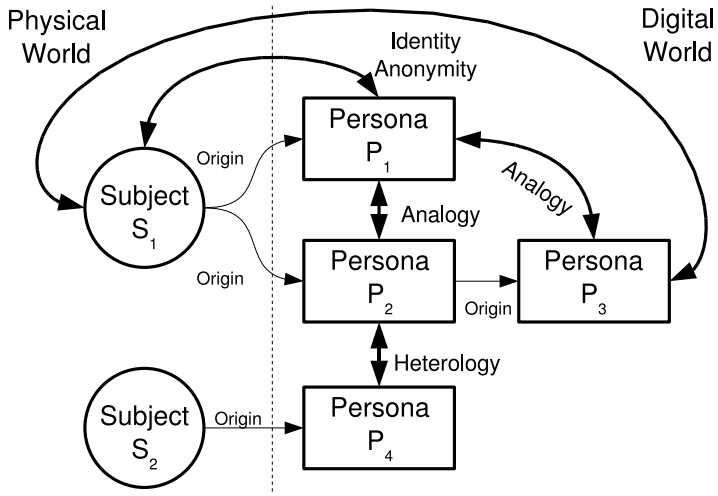

Fig. 3. Subject-Persona Relations

Analogy probability and a world set based on persona databases may provide an estimation of anonymity/identity ratio values in practice. Consider that we have a description of a specific person, specified in a digital form of "test persona". We want to estimate the anonymity ratio of this persona. We cannot do this by comparing the data in persona directly to every physical person, as that may become infeasible even for medium-sized world sets. We need to provide anonymity ratio estimation by a different method, which can be more automated easily.

Let us suppose that we have access to a government database that contains records of all registered citizens of a country. These records are personae, as they are digital representations of physical person characteristics. Instead of comparing our "test persona" to every physical person, we will compare it to the records in the database. We are in fact determining analogy probabilities of the "test persona" and the personae in the government database. We may use these analogy probabilities as an estimation of identity probability. And we may use the set of government database entries as an approximation of the world set.

We will use the terms identity, anonymity, analogy and heterology in the rest of this document to refer to both the deterministic and the probabilistic versions of these metrics. The choice of the specific approach (deterministic or probabilistic) may vary for each application of the model.

2.4 Persona Identifiers

Persona may contain several attributes that do not directly describe the characteristics of a subject, but instead of that they are used for denoting relations to other personae. These attributes are called *identifiers* and are usually unique in some specific identifier scope of validity. We will consider only one special case of identifiers: *persona identifiers*.

Lemma 14 (Persona Identifier)**.** Persona identifier is a persona attribute that uniquely identifies a persona in a given scope of identifier validity.

The identifier may be explicitly assigned to the persona (e.g. a username) or may represent its location in data structures (e.g. table index or memory address) or may have any other form. The interpretation of the identifier may not be the same for all systems. For example an identifier of a persona in one system may represent its position in the lookup table, but when shared with another system it may be seen as an opaque byte string.

The scope of identifier validity is usually limited to single system or a single set of systems; but the identifier may be used to locate or construct more than one persona in some systems. For example the same identifier may be used to construct a persona that represents UNIX account as well as a persona that represents e-mail mailbox. In this case the scope of identifier validity had to be chosen to span only a single subsystem or even a smaller part of the system.

2.5 Persona Linking

The analogy of the personae is frequently explicitly denoted. For example in Identity Management technologies it is common to group all accounts that belong to specific physical user. Similar approach is applied in Single Sign-On systems and it is also used for user management in distributed systems.

The centralization of user data on a single place is seldom an option. Even in relatively tight-coupled distributed systems the persona data is replicated and cached in system modules, thus effectively creating new personae. For the system to work efficiently it has to keep track of the persona relations. That essentially means denoting persona analogy, usually using persona identifiers for that purpose. We define this approach as persona linking:

Lemma 15 (Persona Link)**.** Persona link is an analogy between personae denoted by using persona identifiers.

In contrast with the *identifier* which represents an attribute value, the *link* represents the analogy relation. When an observer sees linked personae, he can trivially determine the analogy of these personae by comparing persona identifiers. Although the link is usually created intentionally for the specific purpose of indicating an analogy, it may also be a side-effect of other operations with the personae. For example

the link may be unintentionally created by sharing an e-mail address with a persona in a remote system.

The persona link may fall into a different set of categories, depending on the link identifier applicability and lifetime. The link may be either global or local, depending on scope of identifier applicability, or the link may be persistent or transient depending on the duration of identifier validity. These two properties are combined to describe a link type (e.g. "global persistent link").

The sections and figures below describe different types of persona linking and illustrate them with examples. The solid lines are used in the figures to denote persistent elements, while dashed lines are used to show transient elements.

2.5.1 Global Link

Global persona link is a situation, when one identifier is shared by more than two personae (Figure 4). All personae sharing the common identifier are linked, regardless of the time and space history of the link. For example when linking one persona with another by copying the shared identifier, the new persona is automatically linked with all other personae sharing the same identifier. In common case the controller of a newly linked persona may not have comprehensive knowledge of all others personae that are linked.

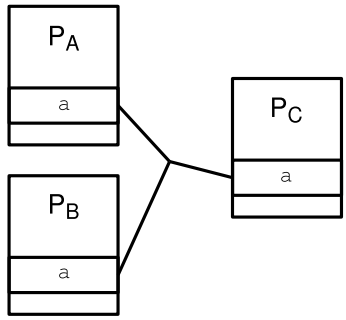

Fig. 4. Global persona link

2.5.2 Local Link

Local persona link is a situation when an identifier is shared by exactly two personae (Figure 8). Only these two personae are linked. When more than two personae have to be linked, more than one link is needed. Each time two personae are linked, new identifier has to be created for the use by that link only. The link identifier cannot be shared with other personae, failing this the situation will revert to global link. This is also the case when sharing other persona attributes that can be used as identifiers to link more than the two already linked personae.

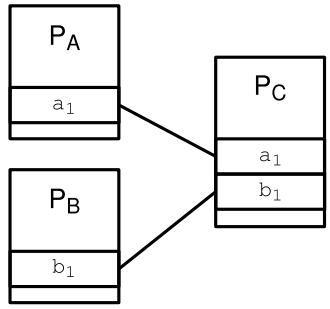

Fig. 5. Local persona link

2.5.3 Persistent Link

Persistent link is a link that is valid for an extended period of time. The link lifetime spans several user sessions and is typically maintained until the linked personae exist.

The persistent link can be efficiently terminated only by changing all but one link identifiers of the linked personae. The termination of a persona may not reliably terminate the link, if that persona may be re-created in the future with the same identifier.

2.5.4 Transient Link

Transient link is a link that is valid for a short period of time. The link lifetime is usually limited to a single user session. When a transient link is re-created to link the same personae, it cannot be decided if and how the same two personae were linked before. For example if a link is created for two personae for the duration of a session, in the next session it cannot be distinguished if it is a session for the same returning user or if it is a different user.

Transient link is usually implemented by creating a random identifier that is discarded when the link expires; but if a persistent attribute exists in one of the linked personae that may be used to correlate it to the other persona, that attribute can be used to determine the analogy of the personae even between several user sessions. In this case, even if the link is transient, the analogy of the personae can be decided beyond the purpose of the transient link (Figure 6 a)). For example a user wants to anonymously use an website using a transient persona (P_T) linked by transient identifier t to the source persona (P_A). But the source persona reveals a persistent attribute x (e.g. an e-mail address) that the target site may use to find the "real" persistent persona (P_B) in its databases and to determine analogy of P_T and P_B ($l_{P_T,P_B} \approx 1$) and therefore to reveal a part of subject's identity that was supposed to be hidden.

A similar situation can be observed if any attribute of a linked persona can be persistently modified by another system. That attribute can be used to set

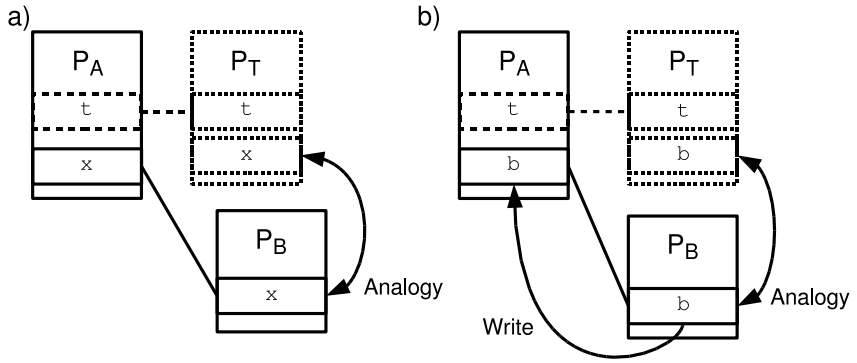

Fig. 6. Transient link reverting to persistent link

a persistent link identifier that may be used to determine an analogy of transient persona (Figure 6 b)).

3 APPLICATION OF THE MODEL

In this section we provide examples of the application of our model. Three systems from different categories are selected to illustrate the breadth of applicability of our model, and the properties that can be inferred about a system given only its description in our model.

The model does not provide sufficient means to describe time-based traceability of personae. That means that the model only describes personae in a specific moment of time and its ability to describe personae histories is very limited.

On the other hand, the model might provide means to describe space-based traceability of personae and persona relations. However, this is out of scope of this document and will require further study. Some of the means for inferring space-based traceability are outlined in following sections.

3.1 Centralized Security Domain

The security domain will usually maintain a centralized database of accounts that is used to construct primary domain personae. The personae will have a primary identifier that is unique for the domain (global identifier in the domain scope, usually username or directory distinguished name). The domain controller will implement a "persona service" (for example a directory service), that may be used to access the persona attributes. Similar personae will exist on the systems in the security domain, either persistent (accounts) or transient (service state). All the accounts in the security domain share the same global identifier (Figure 7), therefore the persona linking is of global persistent (accounts) or global transient type (services).

The systems that have access to the domain database can trivially determine analogy of the "domain" personae with local personae. This can enable the use of so-called identity services such as centralized user management and single sign-on.

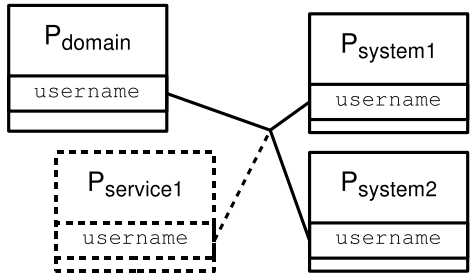

Fig. 7. Centralized security domain

3.2 Public Key Infrastructure and Digital Credentials

The range of designs loosely referred to as a Public Key Infrastructure is a set of mechanisms based on the X.509 [3] specification for digital certificates. The purpose of the original X.509 design was to cryptographically bind directory identifier (distinguished name, dn) to the entity's public key to allow authentication. The directory identifier (dn) was supposed to be globally-unique and might be used to de-reference the subject record in the directory service. This approach can be described as global persistent persona linking and is illustrated in Figure 8.

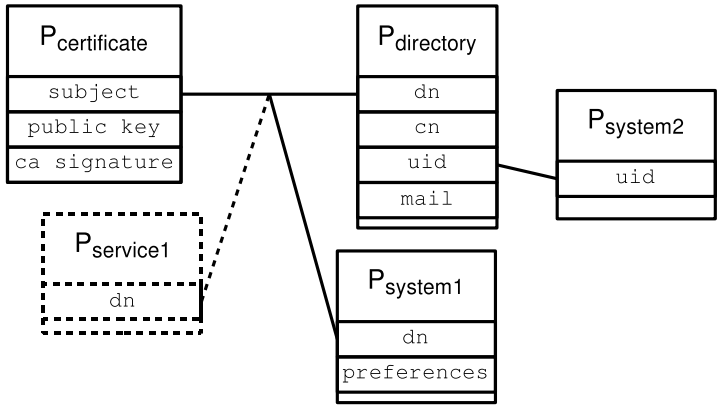

Fig. 8. X.509 PKI original design (directory-oriented)

The original X.509 design is not strictly followed by some applications and the directory identifier (*dn*) is frequently used to store generic attribute-value pairs,

where the *Common Name* (*cn*) field is used as a local entity identifier. There also may be additional attributes in the X.509 public key certificate extensions, as specified by the certificate profile (e.g. [4]). This extended public key certificate can be seen as a stand-alone persona that is linked by global link to other personae (Figure 9).

The distinction of directory-oriented and directory-less X.509 PKI deployments is the existence of the "directory persona" (denoted $P_{directory}$ in Figure 8). This persona stores most of the attributes and may enforce access control on these attributes. It may for example provide identifiers that link "directory persona" to personae in other systems ($P_{system2}$ in Figure 8). In directory-less deployments there is no option to enforce access control on the attributes included in the certificate. The X.509 public key certificate is presented to the relying party in the clear, the attributes are only protected for integrity and are not encrypted. The only options are to show the entire certificate with all attributes or not to show the certificate at all.

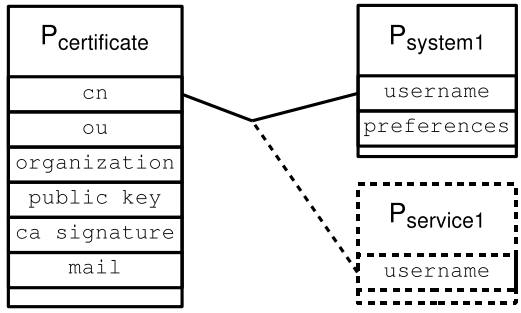

Fig. 9. X.509 PKI directory-less scenario with persona identifier in "cn" attribute.

The primary difference between the directory-oriented and directory-less X.509 scenarios from the point of view of the model is in the attribute access control properties. In the directory-oriented scenario the directory server that stores Pdirectory persona can enforce access control rules to access persona attributes. Therefore an observer who is not in control of the directory server can detect that the personae are analogous, but s/he cannot access any additional $P_{directory}$ persona attributes (except these attributes that are allowed by directory server administrator). On the other hand, in the directory-less scenarios, all persona attributes are stored in the certificate and no attribute access control can be enforced in this case. Anyone that gets the certificate will automatically learn all the $P_{certificate}$ attribute values.

The X.509-based systems generally use global identifiers even in directory-less deployments. Even if no explicit persona identifier is used in the certificate attributes, the subject's public key or the issuer's signature may be used as a globally-unique identifier (Figure 10). Due to their all-or-nothing access-control property, the systems using long lived public key certificates must be considered as persistent global persona linking systems. X.509 certificates cannot be used to define local

links unless a separate certificate is provided for each link. Such approach may be infeasible for most systems, unless certificate issuing procedures are greatly modified.

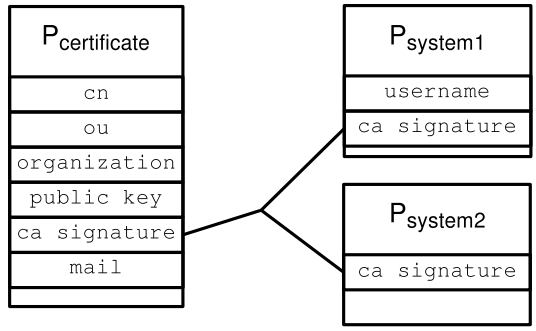

Fig. 10. Linking of Certificate Authority signatures in certificates.

Digital Credentials [5] is a cryptographic technique that addresses some of the drawbacks of X.509-based PKI. The Digital Credential system allows the selective disclosure of attributes in the digital credential and also provides for so-called "zero-knowledge proofs" of some attribute properties without revealing the attribute value. It eliminates the PKI all-or-nothing disclosure drawback and the traceability of issuer's digital signature by the credential authority; but from the persona linking point of view all other properties are similar to the X.509 PKI case, if a single digital credential is used by each subject. The credential authority signature in the digital credential can be used as a globally-unique identifier and can be used to infer persona analogy. Therefore the use of digital credential system with a single digital credential per user must be regarded as a global persona linking system. This may be addressed by the use of multiple digital credentials for the same persona to implement local persona linking system, but no complete proposal of such a system was available to the date of this writing.

3.3 Internet Digital Identity Systems

The goal of a Digital Identity system is to transfer a user's identifiers, attributes and current authentication status from a source site (an Identity Provider) to a destination site (a Service Provider). Most Internet Digital Identity systems follow the proxy-based true Single Sign-On model [6] to transfer the authentication status. The SSO model is usually extended to transfer additional attributes as well. The common drawback of such systems is the traceability of user sign-ons on target systems (service providers) by the source system (identity provider).

As an example of Internet digital identity system we consider the Liberty Alliance Federation Framework (Liberty ID-FF). The Liberty ID-FF specification set [7] is a product of the first phase of the Liberty Alliance Project. It defines a Single Sign-On system with support for federated identities. The Liberty ID-FF

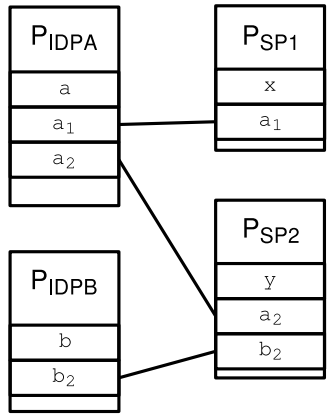

Fig. 11. Liberty ID-FF

uses Security Assertion Markup Language (SAML) [8] assertions as a security token. It supports pseudonymity [1] as a default behavior by using persistent local persona linking. Persona identifiers for target systems (NameIdentifier tag in SAML assertions) are required to be pseudo-random values that have no discernible correspondence with the original persona identifier. The linking itself is carried out by associating the randomly-generated pseudonyms, not primary persona identifiers, as illustrated in Figure 11.

The picture shows that the propagation of links (the identifiers that are used for linking) is limited. For example if an observer controls both the P_{SP1} and P_{SP2} personae, s/he cannot decide if these personae are analogous. The observer also needs to control the P_{IDPA} persona to resolve the analogy of P_{SP1} and P_{SP2}. The same thinking can also be applied for an observer who controls P_{IDPA} and P_{IDPB} personae.

4 CONCLUSION

The persona terminology and model was introduced in this work. The model can be used to describe the use of user data (and other user-like data) in computer systems. The definition of anonymity and identity properties was provided, based on (Bayesian) probability values and entropy of random variables. The hypothesis that the identity and anonymity concepts cannot be directly used by computer system was stated. The analogy and heterology concepts were proposed as a replacement for identity and anonymity in computer systems.

The proposed model also describes the methods of linking personae by the use of identifiers. The global and local persona linking was introduced as well as persistent and transient persona linking. The basic properties or these linking methods and the circumstances of one method reverting to the other were also described.

The application of the model on a common persona linking scenarios was provided as an example of model's applicability. The model was applied on to the most simple scenarios and its applicability for complex system is yet to be proven. The model was developed with the goal of providing an ability to describe at least some privacy properties of computer system; but such an application is out of scope of this document and would require further work.

REFERENCES

[1] Pfitzmann, A.—Kohntopp, M.: Anonymity, Unobservability, Pseudonymity, and Identity Management A Proposal for Terminology. Designing Privacy Enhancing Technologies, International Workshop on Design Issues in Anonymity and Unobservability, 2000.

[2] Shannon, C. E.: A Mathematical Theory of Communication. Bell System Technical Journal, Vol. 27, 1948, pp. 379–423, 623–656.

[3] Information Technology – Open Systems interconnection. ITU-T Recommendation X.509, 2000.

[4] Housley, R.—Ford, W.—Polk, W.—Solo, D.: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 2459, Internet Engineering Task Force, 1999

[5] Brands, S.: Rethinking Public Key Infrastructures and Digital Certificates. MIT Press, 2000, ISBN:0-262-02491-8.

[6] Pashalidis, A.—Mitchell, C.: A Taxonomy of Single Sign-On Systems. Information Security and Privacy, ACISP, 2003.

[7] Cantor, S.–Kemp, J.: Liberty Bindings and Profiles Specification. Liberty Alliance Project Specification, 2003.

[8] Maler, E.—Mishra, P.—Philpott, R. et al.: Assertions and Protocol for the OASIS Security Assertion Markup Language. OASIS Standard, 2003.

Radovan Semančík graduated from the Slovak Technical University with a degree in software engineering. Currently he works as a software architect and information security specialist at nLight, s. r. o, Bratislava, Slovakia. His main areas of interest include digital identity, distributed systems architecture and information security.