Detlef Hühnlein

Identitätsmanagement

Eine visualisierte Begriffsbestimmung

Vor dem Hintergrund aktueller Entwicklungen in Politik, Wirtschaft und Verwaltung gewinnt sowohl die Nutzung als auch das Management elektronischer Identitäten zunehmend an Bedeutung. Um die Erörterung dieses wichtigen Themas zu erleichtern, werden in diesem Beitrag wesentliche Begriffe des *Identitätsmanagements* in Form eines Glossars zusammen getragen.

Für den kompakten Überblick über die Thematik und zur Beleuchtung der Zusammenhänge wird hierfür in Abbildung 2 auch eine „Begriffslandkarte" in einer an die Klassendiagramme der UML (vgl. **[UML]**, Abschnitt 5.19) angelehnten Notation bereit gestellt.

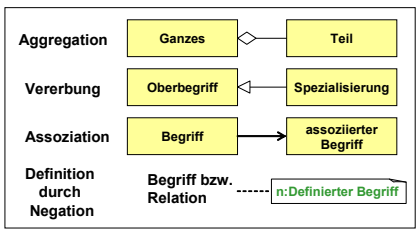
Für die graphische Darstellung der Zusammenhänge zwischen den Begriffen werden die folgenden Beziehungselemente mit der in Abbildung 1 dargestellten graphischen Notation verwendet:

- *Aggregation* – verdeutlicht, dass der eine Begriff ein Teil des anderen Begriffes (Ganzes) ist.
- *Vererbung* – gibt an, dass der eine Begriff eine Spezialisierung des anderen Begriffes (Oberbegriff) ist.
- *Assoziation* – gibt an, dass eine gerichtete Beziehung zwischen den beiden Begriffen existiert.
- Außerdem wird durch n:… angegeben, dass sich ein Begriff durch Negation eines anderen Begriffes bzw. einer Relation zwischen zwei Begriffen definiert.

Dr. Detlef Hühnlein

ist seit mehr als zehn Jahren bei der secunet Security Networks AG – u.a. im Bereich Identitätsmanagement – tätig.
E-Mail: detlef.huehnlein@secunet.com

Abbildung 1



Index

Glossar

Die Erläuterung dieser „Begriffslandkarte" erfolgt durch die schrittweise Einführung der entsprechenden Begriffe.
Eine alphabetische Liste der Begriffe mit entsprechenden Verweisen findet sich schließlich im nebenstehenden Index.

1 Entität

Eine **Entität** ist eine (natürliche oder juristische) Person oder ein Objekt (z.B. eine technische Komponente, ein Dienst, Daten etc.), das durch seine *Attribute* charakterisiert wird (vgl. **[ModTerm]**).

2 Attribut

Ein **Attribut** ist eine bestimmte, mit einem Namen versehene, Eigenschaft einer *Entität*.

3 Identität

Die **Identität** einer *Entität* ist bestimmt durch die Menge ihrer *Attribute*, wobei eine *Entität* genau eine *Identität* besitzt (vgl. **[ModTerm]** und *Partielle Identität*).

4 Identifizierung

Identifizierung bezeichnet den Vorgang unter Verwendung von behaupteten oder beobachteten *Attributen* zu bestimmen, um welche *Entität* es sich handelt (vgl. **[ModTerm]**).

5 Anonymität

Anonymität bedeutet, dass die *Identifizierung* einer *Entität* in einer Menge von

möglichen *Entitäten*, der so genannten Anonymitätsmenge, nicht durchgeführt werden kann (vgl. [**ModTerm**] und [**PfHa07**]).

6 Partielle Identität

Eine **partielle Identität** ist eine bestimmte Untermenge von *Attributen* einer *Entität*, die einem kommunikativen Kontext zugeordnet ist (vgl. [**ClKö01**], [**ModTerm**], *Differentielle Identität*, *Föderierte Identität* und *Identität*).

7 Elektronische Identität

Eine **elektronische Identität** ist eine elektronische Repräsentation einer *partiellen Identität* (vgl. [**ModTerm**]).

8 Identifikator

Ein **Identifikator** besteht aus mindestens einem *Attribut* und bezeichnet eine *Entität* in einem bestimmten Kontext eindeutig (vgl. [**ModTerm**]). Ein Identifikator ist auch ein Teil einer *elektronischen Identität* und Bestandteil der *Behauptung* bei der *Authentisierung*.

9 Realer Name

Der **reale Name** einer natürlichen Person umfasst die Vornamen und den Familiennamen sowie ggf. frühere Namen (z.B. Geburtsname).

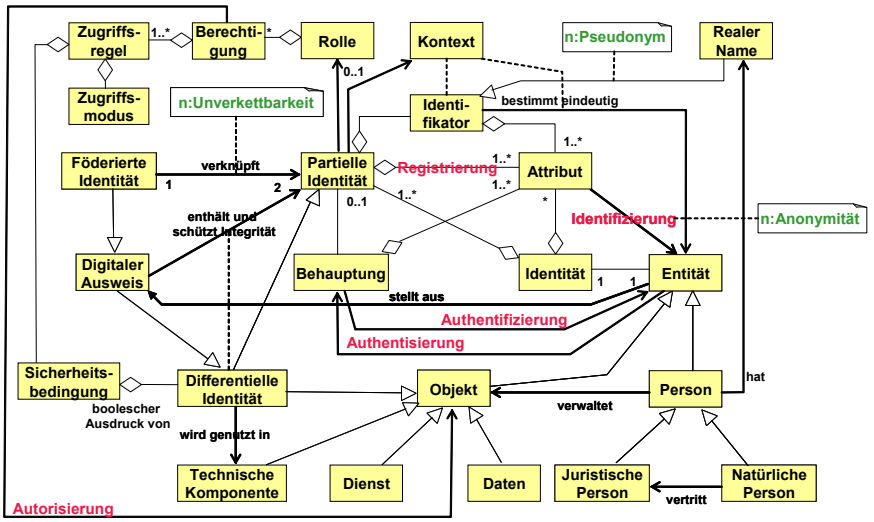
Künstlernamen bzw. Ordensnamen, die zwar gemäß § 2 [**MRRG**] im Melderegister oder gemäß § 2 [**PersAuswG**]) im Personalausweis vermerkt sind und deshalb Teil der *zivilen Identität* sein können sind jedoch nicht Bestandteil des realen Namens, sondern vielmehr *Pseudonyme*.

Der reale Name einer juristischen Person ist im entsprechenden staatlichen Register (z.B. Handelsregister, Vereinsregister) vermerkt bzw. geht bei Körperschaften und Anstalten öffentlichen Rechts aus den konstituierenden Rechtsvorschriften hervor.

10 Pseudonym

Ein **Pseudonym** ist ein *Identifikator* einer *Entität*, der ungleich seinem *realen Namen* ist (vgl. [**PfHa07**] und [**ModTerm**]).

Abbildung 2 | Wesentliche Begriffe des Identitätsmanagements und ihre Abhängigkeiten



11 Registrierung

Die **Registrierung** (engl. Registration oder Enrolment) einer *Entität* ist ein Vorgang, bei dem die *Entität identifiziert* wird und/oder *Attribute* der *Entität* überprüft werden. Als Ergebnis der Registrierung wird der *Entität* eine *partielle Identität* für einen bestimmten Kontext zugewiesen (vgl. [**ModTerm**]).

12 Behauptung

Eine **Behauptung** (engl. Claim oder Assertion) besteht mindestens aus einem *Attribut* und ist abhängig von der Betrachtungsweise eine von einer *Entität* abgegebene Erklärung (vgl. [**WS-Security-1.1**]) oder eine über eine *Entität* getätigte Aussage (vgl. [**WS-Trust-1.3**]).

Insbesondere kann eine *partielle Identität* Gegenstand einer Behauptung sein. In diesem Fall bezeichnet man das Aufstellen der Behauptung als *Authentisierung* und das Überprüfen einer solchen Behauptung als *Authentifizierung*.

13 Authentisierung

Authentisierung ist das Aufstellen einer *Behauptung* über eine *partielle Identität*.

14 Authentifizierung

Authentifizierung ist das Prüfen einer *Behauptung* über eine *partielle Identität*. Nach einer erfolgreichen Authentifizierung kann die *partielle Identität* einer *Rolle* zugeordnet werden.

15 Differentielle Identität

Eine **differentielle Identität** ist eine *partielle Identität*, die in einer technischen Komponente (z.B. einer Chipkarte) zur *Authentisierung*, *Authentifizierung* oder für andere kryptographische Operationen genutzt wird (vgl. [**ISO24727-3**]).

Beispielsweise kann eine differentielle Identität ein Passwort, eine PIN, ein privater Schlüssel, ein oder mehrere geheime Schlüssel, ein öffentlicher Schlüssel, ein *biometrisches* Template oder ein *digitaler Ausweis* sein.

16 Biometrie

Biometrie ist die automatisierte Erkennung von natürlichen Personen anhand ihres Verhaltens und ihrer biologischen Charakteristika (vgl. [**ISO-SC37-Voc**]).

17 Rolle

Eine **Rolle** besteht aus einer Menge von *Berechtigungen*.

18 Berechtigung

Eine Berechtigung wird durch eine Menge von *Zugriffsregeln* dargestellt.

19 Autorisierung

Autorisierung ist das Gewähren des Zugriffs auf ein Objekt, sofern eine entsprechende *Berechtigung* hierzu vorhanden ist.

20 Zugriffsregel

Eine **Zugriffsregel** besteht aus einem Zugriffsmodus (z.B. anlegen, lesen, schreiben, ausführen, löschen etc.) und einer *Sicherheitsbedingung*.

21 Sicherheitsbedingung

Eine **Sicherheitsbedingung** ist ein boolescher Ausdruck, bei dem die Terme *differentielle Identitäten* sind.

22 Digitaler Ausweis

Ein **digitaler Ausweis** (engl. Credential) enthält eine *partielle Identität* und schützt deren Integrität (vgl. [**ModTerm**]).

Ein digitaler Ausweis wird von einer *Entität* – dem sog. Aussteller – unter Verwendung einer *differentiellen Identität* ausgestellt. Darüber hinaus ist ein digitaler Ausweis selbst eine *differentielle Identität* und kann somit zur *Authentisierung* und *Authentifizierung* genutzt werden.

Zu den gebräuchlichen Formen für digitale Ausweise zählen Zertifikate (z.B. gemäß [**X.509**] oder [**ISO7816-8**]), SAML-Assertions [**SAML-v2.0**] oder andere integritätsgeschützte *Sicherheitsmerkmale* [**WS-Security-1.1**].

23 Sicherheitsmerkmal

Ein **Sicherheitsmerkmal** (engl. Security Token) repräsentiert eine oder mehrere *Behauptungen* (vgl. [**WS-Security-1.1**]).

24 Föderierte Identität

Eine **föderierte Identität** (engl. Federated Identity) ist ein *digitaler Ausweis*, durch den eine *partielle Identität* einer *Entität* in einem bestimmten Kontext mit einer anderen *partiellen Identität* dieser *Entität* in einem anderen Kontext verknüpft wird (vgl. [**ModTerm**]).

25 Föderation einer elektronischen Identität

Unter **Föderation einer elektronischen Identität** (Identity Federation) versteht man allgemeiner, dass diese über die Grenzen administrativer Domänen hinaus zur *Authentisierung* verwendet und *authentifiziert* werden kann. Dies kann mit einem Wechsel des Kontexts und der *partiellen Identität* verbunden sein, wobei eine *föderierte Identität* zum Einsatz kommen kann.

26 Unverkettbarkeit

Unverkettbarkeit bedeutet, dass zwei *partielle Identitäten* einer *Entität* nicht verknüpft werden können (vgl. [**PfHa07**]).

27 Zivile Identität

Bei natürlichen oder juristischen Personen ist die **zivile Identität** eine *partielle Identität*, die zumindest den *realen Namen* der Person enthält und in den entsprechenden staatlichen Registern (z.B. Melderegister bei natürlichen Personen und Handelsregister bzw. Vereinsregister bei bestimmten juristischen Personen) vermerkt ist (vgl. [**PfHa07**]).

28 Identitätsmanagement

Identitätsmanagement ist die Verwaltung und Nutzung von *partiellen Identitäten*. Dies umfasst beispielsweise die Definition, Zuweisung und Verwaltung von *Attributen* sowie die Erzeugung, Auswahl und Nutzung von *partiellen Identitäten* (vgl. [ModTerm, Section 4.22]).

Vielen Dank

Dieser Beitrag profitierte maßgeblich von der fruchtbaren Diskussion mit zahlreichen Personen. Besonderer Dank gilt Bud P. Bruegger, Martin Meints, Helmut Reimer, Wolfgang Schneider, Günther Welsch und Torsten Wunderlich.

Literatur

[ClKö01] Sebastian Clauß, Marit Köhntopp: *Identity management and its support of multilateral security*, Computer Networks 37(2): 205-219 (2001), via http://drim.inf.tu-dresden.de/literatur/ClKoe_01CompNetworks.pdf

[ISO-SC37-Voc] ISO SC 37: *Harmonized Biometric Vocabulary*. Standing Document Version 6 – dated 2006-08-31. http://www.3dface.org/media/vocabulary.html, 2006

[ISO7816-8] ISO/IEC 7816-8: *Identification cards – Integrated circuit cards – Part 8: Commands for security operations*. International Standard, 2004

[ISO24727-3] ISO/IEC 24727-3: *Identification cards – Integrated circuit cards programming interfaces – Part 3: Application programming interface*, Final Committee Draft (2007-09-14), 2007

[ModTerm] Modinis IDM Study Team: *Common Terminological Framework for Interoperable Electronic Identity Management*, Modinis Study on Identity Management in eGovernment – Consultation Paper, Version 2.01. https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/GlossaryDoc/modinis.terminology.paper.v2.01.2005-11-23.pdf, 2005

[MRRG] *Melderechtsrahmengesetz (MRRG)*, vom 16. August 1980. BGBl I 1980, 1429, zuletzt geändert durch Art. 12 G v. 21.6.2005

[PersAuswG] *Gesetz über Personalausweise (PersAuswG)*, vom 19. Dezember 1950. Neugefasst durch Bek. v. 21. 4.1986 I 548; zuletzt geändert durch Art. 2 G v. 20.7.2007 I 1566

[PfHa07] A. Pfitzmann, M. Hansen: *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*. Version v0.29. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.29.pdf, 2007.

[SAML-v2.0] S. Cantor, J. Kemp, R. Philpott, E. Maler: *Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard*, 15.03.2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, 2005.

[UML] Object Management Group: *Unified Modeling Language Specification*, Version 1.4.2, entspricht ISO/IEC 19501, via http://www.omg.org/docs/formal/05-04-01.pdf, 2004

[WS-Security-1.1] A. Nadalin, C. Kaler, R. Monzillo, P. Hallam-Baker: *Web Services Security: SOAP Message Security 1.1. OASIS Standard*, 01.02.2006. http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf, 2006.

[WS-Trust-1.3] A. Nadalin, M. Goodner, M. Gudgin, A. Barbir, H. Granqvist: *WS-Trust 1.3*, OASIS Standard, 19.03.2007. http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf, 2007.

[X.509] ITU-T: ITU-T Recommendation X.509:2000 ISO-IEC 9594-8:2000. *Information technology Open Systems Interconnection The Directory: Public-key and attribute certificate frameworks*, März 2000