ID4health - sicheres Identitätsmanagement für das Gesundheitswesen von morgen

ID4health-Team[1]
http://www.id4health.de

Abstract: Vor dem Hintergrund der Einführung des neuen Personalausweises (nPA) und der bevorstehenden flächendeckenden Ausgabe der elektronischen Gesundheitskarte (eGK) sowie des elektronischen Heilberufsausweises (HBA) entsteht der Bedarf für die Vereinheitlichung der hierbei umzusetzenden technischen Verfahren. Der Entwicklung eines zukunftsfähigen und sicheren Identitätsmanagements, welches den Erfordernissen aller beteiligten Domänen gerecht wird, kommt in diesem Zusammenhang eine ganz besondere Bedeutung zu. Aufbauend auf den Vorarbeiten des Bundesamtes für Sicherheit in der Informationstechnik zur Umsetzung der eCard-Strategie und den Erfahrungen aus den verschiedenen Projekten im Kontext der Einführung der eGK, des HBA und des nPA soll im ID4health-Projekt eine umfassende föderierte Identitätsmanagement-Architektur für das Gesundheitswesen entwickelt und mit ausgewählten Anwendungen erprobt werden. In diesem Beitrag werden die wesentlichen bisher bekannten Anforderungen an ein sicheres Identitätsmanagement im Gesundheitswesen zusammengetragen und auf dieser Basis die Skizze einer Systemarchitektur entwickelt, die im Rahmen des ID4health-Projektes mit relevanten Stellen abgestimmt und umgesetzt werden soll.

[1] Die Liste der am ID4health-Projekt mitwirkenden Personen findet sich im Anhang.

1 Einleitung

Die deutsche Bundesregierung hat die grundsätzliche Relevanz sicherer Identitäten für elektronische Prozesse bereits erkannt und führt mit dem neuen Personalausweis (nPA) [nPA-Portal] eine bundesweite Basistechnologie als „digitales Infrastrukturprojekt“ ein. Dadurch wird die Basis für eine kosteneffiziente, sichere und datenschutzfreundliche Umsetzung von elektronischen Geschäftsprozessen in Wirtschaft und Verwaltung gelegt. Leider wurde hierbei nicht berücksichtigt, dass der nPA auf Grund fehlender Funktionalität zur Verschlüsselung und Autorisierung bei vielen Geschäftsprozessen im Gesundheitswesen nicht oder nur sehr eingeschränkt genutzt werden kann. Zusätzlich entstehen durch die verzögerte Einführung der elektronischen Gesundheitskarte (eGK) im deutschen Gesundheitswesen zunehmend isolierte Anwendungen mit applikationsspezifischen Sicherheitsmechanismen. Die Bandbreite der Authentisierungsmechanismen reicht von der einfachen Nutzung von Benutzername und Passwort bis hin zu sehr sicheren Chipkartenbasierten Authentisierungslösungen. Während für den Kartenzugriff bislang verschiedenste Client-Komponenten eingesetzt wurden, ist davon auszugehen, dass langfristig vor allem die frei verfügbare „AusweisApp“ [AusweisApp] für den Zugriff auf die verschiedenen Chipkarten der eCard-Strategie (eGK, Heilberufsausweis (HBA), Secure Module Card (SMC), nPA, diverse Signaturkarten, etc.) eingesetzt werden wird und sich daneben zunehmend ein Bedarf für mobile Lösungen entwickeln wird [CoWo08].

Während in vielen anderen Branchen bereits seit geraumer Zeit Single Sign-On-Lösungen auf Basis von SAML [SAML(v2.0)], WS-* oder OpenID [OpenID-Auth] eingesetzt werden, wird diese dem SOA-Paradigma entsprechende Entkopplung von Identifizierung, Authentifizierung und Autorisierung bislang im Gesundheitswesen nur in wenigen – zumeist forschungsnahen – Projekten genutzt. Zu den möglichen Gründen für die schleppende Verbreitung moderner Ansätze für das Identitätsmanagement im Gesundheitswesen scheinen die besonders anspruchsvollen Anforderungen bzgl. der IT-Sicherheit und dem Datenschutz, das Fehlen branchenweit akzeptierter Standards und Empfehlungen sowie der Mangel an kostengünstig nutzbaren Komponenten und Diensten zu zählen.

Vor diesem Hintergrund soll im ID4health-Projekt (http://www.id4health.de), das vom Bundesministerium für Wirtschaft und Technologie (BMWi) im Rahmen des zentralen Innovationsprogrammes Mittelstand (ZIM) gefördert wird, eine umfassende föderierte Identitätsmanagement-Architektur für das deutsche Gesundheitswesen konzipiert, prototypisch realisiert und in ausgewählten Anwendungen erprobt werden.

In diesem Beitrag werden (siehe Abschnitt 2) die wesentlichen, bisher erfassten[2], Anforderungen an ein sicheres Identitätsmanagement im Gesundheitswesen zusammengetragen, bevor (siehe Abschnitt 3) auf dieser Basis eine Systemarchitektur entwickelt wird, die im Rahmen des ID4health-Projektes mit relevanten Stellen weiter verfeinert, abgestimmt und umgesetzt werden soll. In Abschnitt 4 findet sich schließlich eine Zusammenfassung der wesentlichen Aspekte des Beitrags sowie ein Ausblick auf zukünftige Entwicklungen.

2 Anforderungen für ein zukunftsfähiges Identitätsmanagement

Als Grundlage für das ID4health-Projekt, in dem eine umfassende föderierte Identitätsmanagement-Architektur für das deutsche Gesundheitswesen realisiert werden soll, , werden in diesem Abschnitt die wesentlichen Anforderungen für das sichere und zukunftsfähige Identitätsmanagement im Gesundheitswesen zusammengetragen. Für die genauere Beschreibung der Anforderungen werden die an [RFC2119] angelehnten Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT und KANN verwendet.

A1. Sehr hohes Sicherheitsniveau

Damit die sensiblen Patientendaten adäquat geschützt werden können, MUSS das zu konzipierende Identitätsmanagement-System ein sehr hohes Sicherheitsniveau nach dem jeweiligen Stand der Technik und Wissenschaft gewährleisten können. Insbesondere SOLLEN durch das zu konzipierende System auch die anspruchsvollen Stufen 3 und 4 gemäß der in [NIST-800-63] bzw. [ISO29115-CD] definierten „Assurance Levels“ unterstützt werden können.

A2. Datenvermeidung und Datensparsamkeit

Das in § 3a BDSG formulierte Gebot zur Datenvermeidung und Datensparsamkeit MUSS berücksichtigt werden. Soweit möglich und sinnvollSOLLEN geeignete Verfahren zur Anonymisierung und Pseudonymisierung eingesetzt werden.

A3. Unterstützung der Entwicklungen im Bereich der Gesundheitstelematik

Die zu konzipierende Lösung MUSS die Entwicklungen im Bereich der Gesundheitstelematik berücksichtigen und unterstützen können. Dies umfasst die in § 291a [SGB V] genannten Komponenten und Anwendungen sowie entsprechende Mehrwertdienste. Insbesondere SOLLEN die geplanten Chipkarten eGK [eGK-1], HBA [HBA-1] und SMC [HBA-3] sowie weitere Chipkarten der eCard-Strategie, wie z.B. der neue Personalausweis, zur starken Authentisierung genutzt werden können.

[2] Die in diesem Beitrag zusammengetragenen Anforderungen sind als eine erste Diskussionsgrundlage zu verstehen. Das ID4health-Team nimmt jederzeit gern entsprechende Kommentare und Anregungen entgegen.

A4. Integration in Abläufe und Nutzungsumgebungen

Um Leistungserbringern und Versicherten einen möglichst hohen Nutzungskomfort zu bieten, MÜSSEN Funktionalitäten des Identitätsmanagements leicht in bestehende Abläufe und Anwendungen integrierbar sein und spezifische Eigenheiten der Nutzungsumgebung berücksichtigen. Insbesondere SOLL das Identitätsmanagement auch berücksichtigen, dass in einem digitalen Gesundheitswesen, Daten- und Kontrollflüsse über mehrere Anwendungen hinweg erfolgen bzw. sich Mehrwert-Fachdienste der Telematikinfrastruktur auch ohne Erfordernis einer Nutzer-Interaktion innerhalb eines einmal aufgebauten Sicherheitskontextes untereinander aufrufen können müssen. Spezifische Umgebungsbedingungen von Krankenhäusern, bei denen die Identität weniger an Personen als an Funktionsrollen gebundenen ist und von einer dynamischen Arbeitsorganisation beeinflusste Berechtigungen einzelner Nutzer, MÜSSEN über das Identitätsmanagement aufgefangen werden. Eine wesentliche Anforderung hierbei ist die Anbindung bestehender HR-Lösungen und Verzeichnisdienste an einen ggf. sogar extern betriebenen Identity Provider.

A5. Interoperabilität und Evolutionsfähigkeit

Um die Abhängigkeit von einzelnen Anbietern zu vermeiden MÜSSEN die Schnittstellen zwischen den verschiedenen Komponenten offengelegt sein, so dass Komponenten unterschiedlicher Anbieter eingesetzt und einzelne Komponenten sowie das Gesamtsystem weiterentwickelt werden können.

A6. Modularisierung, Konfigurierbarkeit und Austauschbarkeit

Die einzelnen Komponenten MÜSSEN sich aus Modulen zusammensetzen, die für den jeweiligen Einsatzzweck zusammengefügt und konfiguriert werden können. Durch die ID4health-Architektur MÜSSEN auch mobile Einsatzszenarien und zukünftige Anwendungsfälle unterstützt werden können. Insbesondere im Bereich der kryptographischen Verfahren und Komponenten MÜSSEN die entsprechenden Module austauschbar gestaltet werden, da sich die Sicherheitseignung der eingesetzten Algorithmen im Laufe der Zeit verringern kann. Die Wiederverwendung von technischen Bausteinen des Identitätsmanagements MUSS durch eine geeignete Methodik zur Analyse und zum Design von eHealth-Anwendungen unterstützt werden. Hierzu MÜSSEN entsprechende Vorgaben existieren, die es einem Anwendungsentwickler erlauben, die für einen umzusetzenden Anwendungsfall notwendigen und empfohlenen Funktionalitäten und Dienste eines Identity Providers zu identifizieren und in Form einer Policy über interoperable Schnittstellen bei entsprechenden Anbietern anzufordern.

A7. Standards, Wirtschaftlichkeit und Wettbewerb

Die zu konzipierende Lösung SOLL auf international anerkannten Standards basieren und wirtschaftliche Aspekte MÜSSEN bereits in der Entwurfsphase berücksichtigt werden. Die Lösungsarchitektur MUSS es ermöglichen, dass Identitäts- und Anwendungsdienste von unterschiedlichen Betreibern in einem marktoffenen Modell bereitgestellt werden können.

3 Systemarchitektur für das Identitätsmanagement von morgen

In diesem Abschnitt wird auf Basis der oben dokumentierten Anforderungen eine Systemarchitektur für das sichere Identitätsmanagement im Gesundheitswesen entworfen, die im ID4health-Projektverlauf verfeinert und mit den relevanten Stellen abgestimmt wird.

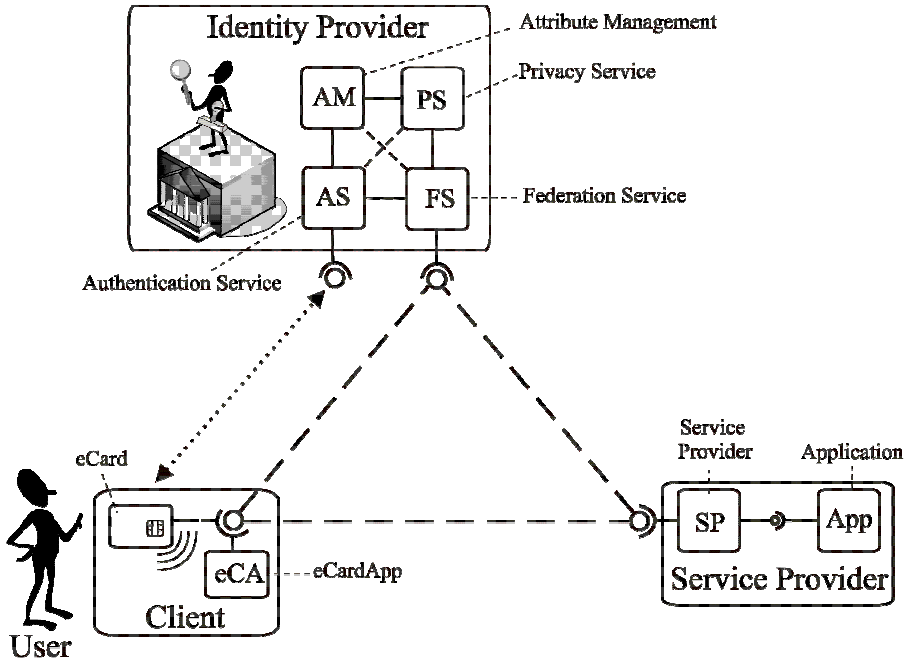

Abbildung 1: ID4health-Systemarchitektur im Überblick

Wie in Abbildung 1 dargestellt, umfasst die vorgeschlagene Systemarchitektur folgende Komponenten:

- ***User*** – in der Rolle des Patienten oder Leistungserbringers, der mittels des „Clients“ auf einen vom „Service Provider“ angebotenen Dienst zugreifen möchte und sich zu diesem Zweck gegenüber dem „Identity Provider“ authentisiert. Dies können

beispielsweise Ärzte sein, die sich bei Abrechnungsportalen anmelden, oder Versicherte, die auf eine Patientenakte zugreifen oder innovative Dienstleistungen, wie das Ausstellen eines elektronischen Rezepts über das Online-Portal einer Arztpraxis, in Anspruch nehmen möchten.

- ***Client*** – umfasst insbesondere eine Anwendung für den Benutzer („eCardApp“[3]), die für den Zugriff auf die verschiedenen Chipkarten der eCard-Strategie des Bundes („eCards“) wie die elektronische Gesundheitskarte [eGK-1], den elektronische Heilberufsausweis [HBA-1], die Secure Module Card (SMC) [HBA-3] und den neuen elektronischen Personalausweis (nPA)[4] genutzt werden kann.
- ***Identity Provider*** – empfängt Authentisierungsanfragen vom Service Provider und führt daraufhin die Authentisierung des Benutzers durch (Authentication Service), bevor das Ergebnis des Vorgangs gegenüber dem „Service Provider“ in sicherer[5] Weise bestätigt wird (Federation Service). Für die Authentisierung sollen insbesondere die unterschiedlichen im Gesundheitswesen relevanten Chipkarten (eGK, HBA, SMC, nPA etc.) und die in [BSI-TR-03112] standardisierten Protokolle genutzt werden können. Darüber hinaus kann der „Identity Provider“ für die Verwaltung der Identitätsattribute (Attribute Management) auf andere „Identity Provider“ und entsprechende Hintergrundsysteme und Verzeichnisse zugreifen und verwandte Dienste zur Autorisierung, Pseudonymisierung (Privacy Service) und partiellen Identifizierung unterstützen. Denkbar ist vor allem, dass die Standesorganisationen und Berufsverbände als „Identity Provider“ für Heilberufler auftreten und Krankenkassen entsprechende Dienste für ihre Versicherten erbringen.
- ***Service Provider*** – beinhaltet eine Schnittstellenkomponente, die über geeignete Protokolle ([SAML(v2.0)], [OpenID-Auth], [BSI-TR-03130], [CEN15480] etc.) mit dem „Identity Provider“ kommuniziert. Hier können von allen Leistungserbringern (Ärzte, Kliniken, Krankenkassen, Verbände, etc.) im Gesundheitswesen auf Basis kostengünstiger Standardkomponenten Mehrwertdienste angeboten werden, die allen Leistungsnehmern (Patienten, Ärzte, etc.) offen stehen. Im Rahmen des ID4health-Projektes soll das System mit ausgewählten Anwendungen pilotiert werden. Dies umfasst insbesondere Lösungen für das eGK-basierte Identitätsmanagement für Krankenkassen sowie eine Internet-basierte eKiosk-Anwendung, mit der Versicherte Ihre Rechte gemäß §§ 19, 20, 34 und 35 [BDSG] wahrnehmen können. Darüber hinaus ist das ID4health-Projekt offen für weitere Anwendungspartner und Pilotprojekte.

---

[3] Bei dieser „eCard-App“ kann es sich um die „AusweisApp“ des Bundes [AusweisApp] oder eine andere Anwendung handeln, die die Schnittstellen des eCard-API-Frameworks [BSI-TR-03112] unterstützt.

[4] Bis auch bei den Angehörigen der nicht-verkammerten Heilberufe (z.B. Pflegekräfte, Hebammen, Therapeuten und Gesundheitshandwerker) flächendeckend Berufsausweise verfügbar sind, bietet sich die ersatzweise Nutzung des neuen Personalausweises zur starken Authentisierung an.

[5] Um die bekannten Angriffe auszuschließen muss eine kryptographische Bindung der übermittelten Assertions an die zu Grunde liegenden TLS-Kanäle erfolgen (vgl. [GLS08], [KSJG10] und [SAML-HoK]).

4 Zusammenfassung und Ausblick

In diesem Beitrag wurden die wesentlichen bisher erfassten Anforderungen für ein sicheres und zukunftsfähiges Identitätsmanagement im Gesundheitswesen zusammengetragen. Innerhalb des Projektes werden diese in den kommenden Monaten präzisiert, vervollständigt und mit den maßgeblichen Stellen und interessierten Kreisen abgestimmt werden

Begleitend zu diesem Prozess werden auf Basis der Anforderungen die notwendigen Spezifikationen erstellt, so dass erste prototypische Entwicklungen ab Anfang 2012 in entsprechenden Pilotanwendungen genutzt werden können.

Literaturverzeichnis

[AusweisApp] BMI/BSI: *Informationen zur "AusweisApp"*, http://www.ausweisapp.bund.de

[BDSG] *Bundesdatenschutzgesetz* in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist, http://www.gesetze-im-internet.de/bdsg_1990/

[BSI-TR-03112] BSI: *eCard-API-Framework*, Technical Directive (BSI-TR-03112), Version 1.1, Part 1-7, 2009, https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03112/index_htm.html

[BSI-TR-03130] BSI: *Technische Richtlinie eID-Server*, Technische Richtlinie (BSI-TR-03130), Version 1.4.1, 2010, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_V1_4_pdf.pdf?__blob=publicationFile

[CEN15480] CEN 15480: *Identification card systems – European Citizen Card*, Part 1-4

[CoWo08] Computerwoche: *Forrester-Studie: Mobile Internet-Nutzung wird immer beliebter*, 26.03.2008, http://www.computerwoche.de/netzwerke/mobile-wireless/1859209/

[eGK-1] gematik: *Die Spezifikation der elektronischen Gesundheitskarte – Teil 1: Spezifikation der elektrischen Schnittstelle*, Version 2.2.2 vom 16.09.2008, http://www.gematik.de/upload/gematik_eGK_Spezifikation_Teil1_V2_2_2_4411.pdf

[GLS08] S. Gajek, J. Schwenk, L. Liao: *Stronger Bindings for SAML Assertions and SAML Artifacts*, In Proceedings of the 5th ACM CCS Workshop on Secure Web Services (SWS'08), ACM Press, 2008, pp. 11–20

[HBA-1] Bundesärztekammer & al: *German Health Professional Card and Security Module Card – Part 1: Commands, Algorithms and Functions of the COS Platform*, Version 2.3.2, 05.08.2009, http://www.bundesaerztekammer.de/downloads/HPC-Spezifikation_2.3.2_-_COS_Teil_1_.pdf

[HBA-3] Bundesärztekammer & al: *German Health Professional Card and Security Module Card – Part 3: SMC Applications and Functions*, Version 2.3.2, 05.08.2009, http://www.bundesaerztekammer.de/downloads/HPC-Spezifikation_2.3.2_-_SMC_Teil_3_.pdf

[ISO29115-CD] ISO/IEC CD 29115: *Information technology – Security techniques – Entity authentication assurance framework*, 2010

[KSJG10] F. Kohlar, J. Schwenk, M. Jensen, S. Gajek: *Secure Bindings of SAML Assertions to TLS Sessions*, ares 2010, International Conference on Availability, Reliability and Security, 2010, pp.62-69

[nPA-Portal] BMI: *Der neue Personalausweis*, http://www.personalausweisportal.de, 2010

[NIST-800-63] National Institute of Standards and Technology (NIST): *Electronic Authentication Guideline*, NIST Special Publication 800-63 Version 1.0.2, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[OpenID-Auth] OpenID Foundation: *OpenID Authentication 2.0*, Final, December 5, 2007. http://openid.net/specs/openid-authentication-2_0.html

[RFC2119] S. Bradner: *Key words for use in RFCs to Indicate Requirement Levels, RFC 2119*, März 1997, http://www.ietf.org/rfc/rfc2119.txt

[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

[SAML-HoK] N. Klingenstein: *SAML V2.0 Holder-of-Key Web Browser SSO Profile*, OASIS Committee Draft 02, 05.07.2009. http://www.oasis-open.org/committees/download.php/33239/sstc-saml-holder-of-key-browser-sso-cd-02.pdf, 2009

[SGB V] *Sozialgesetzbuch - Fünftes Buch (V) - Gesetzliche Krankenversicherung*. Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477, , http://www.gesetze-im-internet.de/sgb_5/ , 2010

Anhang – ID4health-Mitwirkende

- Sören Bittins (Fraunhofer-Institut für Software- und Systemtechnik)
- Dr. Jörg Caumanns (Fraunhofer-Institut für Software- und Systemtechnik)
- Florian Feldmann (Ruhr Universität Bochum)
- Ulf Göres (spectrumK Gesellschaft für Informationsmanagement mbH)
- Dominik Henze (HERE-IT UG (haftungsbeschränkt))
- Stephan Hoffmann-Emden (n-design GmbH)
- Dr. Detlef Hühnlein (ecsec GmbH)
- Andy Kohl (n-design GmbH)
- Florian Kohlar (Ruhr Universität Bochum)
- Dr. Günter Krückemeier (spectrumK Gesellschaft für Informationsmanagement mbH)
- Dirk Petrautzki (Hochschule Coburg)
- Simon Potzernheim (Hochschule Coburg)
- Uli Renz (HERE-IT UG (haftungsbeschränkt))
- Johannes Schmölz (ecsec GmbH)
- Prof. Dr. Jörg Schwenk (Ruhr Universität Bochum)
- Tobias Wich (ecsec GmbH)
- Prof. Dr. Thomas Wieland (Hochschule Coburg)