# Eine Referenzarchitektur für die Authentisierung und elektronische Signatur im Gesundheitswesen

Detlef Hühnlein · Johannes Schmölz · Tobias Wich
Benedikt Biallowons · Moritz Horsch · Tina Hühnlein
ecesc GmbH, Sudetenstrasse 16, 96247 Michelau
vorname.nachname@ecsec.de

**Abstract:** Vor dem Hintergrund der differenzierten Empfehlungen für den Einsatz elektronischer Signaturen und Zeitstempel in Versorgungseinrichtungen des Gesundheitswesens [SKB+10] wird in diesem Beitrag auf Basis der Vorarbeit aus einschlägigen Projekten sowie unter Berücksichtigung der relevanten BSI-Richtlinien und internationalen Standards eine umfassende und zukunftsfähige Referenzarchitektur für die starke Authentisierung und elektronische Signatur im Gesundheitswesen entwickelt.

## 1 Einleitung

Das *Competence Center für die Elektronische Signatur im Gesundheitswesen e.V.* (CCESigG) stellt mit [SKB+10] Empfehlungen bereit, welche Sicherungsmittel bei den verschiedenen typischerweise in Versorgungseinrichtungen des Gesundheitswesens auftretenden Dokumenttypen eingesetzt werden sollen. Hierbei reicht die Bandbreite der empfohlenen Sicherungsmittel von „geeigneten Authentifizierungsverfahren“ über fortgeschrittene elektronische Signaturen und einfachen Zeitstempeln bis hin zur qualifizierten elektronischen Signatur unter Verwendung von qualifizierten Zeitstempeln mit Anbieterakkreditierung. Für die Umsetzung dieser unterschiedlichen Sicherungsmittel sind verschiedene technische Komponenten und Dienste nötig, die in einer für den jeweiligen Anwendungsfall geeigneten Weise integriert und schließlich betrieben werden müssen. Um den Integrationsprozess zu erleichtern, wird in diesem Beitrag auf Basis der Vorarbeiten aus einschlägigen Projekten, wie z.B. ArchiSig [RoSc05], ArchiSafe[1], SkIDentity[2] und ID4health[3], und unter Berücksichtigung der relevanten Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik, wie z.B. [BSI-TR-03112, BSI-TR-03114, BSI-TR-03115, BSI-TR-03125, BSI-TR-03130], und der darin genutzten internationalen Standards, wie [CEN15480, ISO24727, DSS-Core, RFC4998, RFC6283, SAML(v2.0)], eine umfassende und zukunftsfähige Referenzarchitektur für die Authentisierung und elektronische Signatur im Gesundheitswesen entwickelt. Diese Referenzarchitektur umfasst eine Reihe von abstrakten und lose gekoppelten Diensten, die bei geeigneter Implementierung eine sichere, Policy-getriebene und auditierbare Nutzung von Authentisierungs- und

[1] Siehe http://www.archisafe.de
[2] Siehe [HHR+11], http://www.skidentity.de und insbesondere [SkIDentity-D0].
[3] Siehe http://www.id4health.de

Signaturdiensten im Gesundheitswesen ermöglichen, die zukünftig auch in kostengünstiger Art und Weise aus einer „Trusted Cloud“[4] bezogen werden könnten.

Der Rest des Beitrags ist folgendermaßen gegliedert: In Abschnitt 2 sind einige grundlegende Betrachtungen zur Authentisierung und elektronischen Signatur im Gesundheitswesen zusammengetragen. In Abschnitt 3 wird die umfassende Referenzarchitektur für die Authentisierung und elektronische Signatur im Gesundheitswesen vorgestellt. In Abschnitt 4 werden schließlich beispielhafte Anwendungsfälle für die Authentisierung und elektronische Signatur in der Referenzarchitektur betrachtet. In Abschnitt 5 werden schließlich die wesentlichen Aspekte des Beitrags kurz zusammengefasst und ein Ausblick auf zukünftige Entwicklungen gegeben.

## 2 Grundlegende Betrachtungen zur Authentisierung und Signatur

### 2.1 Begriffliche Abgrenzung und Verbindung von Authentisierung und Signatur

#### 2.1.1 Authentisierung und Authentifizierung

[ModTerm] definiert den englischen Begriff „Authentication“[5] als die Bestätigung einer behaupteten Menge an Attributen oder Fakten mit einem spezifizierten oder verstandenen Vertrauensniveau. Im Deutschen (vgl. [Hueh08, Borg10]) kann hier weiterhin zwischen dem Aufstellen einer Behauptung und der damit verbundenen Vorlage von Beweisen („*Authentisierung*“) und der Prüfung und Bestätigung einer aufgestellten Behauptung („*Authentifizierung*“) unterschieden werden. Während eine solche Unterscheidung im Englischen nicht üblich ist, werden in [ModTerm] jedoch entsprechend des Gegenstands der Authentisierung die beiden spezifischen Anwendungsfälle „Data authentication“[6] und „Entity authentication“[7] unterschieden.

#### 2.1.2 Authentisierung von Daten – (Qualifizierte) elektronische Signatur

Betrachtet man nun die Legaldefinition der „elektronischen Signatur“, bei der es sich gemäß § 2 Nr. 1 [SigG] um „Daten in elektronischer Form“ handelt, „die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“, so wird klar, dass die Erstellung einer elektronischen Signatur genau dem Zweck der Authentisierung von Daten dient, wodurch letztlich die Authentizität und die Integrität der fraglichen Daten nachgewiesen werden soll.

An die „qualifizierte elektronische Signatur“ gemäß § 2 Nr. 3 [SigG] hat der Gesetzgeber bezüglich der Form (vgl. § 126a [BGB], § 3a [VwVfG], § 87a [AO], § 36a [SGBI])

[4] Siehe z.B. `http://www.trusted-cloud.de`.

[5] „Authentication is the corroboration of a claimed set of attributes or facts with a specified, or understood, level of confidence.“

[6] „Data authentication is the corroboration that the origin and integrity of data is as claimed.“

[7] „Entity authentication is the corroboration of the claimed identity of an entity and a set of its observed attributes.“

und der Beweiskraft (siehe § 371a [ZPO]) besondere Rechtsfolgen geknüpft. Wie beispielsweise in [HuKn03, RoFD04] erläutert, können qualifizierte elektronische Signaturen grundsätzlich auch in einem automatisierten Verfahren erzeugt werden, wobei sich jedoch die mit der Signatur verbundene Erklärung, die in den Genuss der Beweiserleichterung gemäß § 371a [ZPO] gelangen kann, möglicherweise auf die Tatsache beschränken wird, dass dem Signaturserver die zu signierenden Daten vorgelegen haben. Ähnliche „Massensignaturverfahren“ werden beispielsweise für die Erzeugung von „qualifizierten Zeitstempeln“ gemäß § 2 Nr. 14 [SigG] eingesetzt, mit denen neben dem sehr wirkungsvollen Integritätsschutz insbesondere der Nachweis erbracht werden kann, dass bestimmte Daten bereits zu einem bestimmten Zeitpunkt existiert haben, was wiederum für den langfristigen Erhalt der Beweiskraft von qualifiziert signierten Dokumenten gemäß § 17 [SigV] bzw. [BSI-TR-03125] genutzt wird.

### 2.1.3 Authentisierung von Entitäten – Elektronischer Identitätsnachweis

Sofern Identitätsattribute einer Entität, beispielsweise einer natürlichen Person, Gegenstand der Authentisierung sind, wird hierdurch also ein Identitätsnachweis realisiert. Während ein solcher Identitätsnachweis mit unterschiedlichen Mitteln und verschiedenen Chipkarten erfolgen kann [HSWH12], ist mit dem „elektronischen Identitätsnachweis“ gemäß § 18 [PAuswG] eine besondere Form des Identitätsnachweises gegeben. Dieser elektronische Identitätsnachweis wird mit dem neuen Personalausweis durchgeführt und kann gemäß § 3 [SigV] für die Beantragung qualifizierter Zertifikate und zukünftig bei vielen Verwaltungsprozessen genutzt werden, die bislang zwingend eine qualifizierte elektronische Signatur benötigt haben (vgl. § 3a [VwVfG], § 87a [AO], § 36a [SGBI] und die geplanten Änderungen in [EGovG-RE]).

## 2.2 Synergiepotenzial und gemeinsame Regulierung

Bei der Authentisierung und elektronischen Signatur handelt es sich insgesamt also um sehr eng miteinander verbundene Konzepte, die beide dazu geeignet sind, einen Nachweis über bestimmte Behauptungen zu erbringen. Deshalb verspricht die hier angestrebte Integration der Authentisierung und elektronischen Signatur in eine einheitliche Referenzarchitektur ein sehr großes Synergiepotenzial. Darüber hinaus deutet sich mit dem jüngst von der EU vorgelegten Entwurf [COM(2012)238/2] zur Überführung der Signaturrichtlinie [1999/93/EG] in eine verbindliche Verordnung für elektronische Identifizierungs- und Vertrauensdienste an, dass die eng miteinander verbundenen Konzepte der Authentisierung und Signatur zukünftig auch rechtlich noch stärker miteinander verknüpft sein werden.

### 2.3 Eignung von Authentifizierungsverfahren

Laut [SKB+10, Tabelle 3] können bei verschiedenen Anwendungsfällen, wie z.B. bei der Anamnese, der Anforderung, der Diagnose, der Anordnung und der Pflegedokumentation, „geeignete Authentifizierungsverfahren“ eingesetzt werden. Neben den in [SKB+10, Abschnitt 3.4] aufgeführten beispielhaften Eigenschaften eines „geeigneten Authentifizierungsverfahrens“ scheint es erwähnenswert, dass die Eignung sowohl vom *aktuellen Stand der Technik* als auch von den *konkreten Sicherheitsanforderungen* eines bestimmten Anwendungsfalles abhängt. Daraus ergibt sich, dass für einen angemessenen Schutz in der Regel verschiedene starke Authentifizierungsverfahren eingesetzt werden müssen und im Laufe der Zeit auch ein entsprechender Austausch der Mechanismen vorgesehen werden muss. Vor diesem Hintergrund wurde in der Referenzarchitektur bewusst die Nutzung unterschiedlicher und über Policy-Informationen auswählbarer Authentisierungs- und Signaturdienste vorgesehen. Außerdem wurden Aspekte des langfristigen Erhalts des Beweiswerts kryptograpisch signierter Daten in der Referenzarchitektur explizit berücksichtigt.

## 3 Die Referenzarchitektur für die Authentisierung und Signatur

Im Rahmen des SkIDentity-Projektes, das zu den Gewinnern des „Trusted Cloud“[8] Technologiewettbewerbs des Bundesministerium für Wirtschaft und Technologie (BMWi) zählt, wurde eine Referenzarchitektur [SkIDentity-D0] für die starke Authentisierung in der Cloud entwickelt, die im vorliegenden Beitrag zu einer umfassenden und zukunftsfähigen Referenzarchitektur für die Authentisierung und Signatur im Gesundheitswesen weiterentwickelt wird. Die in Abbildung 1 dargestellte Referenzarchitektur unterstützt

- die starke und Policy-getriebene Authentisierung mit beliebigen Chipkarten und sonstigen Authentisierungstoken (z.B. OTP-Generatoren),
- die Policy-getriebene Erstellung und Prüfung von
  - Personen-gebundenen elektronischen Signaturen mit beliebigen Signatur-fähigen Chipkarten beim Benutzer,
  - automatisiert erzeugten Massensignaturen durch geeignete Signaturdienste,
  - (qualifizierten) Zeitstempeln,
- den langfristigen Beweiskrafterhalt signierter Dokumente und nicht zuletzt
- den kosteneffizienten Bezug entsprechender Infrastrukturdienste für die starke Authentisierung und Signatur aus der Cloud.

[8] Siehe `www.trusted-cloud.de`.

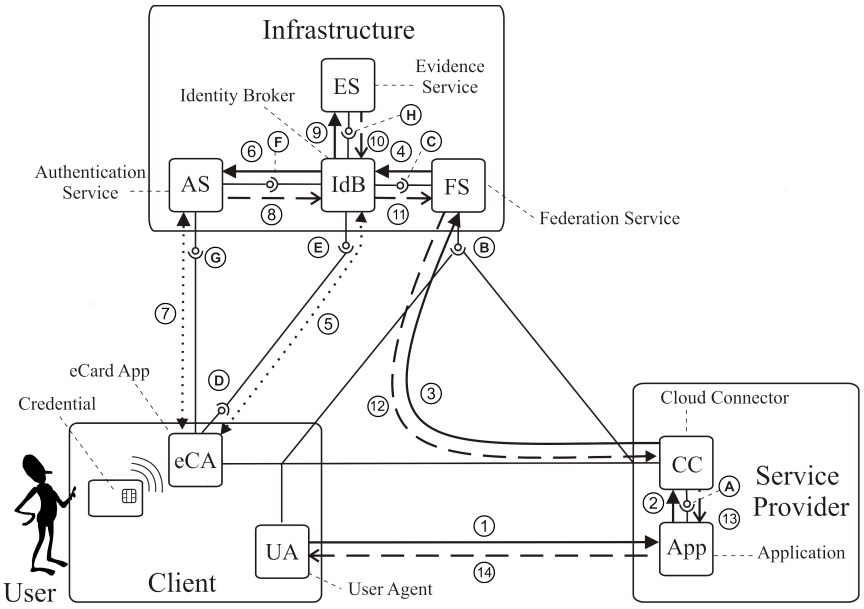


Abbildung 1: Referenzarchitektur für die Authentisierung und Signatur im Gesundheitswesen

### 3.1 Systemkomponenten

Wie in Abbildung 1 ersichtlich, umfasst die hier vorgestellte Referenzarchitektur für die Authentisierung und Signatur im Gesundheitswesen

- Systemkomponenten beim Benutzer (siehe Abschnitt 3.1.1),
- Systemkomponenten beim Applikationsanbieter (siehe Abschnitt 3.1.2) und
- Infrastrukturkomponenten (siehe Abschnitt 3.1.3).

#### 3.1.1 System des Benutzers

Das System des Benutzers (Client) umfasst einen *User Agent* (UA), der beispielsweise durch einen beliebigen Browser realisiert sein kann, und eine so genannte *eCard App* (eCA) (vgl. [AusweisApp, HPS+12]), die unter Verwendung des *digitalen Ausweises (Credential)* des *Benutzers (User)* eine Authentisierung gegenüber dem *Authentication Service* (AS) in der Infrastruktur durchführt oder in Verbindung mit diesem eine elektronische Signatur erzeugt. Darüber hinaus bietet die eCA eine Schnittstelle, die es dem *Identity Broker* (IdB) ermöglicht, die verfügbaren Credentials und Präferenzen des Benutzers

zu ermitteln, so dass ein für die von der Anwendung vorgegebene Policy ein geeigneter Authentisierungs- oder Signaturdienst ausgewählt werden kann.

### 3.1.2 System des Applikationsanbieters

Das System des Applikationsanbieters (Service Provider) umfasst die eigentliche Anwendung (*Application* (App)), einen so genannten *Cloud Connector* (CC), der die Kommunikation mit dem *Federation Service* (FS) oder dem *Identity Broker* (IdB) in der Infrastruktur übernimmt.

### 3.1.3 Infrastruktur

In der hier vorgestellten Infrastruktur für die starke Authentisierung und elektronische Signatur existiert ggf. ein *Federation Service* (FS) und eine Vielzahl von Authentisierungs- und Signaturdiensten *(Authentication Services, (AS))*, die über einen *Identity Broker* (IdB) miteinander verbunden sind. Außerdem existiert hier ein so genannter *Evidence Service (ES)*, der ein System für den langfristigen Erhalt der Beweiskraft der qualifiziert signierten Daten gemäß [BSI-TR-03125] bereitstellt.

## 3.2 Schnittstellen

In der hier vorgestellten Referenzarchitektur für die Authentisierung und Signatur im Gesundheitswesen existieren insbesondere die folgenden Schnittstellen:

(A) *Cloud-Interface* – wird vom CC angeboten und von der App für die Initiierung des Authentisierungs- oder Signaturvorganges genutzt. Für Zwecke der Authentisierung bietet sich hier beispielsweise [PAM, JAAS] und für die Signatur eine entsprechende Client-Bibliothek für die von OASIS in [DSS-Core] spezifizierte und vom BSI in [BSI-TR-03112] profilierte Digital Signature Service Schnittstelle an.

(B) *Federation-Interface* – wird vom FS angeboten und vom CC für die Übermittlung einer Authentisierungsanfrage genutzt. Diese Schnittstelle kann beispielsweise auf Basis von [SAML(v2.0)] realisiert sein und wird dann genutzt, wenn die Authentisierung nicht an einem über den Broker vermittelten Authentisierungsdienst, sondern über andere Wege (z.B. durch vorher erfolgte Anmeldung an einer vertrauenswürdigen Domäne) erfolgen soll. Für Zwecke der Signatur wird diese Schnittstelle in der Regel nicht genutzt.

(C) *Broker-Interface* – wird vom IdB angeboten und vom FS bzw. CC genutzt, um die Authentisierung bzw. Signaturerzeugung bei einem angeschlossenen Authentisierungs- oder Signaturdienst anzustoßen. Eine mögliche Ausprägung ist mit der in [CEN15480, Part 3, Chapter 11] spezifizierten SOAP-basierten `Authenticate`-Schnittstelle gegeben.

(D) *Credential-Interface* – wird von der eCA angeboten und vom IdB für die Ermittlung der aktuell verfügbaren Credentials sowie der Präferenzen des Benutzers genutzt. Hierdurch kann beispielsweise ermittelt werden, ob beim Benutzer aktuell eine Signatur-fähige Chipkarte vorhanden ist, oder ob andernfalls die Erstellung einer Signatur besser durch einen zentralen Signaturserver erfolgen sollte. Die Schnittstelle orientiert sich am Client-Interface wie es in [BSI-TR-03112, Part 7, Section 3.2] definiert ist. Insbesondere wird die eCA hierbei instruiert, über das Dispatcher-Interface (E) des Identity Broker eine XML-Struktur mit weiteren Informationen abzuholen.

(E) *Dispatcher-Interface* – wird vom IdB angeboten und von der eCA für die Ermittlung des für die Transaktion zuständigen Authentisierungs- oder Signaturdienstes genutzt. Über diese Schnittstelle wird der eCA eine XML-Struktur bereit gestellt, in der insbesondere die Adresse des für die Transaktion zuständigen Authentisierungs- bzw. Signaturdienstes enthalten ist (vgl. [BSI-TR-03112, Part 7, Section 3.3]).

(F) *Authentication-Service-Interface* – wird von den verschiedenen AS angeboten und vom IdB für die Initiierung des Authentisierungs- bzw. Signaturvorganges genutzt. Die detaillierte Ausgestaltung dieses Interfaces hängt von den integrierten Authentisierungs- und Signaturdiensten ab.

(G) *Authentication-Interface* – wird vom AS angeboten und von der eCA für die Durchführung des Authentisierungsprotokolles bzw. für die Entgegennahme der zu signierenden Daten genutzt. Bei einer Authentisierung mit dem neuen Personalausweis läuft hier beispielsweise das *Extended Access Control* Protokoll v2.0 gemäß [BSI-TR-03110] ab. Sofern die Signaturerzeugung in einem automatisierten Verfahren ohne aktives Mitwirken des Benutzers erfolgt oder falls Signaturen geprüft werden sollen, wird diese Schnittstelle nicht genutzt.

(H) *Evidence-Interface* – wird vom ES angeboten und vom IdB für den langfristigen Erhalt der Beweiskraft von qualifiziert elektronisch signierten Dokumenten genutzt. Für die Umsetzung dieser Schnittstelle empfiehlt sich insbesondere die Schnittstelle S.4 aus [BSI-TR-03125, Anhang E].

# 4 Anwendungsfälle

Die wesentlichen Abläufe bei der Authentisierung und Signatur in der Referenzarchitektur sollen anhand von beispielhaften Anwendungsfällen verdeutlicht werden.

## 4.1 Registrierung eines Benutzers

In diesem Anwendungsfall möchte sich der Benutzer bei der Anwendung (App) registrieren.

(1) $UA \rightarrow App/CC$: Der Benutzer greift über seinen UA auf eine Ressource zu, die über den CC den Registrierungsprozess initiiert.

(2) $CC$: Im CC wird daraufhin unter Verwendung der konfigurierten Informationen die Registrierung des Benutzers über den FS angestoßen.

(3) $CC \rightarrow FS$: Über die Schnittstelle (B) und ein geeignetes Föderationsprotokoll werden die für die Registrierung akzeptierten Ausweise oder der geforderte Assurance Level (vgl. [ISO29115, NIST-800-63]) sowie eine Liste der benötigten Identitätsattribute an den FS übermittelt. Damit der Benutzer bei einer späteren Authentisierung wieder erkannt werden kann, ist es zweckmäßig, dass die Liste der angefragten Attribute auch einen aus dem Credential des Benutzers extrahierten und bezüglich der Applikation eindeutigen "eIdentifier"[9] enthält.

(4) $FS \rightarrow IdB$: Der FS übergibt wiederum über die Schnittstelle (C) die Registrierungsanforderung an den IdB.

(5) $IdB \leftrightarrow eCA$: Der IdB ermittelt über die Schnittstelle (D) die aktuell an der eCA verfügbaren Credentials sowie etwaige Präferenzen des Benutzers. Auf Basis dieser Informationen und den in Schritt (3) übermittelten Informationen (Assurance Level, gewünschte Attribute) ermittelt der IdB einen geeigneten AS, an den sich die eCA in Schritt (7) wenden kann, um die Authentisierung des Benutzers durchzuführen. Die Adresse dieses Authentisierungsdienstes kann von der eCA über die Schnittstelle (E) beim IdB erfragt werden.

(6) $IdB \rightarrow AS$: In diesem Schritt wird die Registrierungsanfrage über die Schnittstelle (F) an den ausgewählten AS weitergeleitet.

(7) $eCA \leftrightarrow AS$: Die eCA kommuniziert mit dem AS, um die Authentisierung des Benutzers durchzuführen und die gewünschten Attribute aus dem Credential des Benutzers auszulesen.

(8) $AS \rightarrow IdB$: Nach erfolgreicher Authentisierung und dem Ermitteln der angefragten Identitätsattribute liefert der AS diese zurück an den IdB.

(11) $IdB \rightarrow FS$: Der IdB leitet das Ergebnis der Authentisierung und die ermittelten Identitätsattribute unverändert an den FS weiter.

(12) $FS \rightarrow CC$: Der FS bildet daraus eine dem Föderationsprotokoll entsprechende Assertion, die er an den CC sendet.

(13) $CC \rightarrow App$: Der CC prüft die Assertion und stellt der Applikation die Registrierungsinformationen bereit.

(14) $App \rightarrow UA$: Das Ergebnis des Registrierungsvorgangs wird dem UA angezeigt.

[9] Im Fall des neuen Personalausweises würde dieser Identifikator beispielsweise mit dem "Restricted Identification" Protokoll gemäß [BSI-TR-03110-2, Abschnitt 3.5] erzeugt werden.

### 4.2 Authentisierung eines registrierten Benutzers

Der Ablauf bei der Authentisierung eines bereits registrierten Benutzers verläuft analog zur Registrierung, wobei jedoch statt der vollständigen Liste der Identitätsattribute (siehe Schritt (3) in Abschnitt 4.1) lediglich der eIdentifier angefordert wird.

### 4.3 Erstellung einer elektronischen Signatur durch den Benutzer

In diesem Anwendungsfall soll der Benutzer eine elektronische Signatur erzeugen, um beispielsweise eine Willenserklärung zu dokumentieren.

(1) $UA \rightarrow App$: Der Benutzer greift über seinen UA auf die Applikation zu, um den Prozess der Abgabe der Willenserklärung anzustoßen.

(2-4) $App \rightarrow CC \rightarrow IdB$: Die Applikation greift über den CC auf den IdB zu, um die Auswahl der Signaturerstellungseinheit und den darauf folgenden Signaturvorgang anzustoßen.

(5) $IdB \leftrightarrow eCA$: Der IdB ermittelt über die Schnittstelle (D) die aktuell an der eCA verfügbaren Signaturerstellungseinheiten sowie etwaige Präferenzen des Benutzers. Auf Basis dieser Informationen kann ein geeigneter Dienst zur Signaturerzeugung ausgewählt werden, der im nächsten Schritt kontaktiert wird.

(6) $IdB \rightarrow AS$: In diesem Schritt wird der Request zur Signaturerzeugung über die Schnittstelle (F) an den ausgewählten AS weitergeleitet.

(7) $eCA \leftrightarrow AS$: Die eCA kommuniziert mit dem AS, um die Erzeugung der Signatur durch den Benutzer anzustoßen, was typischer Weise die Eingabe einer PIN durch den Benutzer zur Freischaltung des hierfür benötigten privaten Signaturschlüssels umfasst.

(8) $AS \rightarrow IdB$: Nach erfolgreicher Erstellung der Signatur liefert der AS diese zurück an den IdB.

(11-13) $IdB \rightarrow CC$: Der IdB leitet die erzeugte Signatur an den CC weiter, der diese Informationen schließlich an die Anwendung zurück gibt.

(14) $App \rightarrow UA$: Das Ergebnis des gesamten Signaturvorgangs wird dem UA schließlich von der App angezeigt.

### 4.4 Beweiskrafterhalt für qualifiziert elektronisch signierte Dokumente

Sofern die Beweiskraft der im vorherigen Anwendungsfall erstellten Signatur langfristig erhalten werden soll, werden im oben geschilderten Prozess der Signaturerzeugung zwei

zusätzliche Schritte (9) und (10) benötigt. Im Schritt (9) übergibt der IdB die erstellte Signatur zusätzlich an den ES, der in Schritt (10) einen entsprechenden "Archival Object Identifier" (AOID) gemäß [BSI-TR-03125]) zurück liefert. Diese AOID wird in den Schritten (11)-(13) zusätzlich zur Signatur an die Applikation zurückgeliefert, damit diese später bei Bedarf entsprechende Beweisdaten, z.B. in Form von Evidence Records gemäß [RFC4998] oder [RFC6283], anfordern kann.

### 4.5 Automatisierte Erzeugung von Server-seitigen Signaturen

Bei diesem Anwendungsfall ist der Benutzer nicht in die Signaturerzeugung involviert, sondern der Signaturdienst erstellt die benötigte Signatur in Schritt (7) ohne Mitwirkung des Benutzers.

### 4.6 Erstellung einer Server-basierten Signatur nach Authentisierung des Benutzers

In diesem Anwendungsfall besitzt der Benutzer keine für die technische Erstellung der Signatur geeignete Signaturerstellungseinheit, sondern lediglich ein Authentisierungstoken[10] mit dem er sich bei einem geeigneten Authentisierungsdienst ausweisen kann. Damit in diesem Fall trotzdem ein verkehrsfähiger Nachweis für die mit der Authentisierung des Benutzers verknüpfte Willenserklärung erzeugt wird, stößt der IdB nach der erfolgreichen Authentisierung zusätzlich die Erstellung einer automatisiert erzeugten Signatur an einem geeigneten Signaturdienst an. Wie in [HoHH12] erläutert, kann damit in vielen praxisrelevanten Fällen durch eine entsprechende Bevollmächtigung (vgl. § 167 Abs. 2 [BGB]) sogar die Schriftform ersetzt werden, sofern der eingesetzte Signaturdienst qualifizierte elektronische Signaturen erzeugt.

Im Vergleich zum oben in Abschnitt 4.3 erläuterten Ablauf ergeben sich folgende Änderungen:

(5) $IdB \leftrightarrow eCA$: In diesem Schritt wird erkannt, dass beim Benutzer lediglich ein Authentisierungstoken aber leider keine Signaturerstellungseinheit zur Verfügung steht.

(6-8a) $IdB \leftrightarrow AS \leftrightarrow eCA$: In Schritt (6a) wird der Authentisierungsdienst angesprochen, der in Schritt (7a) die Authentisierung des Benutzers durchführt und in Schritt (8a) das entsprechendes Ergebnis zurück liefert.

(6-8b) $IdB \leftrightarrow AS$: Für den verkehrsfähigen Nachweis des Authentisierungsvorganges werden zusätzlich die Schritte (6b, 7b und 8b) benötigt. Im Schritt (6b) werden dem Signaturdienst die zu signierenden Daten übergeben, die in Schritt (7b) signiert werden und in Schritt (8b) wird die so erstellte Signatur an den IdB zurückgeliefert.

[10] Beispielsweise kann es sich hierbei um einen neuen Personalausweis handeln, auf den noch kein qualifiziertes Zertifikat aufgebracht wurde.

## 5 Zusammenfassung

Vor dem Hintergrund der differenzierten Empfehlungen für den Einsatz der elektronischen Signatur bzw. entsprechender Authentisierungsverfahren in Versorgungseinrichtungen des Gesundheitswesens [SKB+10] wurde in diesem Beitrag gezeigt, dass es sich bei der Authentisierung und Signatur um eng miteinander verbundene Konzepte handelt. Deshalb eröffnet eine gemeinsame Betrachtung der Authentisierung und Signatur sehr große Synergiepotenziale. Um die Umsetzung geeigneter Authentisierungs- und Signaturverfahren im Gesundheitswesen zu erleichtern, wurde in diesem Beitrag auf Basis der Vorarbeit aus einschlägigen Projekten sowie unter Berücksichtigung der relevanten BSI-Richtlinien und internationalen Standards eine umfassende und zukunftsfähige Referenzarchitektur für die starke Authentisierung und elektronische Signatur im Gesundheitswesen entwickelt, die interessierten Anwendern bald zur Nutzung zur Verfügung stehen wird.

## Literatur


[1999/93/EG] *Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*. http://europa.eu.int/eur-lex/pri/de/oj/dat/2000/l_013/l_01320000119de00120020.pdf, 2000.

[AO] *Abgabenordnung*. in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), die zuletzt durch Artikel 5 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044) geändert worden ist. http://www.gesetze-im-internet.de/ao_1977, 2002.

[AusweisApp] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. *Offizielles Portal für die „AusweisApp“*. http://www.ausweisapp.de, 2012.

[BGB] *Bürgerliches Gesetzbuch*. RGBl 1896, 195, Neugefasst durch Bek. v. 2. 1.2002 I 42, 2909; 2003, 738; zuletzt geändert durch Art. 1 G v. 21. 4.2005 I 1073. http://bundesrecht.juris.de/bundesrecht/bgb/, 1896.

[Borg10] GEORG BORGES. *Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis*. Ein Gutachten für das Bundesministerium des Innern. http://docs.ecsec.de/Borg10, 2010.

[BSI-TR-03110] FEDERAL OFFICE FOR INFORMATION SECURITY (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK). *Advanced Security Mechanism for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)*. Technical Directive (BSI-TR-03110), Version 2.10. http://docs.ecsec.de/BSI-TR-03110, 2012.

[BSI-TR-03110-2] FEDERAL OFFICE FOR INFORMATION SECURITY (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK). *Advanced Security Mechanism for Machine Readable Travel Documents - Part 2 - Extended Access Control Version 2 (EACv2), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)*. Technical Directive (BSI-TR-03110), Version 2.10. http://docs.ecsec.de/BSI-TR-03110-2, 2012.

[BSI-TR-03112] FEDERAL OFFICE FOR INFORMATION SECURITY (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK). *eCard-API-Framework*. Technical Directive (BSI-TR-03112), Version 1.1.2, Part 1-7. http://docs.ecsec.de/BSI-TR-03112, 2012.

[BSI-TR-03114] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. *Stapelsignatur mit dem Heilberufsausweis*. Technische Richtlinie (BSI-TR-03114), Version 2.0, vom 22.10.2007. http://docs.ecsec.de/BSI-TR-03114, 2007.

[BSI-TR-03115] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. *Komfortsignatur mit dem Heilberufsausweis*. Technische Richtlinie (BSI-TR-03114), Version 2.0, vom 19.10.2007. http://docs.ecsec.de/BSI-TR-03115, 2007.

[BSI-TR-03125] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK). *Beweiswerterhaltung kryptographisch signierter Dokumente*. Technische Richtlinie (BSI-TR-03125), Version 1.1. http://docs.ecsec.de/BSI-TR-03125, 2011.

[BSI-TR-03130] FEDERAL OFFICE FOR INFORMATION SECURITY (BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK). *eID-Server*. Technical Directive (BSI-TR-031030), Version 1.6, 20.04.2012. http://docs.ecsec.de/BSI-TR-03130, 2012.

[CEN15480] COMITÉ EUROPÉEN DE NORMALISATION (CEN). *Identification card systems - European Citizen Card - Part 1-4*. (Draft of) Technical Specification, 2008.

[COM(2012)238/2] *Proposal for a Regulation of the European Parliament and the Council on electronic identification and trust services for electronic transactions in the internal market*, 2012.

[DSS-Core] STEFAN DREES. *Digital Signature Service Core Protocols, Elements, and Bindings, Version 1.0*. OASIS Standard. http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf, 2007.

[EGovG-RE] *Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften*. Referentenentwurf der Bundesregierung, Bearbeitungsstand 16.03.2012. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_EGov.html, 2012.

[HHR+11] DETLEF HÜHNLEIN, GERRIT HORNUNG, HEIKO ROSSNAGEL, JOHANNES SCHMÖLZ, TOBIAS WICH, und JAN ZIBUSCHKA. *SkIDentity - Vertrauenswürdige Identitäten für die Cloud*. DACH-Security 2011, 2011.

[HoHH12] GERRIT HORNUNG, MORITZ HORSCH, und DETLEF HÜHNLEIN. *Mobile Authentisierung und Signatur mit dem neuen Personalausweis – Innovative technische und rechtliche Lösungsansätze*. *Datenschutz und Datensicherheit (DuD)*, Band 36(3):189–194, 2012.

[HPS+12] DETLEF HÜHNLEIN, DIRK PETRAUTZKI, JOHANNES SCHMÖLZ, TOBIAS WICH, MORITZ HORSCH, THOMAS WIELAND, JAN EICHHOLZ, ALEXANDER WIESMAIER, JOHANNES BRAUN, FLORIAN FELDMANN, SIMON POTZERNHEIM, JÖRG SCHWENK, CHRISTIAN KAHLO, ANDREAS KÜHNE, und HEIKO VEIT. *On the design and implementation of the Open eCard App*. In *Sicherheit 2012*, GI-LNI (2012).

[HSWH12] DETLEF HÜHNLEIN, JOHANNES SCHMÖLZ, TOBIAS WICH, und MORITZ HORSCH. *Sicherheitsaspekte beim Chipkarten-basierten Identitätsnachweis*. In GEORG BORGES (Herausgeber), *Tagungsband zum A-I3-Symposium 2011* (Springer, 2012).

[Hueh08] DETLEF HÜHNLEIN. *Identitätsmanagement – Eine visualisierte Begriffsbestimmung. Datenschutz und Datensicherheit (DuD)*, Seiten 163–165. http://www.ecsec.de/pub/2008_DuD_Glossar.pdf, 2008.

[HuKn03] DETLEF HÜHNLEIN und YVONNE KNOSOWSKI. *Aspekte der Massensignatur*. In PATRICK HORSTER (Herausgeber), $D \cdot A \cdot CH$*-Security 2003*, Seiten 293–307 (IT-Verlag, 2003). http://www.ecsec.de/pub/2003_DACH.pdf.

[ISO24727] ISO/IEC. *ISO/IEC 24727: Identification cards – Integrated circuit cards programming interfaces – Part 1-6*, 2008.

[ISO29115] *ISO/IEC DIS 29115: Information technology – Security techniques – Entity authentication assurance framework*. International Standard, 2012.

[JAAS] SUN INC. *Java Authentication and Authorization Service (JAAS)*. Reference Guide for the Java TM SE Development Kit 6. http://java.sun.com/javase/6/docs/technotes/guides/security/jaas/JAASRefGuide.html.

[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. http://ec.europa.eu/information_society/activities/ict_psp/documents/eid_terminology_paper.pdf, 2005.

[NIST-800-63] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *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.

[PAM] THE OPEN GROUP. *X/Open Single Sign-on Service (XSSO) - Pluggable Authentication Modules*. X/Open Document Number: P702, Preliminary Specification. http://www.opengroup.org/onlinepubs/008329799/toc.htm, 1997.

[PAuswG] *Personalausweisgesetz*. vom 18. Juni 2009 (BGBl. I S. 1346), das durch Artikel 4 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 2959) geändert worden ist. www.gesetze-im-internet.de/pauswg/, 2009.

[RFC4998] T. GONDROM, R. BRANDNER, und U. PORDESCH. *Evidence Record Syntax (ERS)*. Request For Comments – RFC 4998. http://www.ietf.org/rfc/rfc4998.txt, August 2007.

[RFC6283] A. JERMAN BLAZIC, S. SALJIC, und T. GONDROM. *Extensible Markup Language Evidence Record Syntax (XMLERS)*. Request For Comments – RFC 6283. http://www.ietf.org/rfc/rfc6283.txt, July 2011.

[RoFD04] ALEXANDER ROSSNAGEL und STEFANIE FISCHER-DIESKAU. *Automatisiert erzeugte elektronische Signaturen*. *MultiMedia und Recht*, Band 3:133–139. http://www.uni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/AR_SFD_MMR_autoSig.pdf, 2004.

[RoSc05] ALEXANDER ROSSNAGEL und PAUL SCHMÜCKER (Herausgeber). *Beweiskräftige und sichere Langzeitarchivierung elektronisch signierter Dokumente – Ergebnisse des Forschungsvorhabens ArchiSig* (Verlagsgruppe Hüthig, Jehle, Rehm, 2005).

[SAML(v2.0)] SCOTT CANTOR, JOHN KEMP, ROB PHILPOTT, und EVE 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.

[SGBI] *Sozialgesetzbuch - Erstes Buch (I) Allgemeiner Teil*. (Artikel 1 des Gesetzes vom 11. Dezember 1975, BGBl I S. 3015), das zuletzt durch Artikel 13 Absatz 14 des Gesetzes vom 12. April 2012 (BGBl. I S. 579) geändert worden ist, 1975.

[SigG] *Signaturgesetz*. vom 16. Mai 2001 (BGBl. I S. 876), das zuletzt durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) geändert worden ist. `http://www.gesetze-im-internet.de/sigg_2001/`, 2001.

[SigV] *Verordnung zur elektronischen Signatur, vom 16.11.2001*. BGBl. 2001 Teil I Nr. 59, S. 3074 ff, geändert durch Art. 2 G v. 4. 1.2005 I 2. `http://bundesrecht.juris.de/bundesrecht/sigv_2001/`, 2001.

[SKB+10] C. SEIDEL, H. KOSOCK, A. BRANDNER, J. BALFANZ, und P. SCHMÜCKER. *Empfehlungen für den Einsatz elektronischer Signaturen und Zeitstempel in Versorgungseinrichtungen des Gesundheitswesens*. Competence Center für die Elektronische Signatur im Gesundheitswesen e.V. CCESigG (Hrsg.), Shaker-Verlag, 2010.

[SkIDentity-D0] SKIDENTITY-KONSORTIUM. *SkIDentity - Referenzarchitektur*. Version 0.1.1 vom 21.05.2012. `https://dms-prext.fraunhofer.de/livelink/livelink.exe/overview/2106422`, 2012.

[VwVfG] *Verwaltungsverfahrensgesetz*. in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), das zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2827) geändert worden ist. `www.gesetze-im-internet.de/vwvfg/`, 2003.

[ZPO] *Zivilprozeßordnung*. in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202 (2006 I S. 431) (2007 I S. 1781)), die zuletzt durch Artikel 3 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044) geändert worden ist. `http://www.gesetze-im-internet.de/zpo/`, 2005.