SkIDentity – Mobile eID as a Service

Detlef Hühnlein · Tina Hühnlein · Tobias Wich
Benedikt Biallowons · Max Tuengerthal · Hans-Martin Haase
Daniel Nemmert · Stefan Baszanowski · Christian Bergmann

ecsec GmbH
vorname.nachname@ecsec.de

Zusammenfassung

Durch den zunehmenden Identitätsmissbrauch im Internet existiert ein wachsender Bedarf an starken Authentisierungsmechanismen und vertrauenswürdigen Identitätsinformationen, wie sie durch elektronische Identitätsdokumente (eID), wie z.B. dem neuen Personalausweis (nPA) in Deutschland oder der österreichischen Sozialversicherungskarte (e-card), bereitgestellt werden. Vor diesem Hintergrund wurde im Rahmen des vom Bundesministerium für Wirtschaft und Energie (BMWi) geförderten SkIDentity Projektes (https://skidentity.de) ein Dienst entwickelt, durch den Bürgerinnen und Bürger aus ihrem elektronischen Ausweis kryptographisch geschützte „Cloud Identitäten" ableiten und bei Bedarf auf ein Mobiltelefon übertragen können, um bei Online-Diensten eine pseudonyme Authentisierung oder einen mobilen elektronischen Identitätsnachweis („Mobile eID") durchzuführen. Anbieter von Online-Diensten können diese vertrauenswürdigen Identitäten und die starke Authentisierung bequem und kosteneffizient als „Software as a Service" aus der Cloud beziehen. Durch die Kombination dieser beiden Aspekte bietet der innovative SkIDentity-Dienst, der im Rahmen des vorliegenden Beitrags vorgestellt wird, gewissermaßen „Mobile eID as a Service".

1 Einleitung

Vor dem Hintergrund des zunehmenden Identitätsmissbrauchs im Internet[1] und den entsprechenden Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI)[2] gewinnen starke, auf mindestens zwei Faktoren (Besitz, Wissen, Sein, etc.) basierende, Authentisierungsmechanismen für die Anmeldung bei Online-Diensten zunehmend an Bedeutung. Durch das kürzlich vom deutschen Bundestag verabschiedete IT-Sicherheitsgesetz [ITSG], das in Artikel 4 eine Änderung von § 13 Abs. 7 TMG mit sich bringt, wonach allen geschäftsmäßigen Anbietern von personalisierten Telemediendiensten „das Angebot eines sicheren und dem jeweiligen Schutzbedarf angemessenen Authentifizierungsverfahren" nahegelegt wird, wird der Trend zur Einführung starker Authentisierungsmechanismen voraussichtlich zusätzlich unterstützt werden. Während für die Implementierung sicherer Authentisierungsmechanismen vielfältige Optionen[3] existieren, ist die Nutzung von bereits im Feld befindlichen elektronischen Ausweiskarten, wie dem neuen Personalausweis (nPA), der österreichischen Sozialversicherungskarte (e-card), der eidgenössischen SuisseID, der elektronischen Gesundheitskarte (eGK)

[1] Siehe z.B. [BSI14c], [BSI14b] und [BSI14a]

[2] Siehe z.B. [BSI11a] und [BSI11b]

[3] Siehe z.B. [BoMa03]

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 37-48.

oder anderen Chipkarten der eCard-Strategie [Kowa07] besonders vielversprechend, da hierdurch auf kostenintensive Ausgabeprozesse verzichtet werden kann und bei Bedarf auch vertrauenswürdige Identitätsinformationen (Name, Vorname, Anschrift, etc.) zur Verfügung gestellt werden können.

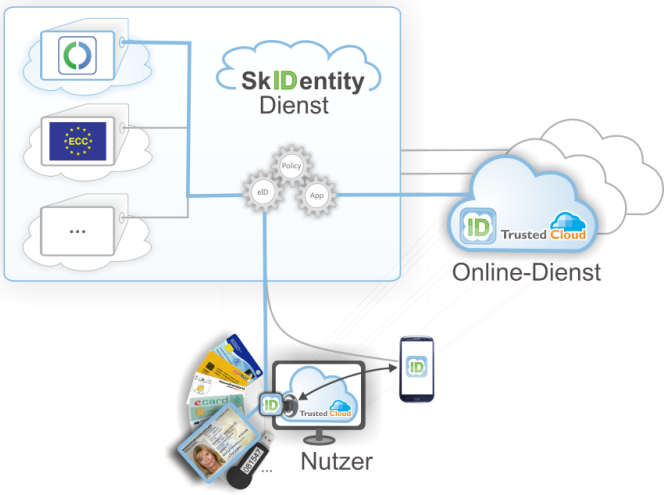

Abb. 1: Das SkIDentity-System im Überblick

Damit elektronische Ausweise und ähnliche Hardwaretoken in einer besonders einfachen, sicheren und gleichzeitig benutzerfreundlichen Weise für die starke Authentisierung und den elektronischen Identitätsnachweis im Internet genutzt werden können, wurde im SkIDentity-Projekt [HHR+11], das zu den Gewinnern des „Trusted Cloud“[4] Technologiewettbewerbs des deutschen Bundesministeriums für Wirtschaft und Energie (BMWi) zählt, mit dem European Identity & Cloud Award 2015[5], dem EuroCloud Deutschland Award[6] und zweimal im bundesweiten Innovationswettbewerb „Ausgezeichnete Orte im Land der Ideen“ [7] ausgezeichnet wurde, der SkIDentity-Dienst (vgl. Abbildung 1) entwickelt, durch den vertrauenswürdige Identitäten und die starke Authentisierung ab sofort sehr einfach und kosteneffizient „aus der Cloud“ bezogen werden können.

Dieses im vorliegenden Beitrag näher vorgestellte „Software as a Service“ Angebot basiert auf der Referenzarchitektur aus [HSW+12], die wiederum konsequent auf international anerkannten Standards, wie z.B. SAML 2.0 [CKPM05], OAuth 2.0 [RFC6749], [CEN15480] und [ISO24727] aufbaut. Neben der unmittelbaren Nutzung der verschiedenen Ausweiskarten[8] unterstützt der SkIDentity-Dienst auch die Erzeugung und Verwaltung von so genannten „Cloud

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

[5] Siehe https://skidentity.de/erhaelt-european-identity-and-cloud-award-2015.

[6] Siehe https://skidentity.de/gewinnt-eurocloud-award-2015.

[7] Siehe http://buergercloud.de, [HoHS14] und https://skidentity.de/ist-ausgezeichneter-ort-im-land-der-ideen-2015

[8] Neben dem elektronischen Personalausweis (nPA), der österreichischen Sozialversicherungskarte (e-card), der estnische Identitätskarte (EstID), der elektronischen Gesundheitskarte (eGK), dem von der Ärztekammer Nordrhein herausgegebenen „eArztausweis light“ werden derzeit auch verschiedene Signatur- und Bankkarten von D-Trust, DATEV, S-Trust und der GAD eG unterstützt. Eine aktuelle Übersicht über die in SkIDentity unterstützten Ausweiskarten findet sich unter https://www.skidentity.de/system/ausweise/ .

Identitäten“, die – ähnlich wie beispielsweise in [ScMo13], [EGAM14] und [NIST14] beschrieben – aus einem ursprünglichen Ausweisdokument abgeleitet werden. Eine solche „Cloud Identität“ wird nach einem entsprechenden Identitätsnachweis unter Verwendung eines ursprünglichen elektronischen Ausweises vom SkIDentity-Dienst erstellt und in einer sicheren Art und Weise auf dem System des Nutzers abgelegt. Diese „Cloud Identität“ kann bei Bedarf mit weiteren kryptographischen Schlüsseln des Nutzers verknüpft oder in sicherer Weise auf ein anderes Gerät, wie z.B. das persönliche Mobiltelefon des Benutzers, übertragen werden. Diese „Cloud Identität“, die etwa den Charakter einer „sicheren elektronischen Ausweiskopie“ besitzt, kann der Nutzer nun eigenverantwortlich verwalten und fortan in benutzerfreundlicher Weise für den selbstbestimmten Identitätsnachweis oder die pseudonyme Authentisierung bei einem angeschlossenen Online-Dienst nutzen. Sofern die angeschlossenen Online-Dienste bereits entsprechende Standards für das föderierte Identitätsmanagement, wie z.B. SAML 2.0 [CKPM05], nutzen, müssen im Management-Interface des SkIDentity-Dienstes (siehe Abschnitt 4) lediglich die standardisierten Metadaten über ein Webformular hochgeladen bzw. erfasst werden. Andernfalls steht mit den im SkIDentity-Projekt entwickelten „Cloud Connectoren“ (siehe Abschnitt 2.3) eine Familie von sehr einfach zu integrierenden Schnittstellenkomponenten für unterschiedliche Plattformen bereit, mit denen die Anbindung eines Online-Dienstes an die SkIDentity-Infrastruktur sehr leicht möglich ist.

Der Rest des Beitrags ist folgendermaßen gegliedert: Abschnitt 2 liefert einen technischen Überblick über das in Abbildung 1 skizzierte SkIDentity-System. Abschnitt 3 beschreibt die wesentlichen Leistungen des SkIDentity-Dienstes aus Sicht des Nutzers. Abschnitt 4 beschreibt, wie Anbieter von Online-Diensten in ihren Anwendungen die über den SkIDentity-Dienst vermittelten Identitäten nutzen können. Abschnitt 5 enthält schließlich eine kompakte Zusammenfassung des Beitrags.

2 Das SkIDentity-System im Überblick

Die technische Realisierung des SkIDentity-Systems basiert auf der Referenzarchitektur [HSW+12] und umfasst verschiedene Systemkomponenten beim Nutzer, beim Online-Dienst und nicht zuletzt beim SkIDentity-Dienst.

2.1 Überblick über die technischen Systemkomponenten

Wie in Abbildung 1 und Abbildung 2 ersichtlich, umfasst das SkIDentity-System

- Systemkomponenten beim Nutzer (siehe Abschnitt 2.2),
- Systemkomponenten beim Online-Dienst (siehe Abschnitt 2.3), sowie entsprechende
- Infrastrukturkomponenten beim SkIDentity-Dienst (siehe Abschnitt 2.4).

2.2 System des Benutzers

Das System des Nutzers (Client) umfasst einen User Agent (UA), der beispielsweise durch einen beliebigen Browser realisiert sein kann, und eine so genannte eCard App (eCA) (vgl. [BSI13], [HPS+12], [WPS+13]), die unter Verwendung eines elektronischen Ausweises (Credential) des Benutzers (User) eine Authentisierung gegenüber dem Authentication Service (AS) in der Infrastruktur durchführt. Darüber hinaus bietet die eCA eine Schnittstelle, die es dem

Identity Broker (IdB) unter Verwendung des in [HSW+13] vorgestellten, CORS[9]-basierten Mechanismus ermöglicht, die verfügbaren elektronischen Ausweise, „Cloud Identitäten“ und Präferenzen des Benutzers zu ermitteln, so dass ein geeigneter Authentisierungsdienst ausgewählt werden oder die Ausstellung einer „Cloud Identität“ angestoßen werden kann.

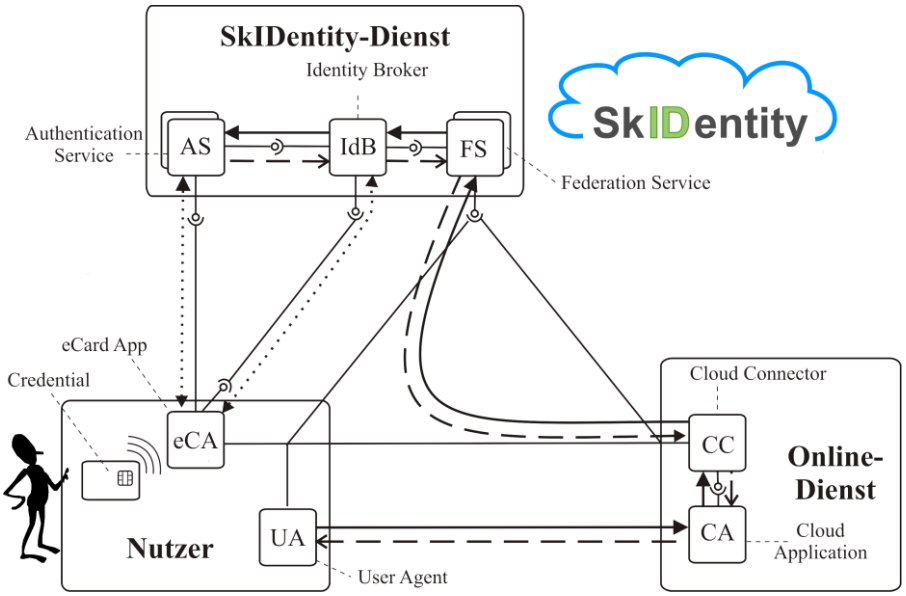

Abb. 2: Technische Architektur des SkIDentity-Systems

2.3 Der SkIDentity-Dienst

Der SkIDentity-Dienst umfasst unterschiedliche Teilkomponenten, wie z.B. verschiedene Federation Services (FS) und verschiedene Authentication Services (AS), die über einen zentralen Identity Broker (IdB) miteinander verbunden sind (vgl. Abbildung 2).

Hierbei führt der AS die Authentisierung des Nutzers unter Verwendung seines Credentials (z.B. seines elektronischen Personalausweises) durch, während der FS die benötigte Funktionalität für ein möglicherweise gewünschtes Single Sign-On bereitstellt und mit dem Cloud Connector (CC) des Online-Dienstes über hierfür vorgesehene Föderationsprotokolle, wie z.B. SAML [CKPM05] oder OAuth 2.0 [RFC6749] kommuniziert. Hierbei werden sogenannte Identitätsbestätigungstoken (z.B. SAML-Assertions) erstellt, mit denen beim Online-Dienst die Echtheit der Identitätsdaten nachgewiesen werden kann. Für die Verwaltung von „Cloud Identitäten“ werden im SkIDentity-Dienst verschiedene interne Dienste für die Erstellung und Prüfung von „Cloud Identitäten“ eingesetzt. Nach einem mit dem echten Ausweis durchgeführten elektronischen Identitätsnachweis kann der SkIDentity-Dienst eine abgeleitete elektronische Identität erstellen und sie im lokalen System des Nutzers ablegen. Hierfür werden moderne Webtechnologien und verschiedene kryptographische Mechanismen, wie z.B. Verschlüsselung und elektronische Signatur, in geschickter Weise miteinander kombiniert, um ein gleichermaßen sicheres und benutzerfreundliches Authentisierungssystem zu realisieren. Wie in Abschnitt 3 näher erläutert, kann der Nutzer seine aus den primären Ausweisdokumenten abgeleiteten „Cloud Identitäten“ eigenverantwortlich verwalten, bei Bedarf auf ein anderes Gerät,

[9] Siehe http://www.w3.org/TR/cors/.

wie z.B. ein Smartphone, übertragen und sofort oder zu einem späteren Zeitpunkt bei einem angeschlossenen Online-Dienst für den selbstbestimmten Identitätsnachweis oder eine pseudonyme Authentisierung nutzen.

2.4 System beim Online-Dienst

Das System beim Anbieter des Online-Dienstes umfasst die eigentliche Anwendung (Cloud Application (CA)) und einen so genannten Cloud Connector (CC) [BHH+14], der die Kommunikation mit dem SkIDentity-Dienst übernimmt.

Ein solcher CC fungiert als Zugriffsfilter für eine geschützte Ressource der CA und fordert bei Bedarf die Authentisierung des Benutzers beim SkIDentity-Dienst an. Zu diesem Zweck wird der Browser des Benutzers zum SkIDentity-Dienst umgeleitet und eine Authentifizierung des Benutzers gemäß der Anforderungen der CA durchgeführt und das Ergebnis der Authentisierung an den CC und schließlich über diesen an die CA zurückgeliefert. Die detaillierten Abläufe sind abhängig vom eingesetzten Föderationsprotokoll, wie z.B. SAML 2.0 [CKPM05] und OAuth 2.0 [RFC6749], welches in einem Protocol-Specific Module (PSM) des CC realisiert ist.

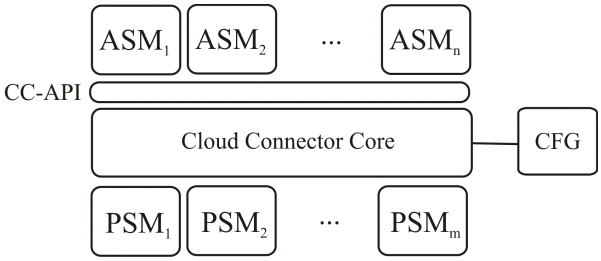

Abb. 3: Interner Aufbau des Cloud Connector

Wie in Abbildung 3 angedeutet, umfasst der CC neben den PSM und einer Kernkomponente (Cloud Connector Core), die über die CC-API angesprochen werden kann, bei Bedarf auch Application Specific Modules (ASM), mit denen die individuelle Integration in eine Webanwendung realisiert ist.

3 SkIDentity aus Sicht des Nutzers

3.1 Überblick

Der Nutzer kann das Identitätsmanagement von SkIDentity über https://service.skidentity.de/ids erreichen und die folgende Funktionalität nutzen:

- Übersicht über verfügbare elektronische Identitäten
- Erstellen einer abgeleiteten elektronischen Identität
- Einsicht in Inhalte einer elektronischen Identität
- Aktivieren und Deaktivieren einer abgeleiteten elektronischen Identität
- Übertragen einer abgeleiteten elektronischen Identität in ein anderes System
- Schützen einer abgeleiteten elektronischen Identität
- Sperren und Löschen einer abgeleiteten elektronischen Identität
- Nutzen eines elektronischen Ausweises oder einer abgeleiteten elektronischen Identität bei einem anderen Online-Dienst

3.2 Übersicht über verfügbare elektronische Identitäten

Nach dem Start des Identitätsmanagements wird dem Nutzer eine Übersicht über die grundsätzlich auf seinem System verfügbaren elektronischen Identitäten geliefert.

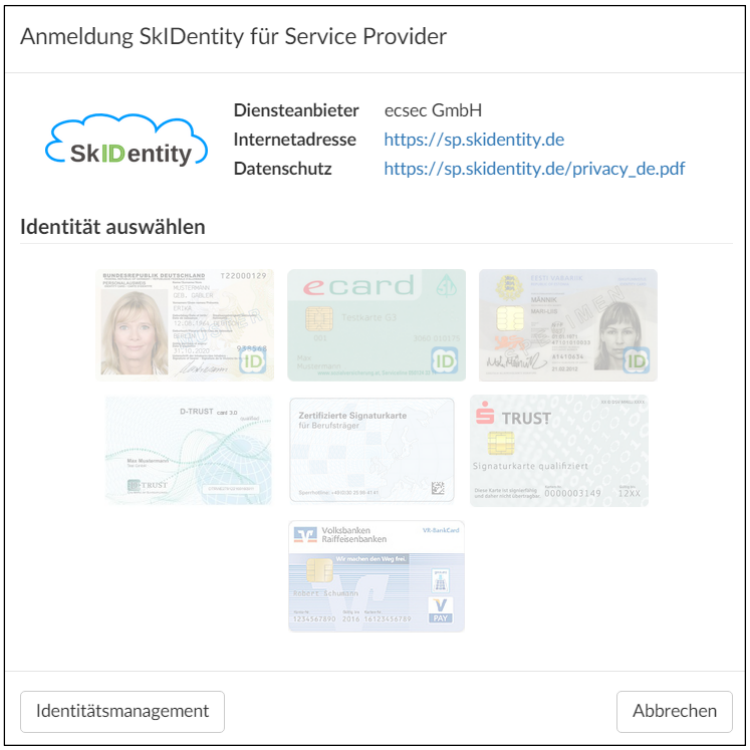

Abb. 4: Auswahl der in SkIDentity zu verwaltenden Identität

Dies umfasst sowohl die aktuell verfügbaren elektronischen Ausweise als auch die aus diesen bereits abgeleiteten elektronischen Identitäten. Ausgehend von dieser Übersicht kann der Nutzer die Datenschutzerklärung des SkIDentity-Dienstes [ECSEC14] und die in einem elektronischen Ausweis enthaltenen Identitätsdaten einsehen und bei Bedarf abgeleitete elektronische Identitäten erstellen, verwalten, schützen, übertragen und schließlich wieder sperren und löschen.

3.3 Erstellung von „Cloud Identitäten“

Die Erstellung einer abgeleiteten elektronischen Identität umfasst den Identitätsnachweis des Nutzers gegenüber dem SkIDentity-Dienst, die Erstellung der abgeleiteten Identität durch den SkIDentity-Dienst und schließlich die Speicherung der abgeleiteten Identität im System des Nutzers.

Im Rahmen der Nutzung des neuen Personalausweises (nPA) fungiert der SkIDentity-Dienst als Diensteanbieter im Sinne von § 2 Abs. 3 PAuswG.

Hierfür benötigt er ein Berechtigungszertifikat der Vergabestelle für Berechtigungszertifikate (VfB) beim Bundesverwaltungsamt (BVA).

Das Berechtigungszertifikat ermöglicht dem SkIDentity-Dienst den technischen Zugriff auf die für den Geschäftszweck auch der weiteren Online-Dienste erforderlichen Daten des neuen Personalausweises. Die Kommunikation zwischen dem Nutzer und dem SkIDentity-Dienst erfolgt

über eine Webanwendung in Verbindung mit einem geeigneten eID-Client gemäß [TR-03124][10]. Für den Datenzugriff muss sich der SkIDentity-Dienst zunächst gegenüber dem Nutzer identifizieren. Im Anschluss kann der Nutzer über die Eingabe seiner eID-PIN die Daten freigeben, die in die abgeleitete elektronische Identität übernommen werden sollen.

Nach der Erstellung der abgeleiteten Identität durch den SkIDentity-Dienst wird diese im System des Nutzers gespeichert und die zwischenzeitlich im SkIDentity-Dienst vorhandenen Daten werden wieder gelöscht.

3.4 Einsicht in Inhalte einer elektronischen Identität

Der Benutzer kann Einsicht in die Inhalte eines elektronischen Ausweises oder einer abgeleiteten elektronischen Identität erhalten. Dies umfasst die Anzeige der enthaltenen personenbezogenen Attribute sowie die Anzeige des Gültigkeitszeitraumes der elektronischen Identität. Bei der Einsicht in eine abgeleitete elektronische Identität liegen die Daten ausschließlich im lokalen System des Nutzers vor. Eine „Cloud Identität“ ist nur einen gewissen Zeitraum gültig und kann bei Bedarf durch den Nutzer erneuert werden. Außerdem kann der Nutzer seine „Cloud Identität“ aktivieren bzw. deaktivieren (siehe Abschnitt 3.5), sie auf ein anderes System übertragen (siehe Abschnitt 3.6), sie an einen kryptographischen Schlüssel binden (siehe Abschnitt 3.7), sie schließlich wieder sperren und löschen (siehe Abschnitt 3.8) oder zur Authentisierung bei einem anderen Online-Dienst nutzen (siehe Abschnitt 3.9).

3.5 Aktivieren und Deaktivieren einer „Cloud Identität“

Eine im System des Nutzers abgelegte abgeleitete elektronische Identität kann vom Nutzer aktiviert oder deaktiviert werden. Der wesentliche Unterschied zwischen einer aktivierten oder deaktivierten abgeleiteten elektronischen Identität besteht darin, dass nur eine aktivierte abgeleitete elektronische Identität, wie in Abschnitt 3.9 näher erläutert, bei einem anderen Online-Dienst genutzt werden kann.

Die Aktivierung und Deaktivierung einer abgeleiteten elektronischen Identität erfolgt ausschließlich im lokalen System des Nutzers.

3.6 Übertragen einer „Cloud Identität“

Der Nutzer kann eine in seinem System abgelegte abgeleitete elektronische Identität an ein anderes technisches System, wie z.B. sein persönliches Mobiltelefon, übertragen. Wie in Abbildung 5 angedeutet, kann dies beispielsweise durch Übertragen eines Links in einen anderen Browser bzw. abfotografieren eines QR-Codes erfolgen. Erwähnenswert ist hierbei, dass der Link bzw. der QR-Code lediglich die für die sichere und über den SkIDentity-Dienst vermittelte Übertragung der kryptographisch geschützten „Cloud Identität“ notwendigen Informationen enthält und der Rest der Transformation vom SkIDentity-Dienst vorgenommen wird.

[10] Sofern neben dem elektronischen Personalausweis auch andere Chipkarten der eCard-Strategie [Kowa07] oder internationale Ausweiskarten genutzt werden sollen, empfiehlt sich hierfür der Einsatz der „Open eCard App“ (siehe [HPS+12] und [WPS+13]).

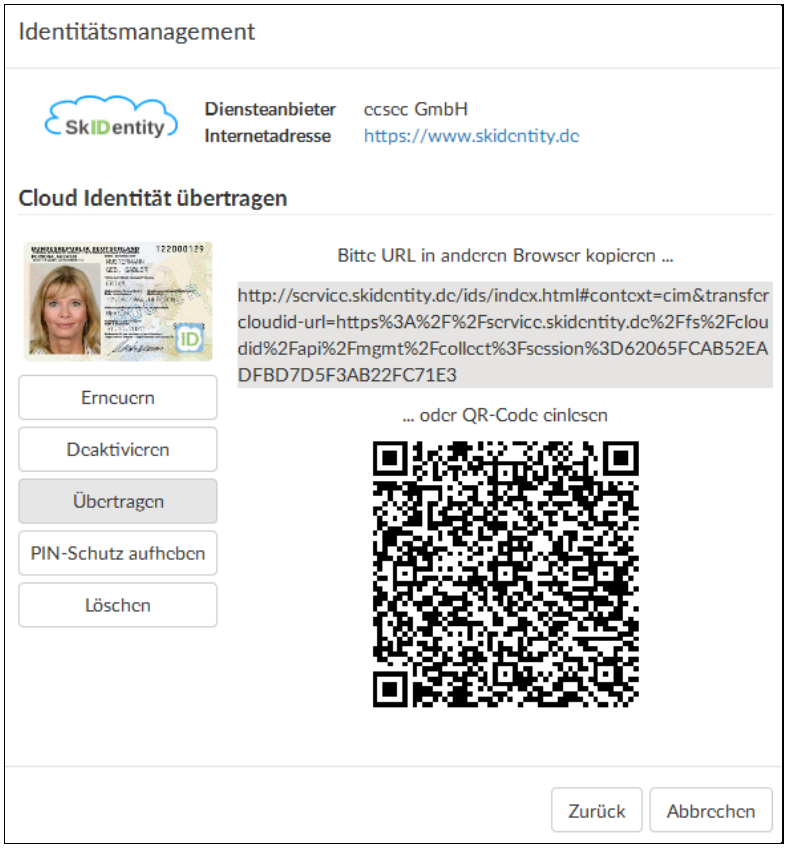

Abb. 5: Übertragen einer „Cloud Identität“ an ein anderes System

3.7 Schützen einer „Cloud Identität“

Zum Schutz vor unautorisierter Einsichtnahme und missbräuchlicher Nutzung kann eine im System des Nutzers abgelegte „Cloud Identität“ vom Nutzer mit einer Sicherheits-PIN geschützt und/oder an zusätzliche kryptographische Schlüssel des Benutzers gebunden werden. Analog zu den im SAML-Umfeld bekannten Holder-of-Key-Bindings (siehe [Scav10], [KlSc10]) kann eine „Cloud Identität“ an ein asymmetrisches Schlüsselpaar gebunden werden, wodurch der Missbrauch einer „Cloud Identität“ wirksam verhindert und ein dem ursprünglichen Ausweis und elektronischen Identitätsnachweis angenähertes Sicherheitsniveau erreicht werden kann. Für die kryptographische Bindung der „Cloud Identität“ kann asymmetrisches Schlüsselmaterial in einem entsprechenden Hardware-Token, wie z.B. einer Signaturkarte, einem FIDO Universal Second Factor (U2F) Authentication Token[11], bzw. alternativ Schlüsselmaterial im Browser genutzt werden, das mit Mechanismen der Web Cryptography API[12] erzeugt werden kann.

[11] Siehe https://fidoalliance.org/certification/fido-certified/ .

[12] Siehe http://www.w3.org/TR/WebCryptoAPI/ .

3.8 Sperren und löschen einer „Cloud Identität“

Der Nutzer kann eine abgeleitete elektronische Identität sperren und unwiederbringlich löschen. Falls ein Gerät mit einer „Cloud Identität“ verloren oder gestohlen wird, können unter Verwendung des ursprünglichen Ausweises alle aus diesem Ausweis abgeleiteten „Cloud Identitäten“ gesperrt werden.

3.9 Nutzen einer elektronischen Identität bei einem Dienst

Der Nutzer kann einen elektronischen Ausweis oder eine auf seinem System abgelegte und aktivierte abgeleitete elektronische Identität bei anderen Online-Diensten für einen vollständig selbstbestimmten Identitätsnachweis oder eine pseudonyme Anmeldung nutzen. Hierbei erfolgt eine Authentisierung des Nutzers gegenüber dem SkIDentity-Dienst, der ein geeignetes Identitätsbestätigungstoken für den entsprechenden Online-Dienst erstellt, mit dem die Echtheit der Identitätsdaten nachgewiesen werden kann.

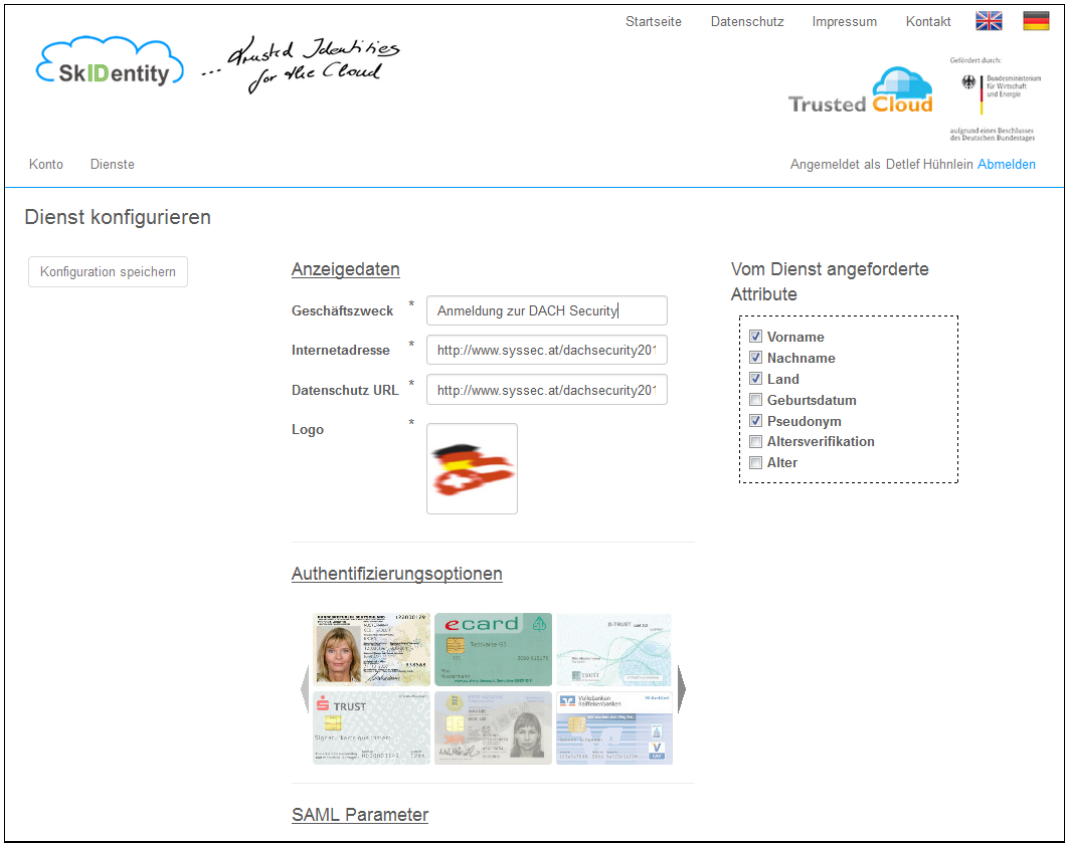

Abb. 6: Konfiguration eines Dienstes über eine komfortable Webanwendung

4 SkIDentity aus Sicht der Onlinedienste-Anbieter

Die Anbieter von Online-Diensten kommen durch SkIDentity in den Genuss, starke Authentisierungsmechanismen und vertrauenswürdige Identitäten bequem und kosteneffizient als Dienstleistung aus der Cloud beziehen zu können. Hierfür können diese Online-Dienste geeignete Föderationsprotokolle, wie z.B. SAML 2.0 [CKPM05] oder OAuth 2.0 [RFC6749] nutzen, um mit dem SkIDentity-Dienst zu kommunizieren. Sofern der Online-Dienst nicht ohnehin bereits diese Standardprotokolle unterstützt, kann diese Funktionalität leicht unter Verwendung

eines entsprechenden „Cloud Connector“ (siehe Abschnitt 2.4) integriert werden. Damit der SkIDentity-Dienst besonders leicht in Online-Diensten genutzt werden kann, steht mit dem SkIDentity-Management-Service eine benutzerfreundliche Anwendung für die Konfiguration und Verwaltung der SkIDentity-Anbindung bereit.

5 Zusammenfassung

Die kürzlich bekannt gewordenen Fälle massiven Identitätsmissbrauchs[13] unterstreichen die Bedeutung der starken Authentisierung in Cloud- und Webanwendungen, wie sie vom BSI seit Jahren[14] gefordert wird. Vor diesem Hintergrund wurden im SkIDentity-Projekt (siehe www.SkIDentity.de) die hierfür maßgeblichen internationalen Standards identifiziert und zu einer umfassenden Referenzarchitektur für die starke Authentisierung in der Cloud integriert. Das Herzstück dieses Systems ist der hier näher vorgestellte SkIDentity-Dienst, der die Nutzung von verschiedenen elektronischen Ausweisen und die Erstellung und Verwaltung von abgeleiteten elektronischen Identitäten ermöglicht. Hierbei können aus beliebigen standardkonformen Ausweisdokumenten sogenannte „Cloud Identitäten“ abgeleitet und beispielsweise auf ein Smartphone übertragen werden, um den mobilen elektronischen Identitätsnachweis („Mobile eID“) zu ermöglichen. Anbieter von Online-Diensten können diese vertrauenswürdigen Identitätsinformationen und starken Authentisierungsmechanismen ab sofort bequem und kosteneffizient als „Software as a Service“ Angebot aus der Cloud beziehen. Durch die Kombination dieser beiden Aspekte bietet der innovative SkIDentity-Dienst gewissermaßen „Mobile eID as a Service“.

Literatur

[BHH+14] S. Baszanowski, H.-M. Haase, T. Hühnlein, M. Tuengerthal, D. Henze, U. Renz: Der SkIDentity Cloud Connector. In: M. Kubach, D. Hühnlein (Hrsg.): Vertrauenswürdige Identitäten für die Cloud: Arbeiten und Ergebnisse des SkIDentity-Projekts, (2014)

[BoMa03] C. Boyd, A. Mathuria: Protocols for authentication and key establishment. Springer, (2003)

[BSI11a] BSI: Sicherheitsempfehlungen für Cloud Computing Anbieter - Mindestsicherheitsanforderungen in der Informationssicherheit. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile, (2011)

[BSI11b] BSI: Mindestanforderungen zur Informationssicherheit bei eCommerce-Anbietern, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Mindestanforderungen-eCommerce-Anbieter.pdf?__blob=publicationFile, (2011)

[BSI13] BSI: Offizielles Portal für die AusweisApp des Bundes, http://ausweisapp.bund.de, (2013)

[13] Siehe z.B. [BSI14c], [BSI14b] und [BSI14a].

[14] Siehe z.B. [BSI11a] und [BSI11b].

[BSI14a] BSI: Milliardenfacher Identitätsdiebstahl: Stellungnahme des BSI. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Milliardenfacher_Datendiebstahl_06082014.html, (2014)

[BSI14b] BSI: Neuer Fall von großflächigem Identitätsdiebstahl: BSI informiert Betroffene. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Neuer_Fall_von_Identitaetsdiebstahl_07042014.html, (2014)

[BSI14c] BSI: Millionenfacher Identitätsdiebstahl: BSI bietet Sicherheitstest für E-Mail-Adressen, https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Mailtest_21012014.html, (2014)

[CKPM05] S. Cantor, J. Kemp, R. Philpott, E. Maler: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0., https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, (2005)

[CEN15480] CEN 15480: Identification card systems – European Citizen Card. Part 1 – 4, (2008)

[ECSEC14] ecsec GmbH: Datenschutzerklärung für SkIDentity Identitätsmanagement, https://service.skidentity.de/privacy_de.pdf, (2014)

[EGAM14] J. Eichholz, H. Grobbel, H. Aschauer, G. Meister: Patentnr. EP 2136528 B1, (2014)

[HoHS14] G. Hornung, D. Hühnlein, S. Sädtler: Eine "BürgerCloud" für mehr Partizipation – Rechtliche Rahmenbedingungen und Ansätze zur Umsetzung, FTVI/FTRI, LNI 229, S. 63-79, https://ecsec.de/pub/2014_FTVI.pdf, (2014)

[HHR+11] D. Hühnlein, G. Hornung, H. Rossnagel, J. Schmölz, T. Wich, J. Zibuschka: SkIDentity – Vertrauenswürdige Identitäten für die Cloud, DACH Security, http://www.ecsec.de/pub/2011_DACH_SkIDentity.pdf, (2011)

[HPS+12] D. Hühnlein, D. Petrautzki, J. Schmölz, T. Wich, M. Horsch: On the design and implementation of the Open eCard App, Sicherheit 2012, http://subs.emis.de/LNI/Proceedings/Proceedings195/95.pdf, (2012)

[HSW+12] D. Hühnlein, J. Schmölz, T. Wich, B. Biallowons, M. Horsch, T. Hühnlein: Standards und Schnittstellen für das Identitätsmanagement in der Cloud, DACH Security 2012, http://www.ecsec.de/pub/2012_DACH_IdM.pdf, (2012)

[HSW+13] D. Hühnlein, J. Schmölz, T. Wich, B. Biallowons, T. Hühnlein: Starke, kosteneffiziente und benutzerfreundliche Authentisierung in der Cloud - ein Widerspruch in sich? BSI-Kongress, S. 177-188, http://www.ecsec.de/pub/2013_BSI-Cloud.pdf, (2013)

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

[ITSG] Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Bundestagsdrucksachen 18/4096 und 18/5121, https://www.bundestag.de/dokumente/textarchiv/2015/kw24_de_it_sicherheit/377026, (2015)

[KlSc10] N. Klingenstein, T. Scavo: SAML V2.0 Holder-of-Key Web Browser SSO Profile Version 1.0, OASIS Committee Specification 02, 10 August 2010,

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-holder-of-key-browser-sso.pdf, (2010)

[Kowa07] B. Kowalski: Die eCard-Strategie der Bundesregierung im Überblick. BIOSIG 2007: Biometrics and Electronic Signatures. LNI 108, S. 87-96, (2007) http://subs.emis.de/LNI/Proceedings/Proceedings108/gi-proc-108-008.pdf

[NIST14] NIST 800-157: Guidelines for Derived Personal Identity Verification (PIV) Credentials, March 2014 (2014) http://csrc.nist.gov/publications/drafts/800-157/sp800_157_draft.pdf

[RFC6749] RFC 6749: D. Hardt: The OAuth 2.0 Authorization Framework, (2012)

[Scav10] T. Scavo: SAML V2.0 Holder-of-Key Assertion Profile Version 1.0, OASIS Committee Specification 02, 23. January 2010, http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml2-holder-of-key.html, (2010)

[ScMo13] M. Schröder, F. Morgner: eID mit abgeleiteten Identitäten, Datenschutz und Datensicherheit (DuD), 530-534, (2013)

[TR-03124] BSI TR-03124: eID-Client. Technical Guideline, Part 1-2, Version 1.2, (2015)

[WPS+13] T. Wich, D. Petrautzki, J. Schmölz, M. Horsch & D. Hühnlein: An extensible platform for eID, signatures and more, Open Identity Summit 2013, LNI 223, S. 55-68, (2013), http://www.ecsec.de/pub/2013_OID_Platform.pdf