Realisierung von vertrauenswürdigem Cloud-Computing mit SkIDentity: Der Anwendungsfall in Wertschöpfungsketten der Automobilindustrie

Guntram Flach, Fraunhofer IGD
Joachim-Jungius-Str. 11, 18059 Rostock
guntram.flach@igd-r.fraunhofer.de

Michael Kubach, Eray Oezmue, Fraunhofer IAO
Nobelstr. 12, 70569 Stuttgart
Eray.Oezmue@iao.fraunhofer.de

Immo Wehrenberg, ENX Association
Bockenheimer Landstraße 97-99, 60325 Frankfurt am Main
immo.wehrenberg@enx.com

Abstract: Ziel des SkIDentity-Projektes ist es, eine tragfähige Brücke zwischen den sicheren elektronischen Ausweisen (eID) und den heute existierenden bzw. sich entwickelnden Cloud-Computing-Infrastrukturen zu schlagen. Somit können vertrauenswürdige Identitäten für die Cloud bereitgestellt und komplette Prozess- und Wertschöpfungsketten sicher gestaltet werden. Hierfür werden existierende Komponenten, Dienste und Vertrauensinfrastrukturen zu einer umfassenden, rechtskonformen, wirtschaftlich sinnvollen und sicheren Identitätsinfrastruktur für die Cloud integriert und in breitenwirksamen Pilotprojekten erprobt. Eine solche Pilotapplikation ist ein Projektworkspace, der auf die Bedürfnisse der verteilten Wertschöpfungsketten der Automobilindustrie abgestimmt ist. Die SkIDentity-Technologie ermöglicht über einen eID-Broker den verschiedenen an einem Projekt beteiligten Entwicklern eine starke Authentisierung am Projektworkspace mit den unterschiedlichen bereits in ihrem Unternehmen vorhandenen Credentials im Sinne eines föderierten Identitätsmanagements. Diese Arbeit stellt die SkIDentity-Technologie vor und illustriert deren Vorteile anhand der Pilotapplikation.

1 Einleitung

Für ein vertrauenswürdiges Cloud Computing werden sichere und zuverlässige Mechanismen zur Authentisierung benötigt. Gleichzeitig ist eine möglichst nutzerfreundliche Gestaltung der Bedienoberfläche und des zugehörigen Prozesses notwendig, um eine hohe Nutzerakzeptanz zu erreichen (vgl. [Senk12]). Nur eine Lösung, die gute Benutzbarkeit mit hoher Sicherheit verbindet, wird die Authentisierung an Cloud Computing Systemen nachhaltig sicherer machen können.

Das Ziel des SkIDentity-Projektes[1] ist es daher, eine Architektur zu schaffen, die von vornherein darauf ausgelegt ist, flexibel mit Lösungen verschiedenster Anbieter zusammen zu arbeiten. Diese Anbieter können dabei einen oder mehrere Authentisierungsdienste anbieten oder auch Identitätsdaten und Authentifikation für die von ihnen betriebenen Anwendungen nutzen; beliebige Kombinationen sind möglich. Dabei werden sowohl die technischen und organisatorischen Aspekte, als auch die rechtlichen Voraussetzungen berücksichtigt.

Im Ergebnis sollen die Nutzer ihren bevorzugten „Ausweis“ (Credential) für die starke Authentisierung bei verschiedenen Anwendungen nutzen können. Dies verringert die Zahl der vom Benutzer zu merkenden oder zu verwaltenden Zugangsinformationen oder Credentials und erspart ihm das wiederkehrende Vertraut machen mit neuen Authentisierungsmechanismen. Diese Vereinfachung erhöht gleichzeitig die Sicherheit, da die ablaufenden Schritte und Abfolgen für den Benutzer nachvollziehbarer, verständlicher und wiedererkennbar werden.

2 Anwendungsszenario

Die Automobilindustrie ist unter anderem dadurch gekennzeichnet, dass die Automobilhersteller (OEM) wesentliche Teile der Wertschöpfung nicht selbst erledigen, sondern auf die verlängerte Werkbank ihrer Zulieferer auslagern. Diese Zulieferer entwickeln und stellen für die OEMs nicht lediglich einfache Teile wie Schrauben her, sondern tragen zum Endprodukt durch die Entwicklung und Produktion komplexer Module, wie etwa kompletter Sitze, entsprechend der Vorgaben des OEMs, bei. Diese Tier1-Zulieferer arbeiten ihrerseits wiederum mit Tier2-Zulieferern zusammen, von welchen sie Komponenten beziehen. Insofern wird von einer verteilten Wertschöpfungskette gesprochen.

Der hohe Wettbewerbsdruck in der Automobilindustrie macht eine Senkung der Time-to-Market unumgänglich. Dies wird unter anderem durch eine interaktive Zusammenarbeit der Ingenieure von OEMs und Zulieferern in Multibenutzerapplikationen erreicht. Aufgrund der komplexen netzwerkartigen Wettbewerbsstruktur der Automobilindustrie arbeiten jedoch sowohl OEMs als auch Tier1- und Tier2-Zulieferer für unterschiedliche Komponenten zur gleichen Zeit mit zahlreichen jeweils konkurrierenden Partnern zusammen. Aus diesem Grund ist eine wirksame Zugriffskontrolle für den Austausch und die gemeinsame Bearbeitung technischer Spezifikationen und Komponentendesigns unbedingt erforderlich (Siehe Abbildung 1).

---

[1] www.skidentity.de; das SkIDentity Projekt zählt zu den Gewinnern des „Trusted Cloud“ Technologiewettbewerbs (www.trusted-cloud.de) des Bundesministerium für Wirtschaft und Technologie (BMWi) und zielt auf die Bereitstellung vertrauenswürdiger elektronischer Identitäten für Cloud Computing Dienste ab. Es wird von einem interdisziplinären Expertenteam unter Leitung der ecsec GmbH und mit Beteiligung der ENX Association, der Fraunhofer Institute IAO und IGD, der OpenLimit SignCubes GmbH, der Ruhr Universität Bochum, der Universität Passau, der Urospace GmbH und der VDG Versicherungswirtschaftlicher Datendienst GmbH durchgeführt. Darüber hinaus wird das SkIDentity Projekt von maßgeblichen Verbänden, wie dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), dem EuroCloud Deutschland_eco e.V., dem ProSTEP iViP e.V. und dem TeleTrusT – Bundesverband IT-Sicherheit e.V. sowie renommierten Unternehmen wie der DATEV eG, der easy Login GmbH, der media transfer AG, der SAP AG und der SiXFORM GmbH unterstützt.

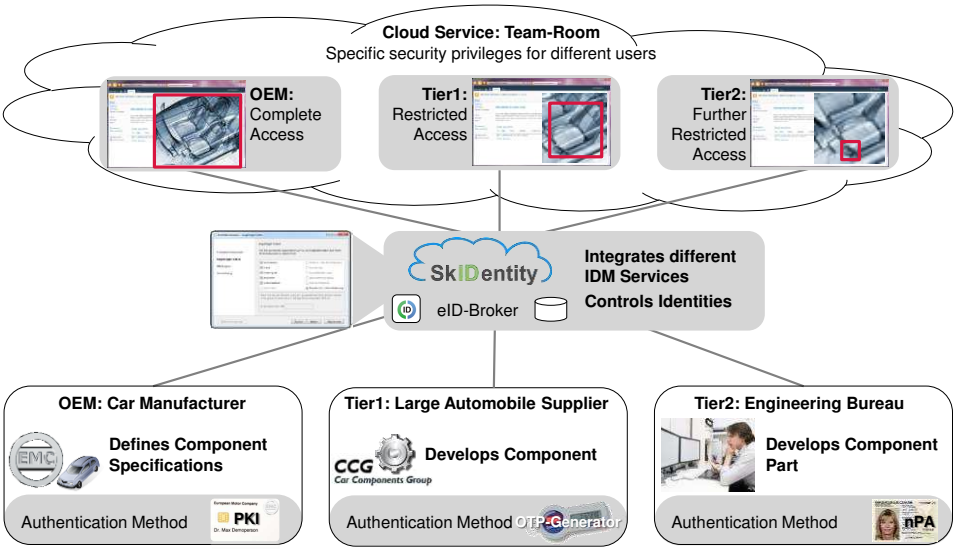

Abbildung 1: Rahmen für das Experimentalsystem

Diese Zugriffskontrolle stellt bereits innerhalb eines Unternehmens eine Herausforderung für das Identitätsmanagement (IdM) dar. Sind jedoch mehrere unabhängige Unternehmen (OEMs, Zulieferer und gegebenenfalls Service/Cloud-Provider) beteiligt, nimmt die Komplexität der Aufgabe einer vertrauenswürdigen Identifizierung aller beteiligten Ingenieure im Sinne eines föderierten Identitätsmanagements deutlich zu. Beispielsweise verwenden die unterschiedlichen Unternehmen jeweils eigene Authentifizierungsverfahren und Sicherheitspolicies, die vom Service/Cloud-Provider zu implementieren sind. Außerdem werden Ingenieure durch die Unternehmen ihrem Bedarf entsprechend dem Projekt zugeordnet oder abgezogen, weshalb die Zugriffsberechtigungen immer aktuell zu halten. Die ökonomische und technische Leistungsfähigkeit insbesondere kleinerer Akteure ohne größere IT-Abteilung stößt somit aufgrund der Vielzahl zu erfüllender Anforderungen schnell an Grenzen.

Der Pilotapplikation stellt in diesem Setting nun einen gemeinsamen Workspace als Cloud-Anwendung zur Verfügung, auf welchen unterschiedliche Akteure mit unterschiedlichen Berechtigungen zugreifen können. Die Authentifizierung erfolgt über den eID-Broker mittels der bereits in den Organisationen vorhandenen Credentials. Sie wurde in die Architektur von SkIDentity integriert und derart entwickelt, dass sie als Experimentalsystem für weitere Forschungs- und Entwicklungsarbeiten sowie für öffentliche Präsentationen genutzt werden kann.

Ausgehend vom geschilderten Anwendungsszenario und den genannten Anforderungen wird im nächsten Abschnitt die SkIDentity-Architektur kurz vorgestellt, bevor darauf folgend einige Realisierungsaspekte genauer präsentiert werden.

3 Systemarchitektur

Im Rahmen des Projektes wurde die in Abbildung 3 dargestellte Systemarchitektur entwickelt. Das SkIDentity-System baut auf dem Konzept des „Föderierten Identitätsmanagements“ (vgl. [HRZ10], [SAM05], [Open07] und Abbildung 2) auf und verfeinert die Komponenten „Client“, „Service Provider“ und „Identity Provider“, so dass unterschiedlichste Authentisierungsmechanismen, -dienste und -protokolle in einer einheitlichen und sicheren Weise in beliebigen Anwendungen genutzt werden können.

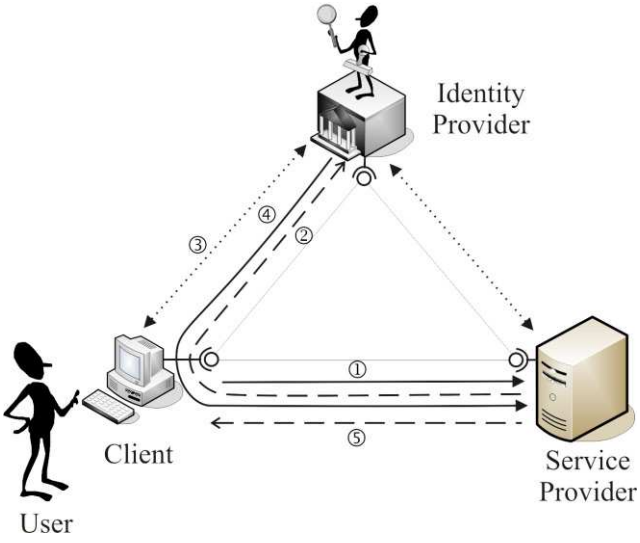

Abbildung 2: Föderiertes Identitätsmanagement

Hierdurch können insbesondere auch die zunehmend verbreiteten eID-Karten, die von staatlicher Seite ausgestellt werden, in der SkIDentity-Infrastruktur genutzt werden. Hierzu zählt insbesondere der neue Personalausweis (nPA) in Deutschland oder vergleichbare Dokumente anderer Staaten. Diese Karten werden wegen des behördlichen Vertrauensankers als sicher wahrgenommen und erreichen nach vollständiger Einführung eine hohe Verbreitung. Beim Entwurf der Systemarchitektur wurde deshalb insbesondere auf Konformität mit den Vorgaben des deutschen Personalausweisgesetzes geachtet [HoHH12].

Wie in Abb. 3 ersichtlich, umfasst die SkIDentity-Referenzarchitektur für die starke Authentisierung in der Cloud Systemkomponenten beim Benutzer, Systemkomponenten beim Dienstanbieter, sowie entsprechende Infrastrukturkomponenten.

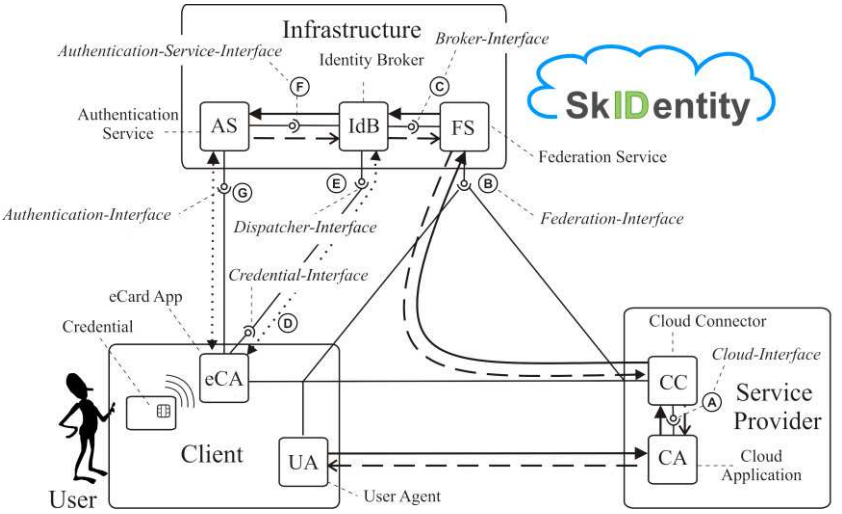

Abbildung 3: SkIDentity-Referenzarchitektur

4 Architekturkomponenten

Die für den Lösungsansatz notwendigen Überlegungen werden im folgenden Abschnitt durch eine Auswahl verschiedener Realisierungsaspekte kurz vorgestellt.

Identity Broker (IdB)

Der IdB ist die zentrale Komponente in der SkIDentity-Infrastruktur, die bei einer vom CC bzw. FS übermittelten Authentisierungsanfrage zunächst ermittelt, welche Credentials beim Benutzer vorhanden sind, so dass ein geeigneter Dienst für die Benutzerauthentisierung ausgewählt werden kann.

Federation Services (FS)

Hierbei handelt es sich um optionale Dienste, die entsprechende Föderationsprotokolle etwa gemäß [SAM05], [Open07] oder [Ham10] unterstützen und bei entsprechend ausgestalteter Authentisierungspolitik ein Single Sign-On ermöglichen. Hierdurch muss sich ein Benutzer nur einmal authentisieren, um (über einen gewissen Zeitraum) eine Vielzahl von Anwendungen nutzen zu können.

Cloud Connector (CC)

Über den CC wird die CA in die SkIDentity-Infrastruktur integriert (Siehe Abbildung 3). Hierbei wird mit dem Federation Service (FS) oder direkt mit dem IdB kommuniziert. Der CC wird bei der CA betrieben. Er erweitert die CA um die Fähigkeit, Identitäten und Authentifikation mit Hilfe eines vom IdB oder von einem FS unterstützten Protokolls zu nutzen. CAs die eine solche Funktionalität von Hause aus bieten, haben einen CC bereits integriert. Sollte eine solche Funktionalität nicht verfügbar sein, kann der CC entweder direkt in die CA integriert werden (etwa durch Nutzung einer Programmbibliothek) oder

als eigenständiger Prozess die Daten von IdB bzw. FS entgegennehmen und der Applikation in einer für sie geeigneten Form weiterleiten.

Authentication Services (AS)

Der AS wird vom IdB aufgerufen, um die tatsächliche Benutzerauthentisierung durchzuführen. Das hierfür einzusetzende Authentisierungsprotokoll hängt vom Credential ab. Beispielsweise wird für die Authentisierung mit dem nPA das Extended Access Control (EAC) Protokoll gemäß [BSI12] sowie eine ENX-spezifische Firmen-Karte genutzt.

5 Demonstrator

Das Automotive-Szenario wurde bereits in Kapitel 2 ausführlich erläutert. Ein beziehungsweise mehrere Unternehmen in einem Hersteller-Lieferantennetzwerk in der Automobilindustrie entscheiden sich für die Nutzung der SkIDentity-Infrastruktur zur sicheren Authentisierung in von ihnen gemeinsam genutzten Cloud Services. Beispielhaft hierfür steht die OwnCloud-Plattform im realisierten Demonstrator[2]. Die Anmeldung via SkIDentity kann über einen in den jeweiligen Service eingebundenen SkIDentity-Button erfolgen. Der Benutzer wird dann von SkIDentity an einen verfügbaren IdP verwiesen und meldet sich dort mit einem verfügbaren sowie erlaubten Credential an. Ist die Authentisierung erfolgreich, erfolgt die Anmeldung im Cloud Service und der Benutzer kann diesen wie vorgesehen nutzen.
Neben der Evaluierung des derzeitigen Demonstrator-Ansatzes wird in zukünftigen Arbeiten die Auswertung der qualitativen Marktanalyse für ein föderiertes Identitätsmanagement durchgeführt. Die Ergebnisse der Analyse fließen in die gesamte SkIDentity-Architektur sowie insbesondere in das Design der Pilotapplikation und der im nächsten Schritt zu entwerfenden Business Cases ein.

Literaturverzeichnis

[BSI12] BSI: 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, 2012

[Ham10] Hammer-Lahav, E.: The OAuth 1.0 Protocol, Request For Comments – RFC 5849, http://www.ietf.org/rfc/rfc5849.txt, 2010

[HoHH12] Hornung, G., Horsch, M., Hühnlein, D.: Mobile Authentisierung und Signatur mit dem neuen Personalausweis, DuD, 36(3):189-194, 2012

[HRZ10] Hühnlein D., Roßnagel, H., Zibuschka, J.: Diffusion of Federated Identity Management, in F. Freiling (Hrsg.), Tagungsband „Sicherheit 2010“, GI-Edition Lecture Notes in Informatics (LNI) 170, 2010, Seiten 25-37, http://www.ecsec.de/pub/Sicherheit2010.pdf

[Open07] OpenID Foundation: OpenID Authentication 2.0. Final, December 5, 2007. http://openid.net/specs/openid-authentication-2_0.html

[SAM05] 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

[Senk12] Senk, C.: Future of Cloud-based Services for Multi-factor Authentication: Results of a Delphi Study, Proceedings of 3rd International Conference on Cloud Computing, CLOUDCOMP, 2012

[2] https://www.skidentity.de/de/demo/