DOI: 10.2195/lj_Proc_schier_de_201605_01
URN: urn:nbn:de:0009-14-43636

Cloud-Architektur für Privacy-Management in kollaborativen Logistikprozessen

Cloud architecture for privacy management in collaborative logistics processes

Arkadius Schier
Lucas Petrich
Michael ten Hompel

Fraunhofer-Institut für Materialfluss und Logistik IML, Dortmund

Björn Schwarzbach
Bogdan Franczyk

Universität Leipzig

Durch den großen Erfolg des Cloud Computing und der hohen Geschwindigkeit, mit der Cloud-Innovationen seither Einzug in die Praxis finden, eröffnen sich für die Industrie neue Chancen im Wettbewerb. Von besonderer Bedeutung sind die Möglichkeiten, Cloud-gestützte Geschäftsprozesse dynamisch, als direkte Reaktion auf einen Kundenauftrag, anzupassen und auszuführen. Dies gilt insbesondere auch für kooperative und unternehmensübergreifende Anwendungen, welche aus mehreren IT-Diensten verschiedener Partner bestehen. Gegenstand dieses Artikels ist die Vorstellung eines Konzeptes und einer Architektur für eine zentrale Cloud-Plattform zur Konfiguration, Ausführung und Überwachung von kollaborativen Logistik-Prozessen. Auf dieser Plattform können Geschäftsprozesse modelliert und in ihren Privacy-Eigenschaften parametrisiert werden. Die einzelnen Prozesselemente werden dabei mit IT-Diensten verknüpft, die beispielsweise auf externen Cloud-Plattformen ausgeführt werden. Ein Schwerpunkt der Veröffentlichung liegt in der Betrachtung der Erstellung, Umsetzung und Überwachung von Privacy-Anforderungen.

[Schlüsselwörter: Management, Cloud, Logistik, Privacy, Organisation und Betrieb]

With the big success of cloud computing and the big velocity, in which cloud-innovations are realized, new chances for competition in the industry are established. Of particular importance are the possibilities to adjust and accomplish cloud-based business processes dynamically as a direct reaction on a customer's order. This applies in particular to cooperative and enterprise-wide applications, which consist of several IT-services from different partners. The subject of this article is the introduction of a concept and an architecture for a central cloud-platform for configuration, execution and monitoring of collaborative logistics processes. On this platform, business processes can be modeled and parameterized in their Privacy properties. The particular process elements are linked with IT-services, which can be executed on external cloud platforms. A focus of the publication on the creation, implementation and monitoring of privacy requirements.

[Keywords: Management, Cloud, Logistics, Privacy, Organization and Enterprise]

1 EINFÜHRUNG

Cloud Computing hat nicht nur großen Erfolg aufzuweisen, sondern ist auch immer weiter verbreitet und findet in vielen Industriezweigen Anwendung [WR13]. Für die Logistik gewinnt das Cloud Computing durch seine Dynamik, dezentrale Verteilung und die Abstraktion sowie Auslagerung von physischen IT-Systemen an Attraktivität besonders in Anbetracht der Kombination verschiedenster IT-Dienste im Supply-Chain-Management. Eine Supply-Chain besteht in der Regel aus mehreren Beteiligten und somit findet eine Kollaboration, welche zumeist von einem Beteiligten organisiert wird, statt. Durch das Outsourcing und die Nutzung des Wissens der verschiedenen Beteiligten ergibt sich eine Vielzahl von Vorteilen, welche die Effizienz einer Supply-Chain steigern können.

Das Management einer Kollaboration in die Cloud zu verlagern ist der logische nächste Schritt. Die Beteiligten können nicht nur einfacher an die von ihnen zur Ausführung benötigten Informationen gelangen, sondern die von ihnen zur Verfügung gestellten Dienste können direkt verknüpft und mit anderen kombiniert werden. Durch ein zentrales Management und die Dynamik des Cloud Computing können Kundenaufträge angepasster und effizienter ausge-

DOI: 10.2195/lj_Proc_autor1_de_jjjmm_01
URN: urn:nbn:de:0009-14-xxxxxx

führt werden. Der Gesamtprozess einer Supply-Chain besteht somit aus einer Verkettung von IT-Diensten unterschiedlicher Partner, welche miteinander interagieren und Informationen austauschen. Der jeweilige Dienst unterliegt dabei jedoch der lokalen Kontrolle des Partners und wird in der Cloud-Umgebung des Partners ausgeführt. Dies wird als Collaborative Business Process-as-a-Service (Collaborative BPaaS) bezeichnet. Dabei gewinnen Datenschutz- (Privacy-), Datensicherheit- und Vertraulichkeitsanforderungen erheblich an Bedeutung. Cloud-Provider müssen gewährleisten, dass sie die bei Collaborative BPaaS von einem Cloud-Dienst empfangenen und erzeugten Daten vertraulich behandeln und nur gemäß der Privacy-Einstellungen des Daten-Eigentümers respektive Dienstnutzers speichern oder an andere Dienste bzw. Provider übermitteln.

Die Verknüpfung der Dienste in der jeweiligen lokalen Cloud und die Ausführung des Gesamtprozesses auf einer zentralen Cloud-Plattform sowie der Datenaustausch und die Zugriffskontrolle müssen dafür jedoch genau geregelt und kontrolliert sein. Nur dadurch ist ein hohes Niveau an Datenschutz (Privacy), Datensicherheit und Vertraulichkeit zu gewährleisten. Es muss nicht nur der vertrauliche Umgang mit den Daten beim jeweiligen Anbieter des IT-Dienstes sichergestellt sein, sondern auch, dass dieser nur Zugang zu so vielen Daten wie nötig, aber zu so wenigen Daten wie möglich erhält. Um dies einheitlich umsetzbar zu gestalten, zu kontrollieren und zu zertifizieren ist eine zentrale Definition der Privacy-Anforderungen für den Umgang mit den jeweiligen Daten in Bezug auf die einzelnen, involvierten IT-Dienste eines Gesamtprozesses eine notwendige Bedingung.

Zusammen mit den Industriepartnern Zimory GmbH Berlin, Salt Solutions GmbH und PSI Logistics GmbH arbeitet das Institut für Wirtschaftsinformatik der Universität Leipzig, das Forschungszentrum FZID der Universität Hohenheim und das Fraunhofer-Institut für Materialfluss und Logistik IML in Dortmund im vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekt PREsTiGE (Privacy-erhaltende Methoden und Werkzeuge für Cloud-basierte Geschäftsprozesse) an der Entwicklung von Methoden und Werkzeugen zur Privacy-Erhaltung im Geschäftsmodell Collaborative Business-Process-as-a-Service (BPaaS). Als Zielgruppenkontakt wird zusammen mit dem Staatsbetrieb Sächsische Informatik Dienste in Dresden und der AHP GmbH & Co. KG in Berlin kooperiert. PREsTiGE adressiert die Privacy-Erhaltung insbesondere in kollaborativen Cloud-basierten Geschäftsprozessen, in denen ein Prozess nur eingeschränkt zentral ausgeführt wird. Als Zielgruppe dienen zum einen IT-Entwickler, welche in einem Service-Repository einzelne Cloud-basierte IT-Services beisteuern können. Zum anderen zielt man auf sogenannte Prozess-Designer in der Logistik, die als Zielgruppe auf die Services zugreifen und diese in der Cloud in Form eines Business Prozesses kombinieren können. Dies erweitert die existierende XaaS („Anything as a Service“) Bereitstellung um ein neues Level, welches als bereits zuvor aufgeführtes Collaborative Business Process as a Service (BPaaS) bezeichnet wird.

Der Artikel gliedert sich wie folgt. Das zweite Kapitel beschreibt den aktuellen Stand der Wissenschaft und der Technik in Bezug auf Cloud Computing und Privacy. Im dritten Kapitel folgt die Beschreibung des Konzeptes und der Architektur für eine zentrale Cloud-Plattform zur Konfiguration, Ausführung und Überwachung von kollaborativen Logistik-Prozessen. Den Schwerpunkt des Artikels bildet das vierte Kapitel, das auf die Privacy-Verwaltung in der Cloud eingeht. Hier werden Privacy-Anforderungen und Privacy-Regeln definiert. Außerdem erfolgt hier die Vorstellung einer flexiblen und standardisierten Beschreibungssprache für die Erstellung und Auswertung von Privacy-Regeln. Den Abschluss bildet das fünfte Kapitel, welches einen Ausblick auf die weiteren Arbeiten gibt.

2 Stand der Wissenschaft und Technik

2.1 Cloud Computing

Nach dem Bundesamt für Sicherheit in der Informationstechnik [BU12] bezeichnet Cloud Computing „das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.“

Bei der Definition von Cloud Computing sollten zudem die vom National Institute of Standards and Technology (NIST) definierten Charakteristiken [NI11] berücksichtigt werden:

- *On-demand Self Service:* Die Provisionierung der Ressourcen (z. B. Rechenleistung, Storage) läuft automatisch ohne Interaktion mit dem Service Provider ab.
- *Broad Network Access:* Die Services sind mit Standard-Mechanismen über das Netz verfügbar und nicht an einen bestimmten Client gebunden.
- *Resource Pooling:* Die Ressourcen des Anbieters liegen in einem Pool vor, aus dem sich viele Anwender bedienen können (Multi-Tenant-Modell). Dabei wissen die Anwender nicht, wo die Ressourcen sich befinden, sie können aber vertraglich den Speicherort, also z. B. Region, Land oder Rechenzentrum, festlegen.

DOI: 10.2195/lj_Proc_autor1_de_jjjmm_01
URN: urn:nbn:de:0009-14-xxxxxx

- *Rapid Elasticity:* Die Services können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher ‚unbegrenzt' zu sein.

- *Measured Services:* Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Anwendern zur Verfügung gestellt und fakturiert werden.

Eine serviceorientierte Architektur (SOA) ist eine der Grundvoraussetzungen für Cloud Computing [BU12]. Außerdem sollte eine Cloud-Umgebung mandantenfähig sein, da sich innerhalb dieser Umgebung viele Anwender gemeinsame Ressourcen teilen müssen. Allgemein betrachtet gibt es in dem Modell-Rahmen XaaS (Everything as a Service) drei Modelle [NI11], nach welchen Cloud Computing Anwendung findet:

- *Infrastructure as a Service (IaaS):* Bereitstellung von Rechenleistung und Speicherkapazitäten

- *Platform as a Service (PaaS):* Laufzeiten bzw. Entwicklungsumgebung als Dienstleistung über das Internet bereitstellen

- *Software as a Service (SaaS):* Software als Dienstleistung über das Internet zur Verfügung stellen

Zusätzlich werden in [NI11] vier Nutzungsmodelle für Cloud Services definiert. In der *Private Cloud* wird diese exklusiv von einzelnen Organisationen betrieben und genutzt. Erweiternd zu dem Modell bietet die *Community Cloud* eine exklusive Nutzung von einer spezifischen Community mit gemeinsamen Zielen. Die *Public Cloud* hingegen dient der offenen Nutzung von der Allgemeinheit, wird dabei von einer geschäftlichen, akademischen oder staatlichen Organisation betrieben. Als Hybrid Cloud wird eine Kombination der genannten Nutzungsmodelle bezeichnet. In den Nutzungsmodellen finden verschiedene Formen der Virtualisierung ihre Umsetzung [RCL]. Diese stellt eine wichtige Komponente dar, weil sie eine Abstraktion der logischen Ressourcen von den darunterliegenden physischen Ressourcen umsetzt und somit die Grundlage für die zuvor beschriebenen, essentiellen Charakteristiken des Cloud Computing darstellt. Durch Server-, Speicher- und Netzwerk-Virtualisierung können IT-Umgebungen einfach und dynamisch erstellt, erweitert, verkleinert und bewegt werden, was wesentlich zur Verbesserung der Agilität, der Skalierbarkeit und der Kosten beiträgt.

Bei der Integration verschiedener Anwendungen entsteht keine Schnittstellenproblematik und es wird eine kurzfristige Nutzung möglich, da die Konfiguration und Provisionierung mittels einer Webschnittstelle durch den Cloud-Nutzer selbst erfolgt, wobei wenig Interaktion mit dem Provider erforderlich ist. Dennoch steigt durch die geteilte Umgebung mit mehreren Nutzern und Internet-ähnlichen Services die Komplexität des Systems. Es kann den subjektiven Eindruck eines Kontrollverlustes erwecken, weil durch eine dynamische Verteilung über mehrere Standorte und die oben genannte Abstraktion subjektiv nicht mehr ermessen werden kann, wo exakt die Daten oder Services gespeichert bzw. gehostet werden. Um dem zuvorzukommen haben sich bereits Cloud Computing Dienstleistungen mit nationalem Hosting entwickelt, um dem Nutzer das Gefühl der Sicherheit zu geben, da der Datenfluss das eigene Land (angeblich) nicht verlässt [BU08].

Der rechtliche Rahmen des Cloud Computing ist selten eindeutig und klar, da die Haftungsbedingungen eines Providers von den zu erfüllenden Leistungspflichten abhängig sind [WE13]. Zudem stehen im Raum der Informationssysteme, besonders unter Betrachtung des Internets und des Cloud Computing, noch nicht eindeutig geklärte Fragen zu Urheberrecht und Datenschutz offen. Dies ist ein juristisch junger und noch umstrittener Bereich, dessen Bedeutung durch den internationalen Charakter der verteilten Systeme zunimmt. In [WE13] wird die offene Frage gestellt, ob Daten schutzfähig sind und unter welchen Bedingungen ein Schutz überhaupt möglich ist, wenn diese doch nicht einzelnen physischen Datenträgern exakt zugewiesen werden können.

Nach den Sicherheitsempfehlungen für Cloud Computing Anbieter [BU12] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sollen Standards geschaffen werden, um die Sicherheit von Cloud Computing Plattformen überprüfbar zu gestalten. Dabei sind Vertraulichkeit und Verfügbarkeit als Grundwerte zu schützen sowie die Sicherheit der Rechenzentren nach aktuellem Stand der Technik zu gewährleisten. Eine Sicherheit der Kommunikation ist dabei durch Verschlüsselung und weitere IT-Sicherheitsmaßnahmen sicherzustellen. Die Verwaltung der kryptographischen Dienste und Schlüssel erweist sich jedoch als komplex und durch einen Mangel der entsprechenden Werkzeuge als kaum umgesetzt. Wie in [J15] beschrieben ist der PGP-Standard zur Mail-Verschlüsselung „hochsicher, kaum genutzt, völlig veraltet". Technisch betrachtet handelt es sich um eine „großartige" Lösung, doch die Nutzung ist schwierig und kompliziert.

2.2 PRIVACY

In der weitesten Fassung ist Privacy in den Menschrechten der vereinten Nationen verankert [VE48], dennoch ist die Definition des Begriffes selbst komplex. Es gibt verschiedene Formen von Privacy, zum Beispiel das Recht „allein gelassen zu werden" oder das Recht „Informationen über sich selbst zu kontrollieren". In [SO06] wurde eine Taxonomie der Privacy erstellt, welche sich auf die Folgen

DOI: 10.2195/lj_Proc_autor1_de_jjjmm_01
URN: urn:nbn:de:0009-14-xxxxxx

von Privacy-Verletzungen konzentriert, was sich als hilfreiche Grundlage für die Entwicklung eine Risiko- und Nutzenanalyse darstellt [PE09].

Innerhalb der EU wurde 1995 die Richtlinie 95/46/EG des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr definiert [DA95]. Eine Neufassung dieses Gesetzes wurde im Jahr 2015 final vorgestellt. Eine endgültige Fassung muss jetzt im Trilog, bestehend aus Ministerrat, EU-Parlament und Kommission abgestimmt werden [ZE15]. In Deutschland wird die bisherige Fassung durch das Bundesdatenschutzgesetz in seiner Neufassung von 2003 umgesetzt [BU90]. Laut dem Electronic Privacy Information Center (EPIC) [JB05] ist „Datenschutz weitestgehend zu verstehen, als das Recht eines Individuums die Sammlung, Nutzung und Verbreitung seiner personenbezogenen Informationen, welche von anderen gehalten werden, zu kontrollieren".

Personenbezogene Informationen (Personally Identifiable Information, PII) sind in [DA95] definiert als „alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind." Dies ist in neueren Definition und Richtlinien [MI08] noch erweitert worden um „sensible PII, welche so wichtig für das Individuum sind, dass diese Informationen eines speziellen Schutzes benötigen."

Zusätzlich wird die Betrachtung des Datenschutzes um juristische Personen, Behörden und anderweitige Einrichtungen erweitert. Die wirtschaftlichen und geschäftlichen Betrachtungen von Privacy und Datenschutz im Speziellen geschehen auf verschiedenen Ebenen der Analyse und Umsetzung [PA09]:

- *Ebene des Individuums*: Das Individuum nimmt Privacy von einem psychologischen und manchmal auch juristischen Standpunkt war.

- *Ebene des ökonomischen Individuums*: Das ökonomische Individuum übt seine Rechte der Privacy, besonders die des Datenschutzes, auf wirtschaftlicher und sozialer Ebene aus (möglicherweise, aber nicht zwingend für den Erhalt eines Einkommens).

- *Ebene des Wirtschaftsverteters (Unternehmen, Regierung):* Der Wirtschaftsvertreter interagiert mit ökonomischen Individuen, falls diese eine Dienstleistung oder ein Produkt in Anspruch nehmen, welche den Wirtschaftsverteter einbeziehen. Das Ausmaß dieser Interaktionen hängt jedoch von den Entscheidungen und Empfindungen des Wirtschaftsvertreters, sowie von juristischen Aspekten ab.

- *Ebene einer Wirtschaft*: Die Wirtschaftsebene besteht aus mehreren Wirtschaftsvertretern, welche zeitweilig unter wirtschaftlichen, sozialen und geschäftlichen Bedingungen interagieren. Die Art dieser Interaktionen hängt letztendlich von den Privacy-Vorstellungen der Individuen, welche davon betroffen sind, ab.

- *Ebene eines Geschäftsprozesses:* Diese Ebene beinhaltet verschiedene Wirtschaftsvertreter und/oder ökonomische Individuen, welche bewusst als Teil eines Geschäftsprozesses miteinander agieren. Die Parteien der Individuen und Vertreter des Prozesses wünschen eine Aufrechterhaltung von Privacy gegenüber Dritten.

In diesem Artikel wird die fünfte Ebene „Ebene eines Geschäftsprozesses" um die Aufrechterhaltung von Datenschutz-Vorstellungen der verschiedenen Parteien eines Prozesses innerhalb des Geschäftsprozesses erweitert. Dies wird als „Business Privacy" bezeichnet. Der Begriff „Business Privacy" wurde im Rahmen des Forschungsprojektes PREsTiGE wie folgt definiert: „Bei Business Privacy handelt es sich um die Privatheit von geschäftlichen und verfahrensbezogenen Daten."

Für Unternehmen ist Privacy ein wichtiges Thema im Kontext von Geschäftsrisiko und Regelkonformität [PC09]. Die Vorteile von Cloud Computing - die Fähigkeit von schneller Skalierbarkeit, Fernspeicherung von Daten und dem Verbreiten von Services in einer dynamischen Umgebung - können zu Nachteilen für den Erhalt eines Datenschutz-Niveaus werden. Dies könnte jedoch zum Beispiel von Nöten sein, um nicht nur juristischen Gesetzgebungen gerecht zu werden, sondern auch um das Vertrauen potentieller Kunden zu erhalten. Um Organisationen und Unternehmen bei der Privacy-Einhaltung zur Seite zu stehen und diese vermehrt in die Pflicht zu nehmen, haben sich Vereinigungen gefunden und Anforderungen von Privacy an neue und bestehende Systeme formuliert. Zum Beispiel wurde im November 2007 vom UK Information Commissioners Office (ICO) ein „Privacy Impact Assessment (PIA) Prozess" veröffentlicht, um Organisationen bei der Beurteilung des Einflusses ihrer Operationen auf den eigenen Datenschutz zu bewerten [PE09]. Das Unternehmen Microsoft hat im Jahr 2008 „Privacy Guidelines for Developing Software Products and Services" veröffentlicht [MI08], um die Einhaltung von Datenschutz bei der Entwicklung neuer Software umzusetzen. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat

DOI: 10.2195/lj_Proc_autor1_de_jjjmm_01
URN: urn:nbn:de:0009-14-xxxxxx

im Jahr 2011 eine „PIA Guideline for RFID Applications“ [BU11] veröffentlicht, um Privacy-Risiken und deren Kontrolle in Bezug auf RFID-Anwendungen zu adressieren. Im Jahr 2011 hat das National Institute of Standard and Technology (NIST) „Guidelines for Security and Privacy in Public Cloud Computing“ veröffentlicht [NI11].

Bei der Entwicklung neuer Produkte und Dienstleistungen, besonders im Bereich des Cloud Computing, ist ein Privacy-by-Design nötig, welches laut [SB15] „vor allem bei Datenschützern als ideales Gestaltungsprinzip gilt. Doch konkrete Umsetzungshinweise und Anregungen für Entwickler gibt es nicht“.

Den aktuelle Stand der Forschung im Bereich von Datenschutz im Cloud Computing beschreibt [IKC09] wie folgt:

> “Research on data privacy in cloud computing is still in its early stages.”

Zu gleichen Aussagen kommen [PC09] und [ZYZ+12] in ihren Artikeln. Hier beschreiben die Autoren ebenfalls, dass Datenschutz im Cloud Computing von Bedeutung ist, jedoch die Problematik noch ungelöst ist, beziehungsweise sich im Anfangsstadium befindet.

3 KONZEPT UND ARCHITEKTUR DER KOLLABORATIVEN CLOUD-PLATTFORM

In diesem Kapitel werden das Konzept und die Architektur für eine zentrale Cloud-Plattform zur Konfiguration, Ausführung und Überwachung von kollaborativen Logistik-Prozessen beschrieben. Die Architektur gliedert sich, wie aus Abbildung 1 ersichtlich ist, in die drei Abschnitte: PREsTiGE Plattform, Gateways und Dienst-Provider. Die PREsTiGE Plattform ist aus den Modulen Konfigurator, Cockpit, Zertifizierung, Privacy-Management, Service Repository, Business Process Management System (BPMS) und Identity and Access Management System (IAMS) aufgebaut. Das IAMS [SSP+15] beantwortet Zugriffsanfragen durch die Auswertung der vom Privacy Management vorgegebenen Privacy-Anforderungen. Im Cockpit werden Privacy-Verletzungen sowie der aktuelle Stand der Ausführung eines Prozesses dargestellt.

Die Dienste der Dienst-Provider können auf unterschiedlichen externen Cloud-Plattformen ausgeführt werden und können über ein Human Interface (HI) des Service-Repositories in PREsTiGE Plattform zur weiteren Überprüfung aufgenommen werden. Bei der Überprüfung wird festgestellt, ob die angegebenen Dienst-Beschreibungen valide sind. Danach werden diese in das Service-Repository übernommen und stehen dem Nutzer in der PREsTiGE Plattform zur Verfügung. Im Konfigurator kann der Nutzer seinen Geschäftsprozess modellieren. Während der Modellierung können Privacy-Anforderungen und -Regeln (siehe Kapitel 4) in Verbindung mit dem Privacy-Management für einzelne Prozessschritte definiert werden. Diese werden mit den zur Verfügung stehenden Diensten aus dem Service-Repository abgeglichen. Existieren keine passenden Dienste, die den eingestellten Privacy-Einstellungen des Benutzers entsprechen, wird der Nutzer darauf hingewiesen und kann daraufhin entweder seine Privacy-Einstellungen verändern oder muss sich um die Aufnahme passender Dienste kümmern. Nach der Modellierung wird der modellierte Prozess, wenn dieser ausführbar ist, im Zertifizierungsmodul zertifiziert und anschließend an das Business Process Management System (BPMS) übergeben.

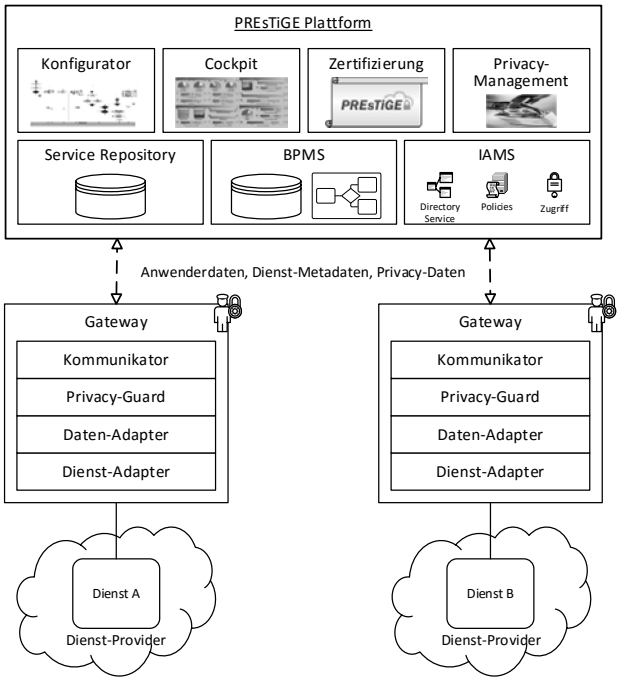

Abbildung 1. *Architektur der kollaborativen Cloud-Plattform*

Im BPMS können die modellierten Prozesse ausgeführt werden. Hierfür wird für jeden einzelnen Prozessschritt ein Gateway instanziiert. Ein Gateway (siehe mittlerer Bereich der Abbildung 1) ist für die Privacy-Erhaltung, die Interoperabilität und die Verschlüsselung bei der Kommunikation zwischen der PREsTiGE Plattform und dem jeweiligen Dienst zuständig. Es umfasst die Komponenten Kommunikator, Privacy-Guard, Daten-Adapter und Dienst-Adapter und stellt sicher, dass nur die freigegebenen Daten zwischen der PREsTiGE Plattform und dem jeweiligen Dienst ausgetauscht werden. Die Instanz eines Gateways existiert nur solange wie der Aufruf des jeweiligen Dienstes dauert und wird nach Beendigung des Aufrufes beendet.

Der Kommunikator dient als Kommunikationsmodul zwischen der PREsTiGE Plattform und dem Gateway. Der Privacy-Guard kontrolliert, ob der Informationsfluss den zuvor festgelegten Privacy-Anforderungen entspricht. Die Regeln sowie die Entscheidungshilfen fragt der Privacy-Guard beim Privacy-Management an. Im Privacy-Guard

DOI: 10.2195/lj_Proc_autor1_de_jjjmm_01
URN: urn:nbn:de:0009-14-xxxxxx

können beispielsweise Daten pseudonymisiert oder anonymisiert werden. Somit stellt der Privacy-Guard sicher, dass nur die Daten transformiert und gesendet werden, welche für den Service von absoluter Notwendigkeit sind. Der Daten-Adapter überführt das Domänen-Datenschema der PREsTiGE-Plattform in das Dienst-Datenschema und umgekehrt. Das Domänen-Datenschema wird für den Datenaustausch innerhalb der kollaborativen Cloud-Plattform verwendet. Der Dienst-Adapter kontaktiert den benötigten Dienstprovider über sein Integrated Database Management System (IDMS) und erhält von diesem die Ergebnisse der Anfrage zurückgeliefert. Die Ergebnisse werden an den Daten-Adapter übergeben, der die eingehenden Daten in das Plattform-spezifische Domänen-Datenschema überführt. Nach der vollständigen Kommunikation eines Services mit dem Provider wird die zugehörige Gateway-Instanz wieder beendet. Somit sind diese Gateways sehr kurzlebig und werden für jeden Dienst-Aufruf neu erstellt.

4 PRIVACY-VERWALTUNG IN DER CLOUD

In diesem Kapitel wird die Privacy-Verwaltung als Schwerpunkt dieses Artikels behandelt. Zuerst werden Privacy-Anforderungen definiert, die als Grundlage dafür dienen, eine geeignete Beschreibungssprache für Privacy-Anforderungen und Privacy-Regeln zu identifizieren. Anschließend wird die Funktionalität der ausgewählten Beschreibungssprache beschrieben und zum Abschluss wird auf deren Nutzung in der kollaborativen Cloud-Plattform eingegangen.

4.1 PRIVACY-ANFORDERUNGEN

Aus der Sicht von Unternehmen ist das Bedürfnis nach dem Schutz von eigenen Privacy-Daten und der der Kunden immer wichtiger. Wenn Unternehmen dies nicht berücksichtigen, können sowohl juristische Konsequenzen sowie Vertrauensverlust auf Kundenseite die Folge sein. [WR13] Um dem entgegenzuwirken und mehr Vertrauen beim Kunden zu schaffen, ist die Formalisierung der Privacy-Anforderungen ein wichtiger Schritt. Dies ermöglicht es Kunden die eigenen Anforderungen selbst zu analysieren und schafft automatisch durch diese Art der Transparenz mehr Vertrauen.

Im Forschungsprojekt PREsTiGE werden Privacy-Anforderungen als eine nichtformale Aussage über die Schutzbedürftigkeit von Daten bezeichnet. Dabei werden vier Arten von Privacy-Anforderungen unterschieden: providerbezogene Privacy-Anforderung, prozessbezogene Privacy-Anforderung, aktivitätsbezogene Privacy-Anforderung und dienstbezogene Privacy-Anforderung.

Unter einer providerbezogenen Privacy-Anforderung versteht man die Privacy-Anforderung eines Providers, die für alle Prozesse, an denen der Provider beteiligt ist, gilt, z. B.: „Die Daten der Fa. Müller dürfen nur von Diensten verarbeitet werden, die in Deutschland gehostet sind.“ oder „Die Daten der Fa. Müller dürfen Deutschland nicht verlassen.

Eine prozessbezogene Privacy-Anforderung ist die Privacy-Anforderung eines Providers, die für einen bestimmten Prozess gilt, zum Beispiel: „In dem Prozess *XYZ* darf das Asset ‚Artikelname‘ nur gelesen werden von: *Versender* und *Empfänger* (d. h. bspw. nicht von *Spediteur 1* und *Hub*).“

Unter einer aktivitätsbezogenen Privacy-Anforderung versteht man die Privacy-Anforderung eines Providers, die für den Zeitraum einer bestimmen Aktivität in einem bestimmten Prozessmodell gilt, zum Beispiel: „Während der Aktivität Reife-Lagerung darf das Asset ‚Sendungsinhalt‘ von dem Provider des Lagerdienstes gelesen werden.“ oder „Während der Aktivität ‘Prüfe Finanzstatus letztes Jahr‘ des Prozesses Elterngeldfestlegung darf die Behörde Jugendamt das Asset ‚Ergebnis der Steuererklärung Vorjahr‘ von der Behörde Finanzamt lesen.“

Eine dienstbezogene Privacy-Anforderung ist die Privacy-Anforderung, die für einen Dienst eines Providers definiert wird, zum Beispiel: „Die Ergebnisdaten dürfen vom direkten Vertragspartner verarbeitet, aber nicht an Dritte weiter gegeben werden.“ oder „Die Ergebnisdaten dürfen nur zu nicht-kommerziellen Zwecken verwendet werden.“.

Um die zuvor erläuterten Anforderungen in auswertbaren Privacy-Regeln auszudrücken, müssen diese in einer maschinen-lesbaren Sprache definiert werden. Diese Sprache muss, damit diese in der Industrie verwendet werden kann, die folgenden Kriterien erfüllen:

- Die Sprache muss leicht handhabbar sein.
- Die Sprache muss flexibel einsetzbar sein.
- Es muss eine ausführbare Implementierung der Sprache geben, die es erlaubt, Privacy-Regeln zu definieren und diese im laufenden Betrieb auszuwerten um eine Entscheidung zu treffen.

Im folgenden Kapitel werden mögliche Beschreibungssprachen zur Privacy-Regel-Definition vorgestellt.

4.2 BESCHREIBUNGSSPRACHEN

Um Privacy-Regeln formulieren zu können sind verschiedene Sprachen verfügbar, um die menschlich lesbaren Anforderungen in maschinen-verständlichen Formaten auszudrücken. Durch die Sprachen ist ein hoher Grad an Automatisierung umsetzbar, was dazu führt, dass Verstöße einfacher entdeckt werden und neue Privacy-Regeln automatisiert umgesetzt werden können. Dafür stehen verschiedene Ansätze zur Verfügung. Manche Sprachen dienen dazu unternehmensinterne Regeln einfacher zugänglich zu

DOI: 10.2195/lj_Proc_autor1_de_jjjmm_01
URN: urn:nbn:de:0009-14-xxxxxx

gestalten. Andere wiederum dienen dazu, dass Nutzer dabei unterstützt werden ihre Privacy-Regeln definieren zu können. Darüber hinaus gibt es Sprachen, die auf bestimmte kontext-sensitive Bereiche optimiert sind, zum Beispiel die Verwaltung von Positionsdaten.

Die Sprachen sind aber nicht universell einsetzbar und die Anwendungsfälle sind hochgradig unterschiedlich. Jede Sprache hat dabei nur ein begrenztes Ausdrucksvermögen und stößt in gewissen Fällen immer an ihre Grenzen. Es gibt keine standardisierten Privacy-Regeln, die im Einsatz sind, da diese je nach Unternehmensfeld variieren und daher gibt es auch eine Vielzahl an Sprachen, die für unterschiedliche Unternehmensfelder eingesetzt werden können. Jedes Unternehmensfeld hat wiederum verschiedene Anwendungen, unterschiedliches Vokabular und unterschiedliche Anforderungen. Dies führt wiederrum zum Einsatz unterschiedlicher Sprachen. Je nach Unternehmensstandort gibt es zudem verschiedene Gesetzgebungen. In Europa wird durch das Datenschutzgesetz primär der Kunde/Nutzer geschützt. In Amerika steht das Unternehmen im Vordergrund und soll vor anderen Unternehmen geschützt werden. In China dient der Datenschutz wiederum primär ‚der nationalen Sicherheit' [BC11]. Im Folgenden folgt eine kleine Übersicht von verfügbaren Sprachen. Die Übersicht ist nicht vollständig, soll aber die Menge und Vielfalt von Beschreibungssprachen verdeutlichen.

Die Platform for Privacy Preferences Project (P3P) wurde 1997 vom World Wide Web Consortium (W3C) entwickelt, um Website Privacy Policies in maschinenlesbares Format zu wandeln. Dies wurde vom W3C als Standard empfohlen, jedoch nur vom Browser „Internet Explorer" der Firma Microsoft unterstützt. Auch 1997 wurde die P3P Preference Exchange Language (APPEL) vom W3C entwickelt [CLM02], um die Privacy Einstellungen von Individuen für P3P auszudrücken und umzusetzen zu können. Die Sprache Customer Profile Exchange (CPExchange) wurde 2000 von Idealliance entwickelt [BH00]. Hier werden online- und offline-Nutzerdaten in einem XML-basierten Datenmodell integriert. Diese Daten können daraufhin innerhalb verschiedener Unternehmensanwendungen genutzt werden. Die Security Assertion Markup Language (SAML) wurde 2001 von OASIS Access Control Technical Committee (TC) veröffentlicht [OA04]. Im darauf folgenden Jahr 2002 wurde im Rahmen der Thesis von Lalana Kagal die Sprache Rei entwickelt [KA02], welche auf der Web Ontology Language Lite basiert. Dies ist eine Logik-basierte Policy Language, welche der Domänen-basierten Zugangskontrolle dient. 2003 wurde von IBM die Enterprise Privacy Authorization Language (EPAL) vorgestellt [AN04], um unternehmensinterne Privacy Policies in maschinen-lesbarem Format ausdrücken zu können [AHK+03]. Bei Anfragen an EPAL muss stets eine Absicht angegeben werden. Zero-Knowledge Systems hat im Jahre 2004 die Privacy Rights Markup Language (PRML) erstellt. Diese erlaubt die Definition von Objekten und Mechanismen. Objekte können dabei Rollen, Operation, Aktionen oder ähnliches sein. Mehrere PRML-Aussagen bilden eine Privacy Policy. 2005 fand die Veröffentlichung von Xpref statt [AKS+05], einer Weiterentwicklung von APPEL. Im gleichen Jahr wurde die Sprache Geographic Location Privacy (Geopriv) von der Internet Engineering Task Force (IETF) entwickelt, um Policies auszudrücken, welche Zugang zu Präsenz- und Positionsdaten kontrollieren. 2005 wurde von dem Unternehmenskonsortium OASIS die *eXtensible Access Control Markup Language (XACML)* in der zweiten Version veröffentlicht [BHL+12]. Mit XACML wurde eine Sprache entwickelt, mit der es möglich ist, Privacy-Anforderungen und –Regeln in maschinenlesbarem Format auszudrücken [OA13].

Bei den zuvor vorgestellten Sprachen handelt es sich um einen Auszug verfügbarer Sprachen, welche im Laufe der Zeit mit verschiedenen Zielen und für unterschiedliche Anwendungsgebiete entwickelt wurden. Damit eine Entscheidung für eine Sprache getroffen werden konnte, welche als Grundlage für die vorgestellten Privacy-Anforderungen dienen soll, wurden die zuvor aufgeführten Beschreibungssprachen auf die in Kapitel 4.1 aufgeführten Kriterien hin untersucht. Dabei wurde XACML als die Sprache für die weiteren Arbeiten ausgewählt, da diese die aufgestellten Kriterien vollständig erfüllt.

4.3 XACML

Für die Verwaltung der Privacy-Regeln im Privacy-Management der PREsTiGE-Plattform wird die Sprache eXtensible Access Control Markup Language (XACML) verwendet. Es handelt sich dabei um einen offenen XML-basierten Standard, um Security-/Privacy-Policies, Zugangsberechtigungen und Unternehmenssicherheits-Anwendungen umzusetzen. Er dient dazu, Regeln aufzustellen, durch deren Auswertung der Zugriff von Subjekten (Anfragenden) auf Ressourcen (IT-Dienste, Daten, …) eines Systems gesteuert werden kann. Der Standard wurde vom OASIS-Konsortium (Organization for the Advancement of Structured Information Standards) definiert, zu welchem Unternehmen wie Sun Microsystems, IBM, Nokia und SAP gehören. Die Version 3.0 wurde im August 2010 ratifiziert. Die wesentlichen Neuerungen zu der Version 2.0 sind die Möglichkeit, Rechte zu delegieren, und erweiterte Möglichkeiten, die Anwendbarkeit von Zugriffsregeln zu spezifizieren. Der zum Zeitpunkt der Entstehung des vorliegenden Artikels aktuelle Versionsstand von XACML ist vom 22.01.2013 [OA13].

Eine Zugriffsanfrage in XACML besteht aus einer Reihe von Attributen (Name-Wert-Paar). Diese Anfragen werden mit Hilfe von Regeln evaluiert, um zu einer Zugriffsentscheidung zu gelangen. Innerhalb der Regeln können die Anfragen mit den typischen aus Programmiersprachen bekannten Funktionen (Vergleiche, Arithmetik, einfache Zeichenkettenoperationen, Datums- und Zeitberechnungen) analysiert werden, wobei beliebig komplexe

DOI: 10.2195/lj_Proc_autor1_de_jjjjmm_01
URN: urn:nbn:de:0009-14-xxxxxx

Ausdrücke möglich sind [GK11]. XACML wurde als eine allgemeine, abstrakte Norm entworfen und kann daher an vielen Stellen ergänzt werden. So können zum Beispiel anwendungsspezifische Attributnamen, Datentypen und Funktionen hinzugefügt werden. Eine Bedingung ist als Objekt-Subjekt-Aktion-Bedingung aufgebaut. Als Subjekt kommt eine Identität, Gruppe oder Rolle in Frage. Objekte können zum Beispiel Elemente eines Dokumentes oder vergleichbare Daten darstellen. Zu den Aktionen gehören „Lesen“, „Schreiben“, „Erstellen“ und „Löschen“. Eigene Aktionen können dabei ergänzt werden. In der Abbildung 2 ist der Kontrollfluss in XACML vereinfacht dargestellt [OA13].

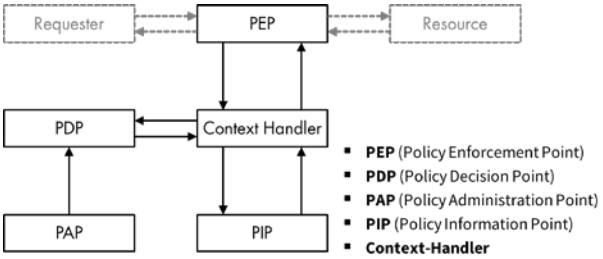

Abbildung 2. *Kontrollfluss in XACML [OA13]*

Nach der Spezifikation von OASIS ist ein XACML-System aus den fünf Komponenten PAP, PEP, PDP, PIP und dem Context Handler (CH) aufgebaut. Die fünf Komponenten realisieren zusammen die Zugriffskontrolle. Der PAP (Policy Administration Point) ist das Teilsystem, in dem die Regeln, nach denen Zugriffe erlaubt oder verboten sind, festgelegt werden. Der PEP (Policy Enforcement Point) ist die Komponente des Systems, welche sich schützend zwischen den Subjekten und den Ressourcen befindet. Im PEP gehen Zugriffsanfragen ein und bei Erlaubnis wird der Zugriff auf die Ressourcen gewährt. Der PDP (Policy Decision Point) trifft die Entscheidung anhand der im PAP erstellten Privacy-Regeln ob ein bestimmter Zugriff erlaubt werden soll oder nicht. Wenn der PDP über eine Anfrage entscheidet, aber nicht über ausreichend Informationen verfügt, um die Anfrage zu beantworten, bittet er den PIP (Policy Information Point) um weitere Informationen. Der PIP hat Zugriff auf Attribute der Subjekte und Arbeitsumgebung sowie auf die Attribute der Ressourcen. Der CH wandelt das Anfrageformat des Anfragers in das XACML-Format um und umgekehrt.

Um XACML in der PREsTiGE Plattform integrieren zu können, wurden bereits existierende Realisierungen von XACML 3.0 betrachtet. Das Ziel war die Identifikation einer Open-Source Lösung mit der Möglichkeit diese weiterzuentwickeln und für die kollaborative Cloud-Plattform verwenden zu können. Bei der Recherche wurden vielfältige kommerzielle Produkte wie zum Beispiel *Compliant Enterprise Entitlement Management SDK* von Nextlabs [NE14] oder der *Axiomatics Policy Server* der Firma Axiomatics [A15] identifiziert, die jedoch in ihrer Funktionalität nicht an die PREsTiGE Plattform angepasst werden können. Neben den kommerziellen Produkten wurden auch freie Produkte gefunden, wie zum Beispiel der *Identity Server* von WSO2 [W15] oder die *Policy Engine* von AT&T [A14]. Der *Identity Server* von WSO2 ist ein Open-Source Produkt unter der Apache Software Lizenz und bietet ein Web-basiertes Interface zur Policy-Administration. Es wird XACML 3.0 und damit PIP, PDP und PEP unterstützt. Die aktuelle Version des WSO2 *Identity* Servers ist 5.0.0. Der Quellcode ist jedoch nur für die bereits veraltete Version 3.2 freigegeben. Die *Policy Engine* von AT&T ist eine Java-Realisierung des PDP, PIP und PAP. Sie wird als Java-Quellcode frei zur Verfügung gestellt und kann komplett in Projekten verwendet und verändert werden. Da die AT&T *Policy Engine* frei verfügbar ist und in Form des Quellcodes zur Verfügung steht, wird diese für die weitere Betrachtung in der kollaborativen Cloud-Plattform verwendet.

4.4 Integration in die kollaborative Cloud-Plattform

Die Abbildung 3 zeigt die Architektur der kollaborativen Cloud-Plattform mit der Zuordnung der einzelnen XACML-Komponenten.

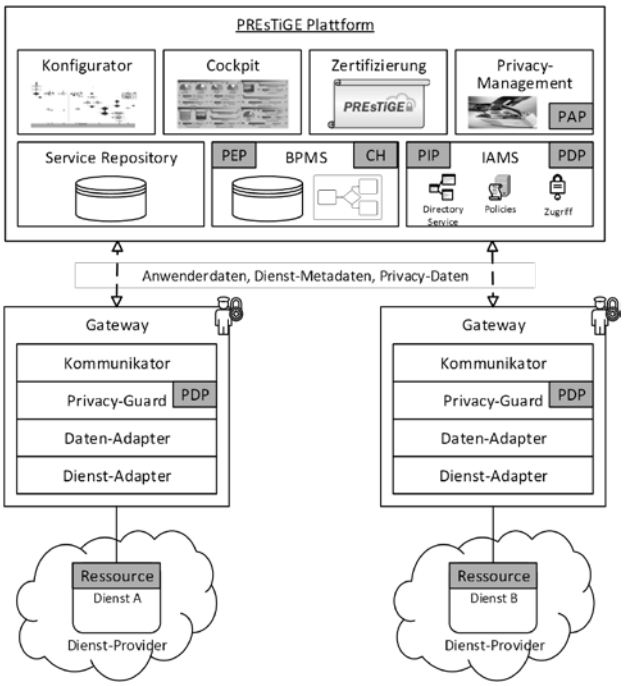

Abbildung 3. *Integration von XACML in die kollaborative Cloud-Plattform*

In der Komponente Privacy-Management ist der PAP verankert. Hier können provider-, prozess-, aktivitäts- und dienstbezogene Privacy-Anforderung definiert werden. Der PAP generiert daraus die Privacy-Regeln und stellt diese dem PDP im IAMS und im Privacy-Guard zur Verfügung. Das IAMS verfügt neben dem PDP auch den PIP. Der PEP sowie der CH sind in der BPMS-Komponente der Architektur zu finden. Die Ressource auf die zugegriffen

DOI: 10.2195/lj_Proc_autor1_de_jjjmm_01
URN: urn:nbn:de:0009-14-xxxxxx

werden soll, befindet sich auf der Seite des Dienst-Providers.

5 ZUSAMMENFASSUNG UND AUSBLICK

In diesem Artikel wurden die Themen Cloud Computing und Privacy behandelt. Neben der Definition beider Themen wurden auch mögliche Realisierungen, Gesetze und Standards in den Bereichen vorgestellt. Des Weiteren wurde ein Konzept zum Schutz von Privacy-relevanten Daten in einer kollaborativen Cloud-Plattform in Form einer Architektur vorgestellt und die Thematik der Privacy-Verwaltung näher erläutert. Abschließend wurde die Integration der Privacy-Verwaltung in die in dem Forschungsprojekt PREsTiGE entwickelte Architektur dargestellt.

Neben der Implementierung der einzelnen Komponenten aus der in der Abbildung 3 dargestellten Architektur, müssen noch Use Case spezifische Privacy-Anforderungen erstellt werden. Da die Definition von Anforderungen in der Praxis in den meisten Fällen keine XACML-Experten durchführen werden, müssen hierfür Methoden und Werkzeuge zur einfachen Formulierung von Privacy-bezogenen „Business-Regeln“ für die Logistikdomäne in Annäherung an den XACML-Standard entwickelt werden. Diese müssen dann anhand von unterschiedlichen Use Cases aus der Logistikbranche evaluiert werden. Unter den Use Cases findet sich der in der folgenden Abbildung 4 aufgeführte Use Case „Sendungsverfolgung“ wieder.

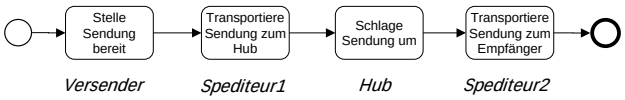

Abbildung 4. *Use Case “Sendungsverfolgung” aus PREsTiGE*

Bei dem Use Case handelt es sich um eine lineare Logistikkette mit vier aufeinander folgenden Aktivitäten, die von vier verschiedenen Akteuren ohne aktive Beteiligung des Empfängers ausgeführt werden. Zwischen den einzelnen Akteuren werden Sendungsdaten zur Abarbeitung der Logistikkette ausgetauscht. Zu beachten gilt jedoch, dass nicht alle Akteure Zugriff auf alle Sendungsdaten haben. Zum Beispiel kann Spediteur 1 auf die Daten zum Eingangstor des Hubs zugreifen aber nicht auf die Daten zum Ausgangstor, auf die Spediteur 2 zugreifen kann. Dieser Use Case wird für die erste Evaluierung der gesamten Architektur verwendet.

DOI: 10.2195/lj_Proc_autor1_de_jjjmm_01
URN: urn:nbn:de:0009-14-xxxxxx

6 LITERATURVERZEICHNIS

[A14] AT&T: AT&T XACML, 2014.

[A15] Axiomatics: Axiomatics Policy Server, 2015.

[AHK+03] Ashley, P. et al.: Enterprise Privacy Authorization Language. IBM Research Report.

[AKS+05] Agrawal, R. et al.: XPref: a preference language for P3P.

[AN04] Anderson, A.: Privacy Policy Languages. XACML vs EPAL, 2004.

[BC11] Bélanger, F.; Crossler, R. E.: Privacy in the digital age: a review of information privacy research in information systems.

[BH00] Bohrer, K.; Holland, B.: Customer Profile Exchange (CPExchange). Specification.

[BHL+12] Brucker, A. D. et al.: SecureBPMN. In (Atluri, V. et al. Hrsg.): the 17th ACM symposium, 2012; S. 123.

[BU08] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standard 100-1, 2008.

[BU11] Bundesamt für Sicherheit in der Informationstechnik (BSI): Privacy Impact Assessment Guideline for RFID Applications (PIA).

[BU12] Bundesamt für Sicherheit in der Informationstechnik (BSI): Sicherheitsempfehlungen für Cloud Computing Anbieter. Mindestanforderungen in der Informationstechnik. Eckpunktepapier, 2012.

[BU90] Bundesdatenschutzgesetz. BDSG, 1990.

[CLM02] Cranor, L.; Langheinrich, M.; Marchiori, M.: A P3P Preference Exchange Language. APPEL 1.0.

[DA95] RICHTLINIE 95/46/EG DES EUROPAISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, 1995.

[GK11] Gaehtgens, F.; Kuppinger, M.: XACML Made Easy: Modeling High Level Policies in XACML. Webinar. https://www.kuppingercole.com/events/n10057, 27.05.2015.

[IKC09] Itani, W.; Kayssi, A.; Chehab, A.: Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures: 2009 International Conference on Dependable, Autonomic and Secure Computing (DASC), 2009; S. 711–716.

[J15] Jäger, M.: Hochsicher, kaum genutzt, völlig veraltet. PGP. http://www.golem.de/news/pgp-hochsicher-kaum-genutzt-voellig-veraltet-1506-114797.html, 05.08.2015.

[JB05] Jutla, D. N.; Bodorik, P.: Sociotechnical Architecture for Online Privacy. In IEEE Security and Privacy Magazine, 2005, 3; S. 29–39.

[KA02] Kagal, L.: Rei. A Policy Language for the Me-Centric Project.

[MI08] Microsoft Corporation: Privacy Guidelines for Developing Software Products and Services.

[NE14] Nextlabs: Nextlabs Data Protection. Why NextLabs Data Protection?

[NI11] NIST Computer Security Division: Guidelines on Security and Privacy in Public Cloud Computing, 2011a.

[NI11] NIST: The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, 2011b.

[OA04] OASIS: SAML 2.0 profile of XACML, 2004.

[OA13] OASIS: eXtensible Access Control Markup Language (XACML) Version 3.0, 2013.

[PA09] Pau, L.-F.: Privacy management service contacts as business opportunity. In IEEE Technology and Society Magazine, 2009, 28; S. 55–63.

[PC09] Pearson, S.; Charlesworth, A.: Accountability as a Way Forward for Privacy Protection in the Cloud. In (Hutchison, D. et al. Hrsg.): Cloud Computing. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009; S. 131–144.

[PE09] Pearson, S.: Taking account of privacy when designing cloud computing services: 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009; S. 44–52.

[RCL] Rimal, B. P.; Choi, E.; Lumb, I.: A Taxonomy and Survey of Cloud Computing Systems: 2009 Fifth International Joint Conference on INC, IMS and IDC; S. 44–51.

[SB15] Stahl, F.; Burgmair, S.: Bollwerk. Top 10 der Datenschutzrisiken in Webapplikationen. In iX, 2015; S. 76–79.

DOI: 10.2195/lj_Proc_autor1_de_jjjmm_01
URN: urn:nbn:de:0009-14-xxxxxx

[SO06] Solove, D. J.: A Taxonomy of Privacy. In University of Pennsylvania Law Review, 2006; S. 477–564.

[SSP+15] Schier, A. et al.: inter-cloud architecture for privacy-preserving collaborative BPaaS.

[VE48] Allgemeine Erklärung der Menschenrechte, 1948.

[W15] WSO2: WSO2 Identity Server, 2015.

[WE13] Welp, J.: Mit Recht in der Cloud. Cloud Computing bietet große Chancen – für Unternehmen aller Branchen. Aber: Der rechtliche Rahmen muss stimmen., 2013.

[WR13] Wolf, M.-B.; Rahn, J.: Cloud Computing für Logistik 2. Akzeptanz und Nutzungsbereitschaft der Logistics Mall bei Anwendern und Anbietern. Fraunhofer Verlag, Stuttgart, 2013.

[ZE15] ZEIT ONLINE: EU-Minister einigen sich auf Datenschutzreform. http://www.zeit.de/digital/datenschutz/2015-06/datenschutz-eu-reform-justizminister-luxemburg, 03.08.2015.

[ZYZ+12] Zhang, G. et al.: Key Research Issues for Privacy Protection and Preservation in Cloud Computing: 2012 International Conference on Cloud and Green Computing (CGC), 2012; S. 47–54.

Prof. Dr. Michael ten Hompel, born in Bergisch-Gladbach, Germany, in 1958, studied Electrical Engineering at RWTH Aachen and graduated from Witten/Herdecke University in 1991. In 2000, he joined the managing board of Fraunhofer Institute for Material Flow and Logistics in Dortmund (since January 2005: Managing Director) and became head of the Chair of Materials Handling and Warehousing at TU Dortmund University.

Dipl.-Inf. (FH) Arkadius Schier, Research Assistant at the Software Engineering, Fraunhofer-Institute for Materialflow and Logistics IML since 2006. Arkadius Schier was born in 1981 in Loben, Poland. Between 2002 and 2006 he studied Technical Computer Science at the University of Applied Sciences and Arts in Dortmund.

Lucas Petrich, Student Assistant at the Software Engineering, Fraunhofer-Institute for Materialflow and Logistics IML. Lucas Petrich was born 1991 in Muenster, Germany. Between 2011 and 2015 he studied Applied Computer Science at the Technical University Dortmund.

Address: Fraunhofer-Institute for Materialflow and Logistics IML, Joseph-von-Fraunhofer Straße 2-4, 44227 Dortmund, Germany

Dipl.-Inf. Björn Schwarzbach, Research Assistant at the Chair of Information Management. Björn Schwarzbach was born in 1983 in Leipzig, Germany. Between 2001 and 2011 he studied Computer Science and Physics at Leipzig University.

Prof. Dr. Ing. Bogdan Franczyk, Chair of Information Management, Leipzig University and Wroclaw University of Economics. Bogdan Franczyk was born 1955 in Lwowek Sl., Poland. He holds the chair of Information Management in Leipzig since 2002 and in Wroclaw since 2010.

Address: Leipzig University, Grimmaische Straße 12, 04109 Leipzig, Germany

Address: Wroclaw University of Economics, ul. Komandorska 118/1290, 53345 Wroclaw, Poland