

Protokollierung in service-orientierten Architekturen

Chancen für den Datenschutz

Christoph Ringelstein

Moderne Infrastrukturlösungen, wie service-orientierte Architekturen, ermöglichen es, Dienstleistungen anzubieten, deren Prozesse über mehrere Organisationen verteilt sind. Als Seiteneffekt treten hierbei neue Problemstellungen für den Datenschutz auf, da personenbezogene Daten über Organisationsgrenzen hinweg übertragen werden. Gleichzeitig fordern Kunden immer detailliertere Auskunft über die Verarbeitung ihrer Daten. Dieser Artikel stellt daher eine Architektur zur Protokollierung vor, die es ermöglicht, die Informationen für eine detaillierte Auskunft zu sammeln, aber gleichzeitig die neu gewonnene Flexibilität der Organisationen nicht einschränkt.



Christoph Ringelstein

Wissenschaftlicher Mitarbeiter der Arbeitsgruppe „Informationssysteme & Semantic Web“ der Universität Koblenz-Landau

E-Mail: cringel@uni-koblenz.de

Einleitung

Die Verbreitung der Umsetzung des Paradigmas der Service-Orientierung innerhalb von Organisationen führt dazu, dass beliebige Geschäftsfunktionalitäten als eigenständige Dienste modelliert werden. Diese Dienste können und werden zunehmend auch als Dienstleistungen für externe Kunden angeboten. Die service-orientierte Architektur (SOA) stellt dabei unter anderem standardisierte Schnittstellen (z. B. Web Services) für die Kommunikation bereit, die eine lose Koppelung der Dienstanutzer an Dienste ermöglicht. Die so gewonnene Flexibilität kann dazu genutzt werden, beliebige Dienste verschiedener Organisationen dynamisch zu neuen Arbeitsprozessen zu verbinden.

Bei der Erbringung vieler Dienstleistungen werden personenbezogene Daten verarbeitet. Im Folgenden werden dabei die personenbezogenen Daten betrachtet, die im Zusammenhang der Dienstleistung zwischen Organisationen, die an der Dienstleistung beteiligt sind, untereinander und zwischen dem Kunden der angebotenen Dienstleistung und beteiligten Organisationen kommuniziert werden. Der jeweilige Auftraggeber sowie der Betroffene¹ hat dabei das Recht, über die Verwendung der Daten zu bestimmen. Der Auftraggeber kann dabei der Betroffene als Kunde der Dienstleistung beziehungsweise im Rahmen einer Auftragsdatenverarbeitung oder Funktionsübertragung eine andere Organisation sein. Die jeweiligen Organisationen, die Zugriff auf die Daten haben, geben dem Auftraggeber Zusicherungen über die Verwendung der Daten. Diese Zusicherungen werden in Verträgen geregelt. Darüber hin-

aus gibt es Datenschutzrichtlinien, die gesetzlich vorgeschrieben sind.

Im Interesse des Auftraggebers liegt die Einhaltung der vereinbarten Zusicherungen und der Datenschutzrichtlinien. Die beteiligten Organisationen können gegen diese verstoßen. Abgesehen davon, dass beteiligte Organisationen Zusicherungen und Datenschutzrichtlinien absichtlich ignorieren und Daten missbrauchen, was mit heutigen Technologien lediglich erschwert, aber nicht verhindert werden kann, kommt es häufig zu unbeabsichtigten Verstößen gegen Datenschutzbestimmungen und Datennutzungsrechten. Verstöße dieser Art bleiben oft unentdeckt, da geeignete Kontrollmechanismen fehlen oder nicht eingesetzt werden. Es liegt allerdings im Interesse aller Beteiligten, solche Verstöße rechtzeitig zu erkennen, um Schaden (zum Beispiel durch Vertragsstrafen oder Bußgelder) zu verhindern.

Um die Einhaltung der gegebenen Zusicherungen und der Datenschutzrichtlinien zu überprüfen, kann der Auftraggeber und der Betroffene Auskunft über die Verarbeitung der Daten verlangen. Ist der Auftraggeber eine andere Organisation, kann die Erteilung der Auskunft in den Verträgen geregelt sein. Die erteilte Auskunft muss Informationen darüber enthalten, wer die Daten genutzt hat sowie warum und wie die Daten genutzt wurden.

Die Auskunft stellt somit ein abstrahierendes Protokoll der Prozessausführung dar. Dieses Protokoll kann auf verschiedene Weise erzeugt werden, zum Beispiel durch Rekonstruktion des Prozesses oder durch direktes Mitprotokollieren der Prozessausführung. In jedem Fall benötigt der Dienstleister eine detaillierte Übersicht über den Gesamtprozess; allerdings fehlt diese Übersicht häufig selbst für organisationsinterne Prozesse. Hinzukommt, dass aus verschie-

¹ Im Sinne des Datenschutzes.

denen Gründen aktuelle Protokollierungslösungen nicht ausreichend sind, um eine solche Übersicht über Prozesse, die über mehrere Organisationen verteilt sind, zu erhalten [7]. Dadurch wird das Erstellen einer gemeinsamen Auskunft erschwert. Ein Grund hierfür ist das Fehlen eines Standards für die Protokollierung von Prozessen, die verteilt auf heterogenen Systemen ausgeführt werden, oder zumindest eines systemunabhängigen Standards für die Formulierung und den Austausch von Protokollen.

In diesem Artikel wird eine Protokollierungsarchitektur diskutiert, die speziell dazu vorgesehen ist, die Verarbeitung personenbezogener Daten während der Ausführung eines verteilten Prozesses zu protokollieren. Grundlegend für diese Architektur ist, dass das Protokoll direkt an das zugehörige Datum, als Metadatum, gehängt wird und dass sie zusätzlich zu existierenden Protokollierungsmethoden, die genutzt werden, um die technische Funktionalität der Dienstauführungen zu überprüfen, eingesetzt werden kann.

In Abschnitt 1 wird ein Szenario vorgestellt und die Anforderungen an eine Architektur zur Protokollierung der Einhaltung von Datenschutzrichtlinien und Zusicherungen in verteilten Umgebungen identifiziert. Aufbauend auf diesen Anforderungen wird in Abschnitt 2 eine Protokollierungsarchitektur beschrieben, die den Anforderungen gerecht wird. In Abschnitt 3 werden die vorgestellte Architektur und deren Auswirkungen auf den Datenschutz abschließend diskutiert.

1 Anforderungen an die Protokollierung

Im Folgenden wird ein Szenario präsentiert, das einen Arbeitsprozess beschreibt, der personenbezogene Daten verarbeitet und der mittels einer service-orientierten Architektur auf mehrere Organisationen verteilt ausgeführt wird. Außerdem werden verschiedene vertragliche und sonstige rechtliche Anforderungen an eine Protokollierungsarchitektur identifiziert, die erfüllt sein müssen, damit die datenschutzkonforme Verarbeitung der Daten protokolliert und kontrolliert werden kann. Ausgehend von diesen Anforderungen werden organisatorische Problemstellungen bei deren Umsetzung betrachtet. Abschließend werden technische Anforderungen hergeleitet, die sich

aus den organisatorischen Problemstellungen ergeben.

Szenario

Die Bücherladen GmbH verkauft Bücher über eine Webseite. Teile der Logistik, wie die Lagerhaltung der Waren und das Verpacken der Sendungen, werden von der Bücherladen GmbH selbst erledigt. Die Auslieferung und der Zahlungsverkehr erfolgt allerdings über Dienstleistungen anderer Organisationen. Der Versand zum Beispiel wird an die Schnell-Liefer AG, eine Logistikfirma, outgesourct.

Der Kunde Herr Schmidt bestellt Bücher über die Webseite der Bücherladen GmbH. Um die Bestellung aufzugeben, gibt er seine Adress- und Kontoinformationen an. Nachdem die Bestellung aufgegeben wurde, besitzt die Bücherladen GmbH verschiedene Daten, die mit der Bestellung verbunden sind: die Liste der bestellten Bücher sowie die Adress- und die Kontodaten von Herrn Schmidt. Als ein Schritt der Auftragsabwicklung verpackt die Bücherladen GmbH die bestellten Bücher und übergibt das Paket zusammen mit einer Kopie der Adressdaten an die Schnell-Liefer AG.

Rechtliche Anforderungen

In der Einleitung wurden die Gründe aufgezeigt, die dazu führen, dass Organisationen über die Verarbeitung von personenbezogenen Daten Rechenschaft ablegen müssen. Daraus lassen sich die folgenden Anforderungen ableiten (siehe auch [4]):

- **Anforderung 1:** Dem Betroffenen muss es möglich sein, Informationen über die Verarbeitung seiner Daten zu erhalten.
- **Anforderung 2:** Die für die Datenverarbeitung verantwortlichen Organisationen müssen in den erteilten Informationen klar benannt sein.
- **Anforderung 3:** Einer Organisation darf es nicht möglich sein, eine erteilte Auskunft abzustreiten.

Organisatorische Problemstellungen

Diese Anforderungen lassen sich allerdings besonders im Umfeld von verteilten Arbeitsprozessen nur bedingt umsetzen. Im Folgenden wird daher eine Auswahl der mit der Umsetzung verbundenen Problemstellungen gegeben; weitere organisatorische Prob-

lemstellungen werden in [3] und [6] aufgezeigt.

Lose gekoppelte Architekturen: Ein Grundbestandteil der SOA ist die lose Kopplung verteilter heterogener Systeme zur Ausführung eines verteilten Prozesses. Die Heterogenität der Systeme erschwert allerdings a posteriori die Erstellung einer detaillierten Übersicht über den verteilten Prozess. Daher kann die Umsetzung von Querschnittsfunktionen, wie zum Beispiel der Protokollierung, nur mit Hilfe vordefinierter und implementierter Standards auf Schnittstellenebene erfolgen.

Fehlende Übersicht über Arbeitsprozesse: Um eine detaillierte Auskunft über die Verarbeitung von Daten zu erteilen, benötigt eine Organisation eine umfassende Übersicht über ihre internen Datenflüsse. Diese umfassende Übersicht fehlt meist selbst innerhalb einzelner Organisationen. Durch die Verknüpfung mehrerer Prozesse zu einem integrierten organisationsübergreifenden Prozess wächst die Komplexität des Prozesses stark und erschwert somit zusätzlich das Erstellen einer Übersicht.

Eigenständigkeit von Organisationen: Das Problem der fehlenden Prozessübersicht wird zusätzlich durch die Eigenständigkeit der beteiligten Organisationen verstärkt, da diese zum Schutz ihrer Geschäftsgeheimnisse ein berechtigtes Interesse daran haben, Dritten keinen Einblick in ihre internen Prozesse und Datenflüsse zu geben.

Technische Anforderungen

Die technische Umsetzung der Protokollierung eines verteilten Prozesses muss die oben erwähnten organisatorischen Problemstellungen berücksichtigen. Daher lassen sich die folgenden technischen Anforderungen ableiten (siehe auch [4]):

- **Anforderung 4:** Um Mehrdeutigkeiten zu verhindern und um eine Standardisierung zu erreichen, müssen die Protokolle in einer wohl definierten semantischen Sprache formuliert werden.
- **Anforderung 5:** Die Sprache muss es ermöglichen, die Informationen über die ausgeführten Aktionen, die Verantwortlichen, die Zwecke und die Reihenfolge der Aktionen im gewünschten Detailgrad auszudrücken.
- **Anforderung 6:** Eine standardisierte Schnittstelle zum Zugriff und Austausch der Protokolle muss gegeben sein.

- **Anforderung 7:** Die Implementierung der Protokollierungsarchitektur muss eine Organisation in die Lage versetzen, Protokolle zu erzeugen, die alle relevanten Informationen enthalten.
- **Anforderung 8:** Organisationen müssen die Möglichkeit besitzen, Interna vor unberechtigten Dritten zu verbergen. Daher muss die Protokollierungsarchitektur Datensicherheitsmechanismen unterstützen.

Darüber hinaus existieren noch andere Anforderungen, wie zum Beispiel, dass die erzeugten Protokolleinträge der Wahrheit entsprechen müssen (siehe [6]). Diese Anforderungen werden hier in diesem Artikel nicht näher betrachtet, da die damit verbundene Problematik sich nicht von der Datenverarbeitung in einzelnen Organisationen unterscheidet.

2 Architektur zum Protokollieren

Die zuvor identifizierten Probleme beeinflussen die Fähigkeiten von Organisationen, über die Verwendung von Daten in verteilten Prozessen verbindlich Auskunft zu geben. Im Folgenden wird eine Architektur zur Protokollierung vorgestellt, die die oben definierten Anforderungen erfüllt. Die Architektur sieht dabei vor, dass alle Protokolleinträge zu einer einzelnen Ausführung eines Arbeitsprozesses direkt, als Metadatum, an die verarbeiteten Daten angehängt und nach Beendigung der Ausführung entlang des Aufrufweges der Dienstleistung an den Auftraggeber zurückübermittelt werden. Außerdem werden Regeln für die Protokollierung und eine Sprache zum Formulieren der Protokolle definiert.

Protokollierungsregeln

Im Folgenden wird ein kurzer Überblick über die Ereignisse, die im Zusammenhang mit der Verarbeitung von Daten auftreten, und die damit verbundenen Handlungsregeln für die Protokollierung gegeben:

Das Erheben und Erstellen eines Datums: Jedes Datum² erhält ein eigenes Protokoll. Der erste Protokolleintrag erfasst alle relevanten Informationen über das Erheben beziehungsweise Erstellen des Datums.

Das Verwenden und Ändern eines Datums: Jede Verwendung und Änderung des

Datums wird mit allen relevanten Informationen im Protokoll festgehalten.

Das Kopieren eines Datums: Jedes Kopieren eines Datums führt zum Erstellen eines neuen Datums (siehe oben). Um die Zurückübermittlung des Protokolls und das Aktualisieren von Referenzen (siehe unten) zu ermöglichen, werden in beiden Protokollen (in das Protokoll des Ausgangsdatums und in das Protokoll der Kopie) Referenzen zu den jeweils anderen Protokollen eingetragen. Nach dem Kopieren des Datums werden neue Protokolleinträge nur noch in das zugehörige Protokoll eingetragen. Falls das neu erstellte Datum außerhalb des Prozesses verwendet werden soll (z.B. Speicherung), wird eine alternative Methode für die Zurückübermittlung des Protokolls bestimmt (z.B. E-Mail). Diese Methode wird dann zur Zurückübermittlung genutzt, wenn die Referenz auf das Protokoll des Ausgangsdatums nicht mehr gültig ist.

Das Übergeben eines Datums: Um ein Datum als Parameter eines Dienstaufrufs zu übergeben, muss dies zuerst kopiert werden (siehe oben). Diese Kopie wird dann mit dem zugehörigen Protokoll übergeben. Dadurch, dass nur das neue Protokoll übermittelt wird, werden keine Informationen über Interna der aufrufenden Organisation weitergereicht. Falls der Dienstaufruf synchron erfolgt, wird das Protokoll nach Beendigung des Aufrufs direkt an den Aufrufenden zurückgegeben. Im Gegensatz dazu wird bei asynchronen Dienstaufrufen die alternative Übermittlungsmethode, die im Protokoll spezifiziert wurde, genutzt. In beiden Fällen wird das zurückerhaltene Protokoll in das Protokoll des Ausgangsdatums integriert. Wird ein Datum bei einem asynchronen Dienstaufruf übergeben, wird dies explizit im Protokoll des Ausgangsdatums erfasst.

Vereinbaren von Zusicherungen über die Verarbeitung eines Datums: Immer wenn bei der Übergabe eines Datums an eine andere Organisation Zusicherungen über die Verarbeitung des Datums vereinbart werden, werden diese Zusicherungen im Protokoll festgehalten.

Löschen eines Datums: Das Löschen eines Datums hat nicht die Löschung des Protokolls zur Folge. Stattdessen wird das Protokoll mit dem des Ausgangsdatums zusammengeführt. Nach der Zusammenführung müssen alle Referenzen in anderen Protokollen, die auf das Protokoll der gelöschten Datei verweisen, auf das Protokoll des Ausgangsdatums angepasst werden. Falls die beiden Protokolle nicht bei dersel-

ben Organisation vorliegen, das Löschen des Datums aber während einer synchronen Dienstauführung stattfindet, wird das Protokoll am Ende der Ausführung als Teil der Antwort übergeben. Ist dies nicht der Fall, muss die alternative Methode zur Zurückübermittlung des Protokolls verwendet werden. Unabhängig davon, welcher dieser Wege genutzt wird, gelangt das Protokoll am Ende zu der Organisation, die das Datum anfänglich erhoben hat und damit zu der Organisation, die in Kontakt mit dem Betroffenen steht.

Protokollieren der Verarbeitung eines Datums: Immer wenn über die Verarbeitung eines Datums weitere Protokolle geführt werden (z.B. zur Überwachung der technischen Funktionalität eines Dienstes), muss dies im angehängten Protokoll festgehalten werden. Dabei werden der komplette Protokolleintrag und eine Referenz auf das andere Protokoll erfasst, um eine spätere Auswertung des Personenbezugs der anderweitig protokollierten Informationen zu ermöglichen.

Protokollsprache

Um die Protokolle zu standardisieren und um die halbautomatische Auswertung der Protokolle zu ermöglichen, werden die Protokolleinträge in einer wohl definierten semantischen Sprache formuliert. Die Syntax der Protokollsprache basiert auf RDF [2], ein Standard zur Beschreibung von Metadaten von Webressourcen. Außerdem nutzt die Sprache ein vordefiniertes Vokabular³, das Begriffe wie Protokolleinträge, Daten, Aktionen auf Daten, Zweck der Verarbeitung, usw. wohl definiert und in Beziehung setzt [5].

Schutz und Zurechenbarkeit

Da die Protokolle zum einen personenbezogene Daten und zum anderen Informationen über Interna von Organisationen enthalten können, müssen die Protokolle vor nicht autorisierten Zugriffen geschützt werden. Dieser Schutz kann mit Hilfe von Verschlüsselungsverfahren erreicht werden. Da die Protokolle für den Betroffenen lesbar sein müssen, empfiehlt sich die Verwendung eines asymmetrischen Verfahrens, wobei der öffentliche Schlüssel des Betrof-

³ Detaillierte Informationen zum Vokabular unter: <http://isweb.uni-koblenz.de/Research/SOA/StickyLogging>

² Jede Kopie ist ein eigenständiges Datum.

fenen beziehungsweise des Auftraggebers zur Verschlüsselung der Protokolleinträge verwendet wird.

Die einzelnen Protokolleinträge werden abschließend von der protokollierenden Organisation digital signiert. Dadurch können die Protokolleinträge eindeutig ihrem Urheber zugerechnet werden und es wird sichergestellt, dass die Protokolle nicht von Dritten modifiziert werden können. Für das Signieren der Protokolle wird der in [1] beschriebene Ansatz, der speziell für das Signieren von RDF-Dokumenten entwickelt wurde, verwandt.

Szenario

Im oben vorgestellten Szenario hat die Bücherladen GmbH drei Daten erfasst: die Liste der bestellten Bücher sowie die Adress- und Kontoinformationen von Herrn Schmidt. Für jedes dieser Daten erstellt die Bücherladen GmbH ein Protokoll. In jedem dieser Protokolle identifiziert die Bücherladen GmbH sich selbst als Protokollant (*Anforderung 2*) und als verantwortlich für das Erheben der Daten. Hierfür und für alle weiteren Einträge nutzt sie die oben beschriebene wohl definierte semantische Sprache (*Anforderungen 4 und 5*). Für den Versand verpackt die Bücherladen GmbH die Bestellung mittels der Liste der bestellten Bücher. Die Verwendung der Liste zum Zweck des Versandes wird protokolliert.

Anschließend wird die Schnell-Liefer AG über ihren Web Service mit der Auslieferung beauftragt und eine Kopie der Adressdaten als Teil des Dienstauftrages übermittelt (*Anforderung 6*). Das Kopieren und dessen Zweck werden ebenfalls protokolliert. Gleichzeitig wird ein zweites Protokoll erzeugt, das mit der Kopie an die Schnell-Liefer AG übermittelt wird. In beiden Protokollen werden beide Organisationen identifiziert. Die Bücherladen GmbH als Erzeuger und die Schnell-Liefer AG als Empfänger der Kopie. Da die Auslieferung asynchron erfolgt, wird ein alternativer Kanal für die Zurückübermittlung im neuen Protokoll festgelegt.

Als nächstes nutzt die Schnell-Liefer AG die Adressdaten, um das Paket auszuliefern; dies wird ebenfalls protokolliert. Nach der Auslieferung und dem Ablauf aller vertraglichen oder gesetzlichen Aufbewahrungsfristen löscht die Schnell-Liefer AG ihre Kopie der Adressdaten. Nach dem Protokollieren des Löschvorgangs wird das Protokoll von der Schnell-Liefer AG signiert (*An-*

forderung 3) und an die Bücherladen GmbH zurückübermittelt. Die Bücherladen GmbH integriert das erhaltene Protokoll in das Protokoll der Originaladressdaten. Am Ende des Bestell- und Versandvorgangs signiert die Bücherladen GmbH ebenfalls ihre Protokolle.

Aufbauend auf den Protokollen erstellt die Bücherladen GmbH eine Webseite, die nur von Herrn Schmidt eingesehen werden kann. Auf dieser Webseite werden alle relevanten Informationen über die Verarbeitung von Daten, die Herrn Schmidt betreffen, bereitgestellt (*Anforderung 1 und 7*).

Während der gesamten Prozessausführung hat die Schnell-Liefer AG niemals Einsicht in die Protokolle der Bücherladen GmbH. In der anderen Richtung kann die Schnell-Liefer AG den öffentlichen Schlüssel von Herrn Schmidt nutzen, um, falls gewollt, die Protokolle zu verschlüsseln. Somit hätte dann auch die Bücherladen AG keine Einsicht in die Protokolle der Schnell-Liefer AG (*Anforderung 8*).

3 Chancen für die Protokollierung

In diesem Artikel wurde eine Architektur⁴ zum Protokollieren der Datenverarbeitung in verteilten Prozessen, wie sie beim Einsatz von SOA auftreten können, vorgestellt. Dabei wurde auch beschrieben, wie die Protokolle ausgetauscht und am Ende dem Betroffenen zugänglich gemacht werden können. Insgesamt ermöglicht die vorgestellte Architektur, Organisationen die Anforderungen der Datenschutzgesetze zu erfüllen. Auch wenn die heutige Rechtslage es erlaubt, dass nur sehr allgemein Auskunft erteilt werden muss (siehe [7]), so dass nur auf freiwilliger oder vertraglicher Basis detailliert informiert wird, ermöglicht die vorgestellte Architektur, detailliert Rechenschaft über die Datenverarbeitung zu geben. Dadurch ergibt sich für den Datenschutz die Chance, durch die Verwendung der vorgestellten Architektur sowohl die Belange der Betroffenen als auch die Anliegen der Organisationen zufriedenstellend zu erfüllen. Darüber hinaus bietet die vorgestellte Architektur Lösungen für organisatorische Probleme, die neben der personenbezogenen

auch die allgemeine Datenverarbeitung betreffen.

Danksagung

Ich danke Rüdiger Grimm, Steffen Staab, Felix Schwagereit und Daniel Pähler von der Universität Koblenz sowie Sebastian Meissner, Martin Rost und Jan Schallaböck vom ULD für ihre Unterstützung und anregende Diskussionen. Dieser Artikel wurde im Rahmen der Untersuchung „Technikanalyse und Risk Management für Service-orientierte Organisationen in Virtuellen Organisationen“ vom BMBF gefördert.

Literatur

1. Carroll, J. J.: Signing RDF Graphs. In: D. Fensel et al. (Eds.): The SemanticWeb? - ISWC 2003, LNCS 2870, pp. 369-384, Springer, Berlin, Heidelberg, 2003.
2. Klyne, G., and Carroll, J. J. (Eds.): Resource Description Framework (RDF): Concepts and Abstract Syntax. <http://www.w3.org/TR/2004/REC-rdf-concepts-20040210/>, retrieved June 2007, 2004
3. Pähler D., Ringelstein C. und Schwagereit F.: Service-orientierte Architekturen in virtuellen Organisationen 2007. 31. Datenschutz und Datensicherheit 9.
4. Ringelstein, C., Schwagereit, F., Pähler, D.: Opportunities and Risks for Privacy in Service-oriented Architectures, to appear at the 5th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods incorporating the 3rd International ODRL Workshop Oct 11 - 13 2007 in Koblenz, Germany.
5. Ringelstein, C. und Staab, S.: Logging in Distributed Workflows, to appear at Workshop on Privacy Enforcement and Accountability with Semantics, Nov. 2007, Busan, Korea.
6. Staab, S., Grimm, R., Bizer, J., Ringelstein, C., Schwagereit, F., Pähler, D., Meissner, S., Rost, M., und Schallaböck, J.: Technikanalyse und Risk Management für Service-orientierte Architekturen in virtuellen Organisationen, Koblenz, 2007.
7. Weichert, T., Auskunftsanspruch in verteilten Systemen, DuD: Datenschutz und Datensicherheit 30 2006, 694-699.

⁴ Ein Prototyp befindet sich zurzeit in Entwicklung und wird sobald verfügbar unter folgendem Link zum Download angeboten werden: <http://isweb.uni-koblenz.de/Research/SOA/StickyLogging>