Neue Basistechnologie zur Lösung der Herausforderungen der Datensicherheit und des Datenschutzes in der Verkehrssystemtechnik

Jäger, Hubert

Uniscon GmbH

Agnes-Pockels-Bogen 1, 80992 München, 089-41615988101, hubert.jaeger@uniscon.de

Schnieder, Lars

Deutsches Zentrum für Luft- und Raumfahrt e.V., Institut für Verkehrssystemtechnik

Lilienthalplatz 7, 38108 Braunschweig, 0531-2953444, lars.schnieder@dlr.de

Abstract

Die Auswertung großer Datenmengen in Echtzeit (Big Data Analysis) ermöglicht neue Anwendungen und Dienstleistungen, die im Verkehr unter dem Schlagwort *intelligente Verkehrssysteme* (IVS) subsummiert werden. Der Wortanteil Intelligenz steht hierbei als Synonym für Informationen und Erkenntnisse, die durch das Sammeln und Auswerten von Daten gewonnen wurden und die es ihren Nutzern ermöglichen, sich sicherer und effizienter im Verkehrssystem zu verhalten [1]. Intelligente Mobilitätsdienste und Aspekte des Datenschutzes sind oftmals unter den derzeitigen technischen Randbedingungen unvereinbar. Die verständliche Skepsis gegenüber komplexen Auswertungsverfahren geht auf die weithin fehlende Möglichkeit einer technischen „Erzwingung der Zugriffspolitik“ zurück.

Bei der mangelnden Transparenz der Datenflüsse erscheinen rein organisatorische Regelungen als nicht dauerhaft durchsetzbar. Dies wird durch eine große Zahl wiederholter Datenschutzverletzungen eindrucksvoll bewiesen [2]. Dieser Beitrag beschreibt ein Verfahren zur Behebung jener Schwäche. Er stellt eine neue Basistechnologie vor, die eine Umsetzung von entweder parlamentarisch oder privatrechtlich vereinbarter Regelwerke („Policies“) zum Lesen gespeicherter Daten auf technische Weise erzwingen kann. Eine solche technische Policy-Bindung kann auch auf die Analyse verkehrlicher Daten durch die „Sealed Analytics“ genannte Technik angewendet werden. Damit eröffnet sie einen generell nutzbaren Weg für eine datenschutzkonforme Ausrichtung von Big Data Anwendungen im Bereich intelligenter Verkehrssysteme. Für die konkrete Anwendung einer solchen datenschutzkonformen Ausrichtung verkehrlicher Big Data Anwendungen werden beispielhafte Anwendungsfälle vorgestellt.

1 Einführung in den Rechtsrahmen

Die Fähigkeit des Einzelnen über personenbezogene Daten selbstbestimmt verfügen zu können, wird als informationelle Selbstbestimmung bezeichnet. Demnach ist der Einzelne in der Lage, anderen genau das Bild von sich selbst zu geben, welches er selbst preisgeben will. Das Bundesdatenschutzgesetz (BDSG) definiert diesen Begriff wie folgt: „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“ (vgl. [3]). Da die Einführung und Nutzung von IVS-Anwendungen und -Diensten mit der Verarbeitung personenbezogener Daten verbunden ist (vgl. [4]), ist eine Betrachtung datenschutzrechtlicher Belange unerlässlich.

1.1 Rechtsstaatlicher Grundsatz der Verhältnismäßigkeit

Der Rechtsgrundsatz der Verhältnismäßigkeit wird auch als Übermaßverbot bezeichnet. Demnach muss jegliches staatliche Handeln verhältnismäßig sein. Verhältnismäßig bedeutet hierbei, dass jede staatliche Maßnahme

geeignet, erforderlich und angemessen im Hinblick auf den verfolgten Zweck sein muss [5]. Demnach ist eine Maßnahme *geeignet*, wenn sie tauglich ist, den angestrebten Zweck zu erreichen. Eine Maßnahme ist *erforderlich*, wenn sie von den geeigneten Maßnahmen die „mildeste“ ist. Eine Maßnahme ist dann *angemessen*, wenn sie nicht außer Verhältnis zum angestrebten Ziel steht. Vor dem Hintergrund der Verhältnismäßigkeit ist auch die Forderungen der IVS-Richtlinie [4] zu verstehen, dass personenbezogene Daten nur dann verarbeitet werden dürfen, wenn ihre Verarbeitung für den Betrieb von IVS-Anwendungen und -Diensten erforderlich ist.

1.2 Datenschutzrechtlicher Grundsatz der Zweckbindung

Nach [4] ist auch der Grundsatz der Zweckbindung auf IVS-Anwendungen anzuwenden. Das Recht auf informationelle Selbstbestimmung darf demnach nur auf das *Unvermeidbare* eingeschränkt werden. Dieser Grundsatz ist der Dreh- und Angelpunkt des Datenschutzrechts, da dieser die zentralen Forderungen an eine zulässige Verarbeitung (Erheben, Nutzen, Speichern) personenbezogener Daten entwirft. Durch den Zweckbindungsgrundsatz wird gefordert, dass das Erheben von personenbezogenen Daten nur für festgelegte eindeutige und rechtmäßige Zwecke erfolgen darf und, dass eine Weiterverarbeitung (Nutzen, inkl. Verändern bzw. Verknüpfen sowie Speichern) der personenbezogenen Daten nur auf eine sich mit der Zweckbestimmung vereinbarende Weise erlaubt ist [5]. Der Zeitraum der Verarbeitung (Erheben, Nutzen, Speichern) der Daten wird grundsätzlich auf das Maß zur Erreichung des Zwecks begrenzt [5]. Das bedeutet konkret, dass eine Vorratsspeicherung personenbezogener Daten grundsätzlich ausgeschlossen ist. Auch wird mit dem Zweckbindungsgrundsatz einer allzu allgemeinen Beschreibung des Zwecks widersprochen, um Gefahren auf das Recht der informationellen Freiheit so gering wie möglich zu halten. Und schließlich ist eine Zweckänderung (beim Weiterverarbeiten) nur dann zulässig, wenn sie mit der ursprünglichen Zweckbestimmung (beim Erheben) vereinbar ist.

1.3 Resultierende Herausforderungen für Big Data Analysen

Abbildung 1 stellt eine durch die beiden zuvor dargestellten zentralen rechtlichen Grundsätze der Verhältnismäßigkeit und der Zweckbindung aufgespannte Fläche dar. Im schlimmsten Fall sind beide Grundsätze nicht erfüllt (Abbildung 1, unten links). So sieht beispielsweise in seiner Rechtsprechung der Europäische Gerichtshof (EuGH) die massenhafte Speicherung von Kommunikationsverbindungsdaten als mit der Charta der Grundrechte der Europäischen Union unvereinbar an (sog. Vorratsdatenspeicherung). Im besten Falle (Abbildung 1, oben rechts) ist neben der Verhältnismäßigkeit auch die Zweckbindung in vollem Umfang erfüllt. Dennoch sind auch in diesem Fall von der verantwortlichen Stelle die Rechte der Betroffenen zu wahren (Benachrichtigung, Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht). Darüber hinaus müssen die Bestimmungen über die Einwilligung in die Verarbeitung personenbezogener Daten eingehalten werden; dies gilt vor allem dann, wenn besondere Kategorien personenbezogener Daten betroffen sind [4]. Auf jeden Fall bedarf es in solchen Fällen einer spezifischen Aufklärung über den Zweck der Erhebung, sowie die Verarbeitung oder Nutzung der damit verbundenen Daten. Liegt keine wirksame Einwilligung für die Verarbeitung und Nutzung der Daten vor, müssen zumindest zureichende tatsächliche Anhaltspunkte für eine Straftat (oder Ordnungswidrigkeit) vorliegen (sog. Anfangsverdacht).

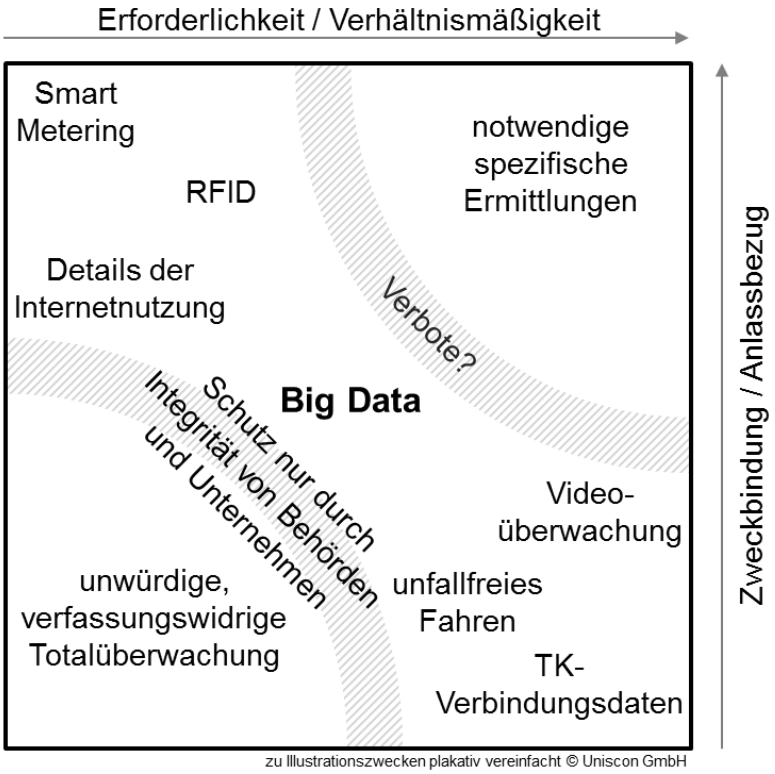

Abbildung 1: Zweckbindung und Verhältnismäßigkeit als Herausforderung

2 Spezifische Problemstellung im Verkehr

Moderne Datenverarbeitung ermöglicht einen flexiblen Umgang mit Daten. Daten können beliebig vervielfacht, fast grenzenlos verfügbar gemacht und beliebig miteinander kombiniert werden. Dies gilt natürlich auch für personenbezogene Daten. Somit ist es möglich, aus einer Vielzahl von personenbezogenen Daten, die für sich alleine stehend kaum „Informationsgehalt“ haben, ein umfassendes Bild einer Person zu erstellen. In der Anwendungsdomäne Verkehr gibt es mit der Sicherheit und Effizienz

des Verkehrsablaufs sowie Aspekten der Wirtschaftlichkeit drei grundlegende Zielstellungen, die grundsätzlich einen Informationsbedarf mit sich bringen, welcher die Erfassung personenbezogener, bzw. –beziehbarer Daten erfordert. Die drei Ziele werden nachfolgend anhand beispielhafter verkehrlicher Anwendungen skizziert:

2.1 Sicherheit des Verkehrsablaufs

Die Überwachung der Einhaltung der zulässigen Höchstgeschwindigkeit dient der Durchsetzung sicherheitsrelevanter Verkehrsvorschriften. Hierfür wird aktuell die abschnittsbezogene Geschwindigkeitsmessung (Section Control) diskutiert. Vorteile dieses Verfahrens der Geschwindigkeitskontrolle werden darin gesehen, dass hiermit gefährliche Straßenabschnitte besser überwacht werden können. Diese Einrichtungen wirken nämlich nicht, wie herkömmliche Kontrollen, nur punktuell. Diese Form der Geschwindigkeitsüberwachung erfordert allerdings, dass Bilddaten von allen Fahrzeugen erhoben werden (auch von den vorschriftsgerecht Fahrenden), um einen möglichen Verstoß festzustellen, sobald der Endpunkt des betreffenden Streckenabschnittes passiert wird. Die aktuelle Diskussion entzündet sich daran, dass ein Anlassbezug hier nicht zweifelsfrei gegeben ist, da kein Anfangsverdacht vorliegt.

Ein weiteres Beispiel sicherheitsgerichteter Maßnahmen sind Telematik-Tarife, welche sich durch eine von der Fahrweise der Fahrer abhängige Tarifbildung auszeichnen. Diese in den USA und Großbritannien üblichen Tarife wurden in Deutschland mit Beginn des Jahres 2014 von ersten Versicherungsanbietern eingeführt. Datenlogger zeichnen, um mögliche Beitragserstattungen zu ermitteln, Informationen über Fahrzeiten, zurückgelegte Kilometer, Geschwindigkeitsüberschreitungen und das Bremsverhalten auf. An die Hintergrundsysteme der Versicherungen werden hierbei Angaben zur Fahrleistung (in km) und eine auf Basis der beobachteten fahrdynamischen Parameter errechnete Punktesumme übertragen, um auf dieser Grundlage Beitragssätze zu erstatten.

2.2 Effizienz des Verkehrsablaufs

Die Abschätzung aktueller Quelle-Ziel-Matrizen (Origin-Destination-Matrizen, ODM) auf der Grundlage verfügbarer Sensordaten ist für die Verkehrsplanung und das strategische, bzw. operative Verkehrsmanagement wichtig. Durch die Kenntnis der konkreten Verkehrsverteilung (möglicherweise auch mit ihrer zeitlichen Dynamik) wird eine gezielte Beeinflussung des Verkehrsablaufs möglich. Auch in diesem Fall ist die Erhebung eindeutig identifizierbarer Merkmale erforderlich, um den konkreten Bewegungspfad eines Verkehrsteilnehmers rekonstruieren zu können.

2.3 Wirtschaftlichkeit des Verkehrs

Mit der Erhebung einer Straßenbenutzungsgebühr werden verschiedene Zielstellungen verfolgt. Unter anderem sollen externe Effekte des Verkehrs über eine nutzungsabhängige Gebühr internalisiert werden. Auch werden nutzungsabhängige Gebühren als Element zur Steuerung der Nachfrage angesehen [7]. In Zeiten zunehmend wirksam werdender Schuldenbremsen der Straßenbaulastträger dienen die erwarteten Einnahmen auch der Finanzierung von Verkehrsinfrastrukturen. Für die technisch gestützte Mauterhebung sind umfassende Erfassungseinrichtungen erforderlich, die potenziell personenbeziehbare Daten erheben. Hier ist sicherzustellen, dass diese ausschließlich für die Zwecke der Gebührenabrechnung verwendet werden und keine Weitergabe an Dritte erfolgt.

3 Lösungsansatz Sealed Analytics Technologie

Sealed Analytics liegt die zuvor erläuterte Tatsache zugrunde, dass die bedeutenden Potenziale von Big Data nur gehoben werden dürfen, wenn durch intelligente Technologien und ggf. neue Gesetze und ergänzende technische Richtlinien die Risiken einer unkontrollierter Datenweitergabe und des Datenmissbrauchs beherrscht werden. Anhand dieser Datenschutztechnik für eine grundrechtskonforme Auswertung von Big Data ist es nun möglich, diese Querschnittstechnologie auf andere

Anwendungen zu übertragen. Auf diese Weise lässt sich der Wirtschaftsstandort Deutschland insbesondere im Bereich Big-Data-stärken. Das technische Funktionsprinzip geht über die herkömmliche verschlüsselte Speicherung hinaus, bei der prinzipiell jedes gespeicherte Datum auch wieder ausgelesen werden kann. Vielmehr soll eine Kombination aus Verschlüsselung und Versiegelung, entsprechend des Prinzips der Sealed Cloud, zum Einsatz kommen.

3.1 Versiegelung

Die Idee der Versiegelung bezeichnet, dass – technisch nachweisbar – nur dezidiert autorisierte Stellen Zugriff auf die Daten erhalten. Der Kernpunkt von Sealed Analytics besteht darin, dass dies mit einer a-priori programmierten „Policy“ erzwungen wird. Diese Policy ist entsprechend datenschutzrechtlicher Vorgaben gestaltet. Es können für Big-Data-Anwendungen unterschiedliche Policies entwickelt werden, die einem dreistufigen Schema folgen:

- Auf der untersten Ebene wird das *gesetzlich geforderte Mindestniveau* der Datenschutzvorschriften umgesetzt.
- Auf der zweiten Ebene werden ergänzende, mit dem Nutzer getroffene *vertragliche Vereinbarungen* zum Datenschutz mit -einbezogen.
- Auf der dritten Ebene wird eine besonders *vorbildliche Umsetzung der Datenschutzprinzipien* z.B. Datensparsamkeit oder Privacy by Design vorgesehen.

Im Ergebnis lassen sich nur die Daten auslesen, die eine bestimmte Partei gemäß der gewählten Policy einsehen darf. Bei Veränderungen werden die rechtlichen Vorgaben ergänzt, jedoch nur mit Wirkung auf die Zukunft. Rückwirkend lässt sich die Policy nicht verändern. Dadurch sorgt Sealed Analytics für die Verbesserung des Datenschutzes: Nämlich indem die erforderlichen Zugriffsmöglichkeiten und Gütekriterien eingehalten werden können, die nötig sind, um den vertraglichen und gesetzlichen Vorgaben zu entsprechen. Die Festsetzung der Policy erlaubt dabei eine flexible

Gestaltung der Kriterien, nach denen Datenzugriffe möglich sind, wie z.B. Beschränkungen auf bestimmte Datentypen, fest eingegrenzte Zeiträume, Volumina, Datenflüsse und Berechtigungen. Die eindeutige Identifizierung der juristisch berechtigten Personen kann dann über Client-Zertifikate erfolgen, die den Endgeräten zugeordnet werden. So kann Sealed Analytics durch die Versiegelung vor Zugriff auf die Daten schützen und bewirkt, dass Unbefugte keine Daten außerhalb der programmierten Policy auslesen und auswerten können.

3.2 Verschlüsselung

In der betreibersicheren Sealed-Cloud-Umgebung [7] ist ein „Schlüsselautomat“ nötig, der eine sehr große Menge an Paaren asymmetrischer Schlüsselpaare erzeugen kann. Die öffentlichen Schlüssel (public keys) können dann an die Orte der Datenerhebung zur blockweisen Verschlüsselung der Daten exportiert werden. Die privaten Schlüssel (private keys), die zur Entschlüsselung benötigt werden, sind in einem mehrfach redundanten, aber rein volatilen Speichersystem innerhalb der Sealed Cloud aufbewahrt. Durch diese Art der Aufbewahrung ist, gemäß des Sealed-Cloud-Schutz-Konzepts, sichergestellt, dass niemand unverschlüsselte Daten auslesen kann – weder bei autorisierten noch unautorisierten Zugriffen auf die Speichereinheiten.

3.3 Zugriff über das Policy Gate

Wenn eine berechtigte Person nun entsprechend der für den konkreten Anwendungsfall definierten Regeln, Daten oder Metadaten auslesen soll, so kann dies ausschließlich über das „Policy Gate“ erfolgen. Das Policy Gate implementiert die Logik, die nur in einen strengen Versionierungsschema geändert werden kann. Diese Logik ist somit nicht rückwärtig änderbar, d. h. sie kann nicht nachträglich umgestaltet werden kann, um bestehende Datenbestände auszuwerten. Die Zertifikate externer Auditoren würden für die Nutzer sichtbar sofort erlöschen. Aus diesem Grund bietet Sealed

Analytics die Möglichkeit, Daten anwendungs- und anlassbezogen auszuwerten, sofern vor der Speicherung eine entsprechende semantische Strukturierung und Anreicherung von Datenbeständen mit Metadaten erfolgte. Damit wird erreicht, dass unterschiedlichen Nutzer durch die Zuweisung entsprechender Rechte auf unterschiedliche Daten zugreifen können. Jede nicht anwendungs- oder anlassbezogene Verwendung kann nachweisbar ausgeschlossen werden. Abbildung 2 stellt die Komponenten von Sealed Analytics wie bereits beschrieben, vor:

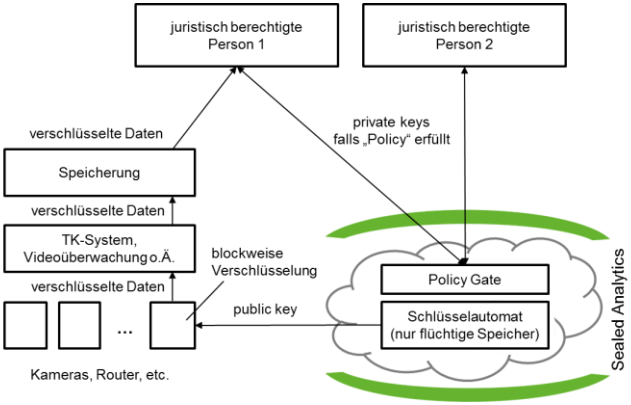

Abbildung 2: Komponenten von Sealed Analytics

4. Konkretes verkehrliches Ausführungsbeispiel

Ein verkehrliches Anwendungsbeispiel des zuvor dargestellten Sealed Analytics-Konzepts ist der Einsatz von Kennzeichenerfassungs-einrichtungen (ANPR, automatic number plate recognition). Diese können unterschiedlichen Zwecken dienen: Zum einen dienen diese der Erfassung originär verkehrsrelevanter Größen wie beispielsweise Reisezeiten zwischen zwei Erfassungseinrichtungen (relevant für die Bestimmung der erreichten Verkehrsqualität (level of service) eines Verkehrsnetzes) oder der Bestimmung von Quelle-Ziel-Relationen (relevant für die

Verkehrsplanung). In diesen Fällen, können Zugriffs-Policies so gestaltet sein, dass sie von personenbezogenen Merkmalen abstrahieren (Pseudonymisierung, besser noch eine Anonymisierung als Grundsatz des Schutzes der Privatssphäre, vgl. [4]). Die juristisch berechtigte Person ist hierfür der Straßenbaulastträger (Bund, Länder, Kommunen).

Ein anderer Anwendungsfall, der auf die gleiche Datenbasis zugreifen kann, ist das Kennzeichen-Scanning für polizeiliche Ermittlungen. Wegen des erforderlichen Anfangsverdachts müssen für diesen Fall strengere Policies vereinbart werden. So könnte beispielsweise ein automatischer Zugriff auf Kennzeichendaten eines normalerweise für andere Zwecke benutzten ANPR-Systems nur bei Vorliegen eines begründeten Anfangsverdacht (bspw. Anzeige eines Kfz-Diebstahls) durch einen automatischen Abgleich der Datenbasen erfolgen. Die juristisch berechtigten Personen sind hierbei die staatlichen Sicherheitsorgane (Polizei).

5. Zusammenfassung

Die in diesem Beitrag vorgestellte Basistechnologie eröffnet verkehrlichen Big Data Anwendungen generell eine datenschutzkonforme Ausrichtung. Durch sie wird sichergestellt, dass die personenbezogenen Daten von IVS-Anwendungen gegen Missbrauch, wie unrechtmäßigen Zugriff, Veränderung oder Verlust, geschützt sind. Der Zugriff auf die potenziell personenbezogenen Daten einer IVS-Anwendung durch die verschiedenen Parteien kann auf eindeutig definierte Datenbestände technisch gewährt, oder nachweisbar verwehrt werden. Die unterschiedlichen Berechtigungen ergeben sich aus einer rechtlichen Bewertung, unter welchen, ggf. abgestuften Voraussetzungen, welche Parteien zugreifen dürfen. Im verkehrstechnischen Umfeld stellt die Technologie einen Weg zur Nutzung von im Verkehrswesen erhobenen Daten zur Steigerung der

Verkehrssicherheit der Effizienz des Verkehrsflusses bzw. der Wirtschaftlichkeit der Verkehrsmittel und -wege dar. Denn mit ihr wäre eine datenschutz- und rechtskonforme Auswertung, und damit eine breite Akzeptanz in Politik und Bevölkerung möglich.

Literatur

[1] Bundesministerim für Verkehr, Bau und Stadtentwicklung: IVS-Aktionsplan ‚Straße' – koordinierte Weiterentwicklung bestehender und beschleunigte Einführung neuer intelligenter Verkehrssysteme in Deutschland bis 2020. Berlin (2012).

[2] Bundesbeauftragter für Datenschutz und Informationsfreiheit Peter Schaar: 24. Tätigkeitsbericht 2011 – 2012, erschienen am 24. April 2013.

[3] Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003.

[4] Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern.

[5] Keil, Oliver: Grundsätze des Datenschutzrechts. https://www2.informatik.hu-berlin.de/~keil/docs/Grundsaetze_des_Datenschutzrechts.pdf; 06.11.2014

[6] Boltze, M.; Roth, N.: Einsatz von Instrumenten des Mobility Pricing zur Optimierung von Verkehr und Transport. In: Straßenverkehrstechnik, Heft 3, März 2009, Seite 125-132.

[7] Hubert Jäger et. al. "A Novel Set of Measures against InsiderAttacks - Sealed Cloud", in: Detlef Hühnlein, Heiko Roßnagel (Ed.): Proceedings of Open Identity Summit 2013, Lecture Notes in Informatics, Volume 223.