Irreversibler Verschluss: DRM-basierter Datenschutz

Ulrich Greveler

Fachhochschule Münster, Labor für IT Sicherheit, 48565 Steinfurt
greveler@fh-muenster.de

Zusammenfassung

Das Prinzip aus dem Datenschutzrecht bekannte der „Datensparsamkeit und Datenvermeidung“ wird technisch um das Konzept des „irreversiblen Verschlusses“ erweitert. Daten können unter Nutzung vertrauenswürdiger Hardware in einer Weise gespeichert werden, die zwar eine Verarbeitung für bestimmte Zwecke erlaubt, ein Abrufen des vollständigen Datenbestandes jedoch zuverlässig verhindert. Die verschlossenen Daten stehen dann keiner Partei mehr zur Verfügung, wodurch insbesondere eine unrechtmäßige vorsätzliche oder fahrlässige Weitergabe des Datenbestandes verhindert wird. Der Beitrag beschreibt das Konzept und stellt mögliche Anwendungsfälle vor.

1 Einführung

Wir skizzieren die Entwicklung einer datenschutzfördernden Technologie auf Basis digitaler Rechteverwaltung. Der technologische Ansatz besteht darin, eine Speicherung sensibler Daten in einer Weise vorzusehen, dass sie „für immer verschlossen“ bleiben, auch aus Sicht der Partei, die die Datenspeicherung vornimmt.

Die Kernidee kann in folgende zwei Aspekte aufgeteilt werden.

- Das Prinzip der „Datensparsamkeit und Datenvermeidung“ wird technisch um das Konzept des „irreversiblen Verschlusses“ erweitert. Wir entwickeln ein System, das zweckgebundene Daten einerseits speichert, sie aber andererseits nie mehr unverarbeitet preisgibt, so dass bei vorsätzlichem wie fahrlässigem Fehlverhalten ein Missbrauch ausgeschlossen wird und die Zweckbindung der Datenhaltung technisch erzwungen wird.
- Eine technische Realisierung des „irreversiblen Verschlusses“ ist unter Verwendung von DRM-Konzepten im Zusammenspiel mit PC-Technologie möglich, wenn ein vorhandenes TPM und die Funktion *Sealing* verwendet werden.

Ein System, dessen Architektur in diesem Beitrag skizziert wird, stellt folgende Funktionen bereit:

- Datenhaltung großer Datenmengen, die nicht ausgegeben werden, jedoch für definierte Prozesse (z. B. einmalige Auswertung) zur Verfügung stehen
- Rechteverwaltung für Datenobjekte und Nutzer bzw. Rollen
- Datenabgleiche von externen mit internen Daten bzw. zwischen internen Daten verschiedener Systeme, wobei nur die „Treffer“ im Detail (in vorbestimmter Maximalzahl) oder als Anzahl ausgegeben werden und die Art des Abgleichs aus einer weißen Liste erlaubter Operationen zu wählen ist

- Gewinnung statistischer Aussagen über die Gesamtheit des Datenbestandes
- Übertragung der Daten in gleichartige Fremdsysteme, sofern ein Vertrauensstatus verifiziert wurde
- Löschung der gespeicherten Daten bei Manipulationen am System
- Beweissichere Protokollierung der Operationen auf dem Datenbestand

Anwendungsfelder sind hier Datenabgleiche zwischen Behörden (z. B. Identifizieren von Personen, zu denen Daten im Bestand mehrerer Behörden vorliegen), die auf klar definierter gesetzlicher Grundlage erfolgen, wobei vermieden werden soll, dass beteiligte Mitarbeiter den Gesamtdatenbestand einsehen, drucken, erheblich modifizieren, versenden oder elektronisch auf Datenträger kopieren können.

1.1 „Datenpannen“ in der jüngeren Vergangenheit

In jüngster Zeit gab es einige Datenschutzverletzungen, die ein beträchtliches Medienecho (Skandale um sog. „Datenpannen“) auslösten. Beispielhaft seien die folgenden genannt.

- Am 4.10.2008 wurde gemeldet, dass beim Netzbetreiber *T-Mobile* bereits im Jahre 2006 mehr als 17 Millionen Kundendatensätze kopiert und „am Schwarzmarkt angeboten“ wurden. [Afp08]
- Die *Deutsche Telekom* hat in den Jahren 2005 und 2006 durch ein Berliner Beratungsunternehmen Telefonverbindungsdaten eigener Manager und von Aufsichtsräten der Arbeitnehmerseite auswerten lassen. [Spie08]
- Im Dezember 2007 wurde bekannt, dass in Großbritannien die gespeicherten Namen, Anschriften und E-Mail-Adressen von rund drei Millionen Führerscheinanwärtern mit dem Datenträger „verloren“ wurden. [Netz07]
- Im September 2008 räumte die Hochschulleitung der Universität Göttingen ein, dass die Daten von 26.000 Studenten ungeschützt auf einem Internetserver zugänglich waren. [Unis08]

Die Liste ließe sich fortsetzen; in der Zeit zwischen der Einreichung dieses Beitrages und der Fertigstellung der Druckversion haben sich weitere öffentlich wahrgenommene Fälle (z. B. *Deutsche Bahn*) ereignet. Obwohl diese Skandale unterschiedlicher Natur sind (Vorsatz versus Fahrlässigkeit), gibt es eine Gemeinsamkeit: Die entwichenen Daten wurden offenbar nicht in technischer Hinsicht ausreichend geschützt, obwohl es anwendbare Technologien und Verfahren gibt. „Skandalös“ aus technischer Sicht ist, dass die „Datenpannen“ möglich waren, unabhängig davon, dass es zudem ein juristisch zu bewertendes Fehlverhalten gab.

2 Stand der Technik, bisherige Arbeiten

Für die Architektur der Plattform ausschlaggebend ist der Stand der Technik in Bezug auf vertrauenswürdige Hardware und *Trusted Computing*. 2003 wurde von führenden IT-Unternehmen eine gemeinnützige Organisation gegründet, die offene Standards für sichere Hardware- und Softwareprodukte erarbeiten soll. Unter dem Namen *Trusted Computing Group* (TCG) versuchen die beteiligten Unternehmen, ihre Sicherheitsinitiativen zu koordinieren. Den Kern der Arbeit der TCG bildet die Spezifikation eines Moduls, auf dem das gesamte Sicherheitskonzept aufbaut: das *Trusted Platform Module* (TPM). Das TPM ist ein passiver Chip, der einen Mikrokontroller enthält und fest mit dem Mainboard oder dem Prozes-

sor verbunden ist. Es ist von seiner Architektur her mit einer Prozessorchipkarte vergleichbar. Wesentliche Funktionen des TPM sind die Bereitstellung eines speziellen Schlüssels, mit dem die Plattform von Dritten als vertrauenswürdig erkannt werden kann, und die sichere Erkennung einer als vertrauenswürdig angenommenen Systemkonfiguration.

Digitale Rechteverwaltung (DRM) bezeichnet Verfahren, mit denen Verbreitung und Nutzung digitaler Inhalte gesteuert und überwacht werden soll. Die unter DRM gefassten Technologien wurden ursprünglich für audiovisuelle Medien und Rundfunkübertragungen konzipiert (Scrambling, DVD, PayTV u. a.), können aber zum Teil auf beliebige Daten in digitaler Form angewandt werden. Ausnahmen stellen forensische Verfahren wie digitale Wasserzeichen dar, die auf starke Redundanz zu schützender Daten abzielen, die außerhalb des audiovisuellen Bereiches allgemein nicht gegeben ist.

Während im Sektor *PayTV* (Bezahlfernsehen) seit den 80er Jahren DRM (und seine Vorläufer) ein erfolgreiches Geschäftsmodell für Multimedia-Inhalte trotz der zunehmenden Digitalisierung der Fernseh- und Filmproduktionen auf der einen Seite und verbesserter Multimediafähigkeit von Privatanwender-PCs auf der anderen Seite ist, scheiterte die Verwendung von DRM beim Vertrieb von Musikstücken und Datei-Downloads. Als Ursache wird meist eine mangelnde Akzeptanz beim Verbraucher angenommen, der – wenn er zur Nutzung von DRM gezwungen wird – den Konsum DRM-geschützter Stücke als unpraktisch und übertrieben restriktiv empfindet bzw. berechtige Sorge haben muss, dass der zukünftige Konsum bei Neuanschaffung von Nachfolgegeräten nicht mehr möglich ist. Ein freier Datenfluss wird durch DRM allgemein verhindert; diese Eigenschaft ist für die in diesem Beitrag beschriebene Anwendung jedoch nicht nachteilhaft, sondern wird ausgenutzt.

Rechtebeschreibungssprachen dienen der Kodierung von Rechtebeschreibungen in maschinenlesbarer Form. Unter Rechtebeschreibung (*Rights Expression*) wird im hier betrachteten Umfeld eine formale Beschreibung verstanden, die ausdrückt, dass einem bestimmten Nutzer (bzw. einer Rolle) ein Recht gewährt oder entzogen wird, unter gewissen Bedingungen eindeutig beschriebene Datenfelder auf eine festgelegte Art und Weise zu nutzen. Die Rechtebeschreibung stellt daher ein formalisiertes Einzelrecht, d. h. eine Zuordnung dieser (max). fünf Objekte untereinander dar. Die für die Plattform interessanten Sprachen sind die XML-basierten Konstrukte *Security Assertion Markup Language* (kurz SAML), *Open Digital Rights Language* (ODRL) und *eXtensible Access Control Markup Language* (XACML). Insbesondere ODRL erscheint für Implementierungen in besonderer Weise geeignet, da es dokumentierte Erfahrungen in der DRM-Anwendung von ODRL und Open-Source-Implementierungen des Interpreters gibt.

2.1 Ansätze zur Nutzung von DRM für den Datenschutz

Eine Nutzung von DRM-Technologie zum Schutz personenbezogener Daten wird von Böhme und Pfitzmann [BöPf08] kritisch betrachtet. Die Autoren weisen darauf hin, dass DRM für Medieninhalte sehr fehleranfällig sei und dass *Privacy-DRM* unter technisch deutlich ungünstigeren Voraussetzungen noch höhere Anforderungen erfüllen müsse. Zudem könnten digitale Wasserzeichen, eine Kerntechnologie heutiger Medieninhalte-DRM-Technik, für Privacy-DRM praktisch nicht eingesetzt werden. Es wird gefolgert, dass Privacy-DRM grundsätzlich anders realisiert werden müsse, nämlich unter Einsatz von manipulationssicherer vertrauenswürdiger Hardware.

Beim zweiten Internet Governance Forum (IGF) der UN gab es für die Idee des *Persönlichen DRM* Zustimmung: Simon Davies, Direktor der Organisation *Privacy International* (PI), sprach sich dafür aus, in Zukunft auf technische Lösungen zu setzen: „Es ist klar, dass rechtliche und Marktlösungen nicht in ausreichendem Maß den individuellen Nutzer in seinen Rechten schützen können, daher müssen wir einen Weg einschlagen, der Nutzerkontrolle durch technische Infrastrukturen einbezieht“ [Davi07].

Schallaböck vom unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) weist darauf hin, dass DRM in der (i. a. kritisch vorgenommenen) Interpretation als *Digital Restrictions Management* gerade für den technischen Schutz personenbezogener Daten geeignet sei, da diese nicht dem *Free Flow of Information* unterliegen sollten und die technische Durchsetzung der Zweckbindung erhobener Daten eine DRM-Infrastruktur nahe lege [Scha06].

Die Verwendung von *Trusted-Computing*-Technologie (hier: TCPA[1]) zur Duchsetzung digitaler Rechte ist Gegenstand zahlreicher Veröffentlichungen [Eric03, GSS03, ReCa05]. Datenschutzaspekte in Bezug auf diese Technologie werden meist kritisch [Bech05] betrachtet oder die Technologie wird in Gänze als gesellschaftliche Gefahr wahrgenommen und verworfen [Gras06]. So schreibt bereits im Jahre 2003 Roy Pfitzner (beim Landesbeauftragten für den Datenschutz Brandenburg): „TCPA wurde oft mit einem datenschutzunfreundlichen DRM-Betriebssystem gleichgesetzt. Fehlerhafte Darstellungen zu der TCPA-Technologie haben ihren Eingang in Fachartikeln, Promotionen und sogar in eine Anfrage der CDU/CSU-Fraktion an den Bundestag gefunden.“ [Pfit03] Hintergrund dieser einseitigen Rezeption einer Technologie ist, dass auch als datenschutzfeindlich betrachtete Zwecke gefördert werden können, insbesondere können Konsumenten digitaler Waren (z. B. Musikstücken) zur Preisgabe personenbezogener Daten gezwungen werden, wenn sie an einem geschlossenen System der Distribution teilnehmen.

3 Prototypische Realisierung

Die Nutzung von PC-Architektur, TPM-Technologie und eines Sicherheitskernels (z. B. emscb/*Turaya*), der einen sicheren Bootvorgang und die Überprüfung einer sicheren Systemkonfiguration zulässt, ermöglicht bereits eine technologische Realisierung, die im folgenden skizziert wird.

Der PC-basierte Prototyp bootet (unter Nutzung von *TrustedGRUB*[2] und einem Linux-basierten Microkernel) in eine als sicher definierte Systemkonfiguration und startet dann die Applikation mit der Datenschutzanwendung. Die zu schützenden Rohdaten sind nur in verschlüsselter Form auf der Festplatte gespeichert; der hier genutzte Schlüssel kann mithilfe des TPM-Chips in der sicheren Konfiguration berechnet werden (er wird vom sog. *Storage Root Key* abgeleitet). Die Applikation liest die (digital signierte) maschinenlesbare Rechtebeschreibung ein und lässt gemäß des DRM-Konzeptes und vorliegender Rechtebeschreibung entsprechende Zugriffe auf die Datenbasis zu.

---

[1] *Trusted Computing Platform Alliance (TCPA)* war ein Konsortium, das 1999 von Microsoft, IBM, und weiteren Herstellern gegründet wurde. Inzwischen wurde es von der von der Nachfolgeorganisation *Trusted Computing Group (TCG)* abgelöst.

[2] Erweiterung des Linux-Bootloaders *GRUB*. URL: http://www.sirrix.com/content/pages/trustedgrub.htm

Der Beitrag beschreibt drei Anwendungsfälle (*Kunden-Datenschutz*, *Mitarbeiter-Datenschutz* und *Elektronische Fahndung / Datenabgleich*).

3.1 Anwendungsbeispiel: Kunden-Datenschutz

Die Anwendung für den *Kunden-Datenschutz* sieht eine Erfassung von (Neu-)Kunden am Mitarbeiter-PC oder automatisiert über eine Webapplikation vor. Hier werden kritische personenbezogene Daten gespeichert (Name, Adresse, Kontodaten: Kontonummer und BLZ u. a.). Die Datenbank umfasst auch operationelle Datensätze eines Kunden (z. B. aktive Bestellungen, abgeschlossene Vorgänge). Der funktionale Rahmen, der hier berücksichtigt wird, umfasst die Anforderungen

- Auskunftsersuchen (Kunden wollen ihre personenbezogenen Daten abfragen)
- Versenden (Adressausgabe) bei Vorliegen eines Auftrages
- Sichere Löschung (nach Ablauf der Aufbewahrungsfrist)
- Marketingkampagnen (Bedrucken von Briefumschlägen mit Kundenadressen)
- Weitergabe eines Datensatzes an dritte Partei nach Zustimmung des Kunden
- Backup-Funktionalität

Die Plattform (siehe Abbildung 1) stellt dabei zuverlässig technisch sicher, dass bestimmte Funktionalitäten ausgeschlossen werden, insbesondere sind dies:

- Kopieren oder Ausdrucken des Datenbestandes
- „Stöbern“ im Datenbestand ohne das Hinterlassen von Protokollspuren
- Wiederherstellen irreversibel verschlossener oder gelöschter Daten (z. B. nach Diebstahl oder Beschlagnahme, auch nicht für den Datenbankbesitzer)
- Weitergabe ohne Zustimmung (sofern dies aus dem Bestand geschieht)[3]
- Gleichzeitiges Verändern mehrerer Datensätzen ohne nachgewiesenes Privileg

[3] Die Plattform kann nicht verhindern, dass bereits bei der Datenerfassung eine Weitergabe erfolgt.

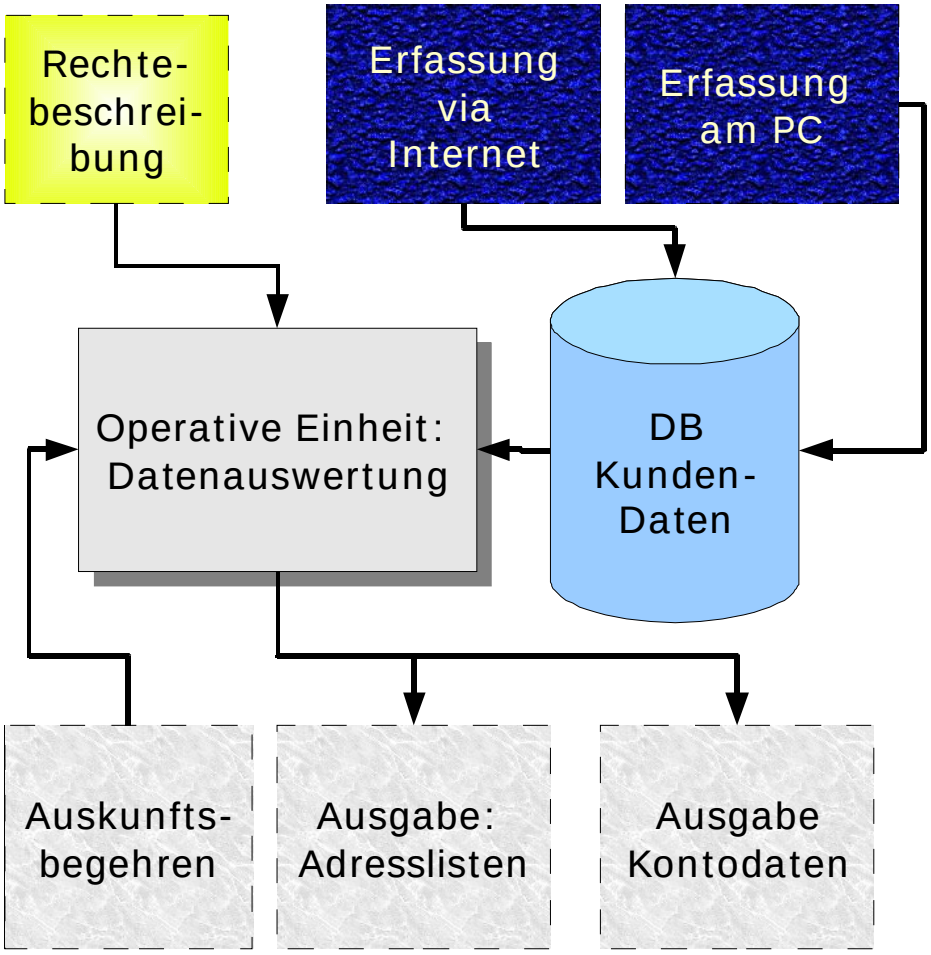

Abbildung 1 Anwendung: Kundendatenschutz

3.2 Anwendung: Mitarbeiter-Datenschutz

Die Anwendung für den *Mitarbeiter-Datenschutz* sieht eine Datenhaltung für Arbeitszeitdaten vor, d. h. es werden Daten gewonnen, die über Arbeitszeiterfassungsgeräte erfasst werden. Diese Geräte können beispielsweise in der Nähe von Zugangstüren angebracht sein, oder es handelt sich um mobile Geräte, mit denen Mitarbeiter den Beginn oder das Ende eines Arbeitseinsatzes oder einer Schicht erfassen.

Es wird folgende Funktionalität benötigt

- Arbeitszeitbeginn und -ende (Arbeitszeitdaten) werden gespeichert
- Für jeden Mitarbeiter wird ein Stundenkonto geführt
- Es werden statistische Daten über Arbeitszeiten ausgegeben
- Eine Backup-Lösung (bzw. tagesaktuelles Cloning einer Datenbank) wird integriert

Die Komponenten und ihre Beziehungen untereinander werden in der Abbildung 2 vereinfacht dargestellt.

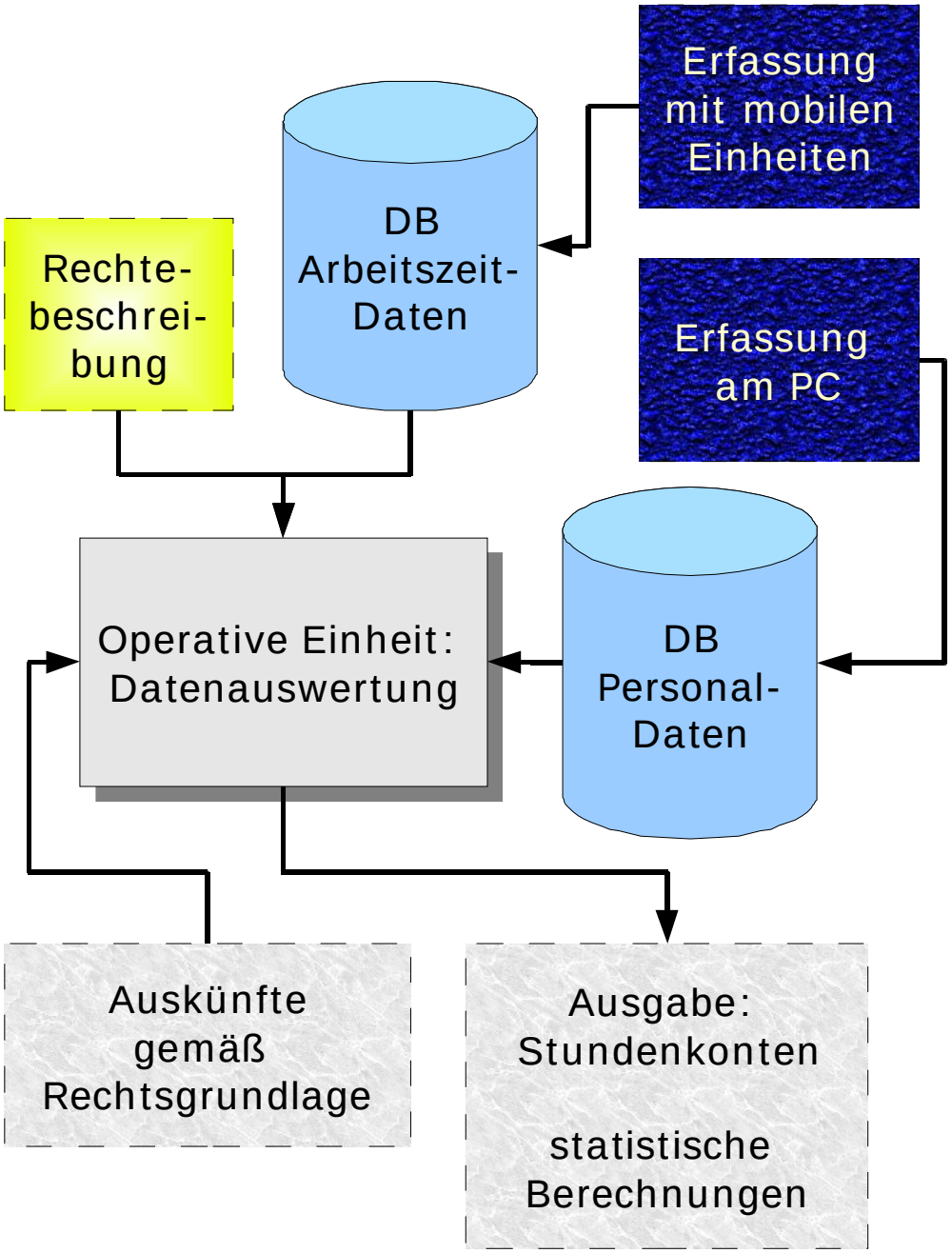

Abbildung 2 Anwendung für den Mitarbeiter-Datenschutz

Die Operative Einheit muss hierbei nicht notwendigerweise eine eigenständige Komponente sein, die eine sichere Kommunikationsbeziehung zu den beiden Datenbanken aufbaut, sie kann durchaus in eine (oder beide) Datenbank-Komponenten integriert sein.

Die Anforderungen an die Komponente *DB Arbeitszeitdaten* sind hierbei:

- Die Arbeitszeitdaten können nicht exportiert werden (von den nun folgenden Ausnahmen abgesehen).
- Die Arbeitszeitdaten sind nach Ablauf der Aufbewahrungsfrist zu löschen
- Die Stundenkontenstände der Mitarbeiter werden regelmäßig (z. B. wöchentlich) ausgegeben (Export im Klartext z. B. an ein SAP-System).

- Arbeitszeitdaten eines einzelnen Mitarbeiters können über eine bestimmte Rolle angefordert und ausgegeben werden. Erlaubte Suchparameter sind durch eine maschinenlesbare *Rechtebeschreibung* definiert.

Der datenschutzrechtliche Rahmen, der hier funktional abgebildet werden soll, besteht in folgenden Anforderungen.

- Arbeitszeitdaten sind personenbezogene Daten, die ausschließlich zu festgelegten Zwecken (Stundenkonto) verarbeitet werden
- Ein Mitarbeiter kann Auskunft über gespeicherte Daten zu seiner Person verlangen (z. B. um Abrechnungsvorgänge nachzuvollziehen)
- In begründeten Fällen (und mit Zustimmung der Personalvertretung) können einzelne Mitarbeiter aufgrund ihrer Arbeitszeitdaten identifiziert werden (z. B. um eine Straftat aufzuklären). Anfragen dieser Art können nur von einer bestimmten Rolle und in einem gewissen Rahmen zugelassen werden.

Der letztgenannte Punkt sieht eine Zusammenführung von Daten beider Datenbanken (*DB Personaldaten* und *DB Arbeitszeitdaten*) vor und erfordert eine detaillierte Feinspezifikation, da hier zunächst zu untersuchen ist, inwieweit der rechtliche Rahmen überhaupt mittels einer technischen Rechtebeschreibung kodierbar ist. Die Komponente kann wirksam gewisse Klassen von unzulässigen Anfragen verhindern (z. B. solche Anfragen, deren Ergebnis eine Ausgabe der Arbeitszeitdaten von zu vielen Mitarbeitern zur Folge hätte).

Statistische Berechnungen sollen zudem möglich sein, sofern keine Gewinnung der Rohdaten (hier: Arbeitszeitdaten) möglich ist. Für die Betriebsleitung kann es beispielsweise interessant (und legitim) sein, zu erfahren, wie viele Mitarbeiter vor einem bestimmen Zeitpunkt mit den Dienstgeschäften beginnen (Parkraumbewirtschaftung), zu welcher Zeit die Mittagspause genommen wird (Kantinenorganisation) oder wie viele Personen sich in einem Gebäude aufhalten (Sicherheitsüberlegungen). Die Rechtebeschreibungssprache muss dabei mächtig genug sein, sowohl die Art der statistischen Berechnung abzubilden (z. B. vollständige SQL-Statements integrieren) als auch Beschränkungen parametrisierbarer Anforderungen zu überwachen, die zur De-Anonymisierung genutzt werden könnten (Parameterkombinationen müssen beschränkt werden können).

Der Aspekt *Auskunftsrecht* ist für die Architektur problematisch, da ein *irreversibler Verschluss* nicht mehr gegeben ist, wenn eine privilegierte Rolle einzelne Rohdatensätze anfordern kann (diese Rolle könnte dann alle Datensätze auslesen). Hier ist unter Abwägung des rechtlichen Rahmens und der Wirksamkeit des Schutzes zu entscheiden, ob diese Schwachstelle akzeptiert wird oder ob das Auskunftsrecht ebenfalls insoweit beschränkt wird, dass nach Erreichen eines Schwellenwertes keine Auskünfte möglich sind. Die Daten könnten dann nur noch in Gänze gelöscht werden, um Einzelinteressen zu befriedigen.

3.3 Anwendung: Elektronische Fahndung / Datenabgleich

Bei einer *Rasterfahndung* werden personenbezogene und personenbeziehbare Daten anhand eines vorgegebenen Rasters (Profil eines Täters) aus verschiedenen meist sehr umfangreichen Datenbeständen zusammengeführt. Ziel ist die Ermittlung des Täters bzw. die Gewinnung einer überschaubaren Menge verdächtiger Personen, die weiter überprüft werden kann. Im hier dargestellten Beispiel (siehe *Abbildung 3*) liegt eine Beschreibung eines verdächtigen Fahr-

zeugs als Rasterinformation vor (Marke, Typ, Farbe) und eine Datenbank mit erfassten Kennzeichen[4] über einen definierten Zeitraum; die Fahndung kann hier elektronisch durchgeführt werden. Im Jahre 2006 erfolgte ein wegweisender Beschluss des Bundesverfassungsgerichtes zur Definition und zur Zulässigkeit einer solchen Fahndungsmaßnahme.

> **Beschluss des BVG vom 4. April 2006 – 1 BvR 518/02 (Auszug):**
>
> **Die Rasterfahndung ist eine besondere polizeiliche Fahndungsmethode unter Nutzung der elektronischen Datenverarbeitung. Die Polizeibehörde lässt sich von anderen öffentlichen oder privaten Stellen personenbezogene Daten übermitteln, um einen automatisierten Abgleich mit anderen Daten vorzunehmen. Durch den Abgleich soll diejenige Schnittmenge von Personen ermittelt werden, auf welche bestimmte, vorab festgelegte und für die weiteren Ermittlungen als bedeutsam angesehene Merkmale zutreffen. (…)**
>
> **Angesichts des Gewichts der mit der Durchführung einer Rasterfahndung einhergehenden Grundrechtseingriffe ist diese nur dann angemessen, wenn der Gesetzgeber rechtsstaatliche Anforderungen dadurch wahrt, dass er den Eingriff erst von der Schwelle einer hinreichend konkreten Gefahr für die bedrohten Rechtsgüter an vorsieht.**

Eine Vornahme der Rasterfahndung kann in technischer Hinsicht darin bestehen, alle erfassten Kennzeichen eines definierten Zeitraums (gemäß Tatzeitpunkt) zu ermitteln und zu diesen mithilfe der Datenbank der KfZ-Meldestelle eine Tabelle zu bilden, die zeilenweise Einträge über das Kennzeichen, den Halter (Name und Meldeadresse) und das Fahrzeug (Marke, Typ, Farbe) enthält. Unter Verwendung der Rasterinformation kann dann eine Menge von Personen (Fahrzeughaltern) bestimmt werden, die gemäß Rasterinformation als Verdächtige in Frage kommen.

Eine derart vorgenommene Fahndung kann rechtlich zulässig sein, wenn die Angemessenheit gewahrt ist (d. h. es wurden schwerwiegende Straftaten begangen bzw. es besteht weiterhin eine erhebliche Bedrohung). Wenn die Datenbankinhalte den Ermittlern aufgrund eines Beschlusses zur Verfügung gestellt werden (z. B. als exportierter *Dump*), lässt sich jedoch i. a. nicht mehr nachverfolgen, ob diese nur zu dem benannten Fahndungsvorhaben eingesetzt wurden und ob die Daten nach der Auswertung gelöscht werden.

[4] Die automatische Erfassung von Autokennzeichen gemäß der Ländergesetze von Hessen und Schleswig-Holstein ist nach Beschluss des BVG vom März 2008 verfassungswidrig (Az.: 1 BvR 2074/05 und 1 BvR 1254/07). Laut Gerichtspräsident Papier (mdl. Erklärung zum Urteil) ist der Grundrechtseingriff vergleichsweise gering, wenn mit der Kennzeichenerfassung nur nach gestohlenen Fahrzeugen oder etwa Versicherungsverstößen gesucht und alle Nichttreffer sofort spurenlos gelöscht werden. Je schwerer aber ein Eingriff ist (z. B. Speicherung), umso klarer und präziser muss auch die gesetzliche Grundlage sein, die die Polizei dazu ermächtigen soll. Zur Zeit bereiten mehrere Bundesländer neue gesetzliche Regelungen vor.

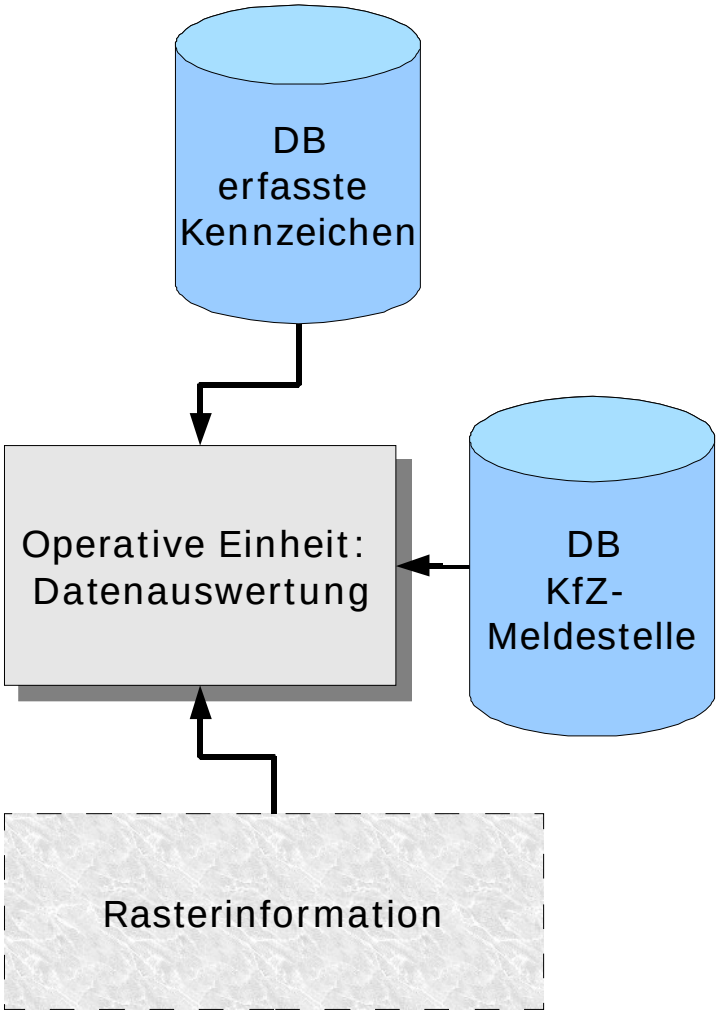

Abbildung 3 Fahndung gemäß eines KfZ-Profils

Anforderungen sind hier, dass die Operative Einheit

- die Rohdaten erfasst, ohne dass diese Daten dem Ermittler zugänglich sind,
- nur eine einmalige Auswertung gemäß des Beschlusses vornimmt,
- nur dann die „Treffer“ ausgibt, wenn die Gesamtzahl einen im Beschluss festgelegten Schwellenwert nicht überschreitet,
- einen signierten Bericht generiert, der die vorgenommenen Operationen dokumentiert und an eine Kontrollinstanz weiterzugeben ist
- und die Daten zu einem definierten Zeitpunkt bzw. nach der Auswertung löscht.

Es sind weitere Eigenschaften denkbar, die gemäß rechtlicher Grundlagen in die Funktionalität eingebracht werden können (z. B. Verwaltung von Privilegien, Einlesen eines Beschlusses in maschinenlesbarer Form, automatisierte Information der betroffenen Personen zu einem späteren Zeitpunkt, Auskunftsrecht).

Eine Besonderheit bei diesem Anwendungsfall ist neben den ausgeprägten rechtlichen Beschränkungen die mobile Natur der Datenerfassung. Geräte, die Kfz-Kennzeichen erfassen, werden nur vorübergehend an „Kontrollpunkten“ aufgestellt (es existieren jedoch auch stationäre Einheiten).

Wir gehen davon aus, dass nach Erfassung ein Transport eines Datenträgers erfolgt, der eine Liste erfasster Kennzeichen enthält. Um einen Missbrauch der Daten (z. B. durch Duplizierung) frühzeitig zu verhindern, kann hier in der Spezifikation eine Speicherung auf einer Chipkarte vorgesehen werden. Das Kennzeichenlesegerät überträgt die Daten unmittelbar an eine eingesteckte Chipkarte, die sowohl als (mobiler) Datenträger fungiert als auch bereits das „Datengrab“ (irreversibler Verschluss) darstellt, d. h. die gelesenen Daten werden die Karte nicht mehr verlassen (die Chipkarte enthält also die *DB Erfasste Kennzeichen* im EEPROM).

Die *Operative Einheit* ist demnach in der Lage, sich gegenüber der Karte zu authentisieren und eine Suche auf den Daten vorzunehmen bzw. die Daten unter DRM-Beschränkung zu importieren.

3.4 Sicherheitsbetrachtungen

Die Durchsetzung der digitalen Rechte zu Datenschutzzwecken stützt sich auf die Fähigkeit der vertrauenswürdigen Hardware, den Zugriff auf unverschlüsselte Daten tatsächlich allein auf sichere Konfigurationen zu beschränken. Angriffe auf Hardware-basierte Sicherheitsfunktionalität auf Grundlage des TPM zeigen [Gree07, Kaue07, KSP05], dass Schwachstellen für (zu dieser Zeit verfügbare) TPM-basierte Plattformen existieren, die unter günstigen Umständen zur Kompromittierung der Plattform ausgenutzt werden können. Eine prototypische Realisierung muss daher den aktuellen Stand der Verwundbarkeit Hardware-basierter Sicherheit berücksichtigen, wenn eine Aussage zur Mechanismenstärke bzw. zum erzielten Sicherheitslevel getroffen wird.

Abgesehen von der potentiellen Verwundbarkeit der Hardware-Plattform sind konzeptionelle Fehler bei der Rechtebeschreibung bzw. dem Parsing der maschinenlesbaren Rechte zu berücksichtigen. Eine Realisierung für produktive Anwendungen sollte daher einer Evaluation gemäß etablierter Sicherheitskriterien (z. B. *Common Criteria*) unterzogen werden, um eine unabhängige Prüfung der Rechtebeschreibung und der technischen Durchsetzung zu gewährleisten.

4 Fazit und Ausblick

Das Konzept des „irreversiblen Verschlusses“ erweitert das Prinzip der „Datensparsamkeit und Datenvermeidung“ durch Einführung eines technischen Werkzeuges. Unter Nutzung vertrauenswürdiger Hardware und technologischer Ansätze der *Digitalen Rechteverwaltung* kann eine Technologie realisiert werden, die Daten speichert und für einen definierten Zweck verarbeitet, eine Weitergabe jedoch wirksam verhindert.

Die Technologie kann für die beschriebenen Anwendungsfälle unmittelbar als Prototyp umgesetzt bzw. gemeinsam mit einem Anwender in einem Pilotprojekt realisiert werden. In weiteren Entwicklungsstufen, die über eine Skizzierung hinausgehen, werden die Realisierung von Pilotprojekten und die damit verbundene Gewinnung von Praxiserfahrungen angestrebt. Projektpartner, die sich an einer Entwicklung und Einführung der Technologie beteiligen möchten, sind willkommen, und werden gebeten, sich mit dem Autor bzw. dem Labor für IT-Sicherheit der Fachhochschule Münster in Verbindung zu setzen.

Literatur und Quellen

[Afp08] Meldung der Agentur AFP vom 04.10.2008

[Netz07] Bericht der Netzeitung vom 17.12.2007, URL: http://www.netzeitung.de/ausland/848950.html.

[Bech05] Stefan Bechtold: Trusted Computing: *Rechtliche Probleme einer entstehenden Technologie*. Oktober 2005. Preprints of the Max Planck Institute for Research on Collective Goods.

[BöPf08] Rainer Böhme, Andreas Pfitzmann: *Digital Rights Management zum Schutz personenbezogener Daten?* DuD (Datenschutz und Datensicherheit), Heft 5/2008.

[Davi07] Zitiert nach heise online: Monika Ermert: *Persönliches DRM als Retter von Datenschutz und Privatsphäre*. Meldung 99163 vom 18.11.2007. URL: http://www.heise.de/newsticker/meldung/99163 (Stand: Okt. 2008)

[Eric03] John S. Erickson: *Fair use, DRM, and trusted computing*. Communications of the ACM, Volume 46, Issue 4 (April 2003).

[Gras06] Volker Grassmuck: *Wissenskontrolle durch DRM: von Überfluß zu Mangel*. Sammelband „Eigentum und Wissen". Jeanette Hofmann (Hrsg.), Bundeszentrale für Politische Bildung, Berlin 2006.

[Gree07] Greene, T.: *Integrity of hardware-based computer security is challenged*. Network-World (2007). URL: http://www.networkworld.com/news/2007/062707-black-hat.html. Stand: 11.03.2009

[GSS03] Dirk Günnewig, Ahmad-Reza Sadeghi, Christian Stüble: *Trusted Computing Platform Alliance* (Technical Report, 10/2003).

[Kaue07] Kauer, B.: OSLO: Improving the security of Trusted Computing. 16th USENIX Security Symposium (2007).

[KSP05] Kursawe, K., Schellekens, D., Preneel, B.: *Analyzing trusted platform communication*. (2005), URL: www.cosic.esat.kuleuven.be/publications/article-591.pdf

[Pfit03] Roy Pfitzner: *TCPA, Palladium und DRM. Technische Analyse und Aspekte des Datenschutzes*. Technischer Report 2003.

[ReCa05] Reid, Jason F. and Caelli, William J.: *DRM, trusted computing and operating system architecture*. Conferences in Research and Practice in Information Technology Series; Vol. 108 Newcastle, New South Wales, Australia 2005

[Scha06] Jan Schallaböck, Ralf Bendrath, Udo Neitzel: *Privacy, Identity, and Anonymity in Web 2.0*. Präsentation vom: 27.12.2006. 23C3 Video Recordings URL: http://chaosradio.ccc.de/23c3_m4v_1611.html (Stand: Okt. 2008)

[Spie08] Bericht von *Spiegel-Online* vom 26.05.2008, URL: http://www.spiegel.de/wirtschaft/0,1518,555491,00.html.

[Unis08] Bericht in der Zeitschrift *Unispiegel* vom 02.10.2008.