

Logo der TU Darmstadt,  
s. [www.isprat.net](http://www.isprat.net)  
(Prof. Buchmann)

## **INNOVATIVE PERSONALAUSWEIS-ANWENDUNGEN**

**Mehrwert des elektronischen Personalausweises jenseits von Portal- und Formularanwendungen:  
Technische Machbarkeit und langfristige Sicherheit**

*Schlussbericht*

### **1 INSTITUT UND MENTOR**

Prof. Dr. Johannes Buchmann

Technische Universität Darmstadt

Fachbereich Informatik

Kryptographie und Computeralgebra

Hochschulstraße 10

64289 Darmstadt

### **2 PROBLEMSTELLUNG UND ZIEL DES PROJEKTS**

Ziel des Projekts war es, eine neuartige Anwendung des elektronischen Personalausweises zu spezifizieren und zu implementieren, den „Lifetime eSafe“. Dieses elektronische Schließfach erlaubt es dem Nutzer, persönliche Dokumente langfristig sicher und vertraulich abzuliegen. Die sichere Authentisierung des Nutzers am eSafe wird durch den elektronischen Personalausweis ermöglicht. Die technischen und rechtlichen Aspekte langfristiger Sicherheit standen im Mittelpunkt des Projekts. Darüber hinaus sollte das Projekt einen Beitrag zur Akzeptanzsteigerung des elektronischen Personalausweises leisten, der im November 2010 bundesweit eingeführt wird.

Das Projekt hatte eine Laufzeit von 24 Monaten von Juli 2008 bis Juni 2010. Im Folgenden gehen auf die wichtigsten Ergebnisse ein, die während dieser Zeit erzielt wurden. Zuvor erläutern wir den Lösungsansatz, der im Hinblick auf die Problemstellung verfolgt wurde.

### 3 LÖSUNGSANSATZ

Die zentrale Fragestellung des Projekts bestand darin, wie die langfristige Vertraulichkeit der im eSafe gespeicherten Daten gewährleistet werden kann. Unser Ansatz bestand darin, für den Betrieb des eSafe ein verteiltes Dienstleisterkonsortium vorzusehen. Selbst wenn mehrere Mitglieder des Konsortiums miteinander kooperieren, um die Vertraulichkeit der gespeicherten Daten zu kompromittieren, bleiben die Daten geheim, solange ein konfigurierbarer Anteil der Konsortialpartner nicht kollaboriert. Dies wird garantiert durch den Einsatz eines Speicherkonzepts, welches auf Shamirs Secret Sharing<sup>1</sup> zurückgeht und bereits von Doi et al. beschrieben wurde.<sup>2</sup> Die grundlegende Idee besteht darin, dass eine Datei auf eine bestimmte Anzahl von Blöcken aufgeteilt wird. Jeder dieser Blöcke wird dann als eigenständiges Geheimnis betrachtet und in Form von *Shares* auf die  $n$  Konsortialpartner verteilt. Nach dem Muster des Secret Sharing mit den Parametern  $(n; k)$  werden dann zur Bereitstellung einer Datei  $k$  verschiedene Shares der  $n$  Konsortialpartner benötigt. Weniger als  $k$  Konsortialpartner sind dagegen nicht in der Lage, eine Datei zu rekonstruieren. Gleichzeitig hat man hierdurch ein skalierbares Maß an Redundanz: Der Verlust oder die Kompromittierung von bis zu  $n-k$  Shares ist unkritisch (siehe dazu auch Abschnitt 5.1).

### 4 VERÖFFENTLICHUNGEN UND PRÄSENTATIONEN

#### 4.1 Wissenschaftliche Publikationen

Ausgangspunkt des Projekts war eine Untersuchung der Anwendungsszenarien des elektronischen Personalausweises. Dazu wurden zunächst Anwendungsszenarien der TUDCard betrachtet. Dies ist seit 2005 die Studierenden- und Mitarbeiterkarte der TU Darmstadt. Sie ist hinsichtlich ihrer Funktionalität mit einem campusweiten Personalausweis vergleichbar. Vorhandene Applikationen der TUDCard wurden hinsichtlich ihrer indirekten Übertragbarkeit auf den elektronischen Personalausweis analysiert. Die Ergebnisse dieser Analyse wur-

---

<sup>1</sup> Adi Shamir. How to share a secret. Commun. ACM, 22(11):612-613, 1979.

<sup>2</sup> Toshiyuki Miyamoto, Shinji Doi, Hiroki Nogawa, and Sadatoshi Kumagai. Autonomous distributed secret sharing storage system. Systems and Computers in Japan, 37(6):55-63, 2008.

den in Form eines Konferenzbeitrags auf der *9th European Conference on e-Government* veröffentlicht und Ende Juni 2009 an der University of Westminster in London präsentiert. Der Beitrag erschien im Tagungsband der Konferenz.

Referenz:

Lucie Langer, Axel Schmidt, Alex Wiesmaier.

From Student Smartcard Applications to the German Electronic Identity Card.

In: *Proceedings of the 9th European Conference on e-Government – ECEG*, London, UK, S.430–435. ACI, 2009.

Weiterhin haben wir einen Technischen Bericht verfasst, der die theoretischen Grundlagen sowie die Komponenten und die Funktionsweise des Lifetime eSafe erklärt.

Referenz:

Lucie Langer, Alex Wiesmaier.

Langfristige Sicherheit am Beispiel eines virtuellen Tresors.

Technical Report No. TI-01/09, Technische Universität Darmstadt, Juni 2009.

<http://www.cdc.informatik.tu-darmstadt.de/reports/TR/TI-09-01.pdf>

Gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie der Firma Secunet haben wir vorgeschlagen, wie der Lifetime eSafe in die Referenzarchitektur für vertrauenswürdige elektronische Langzeitarchivierung integriert werden kann, die das BSI als Technische Richtlinie TR-03125 herausgegeben hat.<sup>3</sup> Die Ergebnisse wurden in Form eines Konferenzbeitrags auf der *International Conference on New Technologies, Mobility and Security (NTMS)* veröffentlicht und Ende Dezember 2009 auf der Konferenz in Kairo präsentiert.

Referenz:

Detlef Hühnlein, Ulrike Korte, Lucie Langer, Alex Wiesmaier.

A Comprehensive Reference Architecture for Trustworthy Long-Term Archiving of Sensitive Data

---

<sup>3</sup> Siehe

[https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index\\_hm.html](https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_hm.html)

In: *Proceedings of the 3rd International Conference on New Technologies, Mobility and Security – NTMS*, Cairo, Egypt, UK, S.1–5. IEEE, 2009.

<http://dx.doi.org/10.1109/NTMS.2009.5384830>

Bei der 8. Europäischen Konferenz über digitale Archivierung (ECA 2010) wurde ein Abstract über den Inhalt und Erkenntnisgewinn des Projekts veröffentlicht. Der Beitrag erschien im Tagungsband der Konferenz.

Referenz:

Lucie Langer, Alex Wiesmaier.

Der Lifetime eSafe – ein sicheres elektronisches Schließfach

In: *Abstract Book of the 8th European Conference on Digital Archiving (ECA 2010)*,

S.155.

<http://www.bar.admin.ch/eca2010/00732/>

#### 4.2 Präsentationen bei IT-Gipfel, CeBIT und Wissenschaftstag

Beim Dritten Nationalen IT-Gipfel im Darmstadt waren wir mit zwei Projekten zum elektronischen Personalausweis vertreten. Ein erster Entwurf der Benutzeroberfläche des Lifetime eSafe wurde in Form eines Mock-ups präsentiert.

Auf Wunsch von ISPRAT wurde der Demonstrator Lifetime eSafe statt wie vorgesehen im Jahr 2010 bereits auf der CeBIT 2009 präsentiert. Das Exponat war beim Messegemeinschaftsstand des TechnologieTransferNetzwerks (TTN) Hessen ausgestellt. Kollegen vom Lorenz-von-Stein-Institut waren ebenfalls am Stand, um die rechtlichen Aspekte des Projekts vorzustellen. Der Messeauftritt war erfolgreich und stieß sowohl bei Vertretern aus Wirtschaft, Politik und Wissenschaft als auch bei der breiten Öffentlichkeit auf Interesse. Bundesjustizministerin Brigitte Zypries hat den Stand ebenso besucht wie Staatssekretär Dr. Beus. Das Projekt wurde zusätzlich im Rahmen zweier Präsentationen auf der Bühne des benachbarten E-Government-Standes vorgestellt. Weiterhin wurde das Projekt sowohl in der CeBIT-Broschüre des TTN Hessen, als auch in der vom Bundesministerium des Innern herausgegebenen Broschüre „Der elektronische Personalausweis“ präsentiert. Dadurch wurden die Informationen über das Projekt einem großen Kreis Interessierter zugänglich gemacht, auch über die CeBIT hinaus.

Auf dem Ersten ISPRAT Wissenschaftstag am 25.06.2009 in Darmstadt wurde das Projekt in Form eines Vortrags mit dem Titel „*Lifetime eSafe: Langfristige vertrauliche Datenspeicherung mit dem elektronischen Personalausweis*“ vorgestellt. Außerdem wurde der Demonstrator gezeigt, und die Kollegen aus Kiel haben im Rahmen der Poster-Session die rechtlichen Aspekte präsentiert.

## 5 SPEZIFIKATION UND IMPLEMENTIERUNG

Teile des Lifetime eSafe wurden zunächst in Form eines Demonstrators realisiert, der einen realitätsnahen Eindruck des implementierten Systems ermöglicht. Gezeigt wird die Authentisierung des Nutzers mit Hilfe des elektronischen Personalausweises (Registrierung des Nutzers und Anmeldung bei wiederholter Nutzung) sowie die Verwaltung persönlicher Dokumente im eSafe. Diese können im eSafe umbenannt oder gelöscht werden sowie auf die lokale Plattform heruntergeladen werden.

Die Anforderungen an den Prototyp Lifetime eSafe wurden im Rahmen einer Spezifikation festgelegt. Die Spezifikation beinhaltet folgende Teile:

- Produkteinsatz (Anwendungsbereiche und Zielgruppen)
- Beschreibung der Nutzersicht
- Definition der Systemarchitektur
- Speicherkonzept
- Abläufe bei Kommunikation zwischen Clients und Servern

Auf der Basis dieser Spezifikation wurde der Prototyp Lifetime eSafe implementiert. Details sind in der Entwicklerdokumentation beschrieben. Außerdem wurde eine Benutzerdokumentation erstellt, die Informationen zur Seitenstruktur und Datenbank eSafe sowie Hinweise für dessen Benutzung enthält.

### 5.1 Skalierbarkeit

Die Dateien der eSafe-Nutzer werden als Shares auf den Stageservern der Konsortialpartner gespeichert (siehe Abschnitt 3). Dabei kann eine Datei nur durch das Zusammensetzen einer gegebenen Anzahl von Shares rekonstruiert und damit gelesen werden. Es kann also insbesondere kein Stageserver eigenständig die Dateien der Nutzer lesen, sondern es muss sich hierzu immer eine bestimmte Anzahl von Stageservern und damit Konsortialpartnern zusammenschließen. Diesen Schwellwert kann der Nutzer selbst festlegen und damit entscheiden, wie viele Shares generell benötigt werden, um eine Datei zu rekonstruieren. Dabei wird ihm seitens der Betreiber ein Standardwert vorgegeben. Hat der Nutzer andere Ansich-

ten über diesen Wert, kann er ihn verändern, um so z.B. die Performance seines eSafe zu erhöhen. Wenige Shares haben den Vorteil, dass weniger Daten übertragen werden müssen und die Datei so schneller bereitgestellt werden kann. Viele Shares sorgen dagegen für mehr Sicherheit, da mehr Konsortialpartner kollaborieren müssten, um die Vertraulichkeit zu brechen.

Das System bietet damit gleichzeitig ein skalierbares Maß an Redundanz: Auch bei Ausfall von bis zu  $n-k$  Stageservern kann der Nutzer seine Dateien rekonstruieren. Sogar der Verlust von bis zu  $n-k$  Geheimnisteilen eines Dateiblocks ist unkritisch für die erfolgreiche Wiederherstellung des Blocks und damit der Datei.

## 5.2 Benutzerfreundlichkeit

Der Lifetime eSafe erlaubt es dem Nutzer, beliebige persönliche Dokumente langfristig sicher und vertraulich in elektronischer Form abzulegen (siehe Abschnitt 5.3). Dem Nutzer wird es durch den eSafe ermöglicht, seine gespeicherten Dateien von beliebigen Rechnern aus einzusehen und zu bearbeiten, was dem Nutzer ein hohes Maß an Mobilität bietet.

Der elektronische Personalausweis ermöglicht die sichere Authentisierung des Nutzers am eSafe durch den Nachweis von Besitz (Personalausweis) und Wissen (zum Personalausweis gehörige geheime PIN). Dies ist eine bewährte Kombination, die dem Nutzer aus vielen anderen alltäglichen Anwendungen bekannt ist (z.B. Geldabheben mittels EC-Karte). Bei erstmaliger Nutzung des eSafe muss sich der Nutzer mittels seines elektronischen Personalausweises registrieren; bei jeder weiteren Nutzung ist eine Anmeldung durch den Nutzer mittels seines elektronischen Personalausweises erforderlich. Nach erfolgreicher Registrierung bzw. Anmeldung wird der Nutzer automatisch auf die Startseite seines eSafe weitergeleitet.

Die im eSafe abgelegten Dateien werden in einer Ordnerstruktur gespeichert, wobei der Nutzer selbst entscheiden kann, wie diese Struktur aussehen soll. Eine transparente, intuitive Benutzerführung erlaubt es dem Nutzer, sich schnell in seinem eSafe zurechtzufinden. Das Hochladen bzw. Herunterladen von Daten erfolgt durch Anklicken entsprechender Buttons; das Generieren bzw. Abrufen der Shares geschieht dabei im Hintergrund, so dass der Nutzer davon nichts merkt. Eine Fortschrittsanzeige gibt dabei an, wie lange das Zerlegen bzw. Zusammensetzen der Datei noch dauert.

## 5.3 Langfristige Sicherheit

Die Vertraulichkeit der gespeicherten Daten wird vor allem dadurch gewährleistet, dass der eSafe von einem verteilten Dienstleisterkonsortium betrieben wird (siehe auch Abschnitt 3). Selbst wenn mehrere Betreiber des Konsortiums miteinander kooperieren, um die Vertraulichkeit der Daten aufzuheben, bleiben die Daten geheim, solange eine bestimmte Mindestanzahl an Betreibern aus dem Konsortium nicht kollaboriert.

Durch das beschriebene Speicherkonzept wird erreicht, dass die Vertraulichkeit der gespeicherten Daten nicht von der Sicherheit eines Kryptosystems abhängt. Diese Sicherheit ist in der Regel zeitlich beschränkt und abhängig von der Wahl der verwendeten Schlüssellängen. Das beschriebene System ist damit in besonderem Maße für eine langfristige Speicherung elektronischer Daten geeignet. Insbesondere muss kein Schlüssel und damit keine zusätzliche, extrem sicherheitskritische Information gespeichert werden.

Um die langfristige Sicherheit des Systems zu gewährleisten, sind beim Betrieb des eSafe einige Maßnahmen zu beachten. Die Software und Betriebssysteme, die auf den Storage-Servern läuft, sollte möglichst heterogen sein, damit eine als kritisch eingestufte Sicherheitslücke in einer Software nicht dazu führt, dass alle Server bzw. alle Shares kompromittiert werden können. Die Konsortialpartner sollten außerdem zu regelmäßigen Backups der gespeicherten Shares verpflichtet werden.

Langfristige Sicherheit beinhaltet auch eine langfristige Lesbarkeit der gespeicherten Dokumente. Hierfür spielt die Wahl geeigneter Datenformate eine zentrale Rolle; diese sollten standardisiert und langlebig sein. Als für die Langzeitaufbewahrung geeignete Formate gelten unter anderem PDF/A sowie XML. Die Wahl geeigneter Datenformate liegt in der Verantwortung des eSafe-Nutzers.

Die Sicherheit des Übertragungsweges der Shares stand nicht im Fokus des Projekts und ist dementsprechend im bestehenden Prototyp nicht implementiert. Sie kann aber wie folgt gesteigert werden: Der Nutzer kann festlegen, dass für jede Verbindung zu einem der Storage-Server ein anderer Verschlüsselungsalgorithmus verwendet wird. Dadurch wird die Sicherheit des Systems erhöht: Tritt der Fall ein, dass die Kommunikation abgehört wurde und eines der verwendeten Verschlüsselungsverfahren gebrochen ist, so sind nicht alle übermittelten Shares auf einmal offen gelegt. Folgende Konfigurationen sind denkbar:

- fixed: Bei jeder Sitzung wird derselbe, vorher festgelegte Algorithmus verwendet.
- random: Bei jeder Sitzung wird zufällig und gleichverteilt ein Algorithmus aus einer festgelegten Menge möglicher Algorithmen gewählt.
- distinct: Bei jeder Sitzung wird garantiert ein anderer Algorithmus verwendet. So kann beispielsweise auch beim Hochladen der Shares auf die Storage-Server für die Verbindung zu jedem einzelnen Storage-Server ein unterschiedlicher Algorithmus zum Verschlüsseln eingesetzt werden.

Der Nutzer des eSafe kann das System dann entsprechend konfigurieren und damit an sein persönliches Sicherheitsbedürfnis anpassen.

## 6 NACHWUCHSWISSENSCHAFTLER

### Dipl.-Math. Lucie Langer



#### Studium

- 09/2000 - 05/2004 Mathematik mit Schwerpunkt Technik und Naturwissenschaften  
an der Fachhochschule Darmstadt (FHD)
- 10/2004 - 07/2006 Mathematik mit Schwerpunkt Informatik  
an der Technischen Universität Darmstadt (TUD)
- 02/2006 - 06/2006 Auslandssemester an der Mathematisch-Physikalischen Fakultät  
der Karlsuniversität Prag, Tschechien, im Rahmen der Diplomarbeit

#### Praxiserfahrung

- 08/2002 - 04/2003 Praktikantin am Fraunhofer Institut für Graphische Datenverarbeitung  
(IGD), Abteilung Sicherheitstechnologie für Graphik und Kommunikati-  
onssysteme (Spezifikation und Implementierung kryptographischer Al-  
gorithmen)
- seit 08/2006 Wissenschaftliche Angestellte in der Arbeitsgruppe von Prof. Dr. Jo-  
hannes Buchmann im Fachgebiet Kryptographie und Computeralgebra  
an der TUD (Mitwirkung an verschiedenen Industrie- und Forschungs-  
projekten, Forschung auf dem Gebiet elektronischer Wahlen)

### Dr.-Ing. Alex Wiesmaier



### Studium

- 10/1996 - 01/2001 Student der Informatik an der Technischen Universität Darmstadt. Schwerpunkte Kryptologie, Kommunikationsnetze, Software-Engineering und Rechnertechnologie.
- 02/2001 - 10/2008 Doktorand an der Technischen Universität Darmstadt, Fachbereich Informatik, Fachgebiet Kryptographie und Computeralgebra. Schwerpunkte IT-Sicherheit und Software-Engineering.

### Praxiserfahrung

- 10/1996 – 04/2000 Softwareentwickler bei GMD – Forschungszentrum Informationstechnik GmbH in Darmstadt, Institut für integrierte Publikations- und Informationssysteme. Software- und Systementwicklung. Schwerpunkte Roomware, Datenbanksysteme und Workflow-Kontrolle.
- 02/2001 – 01/2006 Freier Mitarbeiter bei FlexSecure GmbH in Darmstadt. Entwicklung, Systemanalyse und Beratung. Schwerpunkte IT-Sicherheit und Software-Engineering.
- 02/2001 – 01/2006 Wissenschaftlicher Mitarbeiter an der Technischen Universität Darmstadt, Fachbereich Informatik, Fachgebiet Kryptographie und Computeralgebra. Forschung, Entwicklung, Systemanalyse, Lehre und universitäre Selbstverwaltung. Schwerpunkte IT-Sicherheit und Software-Engineering.
- 10/2006 – 10/2008 Analyst bei Safelayer Secure Communications, S.A. in Barcelona, Spanien. Systemanalyse und -entwicklung, Projektmanagement. Schwerpunkt Sicherheitsinfrastrukturen.

Seit 11/2008

PostDoc an der Technischen Universität Darmstadt, Fachbereich Informatik, Fachgebiet Kryptographie und Computeralgebra. Projektakquise und -management, Lehre und universitäre Selbstverwaltung. Schwerpunkt IT-Sicherheit.