Titel: Der Lifetime eSafe – ein sicheres elektronisches Schließfach

Lucie LANGER, Alex WIESMAIER
Technische Universität Darmstadt
Fachgebiet Theoretische Informatik
Hochschulstraße 10, 64289 Darmstadt, Deutschland

Thema:
Im November 2010 wird in Deutschland der elektronische Personalausweis mit elektronischem Identitätsnachweis eingeführt. Dadurch werden zahlreiche neue Anwendungen ermöglicht, beispielsweise der sichere Zugang zu einem virtuellen Schließfach, welches die langfristige Aufbewahrung persönlicher Dokumente in elektronischer Form erlaubt. Die Entwicklung eines rechtlichen Rahmens sowie der technischen Umsetzung dieses „Lifetime eSafe“ ist Gegenstand eines interdisziplinären deutschen Forschungsprojekts an der Technischen Universität Darmstadt und dem Lorenz-von-Stein-Institut für Verwaltungswissenschaften in Kiel.

Inhalt:

Ziel des vorgestellten Projekts ist die Entwicklung und Umsetzung eines rechtlichen Rahmens und einer technischen Realisierung zur langfristig sicheren Aufbewahrung und mobilen Bereitstellung von Daten durch ein elektronisches Schließfach. Der „Lifetime eSafe“ erlaubt es dem Benutzer Dokumente langfristig sicher und vertraulich abzulegen, und ermöglicht gleichzeitig den mobilen Zugang zu diesen. Die sichere Authentisierung des Benutzers erfolgt durch dessen elektronischen Personalausweis. Des Weiteren soll der Benutzer des eSafe auch anderen Personen feingranulare Zugriffsrechte auf Daten gewähren können.

Die Vertraulichkeit der im eSafe abgelegten Daten wird durch den Einsatz eines Speicherkonzepts gewährleistet, welches auf Shamirs „Secret Sharing“ und eine Idee von Miyamoto et al. zurückgeht. Jedes Archivobjekt wird in Form von „Shares“ auf ein Konsortium von n Archivierungsdienstleistern verteilt. Um das Archivobjekt zu rekonstruieren, müssen k dieser n Konsortialpartner zusammenarbeiten. Die Vertraulichkeit der Daten bleibt somit gewahrt, sofern wenigstens $n-k+1$ Konsortialpartner integer sind. Dies erzeugt zugleich positive Redundanz: Der Verlust oder die Kompromittierung von bis zu $n-k$ Shares eines Archivobjekts ist unkritisch. Der Nutzer des eSafe kann die Werte k und n konfigurieren und den eSafe damit an sein persönliches Sicherheitsbedürfnis anpassen. Durch ein geeignetes Indexierungskonzept wird es einem Angreifer selbst bei Kenntnis aller Shares praktisch unmöglich gemacht Daten zu rekonstruieren.

Erkenntnisgewinn:

Das auf Miyamoto et al. zurückgehende Speicherkonzept ist in besonderem Maße für eine langfristige Speicherung elektronischer Daten geeignet, da die Vertraulichkeit der Archivobjekte nicht von der (zeitlich beschränkten) Sicherheit einer Verschlüsselung abhängt. Das vorgestellte Forschungsprojekt erweitert das ursprüngliche Speicherkonzept und ergänzt es durch einen rechtlichen Rahmen und überträgt es in Form des Lifetime eSafe in die Praxis, wobei der elektronische Personalausweis zur sicheren Authentifizierung des Benutzers eingesetzt wird. Darüber wird ein Konzept entwickelt, um den eSafe als Langzeitspeicher in die vom Bundesamt für Sicherheit in der Informationstechnik entwickelte „Technische Richtlinie zur vertrauenswürdigen Langzeitarchivierung“ zu integrieren.

Schlüsselwörter: E-Archivierung, Online-Archivierung, Langfristige Aufbewahrung, verteilte Speicherung, elektronische Identität

Lebenslauf:

Lucie LANGER

Studium der Mathematik mit Schwerpunkt Informatik (IT-Sicherheit und Kryptographie) an der Technischen Universität Darmstadt und der Karlsuniversität Prag, seit August 2006 wissenschaftliche Mitarbeiterin am Lehrstuhl von Prof. Johannes Buchmann am Fachgebiet Theoretische Informatik der Technischen Universität Darmstadt. Forschung auf dem Gebiet der langfristigen Sicherheit elektronischer Wahlen und der Archivierung elektronischer (Wahl-)Dokumente, Mitwirkung an Projekten zur elektronischen Identität (elektronischer Personalausweis) und zur Langzeitaufbewahrung elektronischer Daten.

Alex WIESMAIER

Studium der Informatik und Elektrotechnik (IT-Sicherheit, Software-Engineering, Kommunikationsnetze, Datenbanken) mit anschließender Promotion (IT-Security, Software-Engineering) an der Technischen Universität Darmstadt. Seit November 2008 PostDoc am Lehrstuhl von Prof. Johannes Buchmann am Fachgebiet Theoretische Informatik der Technischen Universität Darmstadt. Forschung und Projekte unter anderem auf den Gebieten Public Key Infrastrukturen, elektronische Identitäten, langfristige Sicherheit, Informationssysteme und elektronische Wahlen.