Titel: Der Lifetime eSafe – ein sicheres elektronisches Schließfach

Lucie LANGER, Alex WIESMAIER
Technische Universität Darmstadt
Fachgebiet Theoretische Informatik – Kryptographie und Computeralgebra
Hochschulstraße 10, 64289 Darmstadt, Deutschland

Thema:
Ende 2010 wird in Deutschland der neue Personalausweis mit elektronischem Identitätsnachweis eingeführt. Dieser ermöglicht viele neue Anwendungen, z.B. den sicheren Zugang zu einem elektronischen Schließfach zur langfristigen Aufbewahrung und mobilen Bereitstellung persönlicher Dokumente. Dieser „Lifetime eSafe“ ist Inhalt eines interdisziplinären Forschungsprojekts an der Technischen Universität Darmstadt und dem Lorenz-von-Stein-Institut für Verwaltungswissenschaften in Kiel.

Inhalt:

Ziel des Projekts ist es, den Lifetime eSafe technisch umzusetzen sowie einen rechtlichen Rahmen für dessen Einsatz zu schaffen. Der „Lifetime eSafe“ erlaubt es dem Nutzer, Dokumente langfristig sicher und vertraulich abzulegen und flexibel auf sie zuzugreifen. Die sichere Authentisierung des Nutzers erfolgt durch dessen elektronischen Personalausweis. Des Weiteren kann der Nutzer des eSafe auch anderen Personen feingranulare Zugriffsrechte auf seine Daten gewähren.

Die Vertraulichkeit der im eSafe abgelegten Daten wird durch den Einsatz eines Speicherkonzepts gewährleistet, welches auf eine Idee von Miyamoto et al. [1] 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 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 ist es einem Angreifer selbst bei Kenntnis aller Shares praktisch unmöglich, Archivobjekte zu rekonstruieren.

Erkenntnisgewinn:

Das Speicherkonzept ist in besonderem Maße für eine langfristige Aufbewahrung elektronischer Daten geeignet, da deren Vertraulichkeit nicht von der zeitlich beschränkten Sicherheit einer herkömmlichen Verschlüsselung abhängt. Das vorgestellte Forschungsprojekt ergänzt das ursprüngliche Speicherkonzept durch einen rechtlichen Rahmen und überträgt es in Form des Lifetime eSafe in die Praxis, wobei der neue Personalausweis zur sicheren Authentisierung des Nutzers eingesetzt wird. Der eSafe wurde außerdem als Langzeitspeicher in die vom Bundesamt für Sicherheit in der Informationstechnik entwickelte „Technische Richtlinie zur vertrauenswürdigen Langzeitarchivierung“ integriert [2].

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

Literatur:

[1] T. Miyamoto, S. Doi, H. Nogawa, S. Kumagai: Autonomous distributed secret sharing storage system. Systems and Computers in Japan, 37(6):55–63, 2008.

[2] D. Hühnlein, U. Korte, L. Langer, A. Wiesmaier: A Comprehensive Reference Architecture for Trustworthy Long-Term Archiving of Sensitive Data. Proceedings of NTMS 2009, IEEE, to appear.