



Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center – Austria

A-1040 Wien, Weyringergasse 35
Tel.: (+43 1) 503 19 63-0
Fax: (+43 1) 503 19 63-66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

<http://www.a-sit.at>
E-Mail: office@a-sit.at

EXECUTIVE SUMMARY PROJEKT „FILEVERSCHLÜSSELUNG“

Herbert Leitold – Herbert.Leitold@a-sit.at

Die Verschlüsselung einzelner Dateien etwa zur Übermittlung basiert meist auf an PCs gehaltenen Schlüsseln, was die erreichbare Sicherheit abgrenzt. A-SIT hat ein Tool *Citizen Card Encrypted* (CCE) entwickelt, das Dateiverschlüsselung über die Bürgerkarte umsetzt. Hier wird die Motivation des Tools umrissen und eine Erweiterung, die von A-SIT zum Einsatz in sensiblen Bereichen der öffentlichen Verwaltung angeboten wird, beschreiben.

Die Verteilung vertraulicher Daten oder deren sicheres Halten im PC des Benutzers bedarf der Verschlüsselung. Lösungen wie verschlüsselte Email über S/MIME¹ beschränken sich auf die Anwendung und Daten werden auch nur im Mailsystem verschlüsselt gehalten. Für die Verteilung sehr großer Dateien oder auch für die Verwaltung von Daten mit unterschiedlichen Zugriffsrechten im Dateisystem des Benutzers oder in Netzlaufwerken einer Organisation eignet sich dies etwa nicht. Eine Lösung zur Verschlüsselung einzelner Dateien ist sinnvoll, um diese etwa im Intranet oder auf Webservern verschlüsselt ablegen zu können. Ansätze wie Pretty Good Privacy (PGP) oder weitere kommerzielle Lösungen halten die Schlüssel typisch im Dateisystem des PC, was Angriffsmöglichkeiten eröffnet.

Mit der Infrastruktur Bürgerkarte bietet sich an, Dateiverschlüsselung an die Sicherheit der verwendeten Hardwaremodule (Smartcards) zu binden. A-SIT hat dazu ein Werkzeug *Datensafe Bürgerkarte – Citizen Card Encrypted* (CCE) entwickelt. Dieses erlaubt über ein graphisches Benutzerinterface oder auch über Explorer Menüs², eigene Dateien unter dem aus der Bürgerkarte ausgelesenen Zertifikat zu verschlüsseln, oder Zertifikate anderer Personen zu importieren und Dateien für diese zu verschlüsseln.

Das Werkzeug bietet sich an, vertrauliche Dokumente der öffentlichen Verwaltung – etwa Ratsdokumente – für Berechtigte verschlüsselt zu verteilen oder zugänglich abzulegen³. Dazu wird das Tool um Funktionen erweitert, die für den praktischen Einsatz bei potentiell größeren Benutzerkreisen sinnvoll sind. Dies umfasst die Abfrage von Zertifikaten von Verzeichnisdiensten⁴ als Ergänzung zum Import von Zertifikaten, sowie das freie Gruppieren von Empfängern, um etwa die Verschlüsselung von Dateien an Arbeitskreise in einem Arbeitsschritt durchführen zu können.

Das Tool stellt Funktionen zum sicheren Löschen von Dateien bereit. Diese werden verwendet, um beim (wahlweise) automatischen Löschen der Quelldatei nach dem Verschlüsselungsvorgang sonst am physikalischen Medium unverschlüsselt verbleibende Reste zu vermeiden.

Das Projekt ist eine Ergänzung zu „*secureEFS*“, bei dem ganze Bereiche eines Benutzers an deren/dessen PC verschlüsselt werden, um eine Komponente, die gezielt Dateien für bestimmte Empfängerkreise mit der Bürgerkarte sichert.

¹ Secure Multi-Purpose Internet Mail Extension

² Menüführung über „rechte Maustaste“

³ Etwa auf Webservern

⁴ Über Light Weight Directory Access Protocol (LDAP)