Gian Poltéra

Diplomand	Gian Poltéra
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich, ZH
Themengebiet	Software and Systems
Projektpartner	PrivaSphere AG, Zürich, ZH

XClavis

Eine End-zu-End Verschlüsselung für Behörden mit sicherem Schlüsselaustausch

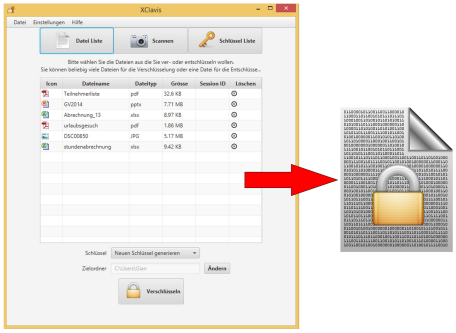

Abbildung 1: Dateiauswahl und AES-GCM Verschlüsselung.

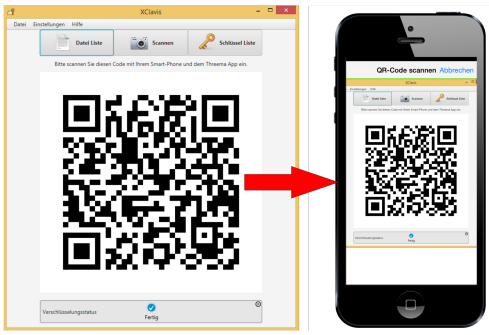

Abbildung 2: QR-Code Generierung und Scan mit dem Threema Smart-Phone App.

Abbildung 3: Scannen des QR-Codes mittels Webcam oder Tastatureingabe.

Ausgangslage: Momentan verwenden die Gerichte in der Schweiz mehrheitlich Transportverschlüsselung für ihren digitalen Datenaustausch. Eine End-zu-End Verschlüsselung auf Basis einer PKI-Infrastruktur ist erlaubt, aber oft unmöglich, da die meisten Gerichte und Behörden keine Verschlüsselungszertifikate besitzen bzw. publiziert haben und deren Einsatz freiwillig ist, sowie die Handhabung für Laien umständlich ist. Threema ist eine Anwendung zur mobilen Kommunikation. Sie beschränkt sich auf den Versand kleiner Datenmengen und ihr Hauptaugenmerk liegt auf einer sicheren End-zu-End-Verschlüsselung und maximalem Schutz der Kommunikationsranddaten. Im Gegensatz zu vielen anderen Konkurrenzprodukten ist Threema so konzipiert, dass nur Sender und Empfänger im Besitz des geheimen Schlüssels sind, welcher die Sicherheit der übermittelten Daten gewährleistet.

Aufgabenstellung: Die in der Ausgangslage beschriebenen Probleme und Einschränkungen sollen mit dieser Arbeit in einer neuen Lösung vereinfacht werden. Dabei soll der bestehende, sichere Kanal über Threema für den Schlüsselaustausch verwendet werden und die Daten symmetrisch-verschlüsselt über einen separaten Server gesendet werden. Die Kernziele sind eine sichere End-zu-End-Verschlüsselung sowie der Versand von grossen Datenmengen (nicht über Threema, sondern über konfigurierbare Drittserver). In einer ersten Phase wird ein Konzept für die Umsetzung erstellt und anschliessend ein Prototyp entwickelt. Die komplette Arbeit soll jeweils, unter Rücksprache mit dem Auftraggeber, an dessen Bedürfnisse angepasst und weiterentwickelt werden. In einer erweiterten Version soll auch noch Perfect Forward Secrecy ermöglicht werden.

Ergebnis: Es wurde ein Konzept mit sieben verschiedenen Umsetzungsvarianten erstellt. Diese wurden zusammen mit dem Industriepartner analysiert und die geeignetste ausgewählt und auf deren Basis ein Prototyp entwickelt. Die Hauptmerkmale dieser Anwendung sind: </text><item>Verschlüsselung beliebig vieler Dateien in eine verschlüsselte Datei mittels AES-GCM. (Abbildung 1)</item><item>Übermittlung des Schlüssels mittels der Smart-Phone App Threema und eines QR-Codes. (Abbildung 2)</item><item>Einlesen von erhaltenen Schlüsseln mittels Webcam oder manuell per Tastatur. (Abbildung 3)</item><item>Austausch von mehreren Schlüsseln in einem QR-Code auf Vorrat.</item><item>Erweiterte Sicherheit mittels ECDH-Schlüsselaustausch, um den Schlüssel nicht in Klartext übermitteln zu müssen.</item><text>