Prof. Dr. rer. nat. Prof. h.c. Ulrich Bühler

Steinsdorfer Straße 7, D-36039 Fulda
Fon: +49-661-9527773
Fax: +49-661-9640 -349
E-Mail: u.buehler@hs-fulda.de
url: www.hs-fulda.de/ndsec

Prof. Dr. Bühler, Steinsdorfer Straße 7, 36039 Fulda

Comcrypto
Technische Universität Chemnitz
Fakultät Informatik
09107 Chemnitz

Fulda, den 15. August 2015

Sicherheitsarchitektur „comcrypto“

Im Rahmen des Gründungsprojekts „comcrypto“ haben sich die Gründer an mich gewandt mit der Bitte, das Konzept für die Erstellung einer Software-Lösung für eine hochsichere Unternehmenskommunikation zu begutachten, ggf. Schwachstellen zu finden und Verbesserungen vorzuschlagen. Diesem Anliegen bin ich gern nachgekommen.

Das Review der Sicherheitsarchitektur mit Stand 05/2015 habe ich nach bestem Wissen auf Grundlage der mir zur Verfügung gestellten Unterlagen und der in mehreren Gesprächsmeetings ausgetauschten tiefgehenden Informationen durchgeführt.

Das zugrundeliegende Konzept ist in sich stimmig und stellt eine echte Alternative zu bisherigen Ansätzen dar. Sowohl die Art und Weise der Verschlüsselung als auch der Authentifizierung heben sich vom Stand der üblichen Techniken (PGP, S/MIME) deutlich ab. So werden kaskadierte symmetrische Verschlüsselungsverfahren (AES und Twofish im Betriebsmodus CTR) ebenso wie auf starken elliptischen Kurven basierende asymmetrische Verfahren (u.a. Edwards Curve Digital Signature Algorithms, EdDSA) zur sicheren Authentifizierung verwendet. Innovationen hierbei sind u.a. Perfect-Forward-Secrecy auf Nachrichtenebene, die zertifikatsfreie Transportverschlüsselung und das sehr einschlägige Schlüsselmanagement. Die Schlüssel werden auf dem jeweiligen Endgerät und nicht zentral erstellt, so dass auch keine privaten Schlüssel transportiert werden müssen. Die verwendeten Schlüssellängen entsprechen dem aktuellen Stand und die Schlüssel werden hinreichend oft erneuert, so dass Angreifer mit ggf. kompromittierten Schlüsseln keine weiteren Informationen erlangen können. Jeder User erzeugt mehrere öffentliche (Verschlüsselungs-) Schlüssel und die zugehörigen Signaturen, die auf dem Server für zukünftige Kommunikation hinterlegt werden. Jedes asymmetrische Schlüsselpaar wird genau einmal zur Verschlüsselung bzw. Entschlüsselung mittels ECIES verwendet.

Die Anwender benötigen weder zur Erstanmeldung noch zur gesicherten Kommunikation Kenntnisse der Kryptografie. Alles Notwendige wird für den User weitestgehend transparent abgewickelt, was der Nutzerfreundlichkeit sehr zu Gute kommt.

Das erarbeite Konzept für die Software-Lösung zur gesicherten Kommunikation über Unternehmensgrenzen hinweg ist sehr innovativ und praktisch effizient anwendbar.

Mit freundlichen Grüßen