

# Verschlüsselung

*Bedarf, Technik, Standards*

*Dr. Häcker, Polifke ZKD Baden-Württemberg*

## 1. Sicherheitsbedarf

Bei der Erfüllung ihrer Aufgaben hat die öffentlichen Verwaltung regelmäßig auch mit personenbezogenen Daten der Bürger zu tun. Die Datenschutzvorschriften verlangen, dass diese Daten u.a. gegen Manipulation und unbefugte Kenntnisnahme geschützt werden.

## 2. Verschlüsselung als universell einsetzbare Sicherheitstechnik

Die Datenverarbeitung ist heute ohne den Einsatz von IuK-Technik mit untereinander vernetzten elektronischen Datenverarbeitungsgeräten nicht mehr bewältigbar. Die einzig bekannte praktikable und inzwischen auch einfach finanzierbare Methode, um Informationen in elektronischen Netzen zu schützen ist die kryptographische Verschlüsselungstechnik. Daher fordern die Datenschützer schon seit längerem, möglichst überall nur noch verschlüsselte Informationen zu übertragen. Diese pauschale Forderung lässt sich wegen der Vielfalt der Verschlüsselungstechnik und ihren organisatorischen Konsequenzen jedoch nur stufenweise umsetzen. Damit Verschlüsselung in der Praxis funktioniert und die wesentlichen angestrebten Ziele erreicht werden, bedarf es sowohl organisatorischer Regelungen als auch technischer Maßnahmen. Das ZKD erarbeitet deshalb mit der Datenzentrale Baden-Württemberg für den staatlich-kommunalen Mail-Verbund eine Sicherheitsstudie, über die zu gegebener Zeit (etwa nächster Erfahrungsaustausch des KoopA ADV) berichtet wird.

## 3. Leitungs- und Ende-zu-Ende-Verschlüsselung

Neben der Verschlüsselung auf Verbindungsebene im Netz, die dann hilft, wenn relativ sichere lokale Netze über weniger sichere Weitverkehrsnetze miteinander verbunden werden sollen - dies wird z.B. bei TESTA-Deutschland diskutiert - rückt auch die Ende-zu-Ende-Verschlüsselung immer mehr in den Mittelpunkt des Interesses. Es ist offensichtlich, dass sich die Vertraulichkeit von Nachrichten durch Verschlüsselungstechnik schützen lässt. Vertraulichkeit ist jedoch nicht das einzige schützenswerte Gut einer Nachricht. Die Aspekte Integrität und Authentizität sind oft mindestens genau so wichtig. Auch diese lassen sich über eine sogenannte Elektronische Signatur mit Hilfe von Verschlüsselungstechnik sichern.

Der **Kommunikationsbedarf** in der Verwaltung erstreckt sich heute von der Europäischen Union über Bund und Länder bis in den kommunalen Bereich. Dabei ist die jeweils eingesetzte Technik sehr unterschiedlich. Es ist schon unter normalen Umständen nicht ganz einfach, zwischen den vielen unterschiedlichen EDV-Systemen eine reibungsarme Kommunikation zu bewerkstelligen. Damit eine Kommunikation mit verschlüsselten Kanälen funktioniert, müssen unbedingt Standards eingehalten werden.

Die **Interoperabilität** verschiedener auf dem Markt angebotener Verschlüsselungssysteme wird vom Bund im Rahmen des Projekts SPHINX getestet. Dabei wird der MailTrust-Standard eingesetzt. Auch der KoopA ADV hat sich für die generelle Anwendung dieses Standards in der öffentlichen Verwaltung ausgesprochen. Das Land Baden-Württemberg hat einen Rahmenvertrag mit **CoCoNet** abgeschlossen und verwendet das MailTrust-konforme MULTISEC Trust-Center 500 sowie MULTISEC Mail Plug-In für MS-Exchange und MS Outlook.

Außerdem wird mit der Client-Software von **Utimaco Crypt and Sign** getestet. Darüber hinaus werden **SSL-Zertifikate** eingesetzt, um differenzierte Zugriffe auf Web-Informationen im ressortübergreifenden Intranet des Landesverwaltungsnetzes zu ermöglichen. Außerdem ist bereits absehbar, dass spezielle Anwendungen (Kassenverfahren, elektronisches Grundbuch) über entsprechend hochwertige Zertifikate geschützt werden müssen.

Zertifikate können grundsätzlich für unterschiedliche Sicherheitsanforderungen eingesetzt werden. Von SW-Zertifikaten für dezentral generierte Schlüssel, über Chipkartenbasierte, bis zu Signaturgesetz-konformen Lösungen.

Wichtig für den praktischen Einsatz, z.B. für die Verschlüsselung von elektronischer Post ist, dass die öffentlichen Schlüssel der Partner jederzeit zur Verfügung stehen. Dies geschieht am einfachsten dadurch, dass auch die Zertifikate über ein elektronisches Adressbuch bereitgestellt werden.

Signaturgesetzkonforme Zertifikate sind zur Sicherung der Kommunikation zwischen Behörden nicht gefordert. Falls jedoch wie angekündigt allgemeine Rechtsvorschriften wie z.B. das BGB so geändert werden, dass für Vorgänge, die heute handschriftliche Urkunden erfordern auch elektronische Dokumente mit SigG-konformer Signatur formal zulässig sind, dann muss die Verwaltung in ihre Kommunikation mit Externen auch in der Lage sein, mit diesen Signaturen entsprechend umzugehen.

Da es sehr aufwändig ist, SigG-konforme Zertifikate zu erstellen, gehen wir davon aus, dass der Betrieb eines eigenen nach dem SigG zertifizierten Trust Centers für das Land Baden-Württemberg nicht wirtschaftlich ist. Zur Abdeckung des künftig entstehenden Bedarfs läuft derzeit eine Ausschreibung mit Verhandlungsverfahren. Dabei wird auch geprüft, in welchem Umfang sich andere Zertifikate wirtschaftlich beschaffen lassen.

## 4. Erfahrungen aus dem Eigenbetrieb von Trust Centern des ZKD

Wer Trust Center ausschreibt, muss auch eigene Erfahrungen mit ihnen erworben haben. In Baden-Württemberg hat die Stabsstelle im Innenministerium ein Pilot-Trust Center für SSL-Zertifikate aufgebaut und, als sein produktiver Einsatz anstand, dieses dem ZKD übergeben. Dort sind inzwischen umfangreiche Erfahrungen entstanden. Beispiele sind:

- Möglicherweise ist es zweckmäßig, für die Verschlüsselung von Nachrichten und für die elektronische Signatur unterschiedliche Schlüsselpaare zu verwenden.
- Die Signatur ist per definitionem ein sehr persönlicher Prozess, während bei der Verschlüsselung grundsätzlich auch Gruppen- bzw. Dienststellenschlüssel umsetzbar wären.
- Beim Einsatz der Ende-zu-Ende Verschlüsselung greifen verschiedene zentrale Konzepte nicht mehr. Beispielsweise besitzen verschlüsselte Daten keine offensichtliche Redundanz mehr. Eine heute übliche Komprimierung während der Übertragung (Leitungskomprimierung) ist dann nicht mehr möglich. Komprimierung muss daher, wenn sie überhaupt erfolgen soll, zeitlich vor der Verschlüsselung vorgenommen werden.
- Auch zentrale Virens Scanner können die Nachrichten nicht mehr analysieren. Denkbar wären zwar Konzepte, bei denen Nachrichten verschlüsselt mit dem öffentlichen Schlüssel einer Dienststelle an den zentralen Posteingang dieser Dienststelle geschickt werden. Diese könnte dann ein zentraler Virens Scanner mit Hilfe des geheimen Schlüssels der Dienststelle entschlüsseln und überprüfen. Danach wäre eine Weiterleitung an den Empfänger, verschlüsselt mit dessen öffentlichem Schlüssel möglich. Derartige Lösungen entsprechen aber nicht dem, was man sich gemeinhin unter Ende-zu-Ende-Verschlüsselung vorstellt. Es sind auch keine Produkte auf dem Markt bekannt, mit denen sich dies ohne zusätzlichen Programmieraufwand bewerkstelligen ließe.
- Andererseits ist durch den generellen Einsatz von Ende-zu-Ende-Verschlüsselung sichergestellt, dass nicht wie in einigen Makroviren üblich, unkontrolliert Mails verschickt werden können. Wird nämlich jede Mail grundsätzlich digital signiert, muss vor einer automatisch generierten Mail-Flut für jede Mail ein Passwort eingegeben werden.

## 5. Situation in Baden-Württemberg

Die Situation in Baden-Württemberg lässt sich wie folgt zusammenfassen:

- Eine mehrjährige Erfahrung mit der X.25-Verschlüsselung zwischen Netzmanagement-Servern (KryptoGuard X.25) liegt vor.

- Die Forderung nach verstärktem Einsatz von Verschlüsselungstechnik und digitaler Signatur kann jetzt von technischer Seite aus erfüllt werden. Die Organisationsreferenten wurden frühzeitig in den Entscheidungsprozess eingebunden. Der Arbeitskreis der Organisationsreferenten plant, allgemeine Nutzungsregelungen auszuarbeiten. Vor dem Hintergrund des verstärkten "Outsourcings" des Betriebs von lokalen Netzen und des Landesverwaltungsnetzes und der zunehmenden Kommunikationsbeziehungen mit Partnern im Internet ist breite Erfahrung beim Einsatz der Verschlüsselungstechnik unverzichtbar, denn die dort immer wieder notwendige lückenlose Abschottung gelingt nur über Verschlüsselungstechniken.
- Es wurde ein Trustcenter eingerichtet (MULTISEC Trust-Center 500 von CoCo-Net)
- Die Verschlüsselung und Signatur von E-Mails werden in Pilotprojekten, auch im staatlich-kommunalen Verbund, erprobt.
- Zur Einstellung der Zertifikate für die Kommunikation über MULTISEC Mail Plug-In und Utimaco Crypt and Sign erarbeiten Innenministerium und ZKD ein zentrales elektronisches Benutzerverzeichnis.
- Für die Kommunikation mit EU, Bund, Ländern und Kommunen gehen wir davon aus, dass MailTrust als Standard genutzt wird.
- Kabinettsvorlagen im Landes-Intranet sind in einem Web-Server gespeichert und werden mit SSL-Verschlüsselung (Microsoft NT 4.0 Option Pack, Microsoft Certificate Server 1.0, MS Internet Explorer ab 4.01, Netscape Communicator ab 4.04) gesichert.
- Für spezielle Anwendungen (z.B. elektronisches Grundbuch) gibt es hohen Sicherheitsbedarf, der den Einsatz von hochwertigen, sicheren Zertifikaten erfordert.
- Für spezielle Anwendungen (Überwachung von Servern) wird Remote Access Security (RAS) angeboten.
- Die SigG-Konformität wird voraussichtlich im Rahmen eines Erprobungsgesetzes zu den elektronischen Bürgerdiensten (e-Bürgerdiensten) Baden-Württemberg genutzt. Das ZKD bereitet sich mit Hilfe des Innenministeriums in der bereits erwähnten Ausschreibung darauf vor, als RA oder CA landesweit alle notwendigen Dienste anzubieten. Der Aufbau des notwendigen Know-hows und die Ausarbeitung der Details sind langwierig und auf Anbieter- und Nutzerseite sind noch viele Diskussionen zu führen. Derzeit können diese Abstimmungen noch in der notwendigen Ruhe erfolgen, später dürfte erheblicher Zeitdruck auftreten.
- Ebenfalls mit Interesse verfolgt wird die multifunktionale Chipkarte. Sparkassen, Kommunen und Land möchten e-Bürgerdienste anbieten, die nach der Identifikation mit einer elektronischen Chipkarte genutzt werden können. Damit der Aufwand für den Bürger überschaubar bleibt, sollen mehrere Funktionen wie ec-Karte, Geldkarte, Zertifikate für Geldtransaktionen und Zertifikate für elektronische Behördengänge auf derselben Karte untergebracht werden. Ob und inwieweit dies in Kürze gelingt hängt davon ab, wieviele und welche Zertifikate sich auf einer physikalischen Karte kombinieren lassen. Das Innenministerium hat beim

FAW Ulm und bei der FhG Karlsruhe eine Studie in Auftrag gegeben, die Zweckmäßigkeit und ggf. den Weg zu einer „Baden-Württemberg Card“ untersucht.