

Fraktionsantrag „Verschlüsselung“ 168/2013 vom 21.10.2013 – hier: Stellungnahme des IT-Dienstleisters KommunalBIT

Die E-Government- und Formular-Anwendungen der Stadt Erlangen bieten bereits überwiegend fundierte Verschlüsselungstechnologien zur sicheren Datenübermittlung. Die Nutzung dieser Technologien entspricht weiterhin dem Stand der Technik und bringt für weniger technikaffine Nutzer keinerlei Hemmschwellen mit sich. Derartige (sichere) Dienstleistungsangebote müssen auch weiterhin im Kernfokus jeglicher e-Government-Aktivitäten stehen.

Mit der Nutzung der Bayerischen Verwaltungs-PKI stellt der Freistaat Bayern Mitarbeitern der staatlichen und kommunalen Verwaltungen in Bayern eine Technologie zur Verfügung, mit deren Hilfe die Vertraulichkeit, Integrität und Verbindlichkeit von Daten bzw. Nachrichten gewährleistet werden kann, allerdings mit der Einschränkung, dass die Kommunikationspartner Zugriff auf das BayBN benötigen. Für die Mail-Kommunikation unter öffentlichen Einrichtungen ist diese Voraussetzung erfüllt, und eine entsprechende Anwendungsmöglichkeit wurde von KommunalBIT den Städten zur Verfügung gestellt. Für die Mail-Kommunikation zwischen Bürger und Stadt stellt dies allerdings keine geeignete Option dar.

Für die Verschlüsselung einzelner Dateien auf Datenträgern oder als Mail-Anhänge können die städtischen Benutzer grundsätzlich bereits jetzt die Möglichkeiten nutzen, die mit den Standard-Werkzeugen zum Komprimieren von Dateien zur Verfügung stehen. Ein sicherer Datenaustausch nach außerhalb des Netzes (ggf. in Kombination mit der Verschlüsselungsmöglichkeit) wird auch durch die Nutzung des von KommunalBIT betriebenen Ajax-Downloaders gewährleistet.

Entsprechend können auch die Kommunikationspartner der Städte grundsätzlich wahlfrei verschiedenste Verschlüsselungsmethoden bei der Übersendung von Daten benutzen, soweit der städtische Empfänger dann die Daten ohne zusätzliche Komponenten im Netz entschlüsseln kann.

Vor Einführung einer weiteren Verschlüsselungsmöglichkeit ist zu beachten, dass diese mit vernünftigem Aufwand zentral administrierbar und in die von KommunalBIT bereitgestellten Lösungen integrierbar sein muss. Wesentlicher Faktor hier ist die Komplexität der Schlüsselverwaltung. Wenn keine zentrale Schlüsselverwaltung implementiert werden kann, droht im schlimmsten Fall bei Schlüsselverlust auch Datenverlust, weil dann nicht einmal der IT-Dienstleister die Verschlüsselung aufheben kann. Weiterhin müssen geeignete Stellvertreterregelungen und organisatorische Festlegungen auf der (städtischen) Absender- und Empfängerseite auch technisch umgesetzt werden können. Grundsätzlich lässt sich dabei der Umgang mit verschlüsselten Daten (z.B. bei E-Mails) innerhalb der Stadt weit effizienter gestalten, wenn eine Verschlüsselung bis zum E-Mail-Gateway – und somit bis zum IT-Dienstleister – stattfindet, als bei einer Entschlüsselung der Daten erst am Client und damit durch den User.

Ob dies für die vorgeschlagene freie Software Gpg4win gewährleistet werden kann, wissen wir nicht, dass lässt sich auch nicht kurzfristig feststellen, sondern bedarf einer genauen Analyse. Dabei wäre dann auch die Kostenseite zu betrachten, auch „freie Software“ ist nicht kostenlos zu betreiben.

Sowohl die Zugangseröffnung der Stadt Erlangen nach Art. 3a des BayVwVfG als auch interne Regelungen des Dienstverkehrs sind derzeit nach unserem Wissen weder für formgebundene noch für einfache formlose Schreiben auf eine verschlüsselte Kommunikation ausgelegt. Damit muss man sich unter Akzeptanzgesichtspunkten fragen, ob dem Bürger eine derartige Verschlüsselungslösung nur empfohlen oder vorgeschrieben werden soll. Es existiert weiterhin eine große Vielzahl anderweitiger Verschlüsselungstechnologien im Markt.

Besonders erwähnt werden soll hier das Produkt DE-Mail. Hierfür machen sich aktuell gleich drei große kommerzielle Konzerne stark. Die Lösung befindet sich auch aktuell im Betrachtungsfokus der drei Städte –insbes. auch der Stadt Schwabach. Unter Synergie- und damit

auch Kostengesichtspunkten müssen sich die Städte überlegen, ob hier ein gemeinsamer Weg beschritten werden soll, auch in Richtung Nutzung der eID beim neuen Personalausweis.

Aus Sicht des IT-Dienstleisters muss vor weiteren konkreten Aktivitäten in der Richtung zunächst eine klare Strategievorgabe zum gewünschten Dienstleistungsportfolio der elektronischen Kommunikation in der Zukunft erfolgen, die entsprechend mit den anderen KommunalBIT-Städten abgestimmt ist, damit Synergie- und Skaleneffekte angemessen berücksichtigt werden können.

KommunalBIT
05.11.2013

Freymüller
IT-Sicherheit

Kopie an Vorstand, Bereichsleitungen und KM KommunalBIT