Hürden **überwunden**

von Gunnar Wolf

Die baden-württembergische Landeshauptstadt Stuttgart hat bereits früh eine Public-Key-Infrastruktur (PKI) aufgebaut, die drei verwaltungsinterne Verfahren mit Zertifikaten versorgt. Die eigene PKI wird nun durch eine ASP-Lösung ersetzt.

Mit dem deutschen Signaturgesetz wurde 1997 eine Technik in das Blickfeld von Politik und öffentlichen wie privaten Dienstleistern gerückt, die im Grunde schon sehr ausgereift war, aber in unterschiedlicher Ausprägung und damit proprietär genutzt wurde. Und es wurde mit diesem Gesetz eine einzige Nutzungsmöglichkeit geregelt, die wichtig, aber nur eine von dreien ist: die elektronische Signatur. Ebenso bedeutsam aber sind die anderen beiden: die Authentifizierung von Personen, Maschinen und Erzeugnissen und die Verschlüsselung von Daten und Kommunikationsprozessen. Insbesondere die Datenschützer fordern seit Jahren die Nutzung dieser Fähigkeiten ein, für die es keine gesetzliche Grundlage gibt und für die auch keine benötigt wird.

Die Zertifikatsdiensteanbieter schmücken sich gerne mit dem Prädikat „qualifizierte Signatur“ – die höchste Signaturstufe, möglichst mit Anbieterakkreditierung, 30 Jahre nachprüfbar. Doch schon der Ansatz ist falsch. Unternehmen und Verwaltungen benötigen Zertifikate, über die sie selbst die Verfügungsgewalt haben, die schnell und unkompliziert erteilt und entzogen werden können – und das nicht nur für natürliche Personen, sondern ebenso für Maschinen, Gruppen und Funktionen. Möglichst alles aus einer Hand und mit einem Werkzeug zur Administration.

Das Signaturgesetz kennt – logischerweise – nur natürliche Personen, wie das BGB auch nur die Rechtsbeziehungen von Privatpersonen regelt. Im Geschäftsablauf eines Unternehmens oder einer Verwaltung kommen aber auf jede nach außen gerichtete rechtswirksame Handlung schätzungsweise 10 bis 20 Vorgänge, die im Vorfeld in einem internen Geschäftsprozess ablaufen. Diese internen Geschäftsprozesse sollten aber ebenso wie die nach außen gerichteten mit den Möglichkeiten der Zertifikatstechnik unterstützt werden. Aufgrund der größeren Fallzahlen ist auch das Rationalisierungspotenzial um etliches größer.

Es lässt sich also feststellen, dass der naheliegende Ruf nach der höchsten Signaturstufe in diesen Fällen in die falsche Richtung führt. Mit der Bindung der Zertifikate an eine natürliche Person ergeben sich einige Probleme, die zwar nicht unlösbar sind, aber doch einigen Aufwand mit sich bringen:

- Es muss arbeitsrechtlich geregelt werden, unter welchen Bedingungen die privaten Zertifikate der Mitarbeiter für den Arbeitgeber mitbenutzt werden können.

Stuttgart: PKI ist ein Leuchtturmprojekt.

- Es muss erfasst und dokumentiert werden, bei welcher Stelle der Arbeitnehmer mit seinem Zertifikat Accounts bedient, damit diese bei einem möglichen Stellenwechsel oder einem Ausscheiden entsprechend geändert werden können.
- Es muss ein Verfahren vereinbart werden, nach dem die Verwaltung oder das Unternehmen das Verschlüsselungszertifikat, mit dem der Mitarbeiter wichtige Daten vor unbefugtem Zugriff geschützt hat, samt PIN wiederherstellen kann, falls es verloren geht oder aus anderen Gründen nicht zur Verfügung steht.

Diese Aufzählung soll deutlich machen, welche Abhängigkeiten und Risiken eine Verwaltung eingeht, wenn sie private Zertifikate ihrer Mitarbeiter ohne weitere Vorkehrungen für ihre Geschäftsprozesse einsetzt. Was ist die Alternative? Ein eigenes Trustcenter zu bauen und zu betreiben kann nicht die Lösung sein. Der Königsweg liegt in der Nutzung der hochwertigen Infrastruktur und des Know-hows der führenden deutschen Trustcenter – aber unter den Bedingungen einer selbstdefinierten und auf den eigenen Bedarf ausgerichteten Zertifizierungsrichtlinie (Certification Practise Statement). Damit werden das Sicherheitsniveau und alle Regeln für die notwendigen Prozesse einer Zertifizierungsstelle (Certificate Authority) festgelegt.

Eine Festlegung betrifft beispielsweise die Identitätsprüfung. Ist persönliches Erscheinen erforderlich? Erfolgt der Abgleich mit dem Passbild eines gültigen Ausweises? Kann man auch eine Gruppe zertifizieren? Ist ein E-Mail-Zertifikat personenbezogen oder maschinenbezogen? Welche Zertifikate können bei Verlust oder Zerstörung wiederhergestellt werden? Eine Fülle von Definitionen mit komplexen Zusammenhängen und Folgewirkungen. Expertenwissen ist hier dringend erforderlich.

Auf der anderen Seite wäre es betriebswirtschaftlich vorteilhaft, wenn nicht jede Verwaltung ihre eigene Policy schaffen müsste. Eine oder wenige Zertifizierungsstellen würden genügen. Und tatsächlich, es gibt für den gesamten Bereich der öffentlichen Verwaltung bereits eine Infrastruktur, die diesen Ansatz verfolgt: Die Verwaltungs-PKI des Bundes ist auch die Wurzelzertifizierungsstelle (PCA) für die Länder und Kommunen. Verschiedene Zertifizierungsstellen (CA) sind bereits an sie angebunden, sodass es naheliegt, zunächst einmal zu prüfen, ob eine davon geeignet wäre um die eigenen Anforderungen zu erfüllen.

Die baden-württembergische Landeshauptstadt Stuttgart hat ihre Anforderungen an die Ausgestaltung dieser Technik bereits von 2002 bis 2004 in dem Pilotprojekt eVAS (elektronische Verschlüsselung Authentifizierung Signatur) ausführlich analysiert. In dieser Phase wurde eine eigene PKI aufgebaut, die Zertifikate auf Chip-Karte und in Dateiform (PKCS#12) ausstellen kann. Diese PKI wurde auch testweise durch die Verwaltungs-PKI zertifiziert. Sie war aber von Anfang an nicht als Dauerlösung konzipiert, sondern sollte durch eine per Ausschreibung ermittelte Nachfolgelösung ersetzt werden. Die Ausschreibung dazu erfolgte 2005, nachdem eine Überprüfung der Zertifizierungsrichtlinien der Verwaltungs-PKI ergab, dass die Anforderungen der Landeshauptstadt nur teilweise abgedeckt werden konnten. Auch die von der Verwaltungs-PKI zertifizierte TESTA-CA wurde in Betracht gezogen. Hier stieß man aber auf nicht ausreichend transparente Prozesse und Akteure und sah auch großen Reformbedarf.

Schließlich führte eine zweite beschränkte Ausschreibung 2006 zum Erfolg: Die eigene PKI der Landeshauptstadt wird nun durch eine ASP-Lösung ersetzt. Technologiepartner hierfür ist die Firma D-Trust in Berlin, eine Tochtergesellschaft der Bundesdruckerei-Gruppe. Sie stellt die notwendige Infrastruktur zur Verfügung. Für die Gestaltung der dabei vorgesehenen Prozesse wurde die Firma Tele-Consulting aus Gäufelden bei Stuttgart hinzugezogen.

Die primären Ziele der Landeshauptstadt Stuttgart sind zunächst die Ablösung der eigenen PKI, die bisher drei verwaltungsinterne Verfahren mit Zertifikaten versorgt, und die Unterstützung der virtuellen Poststelle des Kommunalen DV-Verbunds Baden-Württemberg. Daneben sind aber auch weitere Vorhaben geplant: Die Absicherung von Notebooks durch Pre-Boot-Authentication mit integrierter Anmeldung an der Windows Domain die verschlüsselte Dateiablage mit EFS, WLAN-Authentifizierung mit EAP und einiges mehr.

Der Aufwand für die Stuttgarter Lösung nicht zu unterschätzen. Deswegen hat die Landeshauptstadt versucht Gleichgesinnte zu finden, die ähnliche Anforderungen haben. Mit dem Kommunalen DV-Verbund Baden-Württemberg und der eigenen Tochtergesellschaft Stuttgarter Straßenbahnen AG sind zwei Partner im Boot, die einen Roll-out in ausreichender Stückzahl ermöglichen; denn der IT-Dienstleister der Landeshauptstadt – die Abteilung IuK des Haupt- und Personalamts – ist auch als Profit Center organisiert. Aus diesem Grund wurde die Einrichtung unter dem Branding bw-trust CA eingeführt. Die Verträge mit D-Trust sind inzwischen unter Dach und Fach. Das Grobkonzept ist fertiggestellt. Feinkonzept und Zertifizierungsrichtlinie sind in der Abnahmephase. Zur Jahresmitte soll die Ausgabe von Zertifikaten der bw-trust Basic-CA beginnen.

Gunnar Wolf ist in der Abteilung Informations- und Kommunikationstechnik des Haupt- und Personalamts der Landeshauptstadt Stuttgart tätig.