Zusammenfassung des Prüfungsbefundes

Die EFK hat im Bundesamt für Informatik und Telekommunikation (BIT) die Admin PKI - Basisinfrastruktur und -dienstleistung zur Ausstellung von Zertifikaten - einer Prüfung unterzogen. Der Schwerpunkt der Prüfung lag in der Beurteilung der Entwicklung und des heutigen Betriebes sowie der Zukunftsaussichten. Unter Admin PKI werden alle Prozesse sowie Hard- und Software verstanden, welche für die Ausgabe von Zertifikaten unterschiedlicher Güte benötigt werden.

Nach schwierigen und teilweise unglücklichen Versuchen und Anläufen (siehe Kapitel 4) hat das BIT die Infrastrukturen und Prozesse erarbeiten können, um in der Bundesverwaltung, den Kantonen und auch den Gemeinden Zertifikate für deren Anwendungen zur Verfügung zu stellen. Neben den in der Bundesverwaltung (BVerw) definierten Zertifikaten der Klassen A bis D kann das BIT auf die Bedürfnisse des Kunden bzw. dessen Anwendungen spezifizierte Zertifikate anbieten. Mit der im zweiten Quartal 2007 zu erwartenden Zertifizierung durch die KPMG für Zertifizierungsdienste der Klasse A (ZertES) wird die Admin PKI und damit das BIT seine Fähigkeiten und Qualitäten auf hohem Niveau bewiesen haben. Das praktische Meisterstück war die Ausgabe von rund 25'000 Zertifikaten an die Kantone im Jahre 2006. Zum Zeitpunkt der Revision waren bereits über 40'000 Zertifikate verschiedener Ausprägung im Einsatz.

Das BIT wird heute von allen Kantonen und der Schweizerischen Informatikkonferenz (SIK) als der primäre Anbieter für Zertifikate akzeptiert. Nebst dem SSO-Portal stehen weitere übergreifende Anwendungen wie das Informationssystem Arbeitsvermittlung und die Arbeitsmarktstatistik (AVAM), die elektronische Deklarationen der Zollverwaltung (e-dec), der Versand verschlüsselter, signierter Mails (secure-messaging) usw. vor oder in der Umsetzung. Die Preise für die Zertifikate sind nicht im Zentrum des Interesses, da sie sich in einem konkurrenzfähigen und akzeptablen Rahmen bewegen. Aufgrund der anfänglich schleppenden Entwicklung der heutigen Admin PKI ist es schwierig für die bisher getätigten Investitionen im Umfang von 12 Mio. eine faire Wirtschaftlichkeitsrechnung zu erstellen. Der Hauptnutzen einer PKI liegt grundsätzlich beim Kunden d.h. bei den Anwendungen, da ein hoher Sicherheitslevel mit einfachen Mitteln erreicht werden kann. Das Potential für die Ausstellung weiterer Zertifikate ist entsprechend gross. Der Verkauf von Zertifikaten sollte die laufenden Kosten des Betriebes und technisch bedingter Erneuerungen decken. Alternative Sicherheitsvarianten wären zwar teilweise günstiger, würden jedoch wegen der Heterogenität grosse E-Government-Lösungen erschweren. Die beim BIT verfügbare PKI-Technologie ermöglicht standardisierte Lösungen über alle Verwaltungsebenen hinweg, aber auch gesamtschweizerisch durch die Zusammenarbeit mit anderen nach ZertES zertifizierten Unternehmen wie z.B. der Post mit dem Produkt IncaMail. Die Kantone können Zertifikate auch bei anderen Anbietern beziehen, werden jedoch mit grosser Wahrscheinlichkeit die schon im Einsatz stehenden Zertifikate der Admin PKI mehrfach nutzen. Die auf dem Schweizer Markt vorhandenen, nach ZertES zertifizierten Anbieter (Quo Vadis,Swisscom und die Post) stellen für das BIT potentielle Partner dar, da mit der gegenseitigen Anerkennung der Zertifikate viele E-Government-Lösungen denkbar werden.

Es gibt verschiedene Studien über den Bedarf an PKI-Lösungen in der Schweiz. Eine schweizweite Gesamtsicht über die in der BVerw definierten Klassen A bis D ist jedoch nicht möglich, da andere Anbieter eigene Zertifikats-Klassen definiert haben. Durch die grosse Verbreitung von Zertifikaten in der öffentlichen Verwaltung wird deren Einsatz jedoch mit der Zeit zur Selbstverständlichkeit, was Impulse über die BVerw hinaus geben kann. Die Kosten werden konstant bleiben, sich aber auf wesentlich mehr Zertifikate als heute verteilen lassen. Die Zertifikate der Klasse A sind als einzige in der Schweiz durch ein Gesetz geregelt. Der potentielle Einsatz wird jedoch generell als gering eingeschätzt, da nur sehr wenige Rechtsgeschäfte die Schriftlichkeit mit eigenhändiger Unterschrift (z.B. Vorauszahlungsvertrag) verlangen, welche der qualifizierten elektronischen Signatur gleichkommt. Das Zertifikat als solches - durch die Zertifizierung auf Güte geprüft - bildet jedoch die Grundlage des allgemeinen Vertrauens in den Anbieter selber. Daher scheint es für die EFK absolut sinnvoll, dass das BIT diese Klasse anbieten kann.

Die Erwartungen an und das Vertrauen in das BIT für dessen Zertifikate sind heute sehr gross. Die Anforderungen an Zertifikate werden auch zukünftig nicht aus einer zentralen gemeinsamen Wissensbasis bestimmt, sondern nach Kundenwünschen definiert. Das BIT hat bewiesen, dass es die organisatorischen und technischen Anforderungen an einen Certification Service Provider (CSP) erfüllen kann. Die Zertifizierung nach ZertES betrifft nicht nur die Admin PKI, sondern hat übergreifende Auswirkungen auf das gesamte BIT (Prozesse, Dokumente, Infrastruktur usw.). Durch eine solide Dienstleistung, hohe Verfügbarkeit und ausgewiesene Qualität kann das bereits erarbeitete Vertrauen bei den Kunden weiter ausgebaut und vertieft werden. Darin liegt die Zukunftschance der Admin PKI sowohl aus Sicht des Marktes wie auch bezüglich der Finanzierung.

Die **Stellungnahme des BIT** zu den Empfehlungen der EFK in diesem Bericht sind nach den jeweiligen Empfehlungen aufgeführt. Die **Finanzdelegation** hat an ihrer fünften Sitzung im August 2007 vom Bericht der EFK Kenntnis genommen.