EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
CONTROLLA FEDERALA DA FINANZAS

Bundesamt für Informatik und Telekommunikation

Entspricht die Admin PKI dem ursprünglich definierten Ziel sowie den Bedürfnissen der Bundesverwaltung und der Kantone?

Original Text

11. Juni 2007

Inhaltsverzeichnis

Abkürzungsverzeichnis und Glossar

BIT	Bundesamt für Informatik und Telekommunikation
BVerw	Bundesverwaltung
CA	Certification Authority
CSP	Certification Service Provider
DFS	Digitaler Fahrtenschreiber (Projekt des ASTRA)
EFK	Eidgenössische Finanzkontrolle
e-dec	Elektronische Deklaration zur Abwicklung des Zollverkehrs
E-Gov	Electronic Government (elektronischer Behördenverkehr)
e-pass	Schweizer Pass mit elektronisch lesbaren Informationen wie Passbild, Fingerabdrücke, usw., Zertifikat dient zur Sicherung der Verfälschung
EJPD	Eidg. Justiz- und Polizeidepartement
IRB	Informatikrat des Bundes
ISB	Informatikstrategieorgan des Bundes
KLR	Kosten-/Leistungs-Rechnung
LRA	Local Registration Authority
NRM	Neues Rechnungs-Modell zur Kosten-/Leistungsverrechnung in der BVerw
PKI	Public Key Infrastructure
RA	Registration Authority
ROI	Return of Invest (Refinanzierung von investierten Finanzmitteln)
SCMS	Smart Card Management System
SIK	Schweizerische Informatikkonferenz
SSO-Portal	Single-Sign-On Portal zur zentralen Authentifizierung der externen Benutzer (hauptsächlich aus den Kantonen) auf Anwendungen des EJPD
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur

1 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.

2 Auftrag und Prüfungsdurchführung

2.1 Auftrag

Die EFK hat, gestützt auf die Artikel 6 und 8 des Bundesgesetzes über die Eidg. Finanzkontrolle (FKG; SR 614.0) im April 2007 die Admin PKI einer Prüfung unterzogen. Gemäss Prüfauftrag soll beurteilt werden, ob die Entwicklung und der Betrieb der Admin PKI der ursprünglichen Zielsetzung sowie den Bedürfnissen in der BVerw und den Kantonen entspricht.

Die Prüfungsschwerpunkte lagen entsprechend darin:
- die Geschichte seit 2001 mit den wichtigen Entscheidungen aufzuzeigen
- den heutigen Entwicklungsstand, die Implementierung und den aktuellen Betrieb zu beurteilen
- die bisherigen und zukünftigen Kosten unter dem Aspekt der Wirtschaftlichkeit zu beurteilen
- den Stand der Zertifizierung durch KPMG aufzunehmen
- die aktuellen und zukünftigen Bedürfnisse der Partner (Kantone) und Kunden, sowie die Kundenzufriedenheit zu werten

Als Basis für die Beurteilungen dienten die Projekt-Dokumente ab dem Jahre 2001 sowie die Finanzdaten bis zum Zeitpunkt der Revision.

2.2 Rechtsgrundlagen

- Bundesgesetz über die Eidgenössische Finanzkontrolle vom 28. Juni 1967 (Stand am 20. Juli 1999) (SR 614.0)
- Bundesgesetz über den eidgenössischen Finanzhaushalt vom 7. Oktober 2005 (Finanzhaushaltgesetz, FHG, SR 611.0)
- Finanzhaushaltsverordnung vom 5. April 2006 (FHV, SR 611.01)
- Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES, SR 943.03)
- Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (VZertES, SR 943.032)
- Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1 / Anhang)
- Verordnung des EFD über elektronisch übermittelte Daten und Informationen (EIDI-V, SR 641.201.1)
- Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung vom 26. September 2003 (Bundesinformatikverordnung, BinfV, SR 172.010.58)

2.3 Prüfungsumfang und -grundsätze

Die Prüfung führten die Informatikrevisoren Peter Bürki, Stefan Wagner und Cornelia Simmen (Revisionsleitung) durch. Zur Erfüllung des Prüfauftrages wurden die umfangreichen Dokumentationen gesichtet und Interviews mit den im BIT für die verschiedenen Teilprojekte verantwortlichen Personen gemacht, sowie bei verschiedenen involvierten Stellen (ISB, SIK, Kantone AG und ZH, GS EFD). Einzelheiten über Art und Umfang der durchgeführten Prüfungen gehen aus den Arbeitspapieren hervor.

2.4 Unterlagen und Auskunftserteilung

Alle angefragten Personen erteilten in sehr speditiver und offener Art und Weise die notwendigen Auskünfte. Die angeforderten, zum Teil sehr umfangreichen Dokumente, standen rasch und umfassend zur Verfügung des Revisionsteams.

2.5 Priorisierung der Empfehlungen der EFK

Aus der Sicht des Prüfauftrages beurteilt die EFK die Wesentlichkeit der Empfehlungen und Bemerkungen nach Priorität (1 = hoch, 2 = mittel, 3 = klein). Sowohl der Faktor **Risiko** [z. B. Höhe der finanziellen Auswirkung bzw. Bedeutung der Feststellung; Wahrscheinlichkeit eines Schadeneintrittes; Häufigkeit des Mangels (Einzelfall, mehrere Fälle, generell) und Wiederholungen; usw.], als auch der Faktor **Dringlichkeit der Umsetzung** (kurzfristig, mittelfristig, langfristig) werden berücksichtigt.

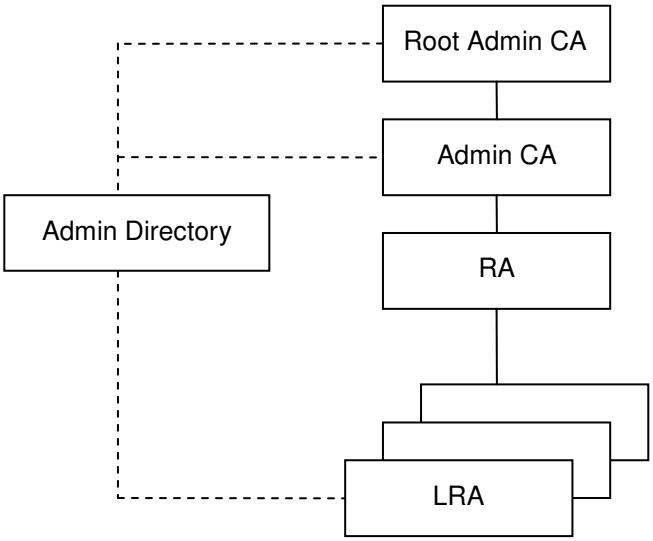
3 Einführung

Mit der Vernetzung von Informatikkomponenten geht eine stetig steigende elektronische Übermittlung von Daten einher. Für rechtlich verbindliche Handlungen benötigt man die Gewissheit, dass übermittelte Daten (z.B. das Mail, die Bestellung, die Bestätigung) auch tatsächlich vom vermuteten Absender stammen, der Inhalt während einer Übermittlung oder Speicherung nicht verändert wird und die Übermittlung nachvollzogen werden kann. Zur Erfüllung dieser zahlreichen Sicherheitsanforderungen braucht es vielfältige Regelungen, d.h.

- rechtliche Grundlagen (Gesetze, Verordnungen) regeln die Gleichstellung des elektronischen mit dem schriftlichen Verkehr;
- organisatorische Grundlagen stellen die Abläufe sicher, damit die Zustellung nachvollziehbar ist - vergleichbar mit einer eingeschriebenen Postsendung -, und schaffen die Vorraussetzungen zur berechtigten Ausübung aller Tätigkeiten in diesem Zusammenhang;
- technische Grundlagen stellen die Identifizierbarkeit und die Unveränderbarkeit sicher, sie sind normiert sowie national und international anerkannt.

Begriffe wie Public Key Infrastructure (PKI), Ausgabestelle für Zertifikate (CA), elektronische Zertifikate, Authentifizierung, Signatur und Verschlüsselung stehen in direktem Zusammenhang zu den rechtlichen, elektronischen und organisatorischen Grundlagen.

Unter **Public Key Infrastructure** (PKI) werden alle Prozesse, Architekturen, Server, Arbeitsstationen und Software verstanden, die zur Ausgabe von Zertifikaten benötigt werden. Eine PKI-Infrastruktur ist hierarchisch aufgebaut und besteht aus den folgenden Hauptkomponenten:



- **Die Root Admin Certification Authority** (CA) ist verantwortlich für die Validierung und Protokollierung der Zertifikatsvergabe, d.h. Kontrolle der Admin CA
- Die **Admin CA** des BIT ist für die Ausgabe, Verwaltung und Publikation von Zertifikaten zuständig
- Die **Registration Authority** (RA) des BIT verwaltet die Zertifikatsanträge
- Die dezentrale **Local Registration Authority** (LRA) ist zuständig für die Identifikation der Antragssteller von Zertifikaten, die Generierung der Schlüsselpaare und deren Übertragung auf die Smartcards
- In der **Admin-Directory** werden alle zugelassenen und gesperrten Zertifikate zwingend geführt und publiziert

Das Bedürfnis für den Einsatz von **Zertifikaten** richtet sich nach den Sicherheitsanforderungen von Anwendungen. Je nach Gebiet bestehen unterschiedliche Anforderungen an die Authentifizierung, die Signatur und die Verschlüsselung, einzeln oder in Kombination untereinander. Zertifikate können hardwarebasierend (z.B. Smartcard, Token) oder softwarebasierend (Softzertifikate) sein. Ähnlich dem Schweizer Pass, stellt ein Zertifikat einen moralischen Anspruch an die Glaubwürdigkeit des Ausstellers und einen technischen an die Sicherheit d.h. Unverfälschbarkeit.

In der Bundesverwaltung wurden vier Klassen von Zertifikaten definiert:

- **Klasse D**, mittlere Güte/Qualität, zur sicheren Authentifizierung von natürlichen Personen oder Maschinen, Softzertifikat, Einsatz z.B. für Zugriffe von fremden Netzen aus auf Applikationen im Bundesnetz
- **Klasse C**, mittlere Güte/Qualität, ermöglicht sichere Authentifizierung, Verschlüsselung und Signatur, Softzertifikat, Einsatz z.B. für die Verschlüsselung von Mailverkehr (secure-messaging) in der BVerw
- **Klasse B**, sehr hohe Güte/Qualität, ermöglicht starke Authentifizierung, Verschlüsselung und Signatur, personenbezogenes Zertifikat auf Smartcard, Vergabe nur gegen persönliche Identifikation mit gültigem Reisepass oder Identitätskarte

- **Klasse A**, sehr hohe, gesetzlich geregelte Qualitätsansprüche, qualifizierte elektronische Signatur, welche einer handschriftlichen, rechtsgültigen Unterschrift gleichkommt, siehe dazu Kapitel 5.6

Zur Abdeckung von spezifischen Anforderungen an die Authentifizierung, die Verschlüsselung und Signatur können vom BIT, basierend auf den vordefinierten Klassen, massgeschneiderte Spezialzertifikate zur Verfügung gestellt werden.

4 Geschichte der Admin PKI

Im Januar 1999 erteilte der Bundesrat, nach Kenntnisnahme des Berichtes „Aufbau und Zertifizierungsinfrastruktur für die Bundesverwaltung“, den Auftrag zum Aufbau einer Zertifizierungsinfrastruktur für die Bundesverwaltung. Er beauftragte das UVEK für die Koordination der Arbeit, das EFD für die Erarbeitung der technischen Grundlagen und das EJPD für die Vorbereitung der Rechtsverbindlichkeiten von digitalen Signaturen.

4.1 Koordination und technische Grundlagen

Zu den Koordinationsaufgaben des UVEK können keine Aussagen gemacht werden, da keine entsprechenden Unterlagen in den gesichteten Akten vorhanden sind und dies auch nicht Ziel der Prüfung war.

Aufgrund des damals geschätzten Projektumfanges von 3-5 Mio. wurde 1999 eine WTO-Ausschreibung für das Projekt „Secure Messaging“ (SHAB Nr. 123, 29.6.1999) vorgenommen. Als im Jahr 2000 der Startschuss für das Projekt fiel, hatte man sich für eine gesicherte E-Mail-Lösung in der gesamten Bundesverwaltung entschieden. Diese basierte auf Zertifikaten der damaligen Firma Swisskey, welche sich ein Jahr später - mitten im Projekt - vom Markt verabschieden sollte. Das BIT musste daher im Jahre 2001 entscheiden, für das damalige Projekt secure-messaging, entweder Zertifikaten ausländischer Anbieter zu vertrauen oder selber den Schritt Richtung Zertifikats-Hersteller zu wagen. Es wurde die interne Variante gewählt und Ende 2001 konnte das BIT eine funktionierende Admin PKI vorweisen, d.h. es wurden eigene Zertifikate erzeugt, veröffentlicht und verwaltet, ein dediziertes Lokal war eingerichtet und gesichert. Das Secure-Messaging-Projekt blieb jedoch in der Pilotphase stecken, weil sich die damals gewählte Lösung nicht durchsetzen konnte und dadurch zuwenig Zertifikate generiert wurden.

Ab dem Jahr 2002 waren weitere Stolpersteine vorhanden. Einerseits hat sich das Informatik-strategieorgan des Bundes (ISB) gegen den Aufbau einer bundeseigenen CA gestellt - keine Bedürfnisse in der BVerw oder den Kantonen, nicht Kernaufgabe des Bundes, Zertifikate können eingekauft werden-, obschon das BIT einen Auftrag des Bundesrates zur Ausgabe von Zertifikaten hatte. Andererseits war man beim BIT über längere Zeit hinweg darauf fixiert, dass eine einzige hardwarebasierende Lösung mit Zertifikaten für die Funktionen Authentifizierung, Verschlüsselung und Signatur für alle Sicherheitsbedürfnisse der einzig richtige Weg sei. Dadurch haben andere PKI-Projekte in den Jahren 2001 bis 2004 eher vor sich hergedümpelt. Diese Situation hat dazu beigetragen, dass im gleichen Zeitraum in den Kantonen eigene Wege zur Lösung der Aufgaben im Bereich der Zertifikate gesucht wurden.

2003 folgte die Ausschreibung und Realisierung der heutigen Klasse B Zertifikate. Die Beschaffung eines Smartcard Management Systems (SCMS) wurde abgebrochen, da die Menge der ausgegebenen Zertifikate zu gering war. Im August des gleichen Jahres gab der IRB sein grundsätzliches Einverständnis zu einer einzigen durch das BIT betriebenen Admin PKI. Im Oktober bzw. Dezember wurde weiter entschieden, dass die Dienstleistungen der damaligen Admin PKI für die Class 2 und 3 (heutige Klassen B und C) auch den Kantonen angeboten werden darf. Dagegen wurde zu diesem Zeitpunkt nie explizit geregelt, wer für die bereits aufgelaufenen aber auch zukünftigen Investitionen und den Betrieb aufkommen würde. In der Staatsrechnung können die Ausgaben der Admin PKI erst ab 2004 verfolgt werden. Rückblickend muss gesagt werden, dass nur dank der Hartnäckigkeit des BIT, die Admin PKI (mit damals ausgewiesenen Investitionen von bereits über 2 Mio.) nicht gestrandet ist.

Im Jahre 2004 führte das ISB in der BVerw und bei den Kantonen eine Umfrage bezüglich Zertifikatsbedarf durch. Die Resultate haben nachfolgend dazu geführt, dass der IRB mit Beschluss vom 24.05.04 dem BIT den „offiziellen" Auftrag gab, die Admin PKI für die Ausgabe von Zertifikaten der Klasse B, C und D als Querschnittsdienstleistung mit entsprechenden Q-Mitteln zu betreiben. Diese Entscheidung hat u.a. dazu geführt, dass die in der Zwischenzeit durch andere Stellen lancierten Lösungen (z.B. Kanton Zürich) mit denjenigen der Admin PKI verglichen werden konnten.

Unter dem Reorganisationsprojekt „Change BIT" im Jahre 2005 wurden die Verantwortlichkeiten im Bereich Admin PKI neu geregelt. Es wurde damals im BIT erkannt, welche Chancen sich mit Projekten wie e-pass, DFS und SSO-Portal eröffneten. Durch wesentlich bessere Kommunikation und dem Aufbau eines grösseren PKI-Teams wurde daraufhin die Admin PKI langsam aber stetig hochgefahren. Der IRB gab dem BIT zusätzlich grünes Licht, sich der Zertifizierung durch KPMG zu unterziehen, damit auch Zertifikate der Klasse A nach ZertES ausgegeben werden können. Dies ist jedoch mit der Auflage verbunden, dass solche Zertifikate nicht mit Querschnittsgeldern finanziert werden dürfen.

Den eigentlichen Schub erhielt die Admin PKI schlussendlich im Jahre 2006 mit dem Rollout von rund 25'000 Zertifikaten der Klasse B für das SSO-Portal des EJPD, was zu einer breiten Anerkennung der BIT-Lösungen in den Kantonen führte. Diese Erfahrung trug wesentlich zum heutigen Stand und Wissen im PKI-Team des BIT bei. Die praxisbezogene Bewährungsprobe wurde zwar teilweise mit Nebengeräuschen, aber gesamthaft gesehen erfolgreich bestanden. Mit dem Erfolg und aus den daraus gemachten Erfahrungen wurden auch die Projekte „Relaunch Secure Messaging (RSM)" und „Smart Card Management System (SCMS)" wieder reaktiviert.

Gemäss Entscheid des IRB wurde im 2006 die Zertifizierung durch die KPMG für Zertifikate der Klasse A durch das BIT eingereicht. Bei diesem Vorhaben stand von Beginn weg nie die Ausgabe der Zertifikate im Vordergrund, sondern das BIT wollte damit erreichen, dass es ein nach nationalen und internationalen Standards festgelegtes Gütesiegel erhält, welches als Vertrauensbasis für die gesamte Admin PKI - und damit auch für das BIT selber - dienen soll.

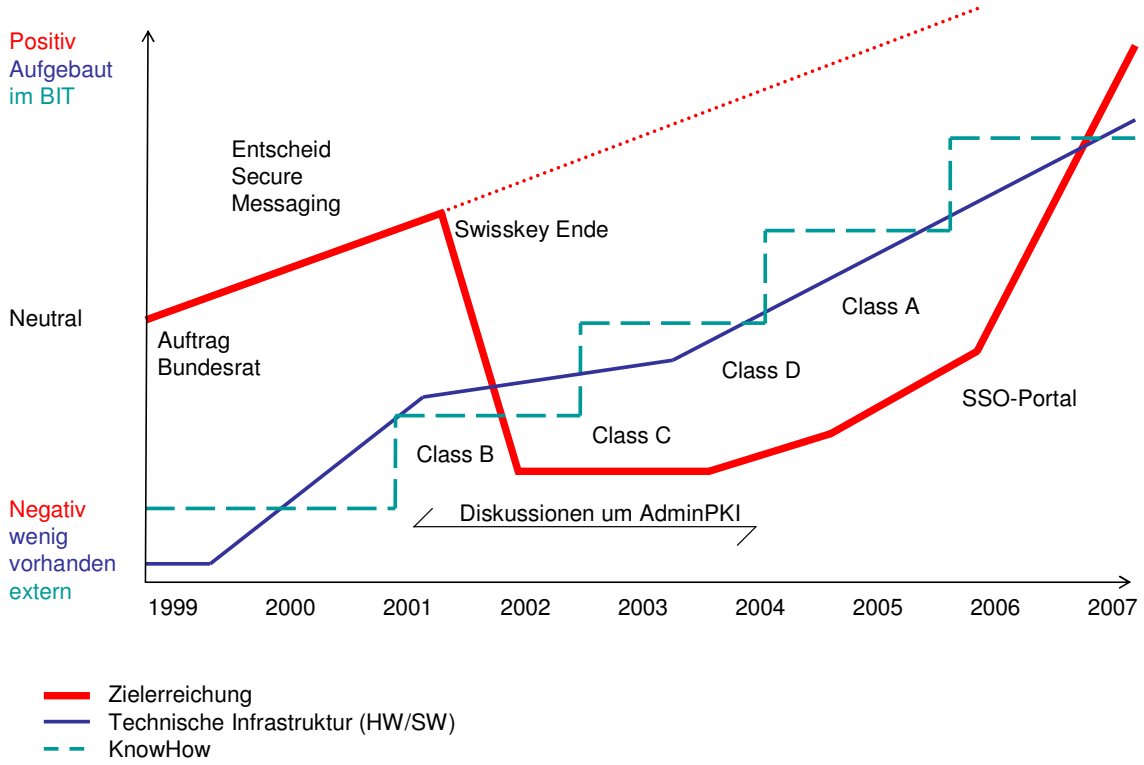
Die zukünftige Entwicklung des Zertifikatmarktes wird zeigen, ob sich die Admin PKI behaupten kann und inwiefern sie durch die Privatwirtschaft beeinflusst wird.

4.2 Rechtliche Grundlagen

Die erforderlichen Regelungen im rechtlichen Bereich wurden generell als erfüllt beurteilt. Es ist allgemein bekannt, dass heute digital signierte Schriften rechtlich den papierenen Schriften gleichgestellt sind, allerdings nur dann, wenn sie die gesetzlich vorgeschriebenen Bedingungen erfüllen. Gesetze und Verordnungen wurden entsprechend angepasst, in die Vernehmlassung geschickt und sind seit einigen Jahren in Kraft.

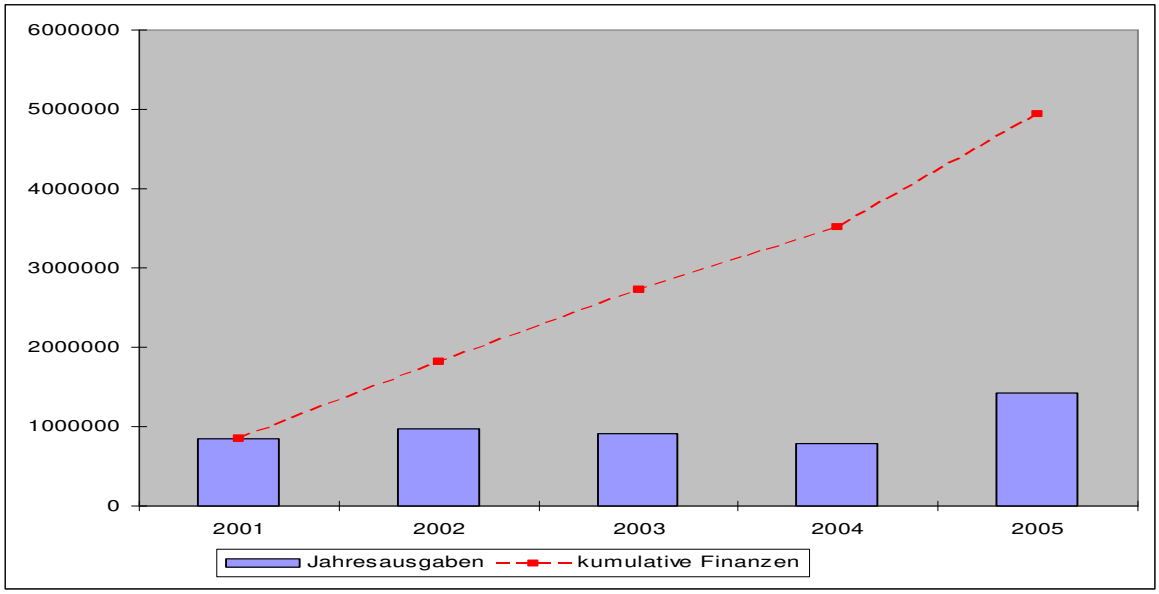
4.3 Grafische Übersicht der Meilensteine

Die **rote** Linie zeigt den Grad der Zielerreichung auf. Mit dem ursprünglichen Auftrag des Bundesrats hat der Fortschritt im geplanten Rahmen stattgefunden. Vorgängig versetzte die Aufgabe der Swisskey dem Vorhaben einen empfindlichen Dämpfer. Mit der Realisierung von Zertifikaten der Klassen B, C und D konnte man kontinuierlich verbessern, den wesentlichen Schub gab jedoch die Verwendung am SSO-Portal.
Die **blaue** Linie zeigt die Entwicklung der technischen Infrastruktur (Hardware und Software).
Die **grüne** Linie drückt das mit dem Aufbau der Infrastruktur erarbeitet KnowHow und die erhaltene Erfahrung aus.



4.4 Grafische Übersicht der Finanzen

Die Grafik basiert auf einer durch die EFK erstellten Zusammenstellung der gesichteten Fakturen. Sie erhebt keinen Anspruch auf Vollständigkeit und beinhaltet nur die externen Kosten.



5 Aktueller Stand

5.1 Ist-Situation

Wie die Geschichte der Admin PKI aufzeigt, mussten viele Anfangsschwierigkeiten überwunden werden, bevor sie sich etablieren konnte. Rückblickend ist nicht nur wertvolle Zeit verstrichen, sondern auch Finanzen sind unwiederbringbar ausgegeben worden. Dies hat jedoch nicht nur das BIT zu verantworten: weder die BVerw noch der Markt Schweiz waren in den Jahren 2001-2004 wirklich reif für den flächendeckenden Einsatz von Zertifikaten. Die mangelnde Nachfrage nach Zertifikaten haben Firmen wie die Swisskey zu Fall gebracht. Die Vorteile und Möglichkeiten wurden damals noch zuwenig erkannt und gewertet.

Mit dem Entscheid des EJPD ein Single-Sign-On-Portal zu schaffen, zur starken Authentifizierung aller Benutzer von Fachanwendungen des EJPD, hat die Admin PKI einen neuen Stellenwert und Aufschwung erhalten. Im letzten Moment ist es dem BIT im Jahre 2005 gelungen, mit einem neu formierten Team die anspruchsvollen Aufgaben wirklich wahrzunehmen und damit die heutige Admin PKI hochzufahren. Der Rollout innert Jahresfrist von über 20'000 Zertifikaten der Klasse B hat hohe Anforderungen an alle Beteiligten gestellt. Der Vergleich mit der kalten Dusche ist hier angebracht, da in der Anfangsphase oft unzufriedene Kundenreaktionen erfolgten.

Schlussendlich ist es aber dem heutigen Team gelungen, die Admin PKI zu neuem Leben zu erwecken und die „Meisterprüfung“ zwar mit Anlaufschwierigkeiten, aber am Ende doch mit guten Noten zu bestehen. Es wurden dabei auch neue wichtige Erkenntnisse gewonnen. Heute sind zwar Standardklassen von Zertifikaten im Produktekatalog des BIT definiert, diese werden jedoch nicht mehr starr verkauft. Zunehmend werden anwendungsspezifische Zertifikate entwickelt und

ausgeliefert. Das PKI-Team ist heute mit dem erworbenen Wissen fit genug, individuell und optimal auf Kundenwünsche zu reagieren. Den interessierten Kunden stehen unter http://internet.bit.admin.ch/adminpki/ nebst den Produktebeschrieben umfangreiche Publikationen zur Verfügung, d.h. Richtlinien, Standards, Checklisten usw. Auch in diesem Bereich wurden grosse Fortschritte erzielt.

Im Kundenumfeld wird es immer positive und negative Reaktionen geben, da eine PKI nie eine vollständige, abgeschlossene Infrastruktur sein wird. Es sind laufend technische Neuerungen, Umbauten und Erweiterungen notwendig. Das Revisionsteam hat jedoch viele positive Echos erhalten und beurteilt daher die heutige Admin PKI als gut. Das BIT hat bewiesen, dass gute Arbeit auch über die BVerw hinaus ihre Akzeptanz findet. Sicher müssen noch vorhandene, erkannte Schwachstellen weiter verbessert bzw. eliminiert werden. Insgesamt besteht jedoch ein solides Fundament, auf welchem das BIT weiter aufbauen kann und damit eine gute Chance für die Zukunft hat, einer der führenden Zertifikatsanbieter in der Schweiz zu sein.

5.2 Kantone

Der Einsatz von Zertifikaten für Zugriffe auf Anwendungen der BVerw ist schon seit vielen Jahren ein Thema zwischen den Kantonen und dem BIT. Mehrere Umfragen sowohl von der Schweizerischen Informatikkonferenz (SIK) wie auch vom Informatikstrategieorgan Bund (ISB) zeigen einen sehr unterschiedlichen Bedarf an Zertifikaten. Das Revisionsteam hat bei den Kantonen Zürich und Aargau im Vorfeld der Revision mittels eines kurzen Fragebogens den aktuellen Stand die Entwicklung der Zertifikatsbedürfnisse nachgefragt.

Die zögerliche Haltung des BIT in den Jahren 2001-2004 hatte dazu geführt, dass im Kanton Zürich eine eigene PKI aufgebaut wurde und auch die Swisscom als Zertifikateanbieter im Gespräch war. Schlussendlich wurde dann doch zugunsten der Admin PKI entschieden. Der Kanton Aargau zeigt auf, dass von Anfang an auf die Admin PKI vertraut wurde. Grundsätzlich ist man mit der technischen Lösung zufrieden, im organisatorischen Bereich werden zumindest von einem Kanton noch Mängel aufgezeigt, welche jedoch vom BIT bereinigt werden können.

Es ist unbestritten, dass in der Vergangenheit seitens der Kantone Widerstand gegen den Einsatz von hardwarebasierenden Zertifikaten gemacht wurde. Für die Kantone und angegliederte Organe war damit ein grosser Kostenfaktor verbunden, weil die entsprechenden organisatorischen Abläufe aufgebaut und die technische Infrastruktur beschafft werden mussten. Das BIT konnte im Gegenzug nicht immer fristgerecht die erwartete Leistung erbringen. Die Korrespondenz zeigt vor allem unakzeptable Antwort- und Lieferfristen auf. Im Laufe des Rollout für das SSO-Portal hat sich jedoch das Blatt zugunsten des BIT gewendet. Mittlerweile sind die kritischen Stimmen leiser geworden und gemäss Auskünften der SIK sind die meisten Kantone heute mit dem Angebot des BIT zufrieden. Gemäss Statistik sind per Mitte April 2007 von den insgesamt 26'580 Zertifikaten der Klasse B rund 24'000 bei den Kantonen im Einsatz. Verschiedene Kantone haben mittlerweile erkannt, dass sich diese Zertifikate auch für die Absicherung eigener Anwendungen einsetzen lassen, entsprechende Projekte sind bereits am Anlaufen (z.B. Gespräche zwischen BIT und Verwaltungsrechenzentrum AG St. Gallen über den Einsatz von Zertifikaten). Diese werden jedoch keine zusätzlichen Einnahmen beim BIT generieren.

Mit dem Einsatz von Local Registration Authorities (LRA) in den Kantonen, aber auch bundesintern, konnte der Ausgabeprozess von Zertifikaten näher an den Endkunden gebracht werden. Eine LRA - heute sind rund 80 im Einsatz - stellt ein wichtiges Glied im ganzen Sicherheitssystem einer PKI dar. Entsprechend muss dort strikte nach den vom BIT aufgestellten Richtlinien gearbeitet werden. Ein im Jahre 2005 durch das BIT in Auftrag gegebenes Audit bei mehreren LRA hat gezeigt, dass Schwachstellen vorhanden waren. Diese sind durch das BIT aufgenommen und zwischenzeitlich kontinuierlich eliminiert worden, allerdings noch nicht vollständig. Es besteht bisher jedoch keine Regelung, wer zukünftig die LRA überprüfen soll.

Empfehlung 5.2 (Priorität: 1)
Da die LRA's ein wichtiges Glied im ganzen Sicherheitsprozess einer Zertifikatsausgabe sind, muss durch regelmässige Audit sichergestellt werden, dass diese Stellen auch den Vorgaben entsprechend arbeiten. Das BIT als Produkteanbieter muss dafür sorgen, dass solche Audit durchgeführt und die entsprechenden Vorgaben durch den IRB verfügt werden.

Das BIT wird bis Ende Jahr ein Auditkonzept für LRA erarbeiten und dem IRB anschliessend einen Vorschlag für entsprechende Vorgaben unterbreiten.

5.3 Konkurrenzsituation

Nach dem Zusammenbruch der Swisskey gab es lange keinen Schweizer Anbieter für Zertifikate. Erst nach dem Inkrafttreten der Signaturgesetzes (ZertES) stand eine juristisch definierte Basis nach Schweizer Recht zur Verfügung, um mit anerkannten Standards einen Weg zu suchen. Es gibt heute zwar einen sehr grossen Beratermarkt in der Schweiz, jedoch erst drei anerkannte Anbieter von ZertES-konformen Zertifikaten. Viele Beraterfirmen bedienen sich entweder firmeninterner Zertifikate oder solcher von grossen ausländischen Anbietern wie Verisign, Cybertrust, Symantec oder andern. Für E-Government-Lösungen sind die Erwartungen an die Vertrauenswürdigkeit und Zuverlässigkeit (Kontinuität) eines Zertifikat-Herstellers gross. Diese Erwartungen bleiben bei ausländischen oder nicht nach ZertES zertifizierten Firmen mindestens teilweise unerfüllt.

Wenn das BIT die Zertifizierung durch die Firma KPMG erreicht haben wird, zeichnet sich eine sehr interessante Perspektive ab. Das BIT konnte mit der Post, eine Vereinbarung treffen und die technische Umsetzung testen, um mit der gegenseitigen Akzeptanz der Zertifikate, den elektronischen eingeschriebenen Brief (IncaMail) auch für die Mitarbeitenden der Bundesverwaltung zu erschliessen. Dieses Beispiel zeigt die Möglichkeit auf, mittels BIT-Zertifikaten die öffentliche Verwaltung und über die Post-Zertifikate Firmen bzw. Private zu bedienen. So könnten an ein breites Publikum ausgerichtete E-Government-Dienstleistungen realisiert werden.

Die Swisscom und die Firma Quo Vadis sind auf absehbare Zeit für den Bereich der öffentlichen Verwaltung keine Konkurrenz, sie bedienen kleinere, spezifischere Märkte. Produkte mit grossen Mengen vergebener Zertifikate der Swisscom sind noch keine bekannt. Es ist auch kein Produkt in der Öffentlichkeit sichtbar, welches den Durchbruch der Swisscom-Zertifikate auf dem engen Markt

der Schweiz ankündigen würde. Eine Kooperation mit dem BIT, wie diejenige der Post, könnte jedoch auch für die Seine interessante Option sein.

Für die Post und die Swisscom scheint die Wirtschaftlichkeit der PKI - wie beim BIT auch - nicht über den Preis der einzelnen Zertifikate rechenbar zu sein. Der Nutzen liegt primär im Potenzial der neuen Möglichkeiten für die einfache Absicherung von Daten und Anwendungen einer grossen Anzahl von Benutzern aus unterschiedlichen Organisationen. Profitieren wird in erster Linie der Kunde, ob die Zertifikate von der Post, der Swisscom oder dem BIT stammen.

Für Zertifikate von schwacher Güte oder mit speziellen Systemkonstellationen werden heute und auch in Zukunft die kommerziellen internationalen Anbieter Zertifikate anbieten und verkaufen können. Für hohe Qualitätsansprüche war bisher in der Schweiz keine Alternative vorhanden, daher sehen die Zukunftsaussichten für das BIT vielversprechend aus.

5.4 Laufende Projekte

Die Admin PKI ist ein Basisprodukt, welches der Ausgabe von Zertifikaten dient. Das entsprechende Projekt zur Schaffung der ersten Infrastrukturen wurde im Jahre 2002 offiziell abgeschlossen, d.h. in den offiziellen Betrieb übernommen. In den darauf folgenden Jahren sind laufend neue Kundenbedürfnisse entstanden und werden auch weiterhin entstehen. Die ursprüngliche nur auf secure-messaging ausgerichtete Dienstleistung des BIT wurde schrittweise ausgebaut und den neuen Erkenntnissen entsprechend verbessert. Für jede Erweiterung der ursprünglichen Basisinfrastruktur wurden bzw. werden zusätzliche, separate Projekte geführt und abgerechnet. Solche Projekte waren: Aufbau der PKI Class 2 (heute Klasse B), Einführung der PKI in den Kantonen im Zusammenhang mit dem SSO-Portal des EJPD, Aufbau der Klassen C und D, Ausbau der Infrastruktur auf CA3 und die Vergabe von Zertifikaten für den digitalen Fahrtenschreiber (DFS). Aktuell wird für das secure-messaging, die Zertifizierung der Klasse A und das Smartcard Management System (SCMS) je ein eigenes Projekt geführt. Diese Aufzählungen sind nicht vollständig, sondern dienen der Darlegung der Vielfältigkeit und Problematik im Umfeld von Admin PKI.

Das Revisionsteam hatte Einsicht in alle bisherigen Projektunterlagen, d.h. Offerten, Verträge und Abrechnungen. Die Unterlagen sind übersichtlich geordnet und der Geldfluss konnte aufgrund der Verträge und ab 2006 auch aus den SAP-Auszügen grundsätzlich nachvollzogen werden. Es erfolgte jedoch weder eine Vollständigkeits- noch eine Beschaffungsprüfung. Die Zusammenstellung aller gesichteten Fakturen dient in erster Linie der Beurteilung der bisher erfolgten Ausgaben gemäss Kapitel 5.5.

5.5 Investitionen, Budget

Wie die vorangehenden Kapitel zeigen, hat das BIT aus einer Notsituation heraus den Entscheid zum Aufbau einer eigenen CA getroffen. Es hat damit entschieden, eine wichtige sicherheitsrelevante Schlüsselposition innerhalb der BVerw zu behalten und diese nicht irgendwelchen Fremdanbietern zu überlassen. Bei der Auswahl eines geeigneten Zertifikatanbieters steht primär das Vertrauen in die Seriosität eines solchen Anbieters, aber auch an dessen Bestehen auf dem Markt im Vordergrund. Je nach Anforderungen an ein Zertifikat muss ein hohes Sicherheitsniveau erfüllt werden. Vertraut man in einem solchen Falle nun einem bundesinternen Leistungserbringer oder gibt man diesen Sicherheitsdienst in fremde Hände? Ob

der damalige Entscheid Richtung hardwarebasierende Zertifikate richtig oder falsch war, ist nicht mehr relevant. Das BIT hat schon vor längerer Zeit erkannt, dass der Markt mehr braucht als ein einziges starres, nur auf Hardware basierendes Zertifikat.

Mit der Entscheidung des EJPD für das SSO-Portal Smartcards einzusetzen, wurden jedoch entscheidende Weichen gestellt. Entweder konnte die damals schlafende Admin PKI geweckt und hochgefahren werden, um den Anforderungen des EJPD und auch der Kantone zu genügen, oder man musste sich auf dem Markt einen anderen Zertifikatsanbieter suchen. Dies hätte unweigerlich zu einem „grounding" der Admin PKI geführt, unter Abschreibung aller bis dahin getätigten Investitionen. Die Entscheide des Informatikrates Bund (IRB) kamen daher zum richtigen Zeitpunkt und beinhalten einen wichtigen Faktor. Um eine funktionierende PKI betreiben zu können, benötigt es vorerst den Aufbau der entsprechenden Infrastruktur und des Know-how. Die hiefür notwendigen Investitionen dürfen nicht unterschätzt werden. Wollte man diese durch den Verkauf von Zertifikaten wieder zurückerhalten, so müssten die Zertifikate zu einem Preis verkauft werden, den die Kunden nicht bezahlen würden. Im direkten Vergleich mit der Swisscom oder der Post liegt die Preispolitik des BIT durchaus im Rahmen und kann als konkurrenzfähig wenn nicht sogar kostengünstig bezeichnet werden. Die Ausgabe und das Management der Zertifikate sollten aber grundsätzlich selbsttragend sein. Der break-even für die Kosten des heutigen Betriebes kann nur über die Ausgabemenge von Zertifikaten - das BIT geht von einer Menge von 100'-130'000 Zertifikaten aus - erreicht werden. Diese Annahmen sind dann realistisch, wenn für weitere Anwendungen der BVerw Zertifikate als Sicherheitselement eingesetzt wird.

Das Revisionsteam hat anhand der zur Verfügung gestellten Unterlagen alle Rechnungen zusammengefasst. Die daraus resultierenden Summen wurden mit den Zusammenstellungen des Produktmanagers verglichen. Die Kosten für die Jahre 2001-2003 konnten auf der Basis von SAP nicht vollständig nachvollzogen werden können. Die Jahre 2004 und 2005 dagegen stimmen unter Berücksichtigung von Abgrenzungen ziemlich genau überein. Seit dem Jahr 2003 sind die Verbuchungen immer präziser geworden, d.h. nicht nur die externen Kosten, sondern auch anteilmässige interne Kosten des BIT wurden der Admin PKI belastet. Ab 2005 werden zudem die verbuchten bzw. umgelagerten Kosten durch den Produktmanager beurteilt und ausgewertet, so dass die Kosten nun einigermassen präzis vorliegen.

Die Zusammenstellung der EFK zeigt für die Jahre 2001-2005 ein Gesamttotal an externen Kosten, d.h. Zahlung an Lieferanten und Dienstleister, von rund 5 Mio. Franken. In diesem Betrag sind nicht nur die Kosten des laufenden Betriebes inkl. Wartung und Lizenzen inbegriffen, sondern auch alle Projektkosten, welche im Zusammenhang mit der Ausgabe von Zertifikaten gestartet worden sind, z.B. Ausbau der Infrastruktur für die Class 2 (heute Klasse B), Klasse C und D, Aufbau Registration für die Kantone usw. Unter der Annahme (basierend auf Einschätzungen der damaligen und heutigen Projektleiter) der jeweiligen PKI-Mitarbeitenden - 2001/02 je zwei, 2003/04 je vier, 2005/06 je sechs - bei einem angenommenen durchschnittlichen Vollkostenarbeitsplatz von Fr. 200'000 pro Mitarbeitenden/Jahr, ergibt sich der Betrag von bisher 4.8 Mio. Franken an aufgelaufenen internen Kosten.

Die ausgewiesenen Erlöse der Jahre 2001-2005 sind zu wenig transparent bzw. aussagekräftig, so dass diese durch das Revisionsteam nicht gewertet werden können. Eine umfassende Vollkostenrechnung wird erst ab 2007 wirklich erstellt werden können. Die entsprechenden

Planwerte gemäss den Vorgaben NRM sehen Ausgaben für den Betrieb der Admin PKI von rund 3,65 Mio. vor, bei einem voraussichtlichen Erlös inkl. Q-Mittel von rund 2,8 Mio. (davon Fr. 700'000 finanzwirksame Einnahmen), was einem budgetierten Verlust von Fr. 850'000 entspricht. Dabei sind die laufenden Projekte in der Grössenordnung von 1 Mio. nicht eingerechnet. Die geschätzten Einnahmen/Ausgaben für die Jahre 2008-2011 zeigen ab 2009 einen zunehmenden „Gewinn", vorausgesetzt die Ausgabe von Zertifikaten kann entsprechend den Annahmen gesteigert und die Kosten im aufgezeigten Rahmen gehalten werden. Eine Wertung dieser Zahlen ist zum heutigen Zeitpunkt sehr schwierig, das Revisionsteam sieht aber eine gute Chance, dass sie realisiert werden können.

Eine faire Wirtschaftlichkeitsrechnung kann unter den mehrfach dargelegten Aspekten nicht erstellt werden. Der Nutzen einer PKI wird erst durch die vereinfachte Absicherung von Anwendungen indirekt generiert. Vom entsprechenden Sparpotential profitieren in erster Linie die involvierten E-Government-Partner. Das Synergiepotiential, welches zu gewinnen ist, wird jedoch durch die aktive Zusammenarbeit mit der Post zusätzlich verstärkt. Aufgrund der bisherigen Erfahrungen muss davon ausgegangen werden, dass die getätigten Investitionen in der Grössenordnung von 12 Mio. nicht unmittelbar zurückgeholt werden können und als abzuschreibende Initialkosten betrachtet werden sollten. Diese Fakten bzw. die Abgrenzungen zwischen den notwendigen Investitionen und dem eigentlichen Betrieb, welcher nach wirtschaftlichen Kriterien stattfinden sollte, müsste in den Berechnungs-Vorgaben auch berücksichtigt werden. Gemäss den geltenden Grundsätzen für die Kalkulation der Verrechnungspreise, dürfen bundesintern erbrachte Leistungen nur auf der Basis der Planvollkosten erfolgen, d.h. es dürfen weder Gewinn- noch Risikoanteile eingerechnet werden. Diese Preispolitik ist bei den aufgezeigten Investitionen und den jährlich fliessenden Querschnittsgeldern nur bedingt nachvollziehbar, vor allem wenn Kosten ausserhalb der BVerw z.B. an die Kantone weiterverrechnet werden. Eine Vollkostendeckung ist nur dann erreicht, wenn keine zusätzlichen Mittel (Querschnittsgelder) notwendig sind, um ein Produkt zu finanzieren. Dabei sind die getätigten Investitionen noch nicht eingerechnet oder zurückgeholt.

Abschliessend stellt das Revisionsteam fest, dass mit dem Aufbau der Admin PKI und der Vergabe von Zertifikaten ein Geschäft entstanden ist, das nicht von einem Tag auf den anderen wieder aufgegeben werden kann. Es müsste mindestens für die sich im Umlauf befindlichen, gültigen Zertifikate eine Nachfolgeregelung getroffen werden, mit möglichen finanziellen Konsequenzen für das BIT.

Empfehlung 5.5 (Priorität: 2)
Bei der Festlegung der Preise für die verschiedenen Zertifikate muss berücksichtigt werden, dass eine Verrechnung zu Vollkosten erst dann erreicht ist, wenn keine Querschnittsgelder mehr fliessen. Entsprechend sollte überprüft werden, ob bundesextern nicht andere, d.h. höhere Preise verrechnet werden könnten, als innerhalb der BVerw, damit die Vollkostendeckung rasch erreicht werden kann.

Das BIT wird die Kostenverteilung und Preisgestaltung überprüfen und die Verrechnung höherer Preise an bundesexterne Stellen mit der EFV besprechen.

5.6 ZertES

Mit dem Entscheid vom 27.6.05 hat der IRB dem BIT bewilligt, dass Zertifikate der Klasse A innerhalb der BVerw angeboten werden dürfen. Gleichzeitig wurde festgelegt, dass diese Dienstleistung nicht wie die Klassen B-D mit Querschnittsgeldern finanziert werden darf, sondern die Zertifikate entsprechend zu Vollkosten weiterverrechnet werden müssen. Aufgrund dieser Ausgangslage hat das BIT grünes Licht erhalten, eine Zertifizierung nach den Vorgaben der ZertES einzuleiten. In einem Voraudit im Herbst 2005 wurde durch die einzige in der Schweiz akkreditierte Zertifizierstelle KPMG primär abgeklärt, wie weit das BIT einer Zertifizierung genügen würde. Nach Vorliegen der Resultate wurde am 31.05.06 der Auftrag erteilt, das Zertifizierungsaudit durchzuführen. Im Zeitraum August 2006 bis Februar 2007 hat die KPMG im BIT die Aufbau- und Ablaufprozesse sowie die logische Infrastruktur des Certification Service Provider (CSP) geprüft. Der entsprechende Auditbericht liegt seit anfangs April 2007 vor.

Das Audit hat gezeigt, dass die Prozesse und Infrastruktur noch nicht in allen Bereichen den vom Gesetzgeber auferlegten sehr hohen Sicherheitsanforderungen entsprechen. Es wurden jedoch keine Mängel festgestellt, welche nicht innerhalb der von der KPMG angesetzten Nachfrist behoben werden können. Daher kann damit gerechnet werden, dass das BIT die angestrebte Zertifizierung im Laufe des 2. Quartals 2007 erreichen wird. Die Zertifizierung hat nicht in erster Linie den Verkauf von Zertifikaten der Klasse A zum Ziel. Der Markt hierfür ist heute realistisch betrachtet noch sehr klein, in der BVerw sind bisher noch keine konkreten Bedürfnisse vorhanden, auch der private Markt reagiert verhalten und zögerlich.

Die offizielle Anerkennung des BIT als CSP soll primär zur Vertrauensbildung beitragen, da nach strikten gesetzlichen Grundlagen und Standards beurteilt wird. Zum Verständnis dieser Zielsetzung muss dargelegt werden, dass die durch die KPMG geprüften Prozesse und Infrastrukturen dieselben sind, welche analog auch für die Ausgabe von allen anderen Zertifikaten dienen. Der Mehrwert, welcher ganz generell für das BIT als Zertifikatsanbieter/-ausgeber entsteht, sollte sich entsprechend in der Menge der insgesamt verkauften Zertifikate niederschlagen, was die Finanzlage generell verbessern würde. Dies geht auch aus der Kosten-/Nutzenberechnung für das Projekt ZertES hervor. Nebst einem geringen Betrag für den Verkauf von Zertifikaten der Klasse A werden die „Einnahmen“ in Form von quantifizierbarem Nutzen mit der wahrscheinlichen Summe von Fr. 450'000 pro Jahr beziffert. Diesem theoretischen Wert stehen Betriebskosten und Zinsen von jährlich rund Fr. 230'000 gegenüber. Somit müsste der ROI innerhalb von 5 Jahren erreicht sein. Das Revisionsteam beurteilt die vom BIT dargelegten Berechnungen grundsätzlich als realistisch, jedoch nicht als wirtschaftlich. Die Zertifizierung hat vielmehr einen strategischen und politischen Hintergrund, welcher bei der Beurteilung mitberücksichtigt werden muss.

Da gemäss Beschluss IRB die Finanzierung der Klasse A Zertifikate nicht über Querschnittsgelder erfolgen darf, wird bis zur Zertifizierung ein separates Projekt „Anerkennung Admin PKI Class A“ geführt, mit Ausweisung der damit verbundenen externen Kosten von rund 1,1 Mio. Franken.

Bei den zukünftigen Budgets müssen die Kosten und Erträge, welche dem oben dargelegten Szenario entsprechen, weiterhin separat ausgewiesen werden und dürfen nicht unter dem globalen Budget „PKI-Kosten_Ertrag“ geführt und auch nicht über die Admin PKI Konten abgerechnet

werden. Damit dem IRB-Beschluss nachgekommen werden kann, muss jederzeit transparent aufgezeigt werden können, wie hoch die bisherigen Kosten und Erträge sind.

Empfehlung 5.6 (Priorität: 1)
Alle Kosten und Erträge (Betriebskosten, Investitionen, Wiederholaudit, Verkaufserträge usw.) welche im Zusammenhang mit der Zertifikatsklasse A stehen, müssen separat budgetiert und abgerechnet werden. Die Vorgaben des IRB-Beschlusses vom 27.6.05, wonach keine Vermischung mit den Klassen B-D (Querschnittsgelder) erfolgen darf, müssen durch das BIT zwingend erfüllt werden.

Das BIT wird die Kosten und Erträge im Zusammenhang mit der Zertifikatsklasse A jährlich separat ausweisen. Da sich in der Praxis die Zertifikatsklassen A und B die gleichen Infrastrukturen und Betriebsprozesse teilen (dies ist auch bei anderen CSP so), basiert dieser Ausweis zwingend auf Modellrechnungen.

6 Ausblick und Beurteilung

Das BIT konnte in den letzten Jahren sowohl die Infrastruktur wie auch das Wissen aufbauen, um den Kundenbedürfnissen nach Zertifikaten unterschiedlicher Güte und Qualität, zur Abdeckung von anwendungsspezifischen Sicherheitsaspekten, nachkommen zu können. Den Nachweis der Befähigung, funktionierende Zertifikate in grossen Mengen zeitkritisch auszustellen, hat das BIT mit dem Rollout der rund 25'000 Zertifikate für die Benutzer des SSO-Portals im Jahre 2006 erbracht. Mit der aktuell laufenden Zertifizierung des BIT als CSP durch die KPMG beweist das BIT zudem die Qualität und Sicherheit der eingesetzten Infrastruktur und der Prozesse zur Ausgabe von Zertifikaten der Klasse A nach den Vorschriften der ZertES. Das BIT wird voraussichtlich der vierte Anbieter auf dem Schweizer Markt sein, welcher diese Art von Zertifikaten anbieten darf. Da für die Ausgabe aller Zertifikatsklassen im BIT dieselbe Infrastruktur und die gleichen Prozesse wie für Klasse A verwendet werden, stehen den öffentlichen Verwaltungen nun Mittel zur Verfügung, um E-Government-Lösungen auf einem sehr hohen Sicherheitsniveau realisieren zu können.

Nach der erfolgreichen Anerkennung durch die KPMG wird eine wichtige Voraussetzung erfüllt sein, dass das BIT im kleinen Markt der Schweiz ein glaub- und vertrauenswürdiger Zertifikatsanbieter wird. Dies kann zu einer wichtigen Bundesaufgabe werden. Die hohen Anforderungen werden jährlich durch die KPMG nachgeprüft werden, so dass von einem gleichbleibenden Gütesiegel ausgegangen werden kann. Die Zertifizierung des BIT ist auch insofern hochwertig einzuschätzen, als bereits über 40'000 Zertifikate, davon 65% der Klasse B, im Einsatz stehen. Die Post und die Swisscom sind zwar bereits seit längerem zertifiziert, haben aber ihre Produkte erst nach der Zertifizierung angeboten und besitzen somit noch nicht die Praxiserfahrungen von grossen Rollouts. Das BIT hat mit der Post im Bereich IncaMail - Versand von elektronisch eingeschriebenen Schriftstücken - eine „Roaming“-Vereinbarung getroffen, was zu einem Synergiepotential auch im privaten Markt führt.

Um Zertifikate nach wirtschaftlichen Grundsätzen verkaufen zu können, muss eine grosse Menge abgesetzt werden. Daher sind Zertifikate der Klasse B-D ein wichtiger Erfolgsfaktor. Ob die ZertES-

konforme Klasse A je selbsttragend bewirtschaftet werden kann, erscheint zumindest heute als eher unwahrscheinlich. Das Obligationenrecht verlangt nur in sehr wenigen Fällen die qualifizierte Schriftlichkeit bei Rechtsgeschäften und solche werden wahrscheinlich auch in Zukunft nur beschränkt elektronisch abgewickelt werden können. Die Zertifizierung der KPMG muss daher primär als Qualitäts- und Gütesiegel nicht nur für die Ausgabe von Zertifikaten sondern auch für das BIT selber verstanden werden. Im Vordergrund steht dabei das Vertrauen der Kunden in die Prozesse und den technischen Betrieb. Das BIT kann diese Chance nutzen, um ein grosses Potenzial an Anwendungen durch die Möglichkeiten der Zertifikate auf einfache Art sicherer zu machen.