EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Prüfung von Entwicklung und Betrieb der Public Key Infrastructure

Bundesamt für Informatik und Telekommunikation

EFK-19465 | inkl. Stellungnahmen | 15. Mai 2020 | FinDel D4/2020

Inhaltsverzeichnis

Das Wesentliche in Kürze ... 3

L'essentiel en bref ... 6

1 Auftrag und Vorgehen ... 10

1.1 Ausgangslage ... 10

1.2 Prüfungsziel und -fragen ... 10

1.3 Prüfungsumfang und -grundsätze ... 10

1.4 Unterlagen und Auskunftserteilung ... 11

1.5 Schlussbesprechung ... 11

2 Anforderungen des Bundes ... 12

2.1 Anforderungen wurden hauptsächlich durch gesetzliche Vorgaben und Bundesratsbeschlüsse generiert ... 12

3 Sicherheit und Verfügbarkeit ... 15

3.1 Ein hoher Sicherheitslevel ist erreicht, aber Systemüberwachung und Logging müssen verbessert werden ... 15

3.2 Probleme müssen speditiver gelöst werden ... 17

4 Nachhaltigkeit ... 19

4.1 Hohe Vertrauenswürdigkeit zu überschaubaren Kosten ... 19

4.2 Das Change-, Release- und Life-Cycle-Management muss verbessert werden ... 20

4.3 Verschlüsselung wird über die Zeit problematisch ... 21

4.4 Zielführende Entscheide zur PKI in allen Lagen ... 22

Anhang 1: Rechtsgrundlagen ... 24

Anhang 2: Abkürzungen ... 25

Anhang 3: Glossar ... 26

Prüfung von Entwicklung und Betrieb der Public Key Infrastructure

Bundesamt für Informatik und Telekommunikation

Das Wesentliche in Kürze

Der Bundesrat beschloss am 18. Dezember 1998, dass für die Bundesverwaltung eine Zertifizierungsinfrastruktur aufgebaut werden sollte. Das Bundesamt für Informatik und Telekommunikation (BIT), damals noch mit anderer Amtsbezeichnung, hat sich dieses Auftrags angenommen. Daraus ist über die Jahre die heutige Swiss Government Public Key Infrastructure (SG PKI) entstanden bzw. gewachsen, zuerst als Querschnittsdienstleistung, seit 2014 als Teilprodukt des Standarddienstes Identity und Accessmanagement. Für die Führung und Steuerung von Standarddiensten (SD) ist das Informatiksteuerungsorgan (ISB) verantwortlich. Der Betrieb der heutigen SG PKI kostet pro Jahr zwischen 8 und 10 Millionen Franken.

Die SG PKI erfüllt seit 20 Jahren die Anforderungen an eine sichere und vertrauenswürdige Infrastruktur zur Ausstellung, Verteilung und Überprüfung von digitalen Zertifikaten. Solche Zertifikate werden zur Absicherung von rechnergestützter Kommunikation benötigt. Es gab bisher nie einen Ausfall, der zu einer flächendeckenden Einschränkung geführt hätte. Trotzdem sind Verbesserungen notwendig: eingehende Problemmeldungen müssen schneller bearbeitet und wenige Schwachstellen im Betrieb so weit wie möglich eliminiert werden.

Die Swiss Government PKI hinterlässt grundsätzlich einen guten Eindruck…

Das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) stellt hohe Sicherheits- und Prozessanforderungen an die Anbieter von Zertifikaten für qualifizierte elektronische Signaturen. Solche entsprechen der händischen Unterschrift einer natürlichen Person. Die SG PKI hat sich schon früh in ihrer Entstehung als eine von vier Anbieterinnen auf dem Schweizer Markt nach ZertES zertifizieren lassen. Sie muss dadurch jährlich wiederkehrende Audits bestehen, um die Zertifizierung beizubehalten bzw. zu erneuern. Der damit erreichte hohe Sicherheitslevel wirkt sich im Wesentlichen auf alle Zertifikate der SG PKI positiv aus, weil dieselbe Infrastruktur verwendet wird.

Die grosse Masse machen rund 130 000 Zertifikate der Klasse B aus. Diese werden von Bundesangestellten sowie in den Kantonen verwendet und dienen in erster Linie der Authentifikation sowie zur Verschlüsselung. Hinzu kommen 60 000 pre-staged Smart Cards, welche als Reserve bei den Local Registration Authority (LRA) lagern. Die Schlüssel der Zertifikate sind bereits auf die Smart Cards geladen, aber die Zertifikate noch nicht ausgestellt.

Die Leistungsbezüger (LB) können Anforderungen über den dafür vorgesehenen Prozess P035 beim ISB stellen. Bisher ist dies wenig erfolgt, da die Produkte der SG PKI hauptsächlich basierend auf den gesetzlichen Vorgaben gebaut wurden. Es konnten keine Nachweise gefunden werden, dass Verwaltungseinheiten konkrete Vorstellungen an das BIT übermittelt hätten, als die PKI aufgebaut worden ist. Vielmehr sind die Mitarbeitenden der PKI eher in einer Beratungsposition, wenn in Projekten Zertifikate zum Einsatz kommen sollten. Die

Eidgenössische Finanzkontrolle (EFK) hat festgestellt, dass bei den LB oft nicht genau verstanden wird, was die Aufgaben der SG PKI sind. Authentifikation, Signatur und Verschlüsselung sind nachgelagerte Dienste, welche die Zertifikate lediglich einsetzen. Sie gehören daher nicht zur SG PKI. Dem BIT wird empfohlen, die LB zukünftig anzuweisen, ihre Änderungswünsche über den Prozess P035 einzugeben.

… einige Schwachstellen bestehen dennoch, können aber verbessert werden

Aufgrund der jährlichen externen Audits wird die SG PKI sehr tief und detailliert überprüft. Die entsprechenden Berichte zeigen, dass immer wieder Schwachstellen gefunden werden. Werden solche als erheblich eingestuft, müssen sie innert Jahresfrist bereinigt werden. Bisher hat das BIT solche Schwachstellen immer zeitgerecht beseitigen können. Das grösste Risiko besteht seit jeher in der nicht vorhandenen Redundanz bei den meisten Systemen der SG PKI. Dieses Manko wird nun mit dem Umzug und Neuaufbau in Frauenfeld bis 2021 eliminiert.

Die Systeme der SG PKI sowie die Tätigkeiten der System- und Netzwerkadministratoren auf der PKI-Infrastruktur [redacted] Die EFK hat entsprechende Empfehlungen abgegeben.

Die schleppende Behandlung von eingehenden Störungen (Incidents) hat in der Vergangenheit immer wieder zu Unmut bei den LB gesorgt. Notwendige Changes blieben zu lange unerledigt, was ebenfalls nicht zu einem besseren Image des BIT beigetragen hat. Seit einigen Monaten wird nun agil und mit Unterstützung von Werkzeugen systematisch jedes Problem erfasst, analysiert und wo nötig einem Change zugeführt. Die neu eingesetzten Product Owner kümmern sich um die Abklärung und Erledigung von Problemen. Das Vorgehen muss sich in der Praxis noch bewähren. Das ISB führt die SG PKI mit den für alle SD eingesetzten Instrumenten. Bei der Produkt- und Serviceentwicklung hat es sich dagegen bisher nicht vertieft eingebracht. Daher empfiehlt die EFK, dass die Steuerung und Führung sowohl beim Anforderungsmanagement wie auch bei der Planung von Changes/Releases und beim Life-Cycle-Management verbessert werden muss.

Ein externes Design-Review hat bisher nicht stattgefunden. Dabei würden in Ergänzung zu den Zertifizierungsaudits die System- und Netzwerkarchitektur sowie die sicherheitsrelevanten Betriebsabläufe überprüft. Die EFK empfiehlt diesen Review durchführen zu lassen, sobald die Umzugsarbeiten nach Frauenfeld abgeschlossen sind.

Zukünftige Herausforderungen müssen gemeistert werden

In der Bundesverwaltung müssen gemäss Informationsschutzverordnung (ISchV) klassifizierte Dokumente ab der Klassifizierungsstufe VERTRAULICH verschlüsselt werden. Die von den Mitarbeitenden dazu verwendeten Zertifikate können aus unterschiedlichen Gründen ungültig werden. Damit müssen alle zuvor verschlüsselten Dokumente umgeschlüsselt werden. Erfolgt dies nicht, so ist der Zugriff später nur noch möglich, wenn die SG PKI die entsprechenden Schlüsselpaare erneut ausliefert. Diese müssen entsprechend über längere Zeit aufbewahrt bleiben. Bisher ist nicht geregelt, wie lange diese Aufbewahrungsfrist sein muss. Die Problematik wird sich über die Jahre verschärfen, daher empfiehlt die EFK die

Aufbewahrungsfrist zu regeln. Die SG PKI ist grundsätzlich nicht für die Verschlüsselungsprodukte verantwortlich. Trotzdem mussten Umschlüsselungstools durch das BIT entwickelt und ausgerollt werden.

Mit der Entflechtung der IT des zivilen und des militärischen Teils im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport ist der Anspruch formuliert worden, dass die PKI über alle Lagen funktionieren muss. Das dafür aufgesetzte Projekt sieht vor, dass dafür eine eigene Instanz innerhalb der SG PKI aufgebaut wird, welche aber durch die Führungsunterstützungsbasis (FUB) betrieben werden soll. Im Ernstfall könnte diese durch die FUB unabhängig von der SG PKI weiterbetrieben werden. Die EFK unterstützt diese Pläne. So ist sichergestellt, dass der Wille des Bundesrates zu einer einzigen PKI Bund eingehalten bleibt.

Audit du développement et de l'exploitation de l'infrastructure à clé publique

Office fédéral de l'informatique et de la télécommunication

L'essentiel en bref

Le 18 décembre 1998, le Conseil fédéral a décidé qu'une infrastructure de certification devait être mise en place pour l'administration fédérale. L'Office fédéral de l'informatique et de la télécommunication (OFIT), qui portait à l'époque un autre nom, a accompli ce mandat. C'est ainsi que l'actuelle infrastructure à clé publique, la Swiss Government Public Key Infrastructure (SG PKI), a vu le jour et s'est développée, d'abord en tant que service transversal puis, depuis 2014, en tant que sous-produit du service standard de gestion des identités et des accès. L'Unité de pilotage informatique de la Confédération (UPIC) est responsable de la gestion et du pilotage des services standard. L'exploitation de l'actuelle SG PKI coûte entre 8 et 10 millions de francs par an.

La SG PKI répond depuis 20 ans aux exigences d'une infrastructure sûre et fiable pour la délivrance, la distribution et la vérification de certificats numériques. Ces certificats sont nécessaires pour sécuriser la communication assistée par ordinateur. Il n'y a jamais eu de panne jusqu'à présent qui aurait entraîné une limitation généralisée. Des améliorations sont néanmoins nécessaires : les problèmes annoncés doivent être traités plus rapidement et les quelques lacunes de l'exploitation doivent être éliminées dans la mesure du possible.

La Swiss Governement PKI donne globalement une bonne impression...

La Loi fédérale sur les services de certification dans le domaine de la signature électronique (SCSE) impose des exigences élevées en matière de sécurité et de processus aux fournisseurs de certificats de signature électronique qualifiée. Ces certificats correspondent à la signature manuscrite d'une personne physique. La SG PKI est très vite devenue l'un des quatre fournisseurs à se faire certifier pour le marché suisse conformément à la SCSE. Pour conserver et renouveler sa certification, elle doit passer des audits annuels. Le niveau de sécurité élevé ainsi atteint a un effet positif sur tous les certificats de la SG PKI, car la même infrastructure est utilisée.

Le grand nombre est constitué d'environ 130 000 certificats de classe B. Ils sont utilisés par les employés de la Confédération ainsi que dans les cantons et servent en premier lieu à l'authentification et au chiffrement. S'y ajoutent 60 000 cartes à puce préparées (prestaged), stockées en réserve par l'autorité d'enregistrement locale (LRA). Les clés des certificats sont déjà chargées sur les cartes à puce, mais les certificats ne sont pas encore émis.

Les bénéficiaires de prestations peuvent soumettre leurs exigences à l'UPIC par le biais du processus P035. Jusqu'à présent, il a peu été fait usage de cette possibilité, car les produits de la SG PKI ont été développés principalement sur la base des exigences légales. Rien n'indique que des unités administratives aient transmis des demandes concrètes à l'OFIT lors de l'élaboration de la PKI. Les collaborateurs de la PKI assument plutôt un rôle de conseil lorsque des certificats sont requis pour des projets. Le Contrôle fédéral des finances (CDF) a constaté que les bénéficiaires de prestations ne comprennent souvent pas exactement

quelles sont les tâches de la SG PKI. L'authentification, la signature et le chiffrement constituent des services en aval qui ne font qu'utiliser les certificats et ne font donc pas partie de la SG PKI. Il est recommandé à l'OFIT d'exiger des bénéficiaires de prestations qu'ils passent à l'avenir par le processus P035 pour soumettre leurs demandes de changements.

... mais il subsiste des lacunes, qui peuvent toutefois être corrigées

Étant soumise à des audits externes annuels, la SG PKI fait l'objet d'examens très approfondis et détaillés. Les rapports correspondants relèvent régulièrement des lacunes. Celles considérées comme importantes doivent être corrigées dans un délai d'un an. L'OFIT y est jusqu'ici toujours parvenu dans les temps. Le plus grand risque a toujours été l'absence de redondance pour la plupart des systèmes de la SG PKI. Ce problème sera résolu avec le déménagement et l'installation à Frauenfeld d'ici à 2021.

Les systèmes de la SG PKI et les activités des administrateurs du système et du réseau responsables de l'infrastructure PKI [redacted] Le CDF a formulé des recommandations en ce sens.

La lenteur du traitement des dérangements *(incidents)* a régulièrement suscité le mécontentement chez les bénéficiaires de prestations par le passé. Des changements *(changes)* nécessaires sont restés trop longtemps en suspens, ce qui n'a pas non plus contribué à améliorer l'image de l'OFIT. Depuis quelques mois, grâce à une approche agile et avec l'aide d'outils, chaque problème est systématiquement saisi et analysé, et un changement est prévu si nécessaire. Des *product owners* nouvellement nommés s'occupent de clarifier et de résoudre les problèmes. La procédure doit encore faire ses preuves dans la pratique. L'UPIC gère la SG PKI avec les instruments utilisés pour tous les services standard. Elle ne s'est par contre jusqu'ici guère investie dans le développement de produits et de services. Le CDF recommande par conséquent d'améliorer la gestion et le pilotage, tant au niveau de la gestion des exigences qu'à ceux de la planification des changements et versions et de la gestion du cycle de vie.

La conception n'a pas encore fait l'objet d'un examen externe. Il s'agirait, en complément aux audits de certification, d'examiner l'architecture du système et du réseau ainsi que les processus opérationnels pertinents pour la sécurité. Le CDF recommande un tel examen dès la fin des travaux de déménagement à Frauenfeld.

Les défis à venir doivent être surmontés

Dans l'administration fédérale, les documents à partir de l'échelon de classification CONFIDENTIEL doivent être chiffrés, conformément à l'Ordonnance concernant la protection des informations (OPrI). Les certificats utilisés à cet effet par les collaborateurs peuvent perdre leur validité pour diverses raisons. Tous les documents chiffrés doivent alors être rechiffrés, faute de quoi l'accès ne sera pas possible ultérieurement que si la SG PKI fournit à nouveau les paires de clés correspondantes. Ces clés doivent donc être conservées pendant une période prolongée. Jusqu'à présent, la durée de conservation n'est pas réglementée. Le problème s'aggravera au fil des ans, c'est pourquoi le CDF recommande de réglementer la

période de conservation. La SG PKI n'est en principe pas responsable des produits de chiffrement. Des outils de rechiffrement ont cependant dû être développés et déployés par l'OFIT.

Avec la dissociation de l'informatique civile et militaire au sein du Département fédéral de la défense, de la protection de la population et des sports, l'exigence a été formulée que la PKI fonctionne dans toutes les situations. Le projet mis en place à cet effet prévoit la création d'une instance propre de la SG PKI, qui sera exploitée par la Base d'aide au commandement (BAC). En cas de crise, la BAC pourrait continuer à exploiter cette instance indépendamment de la SG PKI. Le CDF soutient ces plans. Ainsi, la volonté du Conseil fédéral d'instaurer une PKI unique pour l'administration fédérale est respectée.

Texte original en allemand

Generelle Stellungnahme des Bundesamts für Informatik und Telekommunikation

> Die Prüfung ist in einer konstruktiven und fachlich versierten Weise durchgeführt worden. Die technischen und politischen Abhängigkeiten wurden gut erkannt und sind in die Beurteilung eingeflossen. Wir danken der EFK für die äusserst konstruktive Zusammenarbeit. Die Empfehlungen sind alle nachvollziehbar und werden gemäss Kommentierung weiter unten umgesetzt.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Die Public Key Infrastructure (PKI) ist aufgrund eines Bundesratsbeschlusses (BRB) vom 18. Dezember 1998 entstanden. Dieser BRB besagt, dass eine Zertifizierungsinfrastruktur für die Bundesverwaltung aufgebaut werden soll. Da das Eidg. Finanzdepartement (EFD) für eine Übergangszeit beauftragt wurde, Zertifizierungsdienste anzubieten, hat das damalige Bundesamt für Informatik mit dem Aufbau solcher Dienste begonnen. Nachfolgend entschied der damals dafür zuständige Informatikrat des Bundes (IRB) in den Jahren 2003–2005 mehrfach, dass in der Bundesverwaltung als Querschnittsdienstleistung eine einzige PKI betrieben wird. Das Bundesamt für Informatik und Telekommunikation (BIT) wurde damit offiziell beauftragt. Die vom Eidg. Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) bzw. der Führungsunterstützungsbasis (FUB) 2009 beantragte Ausnahmebewilligung zum Ausbau ihrer bis dahin nur für militärische Zwecke genutzten Swiss Defence PKI wurde daher verweigert. Das VBS wurde angewiesen ihre SD PKI mit der PKI des BIT zusammenzulegen, was zur heutigen SG PKI führte.

Mit BRB vom 13. Dezember 2013 ist die SG PKI zudem ein Teilprodukt des Standarddienstes (SD) Identity und Access Management geworden. Damit liegt die Führung beim Informatiksteuerungsorgan (ISB), für den Betrieb ist weiterhin das BIT verantwortlich.

Die SG PKI ist gemäss Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) zertifiziert, nebst bisher drei weiteren Anbietern auf dem Schweizermarkt. Die qualifizierten Zertifikate (Klasse A) entsprechen der manuellen Unterschrift einer natürlichen Person. Für diese Zertifizierung müssen sehr hohe Anforderungen an die Sicherheit der Infrastruktur, Prozesse und Produkte erfüllt sein. Die zuständige externe Zertifizierungsstelle KPMG führt jährlich vertiefte Audits durch. Die Eidgenössische Finanzkontrolle (EFK) prüfte ergänzend zu diesen Auditergebnissen.

1.2 Prüfungsziel und -fragen

Ziel der Prüfung ist, zu beurteilen, ob der Betrieb und die Weiterentwicklung der SG PKI beim BIT wirtschaftlich ist. Die Prüffragen lauten:

- Entspricht die Leistung der PKI den Anforderungen des Bundes?
- Erfüllt der Betrieb im BIT die Anforderungen an die Sicherheit und Verfügbarkeit?
- Stellt das BIT sicher, dass die PKI nachhaltig weiterentwickelt wird?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Cornelia Simmen (Revisionsleiterin) und Christian Brunner vom 20. Januar bis 7. Februar 2020 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger. Das Team ist durch externe Informations-Sicherheitsspezialisten unterstützt worden. Die Ergebnisbesprechung hat am 13. Februar 2020 stattgefunden. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Ergebnisbesprechung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von allen Beteiligten umfassend und termingerecht erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

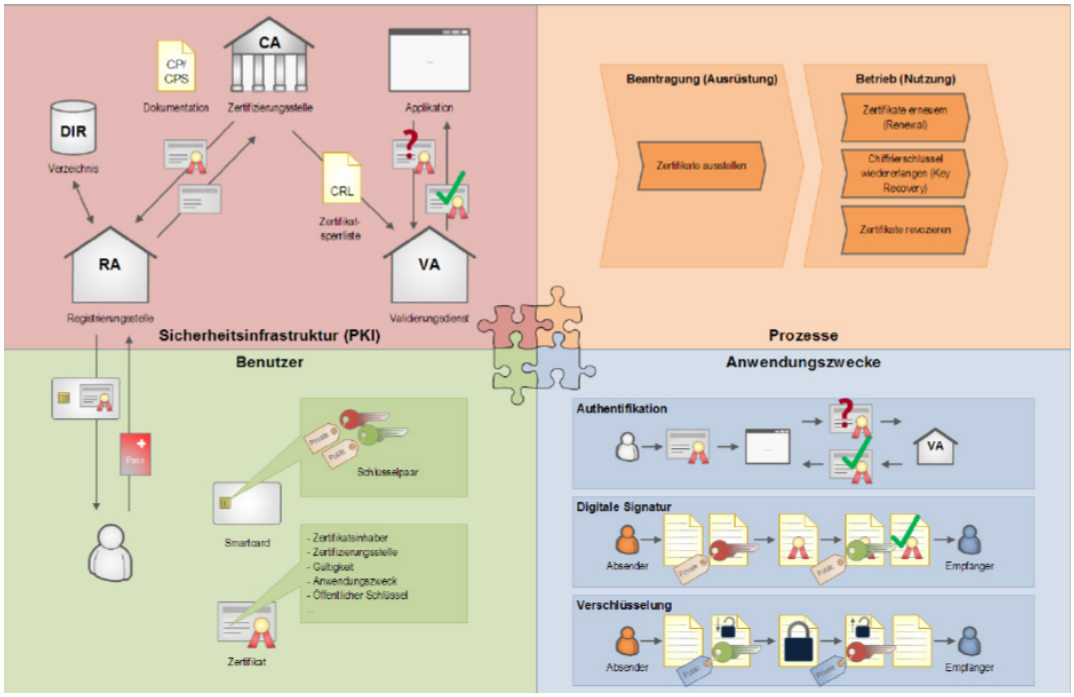
Die Schlussbesprechung fand aufgrund der Corona Massnahmen nicht wie geplant statt. Das Feedback erfolgte schriftlich und wurde mit dem Leiter Betrieb BIT am 8. April 2020 telefonisch ausdiskutiert.

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Amtsleitungen bzw. den Generalsekretariaten obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Anforderungen des Bundes

Eine PKI stellt digitale Zertifikate aus, verwaltet diese und stellt sicher, dass die Zertifikate während ihrer Gültigkeitsdauer validiert werden können. Die Vertrauenswürdigkeit eines Zertifikats - und damit auch der dahinterstehenden PKI - hängt von der Qualität der Identitätsüberprüfung einer Person ab. Um ein Zertifikat von der SG PKI zu erhalten, muss jede natürliche Person ihre Identität persönlich bei einem Local Registration Authority Officer (LRAO) mit gültigem Pass oder gültiger Identitätskarte nachweisen. Dieser Vorgang wird dokumentiert. Danach wird ein Zertifikat auf einem Hardware-Token (Smart Card) aktiviert und mit der erfassten Identität verknüpft. Damit ist sichergestellt, dass das Zertifikat während seiner Gültigkeit nachweisbar einer Person zugeordnet ist und bleibt. Die Zertifikate der SG PKI werden zur Authentifikation, zum Verschlüsseln oder zum Signieren eingesetzt.



Quelle: IKT-Grundschutz_CertifiedPKITerraNova

2.1 Anforderungen wurden hauptsächlich durch gesetzliche Vorgaben und Bundesratsbeschlüsse generiert

Die ZertES-Zertifizierung hat das BIT sehr früh bei Entstehung der PKI selber initiiert. Der IRB hat dies nicht verlangt, sondern mit Auflagen lediglich zur Kenntnis genommen. Das Ziel des BIT war, dass gegen innen und aussen die notwendige Vertrauensbasis für den breiten Einsatz von Zertifikaten geschaffen werden konnte. Die entsprechende Zertifikats-Klasse A[1] war nie für einen flächendeckenden Einsatz vorgesehen. Sie beinhaltet auch nur das Zertifikat für die qualifizierte Signatur bzw. seit jüngstem für das Behördensiegel. Im Einsatz sind von dieser Klasse bisher nur rund 260 Zertifikate, allerdings ist die Tendenz zunehmend.

[1] Entspricht der qualifizierten Signatur; äquivalent zur händischen Unterschrift einer natürlichen Person

Zwei der vier bisherigen Anbieter solcher Zertifikate haben vor Kurzem die Hardware-basierenden Lösungen durch Server-basierte ersetzt. Dies veranlasst bisherige Kunden (z. B. die Bundeskanzlei), sich anderweitig Hardware-basierende Zertifikate zu beschaffen. Das BIT hat schon mehrere dahingehende Anfragen erhalten.

Das grösste Volumen stellen die rund 130 000 Zertifikate der Klasse B[2] dar. Diese Klasse beinhaltet Zertifikate für die Authentifikation, die Verschlüsselung und die Signatur. Letztere entspricht mit kleinen Abweichungen denjenigen der Klasse A, kann jedoch nicht für qualifizierte Signaturen nach ZertES verwendet werden. Primär benutzen die Mitarbeitenden der Bundesverwaltung und Kantone sowie die Angehörigen der Armee die Smart Card mit den Zertifikaten zur Zweifaktor-Authentifikation am Arbeitsplatzsystem. Verschlüsselung und Signaturen werden je nach Amt unterschiedlich oft eingesetzt. Über 60 000 weitere auf Smart Card geladene pre-staged Klasse B Zertifikate stehen bereit, um aktiviert und mit einer Person verknüpft zu werden. Die weiteren Klassen C-E haben teilweise administrativen Charakter und basieren auf Software. Darunter sind auch Speziallösungen für Kunden, die nicht zum SD gehören, z. B. im Bereich der Passausstellung.

Für alle Zertifikatsklassen wird dieselbe Infrastruktur verwendet und grundlegend auch dieselben Prozesse für die Ausstellung der Zertifikate. Dadurch wirkt der hohe Sicherheitslevel der ZertES bei allen Zertifikaten. Den Kunden steht der Prozess P035 zur Verfügung, um Anforderungen an das ISB zu melden. Dies funktioniert bisher jedoch nicht wie bei anderen SD. Sehr oft wird der direkte Weg zu den Mitarbeitenden der PKI gewählt, um irgendwelche Anliegen durchzusetzen. Dieses Vorgehen ist eine Altlast aus der Zeit bevor die SG PKI zum SD wurde.

Es konnten keine konkreten Nachweise gefunden werden, dass bei der Entwicklung der SG PKI Anforderungen gestellt worden sind. Vielmehr haben die Entwickler der PKI entlang den Anforderungen der ZertES und gemäss BRB die verschiedenen Zertifikatsklassen gebaut. Auch war das ISB in der Definition der Zertifikatsklassen noch nicht involviert, da die SG PKI erst später zum SD wurde. Seitens LB besteht oft auch ungenügendes oder falsches Wissen zu den Zertifikaten und deren Einsatz. Dies gilt nicht für die FUB, deren Kryptospezialisten aktiv bei der SG PKI mithelfen. Das Competence Center PKI der FUB stellt zunehmend neue Anforderungen. Darauf wird im Kapitel 4.4 eingegangen.

Die heutige Authentifikation am Arbeitsplatzsystem mit dem Zertifikat auf der Smart Card wird oft als benutzerunfreundlich reklamiert. Es existieren heute bereits einfachere Zweifaktor-Authentifikationen in unterschiedlicher Ausprägung. Sowohl das BIT wie auch das ISB verfolgen die Entwicklungen und streben Vereinfachungen an. Nach heutigem Stand wird jedoch daran festgehalten, dass die heutigen Hard-Crypto-Token[3] basierenden Zertifikate als Basis dienen werden. Damit wird auch der Registrierungsprozess für den Erhalt dieser Zertifikate nicht angetastet.

Beurteilung

Bei Anforderungen muss differenziert werden, wer die Kunden sind. Wichtig sind die LRAO, welche den Ausstellprozess der Zertifikate verantworten. An diese Mitarbeitenden werden hohe Anforderungen seitens SG PKI gestellt, da deren Arbeit absolut zuverlässig sein muss. Von Ihnen kommen Anforderungen jedoch weniger bezüglich Produkte, sondern mehr zur Vereinfachung der Prozesse und beim Incident-Management. Die grösste Kundengruppe sind die Mitarbeitenden, welche die unterschiedlichen Zertifikate einsetzen. Diese fühlen

[2] Entspricht der fortgeschrittenen Signatur. Nicht äquivalent mit der eigenhändigen Unterschrift.

[3] Hardwarebasierte Komponente zur sicheren Verwahrung eines Zertifikates resp. eines elektronischen Schlüssels

sich dadurch im täglichen Arbeitsumfeld eher eingeschränkt. Ein Grossteil versteht nicht, dass authentifizieren, verschlüsseln und signieren Dienste sind, die nicht in der Verantwortung der SG PKI liegen. Daher sind deren Anforderungen weniger die Zertifikate betreffend, sondern bezüglich der Vereinfachung bei deren Einsatz. Die Verwaltungseinheit bzw. die Kantone sind die LB, welche die Dienstleistungen der SG PKI bezahlen. Diese interessiert hauptsächlich der Preis der einzelnen Produkte und ein möglichst störungsfreier Betrieb. Wenn die LB Anforderungen stellen, dann kommen diese meistens von den Benutzenden her.

Der Entscheid des BIT nebst der bestehenden Klasse B die zusätzliche Klasse A nach ZertES zertifizieren zu lassen, ist aus Sicht der EFK zielführend gewesen, auch wenn der IRB formell dazu keinen Auftrag gegeben hatte. Die SG PKI hat sich durch die Einhaltung der strengen gesetzlichen Vorgaben die notwendige Vertrauenswürdigkeit auch ausserhalb der Bundesverwaltung gesichert und kompensiert damit ein eher schwaches Anforderungsmanagement. Die EFK ist aus diesem Grund der Ansicht, dass die Zertifizierung auch weiterhin wertvoll ist, auch wenn die Klasse A Zertifikate nicht das Hauptgeschäft der PKI ausmachen. Mit der Einführung des Behördensiegels und aufgrund der neuen Marktverhältnisse wird die Nachfrage nach diesen Zertifikaten wachsen. Die Anforderungen an die Zertifikatsklasse A ergeben sich aus den gesetzlichen Vorgaben. Die Klasse B wurde dagegen mit dem BRB zur flächendeckenden Zweifaktor-Authentifikation und zusätzlichen Vorgaben (z. B. bezüglich Verschlüsselung) stark ausgebreitet. Sie beinhaltet drei Zertifikate.

Anforderungen kommen heute am ehesten von Projekten, welche Zertifikate einsetzen wollen oder von Seiten der FUB. Sowohl das BIT wie auch das ISB müssen aktiv dazu beitragen, dass eingehende Anforderungen kanalisiert, darüber in den dafür vorgesehenen Gremien entschieden und erst danach von der PKI umgesetzt werden. Das ISB hat sich bisher bei der SG PKI zu wenig eingebracht. Es sollte zukünftig seine Steuerungs- und Führungsfunktion aktiver wahrnehmen.

Ergänzend muss bemerkt werden, dass weder die PKI noch das ISB oder das BIT verhindern können, dass anderweitige Zertifikate als diejenigen der SG PKI eingesetzt werden. Allerdings ist solches nur im Bereich von Fachanwendungen oder bei Websites möglich. Dies muss jedoch in den Informations- und Datenschutzkonzepten ausgewiesen werden.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt dem Bundesamt für Informatik und Telekommunikation die Kunden anzuweisen, Anforderungen an den Standarddienst Public Key Infrastructure über den dafür vorgesehenen Prozess P035 des Informatiksteuerungsorgans anzumelden.

Stellungnahme des BIT

Das BIT wird die Empfehlung 1 in Kooperation mit dem ISB umsetzen.

3 Sicherheit und Verfügbarkeit

3.1 Ein hoher Sicherheitslevel ist erreicht, aber Systemüberwachung und Logging müssen verbessert werden

Durch die Zertifizierung nach ZertES sind die Sicherheitsanforderungen an die Infrastruktur und die Prozesse hoch. Dabei gelten auch zahlreiche Europäische Standards (ETSI EN) für die verschiedenen Komponenten und Zertifikate. Deren Anforderungen müssen ebenfalls eingehalten werden, damit die Dienste der SG PKI schweizweit auch ausserhalb der Bundesverwaltung anerkannt sind. In jährlichen externen Audits wird die Umsetzung der Anforderungen immer wieder überprüft. Die externe Überprüfung kostet 150 000 Franken pro Jahr. Die Sicherheitsberichte dieser Audits zeigen immer wieder Verbesserungspotential. Es sind auch einige Schwachstellen vorhanden, welche von den externen Auditoren in die zweithöchste Kritikalitätsstufe (erheblich) eingestuft worden sind. Solche müssen innerhalb eines Jahres behoben werden, sonst wird die Zertifizierung nicht mehr bestätigt.

Die EFK hat folgende Schwachstellen eruiert, welche sich mehrheitlich mit denen der externen Audits decken:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Keine Design-Reviews

[redacted]

[redacted]

[redacted]

Beurteilung

Die Zertifizierung gemäss ZertES zwingt die SG PKI, die damit verbundenen hohen Sicherheitsanforderungen kontinuierlich zu erfüllen. Durch die jährlichen Audits wird das Risiko

von Sicherheitslücken minimiert. Die Zertifizierung hat auch den Vorteil, dass Anforderungen seitens der LB, welche den Sicherheitslevel beeinträchtigen würden oder gegen die gesetzlichen Vorgaben verstossen, ohne lange Diskussionen abgelehnt werden können. So ist gewährleistet, dass die erreichte Vertrauenswürdigkeit der ausgestellten Zertifikate und damit die breite Anerkennung der SG PKI keinen Schaden nimmt. Die EFK erachtet die Kosten der Zertifizierung gegenüber dem Nutzen der jährlichen Audits als angemessen. Der hohe Sicherheitslevel garantiert, dass die Zertifikate der SG PKI nur mit grossem Aufwand korrumpiert werden könnten.

In den folgenden Bereichen sind aus Sicht der EFK Verbesserungen notwendig.

Um sicherheitsrelevante Ereignisse [redacted]

[redacted] Bei einem sicherheitsrelevanten Vorkommnis kann heute [redacted].

Bisher wurden keine externen Design-Reviews durchgeführt. Dabei werden die System- und Netzwerkarchitektur sowie sicherheitsrelevante Betriebsabläufe überprüft, was bei den Zertifizierungs-Audits nicht erfolgt. Backup-Probleme, wie sie im 2014 auftraten, hätten durch ein solches Review vermieden werden können. Die Ursachen, welche zu den Problemen führten, wären vorher entdeckt worden. Es ist aus Sicht der EFK sinnvoll, ein solches Review nach Inbetriebnahme der neuen Infrastruktur in Frauenfeld in Auftrag zu geben.

Die [redacted] hat bisher noch nie zu grösseren Problemen geführt. Gemäss Schutzbedarfsanalyse bestehen [redacted]

Da die [redacted] bereits in Realisierung ist, verzichtet die EFK auf eine entsprechende Empfehlung.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt dem Bundesamt für Informatik und Telekommunikation [redacted]

Stellungnahme des BIT

Im Rahmen des Technologie-Life-Cycle und der Verfügbarkeitserweiterung [redacted]

Empfehlung 3 (Priorität 2)

Die EFK empfiehlt dem Bundesamt für Informatik und Telekommunikation [redacted]

Stellungnahme des BIT

Die Empfehlung wird auch mit der Technologieerneuerung PKI-NextGen mitberücksichtigt und umgesetzt.

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt dem Bundesamt für Informatik und Telekommunikation nach Inbetriebnahme der PKI-Infrastruktur in Frauenfeld ein externes Design-Review machen zu lassen.

Stellungnahme des BIT

Die Empfehlung wird dann umgesetzt werden können, wenn die Technologieerneuerungen und Implementierung in CAMPUS Frauenfeld abgeschlossen sind.

3.2 Probleme müssen speditiver gelöst werden

Die SG PKI hat in den fast 20 Jahren ihres Betriebes bisher nie einen grösseren Ausfall gehabt. Auftretende Probleme (Incidents) müssen in der Regel nicht innert Stundenfrist behoben werden. Dennoch sollten sie rasch abgeklärt und nachfolgend zeitnah erledigt werden. Die EFK hat Kenntnis von Incidents, auf die monatelang nicht reagiert wurde. Allerdings gehen bei der PKI auch oft Störungsmeldungen ein, welche diese nicht betreffen. Der Endbenutzer versteht mehrheitlich nicht, dass beim Anmelden, Signieren oder Verschlüsseln nicht die Zertifikate der PKI das Problem verursachen, sondern die dahinterliegenden Dienste und wenden sich dann an die falsche Stelle. Incidents, welche eine massive und/oder flächendeckende Einschränkung zur Folge haben, werden durch die Security Officer aufgenommen und weiterverfolgt. Nach der Behebung wird analysiert und festgehalten, was verbessert werden muss (lessons learned). Die Anzahl solcher Vorfälle ist gemäss geführten Nachweisdokumenten durchschnittlich unter 10 pro Jahr.

Die LRAO an den über 200 Standorten in der ganzen Schweiz sind bezüglich Incidents in einer speziellen Situation und müssen rasch Hilfe erhalten. Bei ihnen treten Probleme in der Regel auf, wenn für eine anwesende Person Zertifikate ausgestellt oder erneuert werden müssen. Kann dies nicht erfolgen, so muss sich diese Person zu einem späteren Zeitpunkt nochmals zum LRAO begeben, was bei allen Beteiligten zu Unmut führt.

Das BIT hat die Notwendigkeit erkannt, das Incidentmanagement zu verbessern. Dazu sind verschiedene Neuerungen in die Wege geleitet worden. Jedem Produkt sind nun Product Owner zugewiesen. Diese sollen proaktiv auf die Kunden zugehen und ihr Produkt betreuen. Im Gegenzug wird die bisherige Mailadresse für Problemmeldungen aufgehoben. Alle Incidents müssen zukünftig über den normalen Helpdesk laufen. Damit werden die Meldungen in Remedy erfasst, sind nachvollziehbar und unterliegen einem Eskalationsprozess, wenn das Problem nicht innert einer bestimmten Frist gelöst ist. Ein entsprechend

[redacted]

geschulter Helpdesk ist somit die Grundvoraussetzung für die Wirksamkeit dieser Massnahme. Die eingehenden Incidents werden danach in einer täglich morgens früh stattfindenden Sitzung besprochen, beurteilt und einem Product Owner zur Erledigung zugeteilt.

Seit einiger Zeit ist die Information über Störungen verbessert worden. Die Meldungen werden nun über die auf jedem Client installierte Software IBI-aws[5] verbreitet. Weiter sind neue Merkblätter in Arbeit. Für den Benutzer von Zertifikaten sind die publizierten Fact Sheets jedoch wenig verständlich. Deshalb wird nun versucht, die Aufgaben und den Zweck der PKI vereinfacht darzustellen. Dadurch erhofft sich der Betrieb weniger Fehlermeldungen, welche nicht die PKI betreffen.

Beurteilung

Die Führung der PKI hat erkannt, dass gemeldete Incidents schneller abgeklärt und behoben werden müssen. In der Vergangenheit sind notwendige Änderungen durch unkoordinierte Vorgehensweisen zu lange liegen geblieben. Daher sind Verbesserungen bei der Erfassung, der Triage, der Abarbeitung und Kommunikation eingeleitet worden. Die aufgesetzten Prozesse mit täglichen Kurzsitzungen und einer nachvollziehbaren Erfassung der eingehenden Meldungen muss sich in der Praxis noch festigen.

Da keine erhöhte Verfügbarkeitsanforderung an die Produkte der PKI besteht, müssen Probleme nicht innert Stundenfrist behoben werden. Probleme betreffen oft auch nur einzelne Benutzende oder eine Benutzergruppe, wobei diese meistens nicht in ihrer Arbeit eingeschränkt werden. Aber es gab auch schon Probleme, die dazu führten, das Mitarbeitende nicht mehr arbeiten konnten. Vor allem die LRAO, welche beim Aktivieren oder Revozieren von Zertifikaten auf Schwierigkeiten stossen, müssen rasch direkt von einem PKI-Spezialisten Hilfe erhalten können. Die EFK sieht die nun eingesetzten Product Owner als diese Ansprechpersonen. Der Helpdesk ist als Anlaufstelle für die LRAO nicht geeignet.

Die SG PKI muss das Incident-Management verbessern d. h. gegenüber den Kunden rascher reagieren. Die aufgesetzten Verbesserungen sind aus Sicht EFK geeignet, dass die PKI Incidents zeitnaher erledigt und dadurch das Image der PKI gegenüber den LB verbessert werden kann. Da bereits Verbesserungen in Umsetzung sind, verzichtet die EFK auf eine diesbezügliche Empfehlung.

[5] Software zur zielgenauen Information betroffener Anwender über Incidents oder Wartungen.

4 Nachhaltigkeit

4.1 Hohe Vertrauenswürdigkeit zu überschaubaren Kosten

Die Software der SG PKI ist zum grössten Teil seit Beginn eine kontinuierliche Eigenentwicklung. Der Sourcecode hat über die fast 20 Jahre ein beachtliches Volumen erreicht. Die verwendete Programmiersprache wird im Bundesumfeld wenig eingesetzt. Die SG PKI muss daher auf externe Spezialisten zurückgreifen. Durch die Eigenentwicklung von langjährigen Mitarbeitenden ist ein hohes Verständnis und breites Know-how für die Produkte der SG PKI vorhanden. Dennoch müssen bei Änderungen Externe mithelfen, da die internen Ressourcen zu knapp sind.

Um die Wartbarkeit des Sourcecode zu verbessern, ist die Entwicklungsgruppe der SG PKI daran, diesen zu modularisieren. Ziel ist, dass pro Certificate Authority (CA) getrennte Programme bestehen.

Alle Komponenten der SG PKI sind grundsätzlich auch auf dem Markt erhältlich. Auch die kommerziellen Produkte müssen den Sicherheitsanforderungen genügen, welche für die PKI gelten. Schon seit längerem kauft die SG PKI die Webserver-Zertifikate der Klasse C extern ein. Bei diesem Entscheid wurden Aufwand (d. h. die Kosten für die Anerkennung eigener Zertifikate bei externen Webseiten-Betreibern) und Nutzen abgewogen. Der Einkauf hat sich als vorteilhafter erwiesen. Dagegen haben sich beim Einsatz von extern beschafften Druckerzertifikaten die Lizenzkosten innert kurzer Zeit stark erhöht. Dieses Beispiel zeigt, dass rasch eine starke Lieferantenabhängigkeit entstehen kann.

Der Betrieb der heutigen SG PKI kostet pro Jahr 7,7 Mio. Franken. Dieser Betrag wird über die Produktpreise den LB weiterverrechnet. Grössere Investitionen oder Erweiterungen werden wie bei anderen SD über zentral eingestellte Finanzmittel des ISB realisiert.

Beurteilung

Der Vorteil bei Eigenentwicklungen liegt in der vollen Transparenz über die Funktionsweise der Programme. Der Sourcecode kann jederzeit einer internen oder externen Überprüfung unterzogen werden. Dies ist im Sicherheitsbereich eine wichtige Grundvoraussetzung. Bei eingekauften Produkten hat der Käufer oft keine Einsicht in den Sourcecode und muss sich mit Gutachten oder Zertifizierungen behelfen. Den kryptografischen Mechanismen der SG PKI, welche die Zertifikate absichern, kann aufgrund der Eigenentwicklung ein grosses Vertrauen entgegengebracht werden. Der Bund kann aufgrund der Eigenentwicklung auch Abhängigkeiten von externen Lieferanten vermeiden und die Kosten bzw. den Preis für die LB selber steuern.

Der Unterhalt und Betrieb einer PKI ist allerdings aufwändig. Es braucht dazu spezielles und nur knapp verfügbares Fachwissen. Die technische Entwicklung, Änderungen in der IT-Sicherheitspolitik, neue gesetzliche Vorgaben sowie sich rasch ändernde Ansprüche aufgrund der fortschreitenden Digitalisierung zwingen zu kontinuierlichen Anpassungen. Daher müssen die Mitarbeitenden der SG PKI agil sein und sich kontinuierlich weiterbilden. Die SG PKI ist mit rund 30 Mitarbeitenden eher knapp dotiert. Sie besteht aus langjährigen Mitarbeitenden. Vereinzelt sind diese sogar seit Beginn der Entwicklung der Zertifikatsdienste dabei. Alle Abgänge sind mit einem Abfluss von viel Fachwissen verbunden. Um sich trotz Eigenentwicklung nicht abhängig von Externen zu machen, muss die SG PKI sicherstellen, dass genügend Mitarbeitende mit dem notwendigen Fachwissen zur Verfügung stehen.

Die EFK beurteilt die Kosten für die Bereitstellung der Zertifikatsdienste als überschaubar. Ob es kommerzielle Angebote gibt, welche die Anforderungen des Bundes zu einem tieferen Preis abdecken könnten, wurde im Rahmen dieser Prüfung nicht abgeklärt. Ein Wechsel von der Eigenentwicklung zu einem kommerziellen Produkt würde aber mit hoher Wahrscheinlichkeit eine lange Amortisationszeit haben. Zudem müsste sorgfältig beurteilt werden, welche Risiken bei einem externen Bezug eingegangen würden.

4.2 Das Change-, Release- und Life-Cycle-Management muss verbessert werden

Das Change- und Release Management folgt heute dem BIT-Prozess und nutzt dessen Tools (Jira, Confluence). Die PKI ist seit Kurzem in die Release-Konferenz des BIT eingebunden. So können geplante Änderungen bzw. Updates angemeldet und besser koordiniert werden. Damit passt sich die PKI dem übrigen BIT an d. h. es gibt sein bisheriges Silodenken auf und schafft mehr Transparenz. Zur Nachvollziehbarkeit wird ein PKI-Plan über vorgesehene und erfolgte Releases geführt.

In der Vergangenheit sind Changes oder auch Problemmeldungen, welche einen Change auslösten, oft längere Zeit liegen geblieben. Wie bei den Incidents führte auch das zu Unzufriedenheit bei den LB. Insbesondere die FUB ist mit den Reaktionszeiten der PKI nicht zufrieden. Die Liste mit unerledigten Problemen dieses LB ist gross (backlog). Sie geht jedoch mindestens teilweise auf die nicht ganz korrekt durchgeführte Integration der Swiss Defence PKI zurück. Der Handlungsbedarf ist seitens SG PKI erkannt und die offenen Punkte sollen nun möglichst rasch bearbeitet werden.

Für das Life-Cycle-Management (LCM) ist grundsätzlich der LE verantwortlich. Er hat dafür zu sorgen, dass die Hardware, die Software und andere zum Betrieb der Dienste notwendigen Komponenten zeitgerecht erneuert werden. Dies bedingt eine mehrjährige Planung mit genügend Vorlaufzeit. Bei der SG PKI existiert diese nicht in der erwarteten Form. Es wird zu kurzfristig gehandelt. Die letzte Migration auf eine neue Plattform verlief chaotisch. Ein Ausfall der PKI konnte nur knapp verhindert werden. Auch die nächste anstehende Plattformablösung wurde zu spät in Angriff genommen. Sie hat bereits mindestens ein Jahr Verspätung.

Die Kunden werden vorgängig über die PKI Website und via direkte Kanäle (z. B. LRAO Treffen) über bevorstehende Releases und Changes informiert. In der Regel finden ein bis zwei Releases und mehrere Changes pro Jahr statt.

Das ISB führt die SG PKI wie jeden anderen Standarddienst wirtschaftlich und funktional über die dafür vorhandenen Instrumente d. h. Roadmap, Produktkatalog, Tarife und Benchmarking. Das Angebot, was die PKI leisten und kosten soll, wird aufgrund der Anforderungen aus den Departementen gesteuert. Bei der eigentlichen Produkt- und Serviceentwicklung hat sich das ISB bisher nicht vertieft eingebracht. Damit nimmt es seine Führungsrolle zu wenig wahr und überwacht die SG PKI nicht entsprechend.

Beurteilung

Das Changemanagement sollte verbessert werden, nicht nur seitens PKI, sondern auch beim ISB. Die EFK erwartet, dass das ISB aktiv eingebunden wird in die Planung der Changes. Die bisherige Praxis hat einen direkten Zusammenhang mit dem Anforderungsmanagement

(siehe Empfehlung 1). Wenn zukünftig die Kunden Änderungswünsche über den dafür vorgesehenen Prozess beim ISB deponieren müssen, so bedingt dies eine engere Zusammenarbeit und eine stärkere Führungsrolle des ISB. Anträge auf Individualentwicklungen sollen vom ISB abgeklärt, analysiert und genehmigt oder abgelehnt werden. Dies entspricht der normalen Rolle des ISB in einem SD.

Das Release Management hat einen guten Eindruck hinterlassen, auch wenn damit nicht alle Kunden zufrieden sind. Es obliegt dem Betreiber zu entscheiden, wie oft es notwendig ist, Updates einzuspielen. Die EFK sieht eine positive Entwicklung in der Auflösung der bisherigen «PKI Silos».

Auch wenn das BIT für das LCM verantwortlich ist, so sollte das ISB mindestens bezüglich der Roadmap involviert werden. Es muss sichergestellt werden, dass genügend Vorlaufzeit besteht, bevor Infrastrukturen ersetzt werden müssen. Ansonsten besteht das Risiko, dass durch zu knappe Testphasen nachfolgend in der Produktion unvorhergesehene Probleme auftreten, die auch zu einem Ausfall der SG PKI führen könnten.

Empfehlung 5 (Priorität 1)

Die EFK empfiehlt dem Informatiksteuerungsorgan Bund sich beim Change- und Release- sowie Life-Cycle-Management der SG PKI aktiv einzubringen und die Tätigkeiten zu überwachen.

Stellungnahme des ISB

Das ISB wird die Prozesse, Methoden, Tools und Rollen prüfen und gegebenenfalls anpassen. Als Basis soll das mit dem BIT bereits weiterentwickelte Zusammenarbeitsmodell für die Produktentwicklung im Bereich des Services eIAM dienen.

4.3 Verschlüsselung wird über die Zeit problematisch

Grundsätzlich müssen Informationen gemäss Informationsschutzverordnung (ISchV) ab der Klassifizierungsstufe VERTRAULICH verschlüsselt übertragen und auf Systemen gespeichert werden. Dieses Vorgehen ist an den einzelnen Mitarbeitenden gebunden, welcher klassifizierte Dokumente verfasst. Die SG PKI stellt mit der Klasse B die Zertifikate für die Verschlüsselung von Dateien und E-Mailverkehr zur Verfügung, nicht aber die Werkzeuge, mit welchen nachfolgend verschlüsselt wird.

Beim Austritt von Mitarbeitenden wird die Smart Card mit den Zertifikaten vernichtet. Damit sind die Schlüsselpaare nur noch bei der SG PKI vorhanden. Sind nicht mehrere Personen berechtigt auf verschlüsselte Dokumente zuzugreifen, so sind diese nicht mehr direkt lesbar. Daher sollte vor Austritt von Mitarbeitenden sichergestellt werden, dass der Zugriff auf verschlüsselte Informationen weiterhin möglich ist, wenn notwendig durch Umschlüsselung auf eine andere Person. Wenn dies nicht erfolgt, werden immer mehr Informationen unzugänglich sein, ausser die SG PKI wird jedes Mal involviert um alte Zertifikate wieder verfügbar zu machen. Dies ist mit einem komplizierten und aufwändigen Prozess verbunden. Auch bei der regelmässigen Erneuerung der persönlichen Zertifikate wird die Umschlüsselung empfohlen. Die vorgängigen Zertifikate können zwar über eine bestimmte Zeit weiterhin zum Lesen von verschlüsselten Informationen verwendet werden, aber nicht mehr zum zurückschreiben derselben.

Auch bei der Übermittlung von klassifizierten Informationen oder heiklen Personendaten via E-Mail ergibt sich dasselbe Problem der Umschlüsselung, weil viele Mitarbeitende das

Mailsystem quasi als Archiv benutzen und auch hier die der Verschlüsselung zugrundeliegenden Zertifikate verfallen können.

Die Verschlüsselung gehört grundsätzlich nicht zu den Aufgaben der SG PKI. Die Umschlüsselungsproblematik hat trotzdem bei ihr aufgeschlagen. Es mussten dazu spezielle Programme erstellt und verteilt werden. Problematisch sind auch die fehlenden Regelungen hinsichtlich der Aufbewahrungsdauer oder Archivierung der Schlüsselpaare.

Beurteilung

Da durch die ISchV auf Dokumentenebene verschlüsselt werden muss, erfolgt dies über die personenbezogenen Zertifikate der Klasse B. Die EFK stellt in diesem Zusammenhang immer wieder fest, dass zu viele Dokumente unnötiger- bzw. fälschlicherweise klassifiziert und auch verschlüsselt werden. Diese Verschlüsselungsproblematik wird sich auch mit der Einführung des neuen Geschäftsverwaltungssystems der Bundesverwaltung (acta nova) nicht entschärfen. Das Problem mit den alten Schlüsseln und deren Aufbewahrung bei der SG PKI wird sich über die Jahre drastisch verschärfen. Daher sollte dringend geregelt werden, wie lange das BIT verpflichtet ist, die Schlüsselpaare aufzubewahren. Es muss auch grundsätzlich geregelt werden, wie die Umschlüsselung über die Zeit systematisch gelöst werden kann. Die Verwaltungseinheiten sind sich dieser Problematik zu wenig bewusst.

Empfehlung 6 (Priorität 2)

Die EFK empfiehlt dem Informatiksteuerungsorgan Bund die Aufbewahrung der Schlüsselpaare sowie die Umschlüsselungsproblematik für alle Beteiligten verbindlich zu regeln oder regeln zu lassen.

Stellungnahme des ISB

Der Umgang mit Schlüsseln und deren Aufbewahrung wird von der ISchV und den nutzenden Anwendungen geprägt. Die SG PKI ist nur der Schlüssellieferant. Eine Lösung muss übergreifend abgestimmt werden. Das ISB wird eine Expertise beauftragen und Lösungsansätze evaluieren. Für darauf gestützte Umsetzungsmassnahmen wird das ISB die SG PKI beauftragen.

4.4 Zielführende Entscheide zur PKI in allen Lagen

Wie im Kapitel 1.1 dargelegt, basiert die SG PKI auf mehreren Bundesratsbeschlüssen. Die Zusammenlegung der von der FUB ausgerollten PKI mit derjenigen des BIT hatte damals einen 2-stellige Millionenbetrag gekostet. Die genauen Kosten sind nicht mehr nachvollziehbar, da keine Vollkostenrechnung geführt wurde. Der Entscheid zur Entflechtung von zivilen und militärischen Bereichen führt nun zum Anspruch des VBS, dass die PKI in allen Lagen funktionieren muss. Bereits 2017 - also noch vor Abschluss der Migrationsarbeiten zur SG PKI - wurde dazu eine externe Studie vom ISB in Auftrag gegeben. Diese kam zum Schluss, dass eine redundante SG PKI mit Standort bei der FUB und beim BIT die einfachste Lösung darstellen würde. Aufgrund der Studie wurde im August 2018 das Projekt PKI in allen Lagen (PKIiaL) gestartet mit dem Leiter Betrieb BIT als Projektauftraggeber. Dieser leitet bis heute die regelmässig stattfindenden Sitzungen des Projektausschusses (PAS). In diesem sitzen nebst Vertretern des ISB und des BIT auch der Chef Erneuerung FUB und der Leiter Informatik VBS.

Zur Erarbeitung der Detailanforderungen der FUB an die PKIiaL fanden bis heute mehrere Workshops statt. Aufgrund der Resultate wurde entschieden, dass für die FUB innerhalb

der bestehenden SG PKI eine eigene Instanz erstellt werden soll, welche die Bedürfnisse in einer ausserordentlichen Lage erfüllt. Die vom Projektausschuss am 3.10.2019 genehmigte Arbeitshypothese hält fest:

- Die Gesamtverantwortung für die PKI ist im BIT.
- Die FUB betreibt eine in sich lauffähige Instanz der SG PKI für sämtliche Kernleistungen über alle Lagen. Ein reiner Service gemäss Projektstudie PKIiaL erfüllt die Anforderungen der Entflechtung V nicht.
- Die FUB stellt die notwendigen Ressourcen für den Betrieb der eigenen Instanz.

Die EFK geht davon aus, dass die durch den PAS getroffenen Grundsatzentscheide umgesetzt werden, auch wenn diese vom Projektteam immer wieder in Frage gestellt werden.

Beurteilung

Die vom PAS angestrebte Lösung gibt der FUB die Möglichkeit, bei einer ausserordentlichen Lage oder beim Ausfall der SG PKI, ihre Instanz unabhängig weiter zu betreiben. Es bestehen aufgrund der eingesehenen Dokumente und der geführten Interviews aus Sicht der EFK keine stichhaltigen Argumente für eine eigenständige PKI bei der FUB. PKIiaL muss die Anforderungen definieren, welche von der heutigen SG PKI nicht erfüllt werden. Die Lösungen zu finden, um diese Anforderungen umzusetzen, ist Aufgabe des BIT in Zusammenarbeit mit dem ISB.

Die EFK hält fest, dass der Bundesratsentscheid zu einer PKI für die ganze Bundesverwaltung nach wie vor gilt und durchzusetzen ist.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Bundesgesetz über den eidgenössischen Finanzhaushalt (Finanzhaushaltgesetz, FHG) vom 7. Oktober 2005, SR 611.0
Finanzhaushaltverordnung (FHV) vom 5. April 2006, SR 611.01
Bundesgesetz über die Eidgenössische Finanzkontrolle (Finanzkontrollgesetz, FKG) vom 28. Juni 1967. SR 614.0
Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES) vom 18. März 2016, SR 943.03
Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Verordnung über die elektronische Signatur, VZertES) vom 23. November 2016, SR 943.032
Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 23. November 2016, SR 943.032.1
Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (Bundesinformatikverordnung, BinfV) vom 9. Dezember 2011, SR 172.010.58
Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung vom 16. Januar 2019
Si001 - IKT-Grundschutz in der Bundesverwaltung vom 19. Dezember 2013
Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) vom 4. Juli 2007, SR 510.411

Anhang 2: Abkürzungen

BIT	Bundesamt für Informatik und Telekommunikation
BRB	Bundesratsbeschluss
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
FUB	Führungsunterstützungsbasis
IRB	Informatikrat Bund
ISB	Informatiksteuerungsorgan Bund
LB	Leistungsbezüger
LRAO	Local Registration Authority Officer
PAS	Projekt Ausschuss
PKI	Public Key Infrastructure
SD	Standarddienst
SG	Swiss Government
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport

Anhang 3: Glossar

CA	Certificate Authority Ist die Organisation, welche das CA-Zertifikat bereitstellt und die Signatur von Zertifikatsanträgen übernimmt.
LRA	Local Registration Authority Bei der SG PKI ist die LRA jene Stelle, bei der natürliche Personen vorsprechen müssen, um Zertifikate erhalten zu können. Der LRA Officer prüft die Richtigkeit der Daten (Reisedokument, Antrag usw.) und aktiviert die Zertifikate auf dem dafür vorgesehenen Datenträger.
PKI	Public Key Infrastructure ist ein System, das digitale Zertifikate ausstellt, verteilt und prüft. Die Zertifikate werden zur Absicherung rechnergestützter Kommunikation verwendet.
Einfache elektronische Signatur	Gemäss ZertES sind dies Daten, «die anderen elektronischen Daten beigefügt oder die logisch mit ihnen verknüpft sind und zu deren Authentifizierung dienen». Das Zertifikat stellt beispielsweise die Integrität eines Dokuments sicher.
Fortgeschrittene elektronische Signatur	Im Gegensatz zur einfachen elektronischen Signatur dient die fortgeschrittene elektronische Signatur der Personenidentifikation. Das bei der Signatur ausgestellte Zertifikat ordnet die Unterschrift der Inhaberin oder dem Inhaber zu, d. h., dass diese die alleinige Kontrolle über die Mittel haben, mit der die Signatur erstellt wird.
Qualifizierte elektronische Signatur	Die qualifizierte elektronische Signatur besitzt im Grundsatz dieselben Eigenschaften wie die fortgeschrittene; jedoch beruht sie auf einem qualifizierten Zertifikat, das von einem gemäss ZertES anerkannten Anbieter ausgestellt wird.

Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).