INFORMATIKPROJEKTE

Prüfung der Identitäts- und Zugriffsverwaltung eIAM

Bundeskanzlei – Bereich Digitale Transformation und IKT-Lenkung

EFK-24141

VERSION INKL. STELLUNGNAHMEN

17.02.2025

EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
CONTROLLA FEDERALA DA FINANZAS
SWISS FEDERAL AUDIT OFFICE

DOKUMENTINFORMATION

BESTELLADRESSE ADRESSE DE COMMANDE INDIRIZZO DI ORDINAZIONE ORDERING ADDRESS	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45 3003 Bern Schweiz
BESTELLNUMMER NUMÉRO DE COMMANDE NUMERO DI ORDINAZIONE ORDERING NUMBER	104.24141
ZUSÄTZLICHE INFORMATIONEN COMPLÉMENT D'INFORMATIONS INFORMAZIONI COMPLEMENTARI ADDITIONAL INFORMATION	www.efk.admin.ch info@efk.admin.ch + 41 58 463 11 11
ABDRUCK REPRODUCTION RIPRODUZIONE REPRINT	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

PRIORITÄTEN DER EMPFEHLUNGEN

Die Eidgenössische Finanzkontrolle priorisiert ihre Empfehlungen auf der Grundlage definierter Risiken: 1 = hoch, 2 = mittel, 3 = gering.
Als Risiken gelten beispielsweise unrentable Projekte, Verstösse gegen die Legalität oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Damit werden die Auswirkungen und die Wahrscheinlichkeit des Eintretens beurteilt. Diese Beurteilung richtet sich nach dem konkreten Prüfungsgegenstand (relativ) und nicht nach der Relevanz für die Bundesverwaltung als Ganzes (absolut).

INHALTSVERZEICHNIS

Das Wesentliche in Kürze **4**

L'essentiel en bref **6**

L'essenziale in breve **8**

Key facts **10**

1 Auftrag und Vorgehen **13**

1.1 Ausgangslage 13

1.2 Prüfungsziel und-fragen 13

1.3 Prüfungsumfang und-grundsätze 13

1.4 Unterlagen und Auskunftserteilung 13

1.5 Schlussbesprechung 14

2 Governance des Standarddienstes **15**

2.1 Die Führung des Standarddienstes ist zielführend aufgebaut 15

2.2 Die Risiken einer Abhängigkeit zum Schlüssel-Lieferanten sind adressiert 16

3 Betrieb des eIAM durch das Bundesamt für Informatik und Telekommunikation **18**

3.1 Der Betrieb ist grundsätzlich stabil, Prozesse sind etabliert und die Sicherheitsdokumente unterliegen einer laufenden Überarbeitung 18

3.2 Tests der Redundanzen haben zu unterschiedlichen Verbesserungsmassnahmen geführt 18

3.3 Notfallpläne im Krisenfall sind nicht vorhanden 21

Anhang 1 – Rechtsgrundlagen 22

Anhang 2 – Abkürzungen 23

Anhang 3 – Glossar 24

PRÜFUNG

Prüfung der Identitäts- und Zugriffsverwaltung eIAM

Bundeskanzlei – Bereich Digitale Transformation und IKT-Lenkung

DAS WESENTLICHE IN KÜRZE

Die Lösung eIAM (Electronic Identity and Access Management) des Bundesamts für Informatik und Telekommunikation (BIT) stellt die zentrale Authentifizierungsplattform für die gesamte Schweizer Bundesverwaltung dar. Sie dient der Verwaltung von digitalen Identitäten und Zugriffsrechten über alle angebundenen Webanwendungen und Dienste hinweg und soll eine sichere, effiziente und zentrale Authentifizierungslösung für die Bundesbehörden gewährleisten.

Per September 2024 nutzen täglich etwa 100 000 Benutzerinnen und Benutzer die eIAM-Lösung, um auf über 800 Anwendungen zuzugreifen, wobei täglich rund 250 000 Anmeldungen verarbeitet werden. Die jährlichen Betriebs- und Weiterentwicklungskosten der eIAM-Lösung betragen rund 20 Millionen Franken.

Die Führung des Standarddienstes ist zielführend aufgebaut und ermöglicht eine effektive Umsetzung der Aufgaben. Die Risiken im Zusammenhang mit der Abhängigkeit vom Schlüssellieferanten wurden adressiert und werden überwacht. Der Betrieb läuft stabil, Prozesse sind etabliert, und die Sicherheitsdokumente werden kontinuierlich aktualisiert. Zudem wurden seit der letzten Prüfung im Jahr 2018[1] beachtliche Fortschritte im Bereich der Virtualisierung sowie in der Verwaltung mehrerer Instanzen erzielt.

Verbesserungsbedarf besteht jedoch bei den Massnahmen zur Minderung der Risiken im Zusammenhang mit der Abhängigkeit von eIAM.

Die Tests zur Notfallumschaltung sollten erweitert werden

Das BIT hat die eIAM Lösung georedundant in zwei Rechenzentren (RZ) aufgebaut. Die erste Notfallumschaltung (Failover-Test), bei dem der eIAM-Kern vom RZ «Primus» auf «Campus» umgestellt wurde, verlief erfolgreich. Er zeigte jedoch auch unterschiedliche Probleme auf. Zur Optimierung wurden Lehren aus der Übung gezogen, insbesondere hinsichtlich der sofortigen Verfügbarkeit der Teams und der Automatisierung von Prozessen. Weitere technische Herausforderungen müssen vor einem erneuten vollständigen Failover-Test gelöst werden.

Im September 2024 hat das BIT entschieden, dass bei jedem Release ein Failover-Test der eIAM-Kernkomponenten auf der Referenzumgebung durchgeführt wird. Bei diesen Tests werden jedoch wichtige Komponenten ausgeschlossen. Diese Komponenten zu testen, würde wiederum den Einbezug weiterer Anwendungsteams erfordern. Die bewusste Ausklammerung der Komponenten aus den Tests birgt ein Risiko, da diese eine zentrale Rolle in der Authentifizierungs- und Zugriffskontrollstruktur des eIAM-Systems spielen. Ein Ausfall oder eine Fehlkonfiguration könnte gravierende Auswirkungen auf den Zugang zu kritischen Anwendungen haben. Daher sollten diese Komponenten auch in die Tests einbezogen werden.

Es fehlen Betriebslösungen beim Ausfall der Rechenzentren

Das BIT hat Notfall- und Neustartpläne erarbeitet für die RZ, in denen eIAM betrieben wird. Der Neustartplan für eIAM wird beim BIT unter der Leitung des Business Continuity Managements (BCM) geregelt und ist Teil des Programms zur Dienstkontinuität des BIT. Das BIT hat ein Dokument für den Neustart von eIAM formalisiert, das sich derzeit in der internen Validierung befindet und zunächst nur das RZ «Primus» in Bern betrifft. Die Umschaltung zum RZ «Campus» ist ebenfalls dokumentiert und wird unter der BCM-Leitung durchgeführt. Zum Prüfzeitpunkt gibt es jedoch keine konkreten Pläne für einen möglichen Ausfall beider RZ.

[1] «Prüfung von Führung und Betrieb des Standarddienstes «Identitäts- und Zugangsverwaltung» (PA 18502).

AGOV wird als erster grosser Anwendungsfall die E-ID als weiteres Identitätsnachweismittel für den Zugang auf Behördenanwendungen nutzen. Dadurch wird die zentrale Rolle von eIAM/AGOV im Identitätsmanagement des Bundes und der Schweizer Behörden weiter ausgebaut.

AUDIT

Audit de la gestion des identités et des accès (eIAM)

Chancellerie fédérale – secteur Transformation numérique et gouvernance informatique

L'ESSENTIEL EN BREF

La solution eIAM *(electronic Identity and Access Management)* de l'Office fédéral de l'informatique et de la télécommunication (OFIT) constitue la plateforme centrale d'authentification pour l'ensemble de l'administration fédérale. Elle sert à gérer les identités numériques et les droits d'accès à toutes les applications et à tous les services Web qui lui sont rattachés et doit offrir aux autorités fédérales une solution d'authentification à la fois sûre, efficace et centralisée.

En septembre 2024, quelque 100 000 utilisateurs recouraient chaque jour au système eIAM pour se connecter à plus de 800 applications, ce qui représente environ 250 000 connexions par jour. Les coûts d'exploitation et de développement du système eIAM se montent à environ 20 millions de francs par an.

La gestion du service standard a été conçue de manière ciblée et permet d'assurer une exécution efficace des tâches. Les risques associés à la dépendance vis-à-vis du fournisseur clé ont été évalués et font l'objet d'un suivi. L'exploitation est stable, les procédures sont définies et les documents de sécurité sont mis à jour en continu. Depuis le dernier audit, réalisé en 2018[2], des progrès remarquables ont été réalisés dans le domaine de la virtualisation et de la gestion de plusieurs instances.

Des améliorations sont néanmoins nécessaires en ce qui concerne les mesures destinées à réduire les risques inhérents à la dépendance vis-à-vis de l'eIAM.

Il convient d'élargir les tests de basculement d'urgence

L'OFIT a installé le système eIAM dans deux centres de calcul (CC) pour assurer sa géo-redondance. Le premier test de basculement *(failover test)*, au cours duquel le cœur du système eIAM a été basculé du CC PRIMUS au CC CAMPUS, s'est déroulé avec succès. Il a cependant révélé l'existence de différents problèmes. Les enseignements tirés de ce test ont conduit à optimiser le fonctionnement, notamment pour ce qui est de veiller à la disponibilité immédiate de l'équipe et d'automatiser les processus. D'autres défis techniques restent à résoudre avant un nouveau test de basculement complet.

En septembre 2024, l'OFIT a décidé de réaliser un test de basculement des composants essentiels du système eIAM vers l'environnement de référence lors de chaque mise à jour. Ces tests font cependant l'impasse sur des composants importants, car tester ces composants exigerait d'impliquer les équipes responsables d'autres applications. L'exclusion délibérée de ces composants des tests comporte cependant un risque, car ils jouent un rôle central dans la structure d'authentification et de contrôle d'accès du système eIAM. Une défaillance ou une erreur de configuration pourraient entraîner des conséquences graves pour l'accès aux applications critiques. Il convient dès lors d'inclure également ces composants dans les tests.

Des solutions opérationnelles font défaut en cas de panne des centres de calcul

L'OFIT a élaboré des plans d'urgence et de redémarrage pour les centres de calcul qui hébergent le système eIAM. Au sein de l'office, le plan de redémarrage est régi par le service chargé de la continuité des activités *(Business Continuity Management, BCM)* et intégré dans le programme de la continuité du service de l'OFIT. L'OFIT a établi un document formel concernant le redémarrage du système eIAM, qui est en cours de validation interne et qui ne concerne, dans un premier temps, que le CC PRIMUS à Berne.

[2] Audit de la gestion et de l'exploitation du service standard « gestion de l'identité et de l'accès » (nº d'audit 18502).

Le basculement vers le CC CAMPUS est également consigné dans un document et sera effectué sous la conduite du service BCM. Au moment de l'audit, aucun plan concret n'existait cependant pour le cas d'une panne simultanée des deux centres de calcul.

AGOV sera le premier grand service à utiliser l'identité électronique (e-ID) comme preuve d'identité pour accéder aux applications des autorités. Cette solution renforcera encore le rôle central du système eIAM/AGOV dans la gestion des identités de la Confédération et des autorités suisses.

VERIFICA

Verifica della gestione delle identità e degli accessi eIAM

Cancelleria federale, Settore Trasformazione digitale e governance delle TIC

L'ESSENZIALE IN BREVE

La soluzione «Electronic Identity and Access Management» (eIAM) dell'Ufficio federale dell'informatica e della telecomunicazione (UFIT) funge da piattaforma centrale di autenticazione per l'intera Amministrazione federale svizzera. eIAM serve a gestire le identità digitali e i diritti di accesso di tutte le applicazioni web e i servizi collegati, oltre a garantire alle autorità della Confederazione una soluzione di autenticazione sicura, efficiente e centralizzata.

Stando a quanto rilevato nel mese di settembre 2024, circa 100 000 utenti utilizzano quotidianamente eIAM per accedere a oltre 800 applicazioni e vengono gestiti circa 250 000 accessi al giorno. I costi annui di gestione e di sviluppo della soluzione ammontano a circa 20 milioni di franchi.

La gestione del servizio standard ha una struttura adeguata, che favorisce un'attuazione effettiva dei compiti. I rischi legati alla dipendenza dai fornitori principali sono stati individuati e verranno monitorati. L'esercizio è stabile, i processi sono consolidati e i documenti di sicurezza vengono aggiornati regolarmente. Inoltre, dall'ultima verifica nel 2018[3] sono stati compiuti notevoli progressi nell'ambito della virtualizzazione e della gestione di diverse autorità.

Sussiste tuttavia un margine di miglioramento per quanto concerne le misure volte a ridurre i rischi legati alla dipendenza di eIAM dai fornitori.

È necessario ampliare i test di failover

L'UFIT ha strutturato la soluzione eIAM in modo georidondante, utilizzando due centri di calcolo. Il primo test di failover, che consisteva nel trasferire i componenti principali di eIAM dal centro di calcolo «Primus» al centro di calcolo «Campus», è stato eseguito con successo, tuttavia, sono emersi diversi problemi. Per ottimizzarli, sono state applicate delle nozioni apprese durante il test, in particolare per quanto riguarda la disponibilità immediata dei team e l'automatizzazione dei processi. Prima di condurre un nuovo test di failover completo, è necessario risolvere altre sfide tecniche.

A settembre 2024, l'UFIT ha stabilito che per ogni release va svolto un test di failover dei componenti principali di eIAM nell'ambiente di riferimento. Tramite questi test vengono però esclusi componenti importanti, che per essere testati richiederebbero a loro volta il coinvolgimento di ulteriori team responsabili dell'applicazione. L'esclusione voluta di alcuni componenti dai test comporta un rischio, poiché tali elementi svolgono un ruolo centrale nella struttura di autenticazione e controllo degli accessi del sistema eIAM. Un guasto o una configurazione errata potrebbe avere ripercussioni gravi sull'accesso alle applicazioni critiche. Pertanto, sarebbe opportuno includere anche questi componenti nei test.

Mancano soluzioni operative in caso di guasti nel centro di calcolo

L'UFIT ha elaborato piani d'emergenza e piani di ripristino per i server dei centri di calcolo in cui viene gestito eIAM. Il piano di ripristino per eIAM è regolato dall'UFIT sotto la guida del team responsabile della gestione della continuità operativa («business continuity management», BCM) e fa parte del programma di continuità del servizio dell'UFIT. L'UFIT ha formalizzato un documento per il ripristino di eIAM, che è attualmente in fase di convalida interna e riguarda inizialmente solo il centro di calcolo «Primus» a Berna.

[3] Verifica della gestione e dell'esercizio del servizio standard relativo alla «gestione delle identità e degli accessi» (PA 18502).

Anche il trasferimento della soluzione al centro di calcolo «Campus» è documentato e viene svolto sotto la guida della BCM. Tuttavia, al momento della verifica, non erano disponibili piani concreti per contrastare un eventuale guasto in entrambi i centri di calcolo.

AGOV rappresenta il primo caso d'applicazione a larga scala di e-ID utilizzata come ulteriore mezzo d'identificazione per accedere alle applicazioni delle autorità. In questo modo si consolida ulteriormente il ruolo centrale di eIAM e AGOV nella gestione delle identità da parte della Confederazione e delle autorità svizzere.

Audit of the identity and access management system eIAM

Federal Chancellery – Digital Transformation and ICT Steering Sector

KEY FACTS

The eIAM (electronic identity and access management) solution provided by the Federal Office of Information Technology, Systems and Telecommunication (FOITT) is the central authentication platform for the entire Swiss Federal Administration. It is used to manage digital identities and access rights across all connected web applications and services and is intended to ensure a secure, efficient and centralised authentication system for the federal authorities.

As at September 2024, some 100,000 users use the eIAM solution every day to access over 800 applications, with around 250,000 logins processed daily. The annual operating and development costs for eIAM are around CHF 20 million.

Management of the standard service is well structured for meeting objectives, and enables tasks to be implemented effectively. The risks associated with dependence on the key supplier have been addressed and are being monitored. Operations are stable, processes are established and the security documents are continuously updated. In addition, considerable progress has been made on virtualisation and multi-instance management since the previous audit in 2018[4].

However, there is room for improvement in terms of measures to mitigate the risks associated with reliance on eIAM.

Failover testing should be expanded

The FOITT has a georedundant set-up for eIAM at two data centres. The first failover test, in which the eIAM core was switched from the Primus to the Campus data centre, was successful. However, it also highlighted various problems. Lessons were learnt from the exercise to improve operations, particularly with regard to the immediate availability of teams and the automation of processes. Further technical challenges must be resolved before another full failover test can be conducted.

In September 2024, the FOITT decided that a failover test of eIAM's core components would be performed on the reference environment with each release. However, these tests exclude important components. Testing these components would in turn require the involvement of additional application teams. The deliberate exclusion of the components from the tests carries a risk, as they play a key role in the eIAM system's authentication and access control structure. A failure or misconfiguration could have a serious impact on access to critical applications. These components should therefore also be included in the tests.

Lack of operational solutions in the event of data centre failure

The FOITT has drawn up emergency and restart plans for the data centres in which eIAM is operated. The eIAM restart plan is managed by the FOITT under the direction of Business Continuity Management (BCM) and is part of the FOITT's service continuity programme. The FOITT has formalised an eIAM restart document, which is currently undergoing internal validation and initially applies only to the Primus data centre in Bern.

The switchover to the Campus data centre is also documented and is being led by BCM. However, at the time of the audit, there were no concrete plans for a possible failure of both data centres.

[4] Audit of the management and operation of the "identity and access management" standard service (audit mandate 18502).

AGOV will be the first major use case to utilise e-ID as an additional means of identity verification for accessing government applications. This will further expand the key role of eIAM/AGOV in identity management for the federal government and the Swiss authorities.

GENERELLE STELLUNGNAHME DER BUNDEKANZLEI, BEREICH DIGITALE TRANSFORMATION UND IKT-LENKUNG

Die Bundeskanzlei bedankt sich bei der EFK für die gute Zusammenarbeit und den konstruktiven Austausch bei dieser Prüfung. Die Empfehlungen decken sich mit den Einschätzungen der Bundeskanzlei und werden umgesetzt.

GENERELLE STELLUNGNAHME DES BUNDESAMTS FÜR INFORMATIK UND TELEKOMMUNIKATION

Das BIT bedankt sich bei der EFK für die konstruktive und angenehme Zusammenarbeit.

Die EFK hat dem BIT eine wertvolle Empfehlung für die Verbesserung der Verfügbarkeit von eIAM gegeben. Das BIT wird diese Empfehlung mit zielführenden Massnahmen umsetzen, sofern es korrekt beauftragt wird.

1 AUFTRAG UND VORGEHEN

1.1 Ausgangslage

Das eIAM ist ein Service des Standarddienstes (SD) «Identitäts- und Zugangsverwaltung (IAM-Bund)», welcher in der Verantwortung des Bereichs Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei (BK) steht. Der SD ist das Werkzeug des Bundes zur Identifikation, Authentifizierung, Zugriffsverwaltung und Berechtigungssteuerung für Webanwendungen, Apps und Dienste. In den letzten Jahren wurde eIAM sowohl funktional als auch hinsichtlich der Nutzerzahlen kontinuierlich ausgebaut und hat eine Bedeutung erhalten, die zu Beginn nicht vorhersehbar war. Derzeit läuft das Vorhaben "Authentifizierungsdienst der Schweizer Behörden (AGOV)[5]", das die Nutzung von eIAM durch die Kantone und Gemeinden weiter fördern soll. Zudem strebt der Bund die Einführung einer eigenen elektronischen Identität (E-ID) für alle Bürgerinnen und Bürger an. AGOV ersetzt die heutige Service-Option CH-Login von eIAM. AGOV wird als erster grosser Anwendungsfall die E-ID als weiteres Identitätsnachweismittel für den Zugang auf Behördenanwendungen nutzen. Dadurch wird die zentrale Rolle von eIAM/AGOV im Identitätsmanagement des Bundes und der Schweizer Behörden weiter ausgebaut.

eIAM stellt heute einen «Single Point of Failure» für die Bundesinformatik dar und wurde in der Vergangenheit mit zunehmenden Störungen konfrontiert. Die EFK prüfte bereits im Jahr 2018 den SD «Identitäts- und Zugangsverwaltung».[6]

1.2 Prüfungsziel und -fragen

Die Prüfung soll beurteilen, ob eIAM innerhalb des Standarddienstes die Risiken und die Einflüsse von Vorhaben im Umfeld des Dienstes analysiert und wo nötig Massnahmen umsetzt.

Prüffragen:

1. Werden aus den erhobenen Bedürfnissen der Leistungsbezüger und den neuen technologischen Möglichkeiten Weiterentwicklungen des eIAM vorangetrieben?
2. Werden Massnahmen ergriffen, um die Abhängigkeiten von Lieferanten zu reduzieren?
3. Werden Massnahmen ergriffen, damit die Risiken bezüglich Abhängigkeit von eIAM auf den täglichen Betrieb reduziert werden?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Roland Gafner (Revisionsleitung), Warren Paulus, Adrian Allenbach und Fernando Guntern vom 12. August 2024 bis 29. September 2024 durchgeführt. Sie erfolgte unter der Federführung von Bernhard Hamberger. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Prüfungsdurchführung.

Die Beurteilungen orientieren sich an den Vorgaben der Bundesverwaltung zur Informationssicherheit.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von dem Bereich DTI und dem Leistungserbringer BIT umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung.

---

[5] https://www.agov.admin.ch/de.

[6] «Prüfung von Führung und Betrieb des Standarddienstes «Identitäts- und Zugangsverwaltung» (PA 18502).

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 22. Januar 2025 statt. Teilgenommen haben seitens BIT der Leiter Interne Revision und der Chief Information Security Officer AGOV und eIAM. Die BK DTI wurde durch den Leiter Digitale Standardleistungen, den Leiter und den Serviceverantwortlichen Digitale Basis- und Sicherheitsleistungen verstreten. Seitens der EFK waren der Mandatsleiter, der Federführende und der Revisionsleiter anwesend.

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

EIDGENÖSSISCHE FINANZKONTROLLE

2 GOVERNANCE DES STANDARDDIENSTES

Informatikleistungen, die von den Verwaltungseinheiten des Bundes in gleicher oder vergleichbarer Funktionalität und Qualität benötigt werden, werden als sogenannte IKT-Standarddienste zentral für die gesamte Bundesverwaltung bereitgestellt und zur Nutzung angeboten. Die Verantwortung für die SD liegt beim Bereich DTI der BK. Dafür erarbeitet und aktualisiert der Bereich DTI Standards für IT-Systeme und digitale Dienstleistungen, die in der Bundesverwaltung verwendet werden. Diese Standards sorgen für Einheitlichkeit und Interoperabilität zwischen verschiedenen Behörden und Systemen und bilden eine Grundlage für eine reibungslose und kosteneffiziente IT-Infrastruktur.

eIAM ist ein Service des SD «IAM», für den der Bundesrat eine Bezugspflicht beschlossen hat. Der SD «IAM» wird gemäss der Risikoanalyse der BK wegen seiner zentralen Bedeutung als Risiko auf Stufe BR geführt.

2.1 Die Führung des Standarddienstes ist zielführend aufgebaut

Das für den SD zuständige Team innerhalb des Bereichs DTI wurde klar strukturiert, um die wichtigsten Aufgaben effektiv abzudecken. Die Kommunikation innerhalb der Organisation erfolgt sowohl vertikal als auch horizontal, um sicherzustellen, dass die relevanten Informationen weitergeleitet werden. Die Prozesse im Bereich der SD sind weitgehend vereinheitlicht und klar definiert. Eine systematische Dokumentation stellt sicher, dass Arbeitsabläufe nachvollziehbar und transparent sind.

Der Austausch zwischen DTI und dem BIT ist sehr eng und zeichnet sich durch eine proaktive und strukturierte Kommunikation aus. Beide Organisationseinheiten stehen in stetigem Kontakt, um eine reibungslose Koordination der IT-Dienstleistungen sicherzustellen. Die enge Abstimmung erfolgt vor allem auf operativer Ebene.

Wichtige Neuerungen und sich verändernde Anforderungen werden in regelmässigen Meetings besprochen. Diese Besprechungen bieten die Möglichkeit, neue Projekte und technische Entwicklungen zeitnah zu evaluieren und Entscheidungen zu treffen.

Neben der engen Kooperation mit dem BIT ist auch der Austausch zwischen DTI und externen Lieferanten institutionalisiert und gut etabliert. Regelmässige Meetings mit Lieferanten ermöglichen eine stetige Überprüfung der Leistungserbringung und unterstützen die Einhaltung der vertraglichen Vereinbarungen. Zudem bieten diese Treffen die Möglichkeit, neue technologische Entwicklungen und Verbesserungen der angebotenen Dienste zu besprechen. Die strukturierte Zusammenarbeit mit externen Partnern stärkt die Flexibilität und Innovationskraft der DTI, da technologische Trends frühzeitig erkannt und in die eigenen Produkte integriert werden können.

Kommunikation mit weiteren Anspruchsgruppen

Die eigens für den Dienst eingerichtete Webseite informiert die Anspruchsgruppen über Erweiterungen, neue Funktionen oder Änderungen der eIAM-Dienste. Ein vertiefter Austausch erfolgt über ein Sounding Board und ein Diskussionsforum. Geplante Änderungen oder Anforderungen der Kunden des SD sind in einer Roadmap des Bereichs DTI festgehalten und erfolgen in enger Absprache mit dem Leistungserbringer BIT und den zuständigen departementsübergreifenden Fachgremien. Zudem hat das BIT einen formalen Versionsmanagement-Prozess etabliert, der alle Phasen von der Validierung bis zur Produktionsfreigabe, inklusive Tests, abdeckt.

Bei Sicherheitsvorfällen greifen die Kommunikationspläne des BIT in enger Abstimmung mit dem Bereich DTI. In diesen Fällen hat der Bereich DTI die Hoheit über die Kommunikation.

BEURTEILUNG

Der Bereich für die Standarddienste innerhalb von DTI ist insgesamt gut aufgestellt und erfüllt seine Aufgaben zuverlässig. Die vorhandenen Strukturen und Prozesse unterstützen die Erreichung der gesetzten Ziele.

Die aufgezeigten Kommunikationsprozesse und Abstimmungsmechanismen rund um die eIAM-Dienste sind gut strukturiert und durchdacht. Die Einrichtung einer Webseite für die Information der Anspruchsgruppen sowie die Nutzung eines Sounding Boards und eines Diskussionsforums fördern einen transparenten und kontinuierlichen Austausch. Die Bedürfnisse der Anspruchsgruppen werden in einer geeigneten und strukturierten Form erhoben und bearbeitet.

Besonders hervorzuheben ist die Roadmap des Bereichs DTI, welche die geplanten Änderungen des SD systematisch festhält. Diese Methode schafft eine klare Übersicht und ermöglicht eine vorausschauende Planung. Die enge Abstimmung mit dem Leistungserbringer BIT sowie mit den zuständigen departementsübergreifenden Fachgremien zeigt ein hohes Mass an Koordination, was für die reibungslose Umsetzung von Änderungen von zentraler Bedeutung ist.

2.2 Die Risiken einer Abhängigkeit zum Schlüssel-Lieferanten sind adressiert

Die Abhängigkeit sowohl vom Schlüssellieferanten «Adnovum» als auch von dessen Produkt «Nevis» erstreckt sich über verschiedene IAM-Lösungen in der zivilen Bundesverwaltung, im Polizeiwesen und im Militär. Dies wurde bereits in einer von DTI in Auftrag gegebenen externen Studie vom letzten Jahr so festgestellt.

«Nevis» ist eine umfassende Sicherheitsplattform, welche digitale Identitäten verwaltet, die Authentifizierung und Autorisierung von Benutzern steuert und den sicheren Zugriff auf Anwendungen und Systeme gewährleistet. Damit stellt «Nevis» den Kern des eIAM Dienstes dar. Eine Ablösung von «Nevis» würde signifikante Kosten verursachen und erfordert einen längeren Parallelbetrieb bis zur vollständigen Implementierung einer neuen Lösung.

Daher müssen gewisse Grundleistungen weiterhin von «Adnovum» bezogen werden. Dazu wurde die Zusammenarbeit zwischen dem BIT und «Adnovum» im Rahmen eines neuen Vertrags über Rund 110 Millionen Franken für die kommenden acht Jahre festgelegt. In dieser Beschaffung wurden explizit weitere Firmen für Dienstleistungen im Volumen von 70 Millionen Franken ausserhalb des Kernsystems berücksichtigt. Zudem wurde eine Vereinbarung getroffen, welche sicherstellt, dass im Falle einer Handlungsunfähigkeit der Lieferantin der Quellcode als Absicherung zur Verfügung steht. Darüber hinaus befinden sich etwa 80 % des Quellcodes bereits beim BIT, verteilt auf eigene Systeme und Umsysteme. Ein Beispiel hierfür ist der Bundes Trustbroker (BTB), der in Zusammenarbeit mit «Adnovum» entwickelt wurde, wobei der Quellcode im Besitz der Bundesverwaltung blieb.

«Adnovum» hat ein Betriebssicherheitsverfahren durchlaufen und das Auditrecht wurde vertraglich festgelegt. Bis zum Prüfzeitpunkt wurden jedoch noch keine Sicherheitsaudits durchgeführt.

Die Abhängigkeit von externen Entwicklern bei der Erarbeitung des Bundes Trustbroker bleibt trotz Gegenmassnahmen hoch (siehe Einleitung in Kapitel 3). Internes Wissen ist auf wenige Personen beschränkt, während der Grossteil extern liegt. Dies stellt ein Risiko dar, besonders im Hinblick auf die Erweiterung des Dienstes.

BEURTEILUNG

Die langfristige Vertragsregelung für die kommenden acht Jahre schafft Klarheit und Stabilität in der Zusammenarbeit, was für die Sicherstellung von Grundleistungen von grosser Bedeutung ist. Die Berücksichtigung weiterer Lieferantinnen und der Erweiterung der Architektur trägt zu einer Verringerung der Abhängigkeit von «Adnovum» bei. Besonders hervorzuheben ist die Implementierung eines Treuhandvertrags, welches den Zugang zum Quellcode auch im Falle einer Handlungsunfähigkeit von «Adnovum» sicherstellt.

Dies reduziert das Risiko eines potenziellen Lieferausfalls weiter. Zudem ist es von Vorteil, dass der Grossteil des Quellcodes bereits beim BIT auf eigenen oder verteilten Systemen verfügbar ist und die Rechte am Code geregelt sind. Dadurch wird die Abhängigkeit weiter verringert und die Handlungsfähigkeit der Bundesverwaltung gestärkt. Durch den gezielten Wissensaufbau innerhalb des BIT kann die Abhängigkeit von externen Entwicklern ebenfalls reduziert und die langfristige Stabilität sowie die Handlungsfähigkeit, verbessert werden.

Am Beispiel der Entwicklung des BTB zeigt sich eine signifikante Abhängigkeit von externen Entwicklern, welche trotz ergriffener Gegenmassnahmen – wie beispielsweise die Veröffentlichung des Codes als Open-Source – weiterhin hoch bleibt. Insbesondere die Tatsache, dass das interne Wissen auf wenige Schlüsselpersonen beschränkt ist, während der Grossteil des Know-hows extern liegt, stellt ein erhebliches Risiko dar. Dies könnte sich vor allem in Phasen der Erweiterung des Diensts als problematisch erweisen, da die Flexibilität und Reaktionsfähigkeit des internen Teams eingeschränkt sind.

Die EFK anerkennt, dass mit verschiedenen technischen und organisatorischen Massnahmen die Reduktion der Abhängigkeit von Adnovum adressiert wurde. Sie vermisst jedoch eine Beurteilung, aus Sicht der Bundesverwaltung als Ganzes, ob die Abhängigkeit damit im akzeptablen Bereich liegt, oder ob weitere Massnahmen notwendig sind.

EMPFEHLUNG 1 — PRIORITÄT 2

Die EFK empfiehlt dem Bereich DTI zusammen mit den betroffenen Leistungserbringern die Kontinuität des NEVIS-Einsatzes – mit der Perspektive ganze Bundesverwaltung – und der resultierenden Abhängigkeit von Lieferanten dahingehend abzusichern, dass bei sich verändernden Rahmenbedingungen die Bundesverwaltung mehrere Jahre störungsfrei die bestehenden NEVIS-Instanzen einsetzen, warten und weiterentwickeln kann.

STELLUNGNAHME DES BEREICHS DTI

Die Empfehlung ist akzeptiert.

Der Zugriff des Bundes auf den Quellcode ist im Konkursfall der Nevis Security AG bereits heute mit einem sogenannten Escrow-Agreement abgesichert. Weitere Massnahmen werden zusammen mit den anderen involvierten Stellen bei der Bundesverwaltung angegangen.

3 BETRIEB DES EIAM DURCH DAS BUNDESAMT FÜR INFORMATIK UND TELEKOMMUNIKATION

Stand September 2024 nutzen täglich rund 100 000 Benutzerinnen und Benutzer die eIAM-Lösung, um auf mehr als 800 verschiedene Anwendungen und Systeme der Bundesverwaltung zuzugreifen. Im Schnitt werden täglich etwa 250 000 Anmeldungen über die Plattform verarbeitet, was die hohe Bedeutung dieser Lösung für den laufenden Betrieb der Verwaltung unterstreicht.

Die Teams des BIT, welche die eIAM-Lösung weiterentwickelt und betreibt, besteht zum Prüfzeitpunkt aus 43 externen (davon 39 von der Firma «Adnovum») und 7 internen Mitarbeitenden, welche in den Bereichen Identitätsmanagement, Systementwicklung und-betrieb tätig sind. Neben der kontinuierlichen Weiterentwicklung und Optimierung der Lösung ist das Team auch für die Behebung potenzieller Störungen zuständig. Hierfür unterhält das Team eine 7/24-Betriebsorganisation mit automatischem Monitoring, Alarmierung sowie einem Telefonpikett.

Die jährlichen Betriebs- und Weiterentwicklungskosten der eIAM-Lösung belaufen sich auf rund 20 Millionen Schweizer Franken. Diese umfassen Kosten für Personal, Infrastruktur, Wartung und funktionale und betriebliche Weiterentwicklung der Plattform, sowie Aufwendungen für Sicherheitsmassnahmen und die Einhaltung der regulatorischen Vorgaben. Die in Kapitel 2 erwähnte externe Studie kommt zum Schluss, dass die Kosten sich auf dem Niveau vergleichbarer Organisationen bewegen.

3.1 Der Betrieb ist grundsätzlich stabil, Prozesse sind etabliert und die Sicherheitsdokumente unterliegen einer laufenden Überarbeitung

Der Betrieb der eIAM-Lösungen läuft grundsätzlich stabil und unproblematisch. Die vom BIT regelmässig an den Bereich DTI gelieferten Reports zeigen, dass die vereinbarten Leistungen in einer hohen Qualität erbracht werden.

Das Change- und Releasemanagement erfolgt gemäss institutionalisierten Prozessen und erfolgt beim BIT mehrheitlich in Absprache mit dem Bereich DTI.

Die grundlegenden Sicherheitsdokumente, wie Schutzbedarfsanalysen und Informationssicherheits- und Datenschutzkonzept (ISDS) konnten der EFK vorgewiesen werden. Sie entsprechen den Anforderungen und sind zum Prüfzeitpunkt in Überarbeitung.

BEURTEILUNG

Die EFK beurteilt den Betrieb des SD IAM als zuverlässig. Mit wenigen Ausnahmen sind keine grösseren Probleme aufgetreten. Die aufgesetzten Prozesse sind für alle verbindlich und etabliert. Die internen Prozesse beim BIT stellen ein nachvollziehbares Change- und Releasemanagement sicher.

Die Sicherheitsdokumente, als wichtiges Instrument zur Spezifikation der Anforderungen an die Sicherheit der Systeme, entsprechen den Anforderungen. Die aktuell laufende periodische Überarbeitung dieser Dokumente ist hinsichtlich der technischen Veränderungen und den sich wandelnden äusseren Einflüssen essenziell.

3.2 Tests der Redundanzen haben zu unterschiedlichen Verbesserungsmassnahmen geführt

Die Systeme des eIAM haben hohe Anforderungen an die Verfügbarkeit. Daher sind diese in der höchsten Verfügbarkeitsklasse VK3 eingestuft. Die Verfügbarkeitsklassen beziehen sich auf die Häufigkeit von Ausfällen pro Quartal und deren Dauer. Um diese hohe Verfügbarkeit zu gewährleisten, sind die Systeme innerhalb der Rechenzentren (RZ) «Primus» in Bern und «Campus» in Frauenfeld jeweils dreifach

redundant aufgebaut. Die Redundanzen der wichtigsten Komponenten der eIAM-Umgebung werden durch die Plattform verwaltet, die die Bereitstellung, Skalierung und Implementierung von Anwendungscontainern auf den Servern automatisiert. Die Plattform ist in beiden Rechenzentren implementiert und jede Komponente wird in drei getrennten Verfügbarkeitszonen (Availability Zones) für das entsprechende Rechenzentrum bereitgestellt.

Zudem kann bei einem Ausfall eines der beiden RZ bestenfalls innert zwei Stunden auf das andere RZ gewechselt werden. Da die Architektur und die Latenzzeiten einen Aktiv-Aktiv-Betrieb zwischen den beiden RZ nicht erlauben, müssen die Systeme bei einem Wechsel neu hochgefahren und die Verbindungen umkonfiguriert werden. Diese Konfigurationen erfolgen zum Prüfzeitpunkt manuell, sollen aber in der Zukunft automatisiert werden. Weiter müssen die Datenbanken jeweils an den Ausweichstandort repliziert werden. Dies kann zu einem marginalen Verlust der jüngsten Veränderungen auf den Datenbanken führen.

Während das eIAM in der Verfügbarkeitsklasse VK3 eingestuft ist, erfüllen jedoch mehrere benötigte Basisdienste nicht dieselbe Verfügbarkeitsklasse. Dadurch ist die geforderte VK3-Verfügbarkeit für das Gesamtsystem nicht durchgängig gewährleistet.

Failover-Test «Primus-Campus»

Am 15. August 2024 wurde ein Failover-Test, bei dem der eIAM Kern von «Primus» auf «Campus» umgestellt wurde, durchgeführt. Dabei wurde die Umstellung und das Starten des eIAM Kerns in «Campus» zum ersten Mal geprobt. Es traten Schwierigkeiten im Zusammenhang mit dem Failover der Datenbanken, den manuellen DNS-Einstellungen sowie bei Anpassungen der Load-Balancer- und Firewall-Konfigurationen auf. Der Test bestätigte, dass das Failover grundsätzlich funktioniert, allerdings sind Anpassungen notwendig. Insbesondere soll die sofortige Verfügbarkeit der zuständigen Teams sichergestellt und Prozesse so weit wie möglich automatisiert werden, um die maximal geforderte Ausfallzeit einhalten zu können. Die Bewältigung verschiedener technischer Herausforderungen muss gelöst werden, bevor ein vollständiger Notfallumschaltungs-Test wiederholt werden kann.

Im September 2024 hat der Product-Owner entschieden, dass das BIT bis auf weiteres im Rahmen jedes Releases einen Test auf der Referenzumgebung für die eIAM Kern Komponenten durchführen muss. Dabei sollen die Reverse Proxy-Policy Enforcement Point (RP-PEP) Integrationen jedoch vom Test ausgeschlossen werden. Dies bedeutet, dass die angebundenen Fachanwendungen somit von den Tests ausgeschlossen werden. Ein Notfallumschaltungs-Test welcher auch RP-PEPs beinhaltet, kann durch das eIAM Team nicht selbständig durchgeführt werden. Hierfür müssten auch die betroffenen Anwendungen miteinbezogen werden, was nicht in der Kompetenz des eIAM Teams liegt. Ein solcher Test macht jedoch Sinn, wenn die angebundenen Fachanwendungen auch georedundant, also an beiden Standorten vorhanden sind.

BEURTEILUNG

Die eIAM-Systeme erfüllen mit der Einstufung in die Verfügbarkeitsklasse VK3 hohe betriebliche Anforderungen. Die dreifache Redundanz innerhalb der Rechenzentren (RZ) trägt entscheidend zur Ausfallsicherheit bei. Dies stellt sicher, dass bei einem internen Ausfall auf redundante Komponenten zurückgegriffen werden kann, wodurch die Verfügbarkeit gesteigert wird. Die Nutzung einer Plattform zur Automatisierung der Bereitstellung, Skalierung und Implementierung von Anwendungscontainern optimiert den Betrieb und verringert das Risiko menschlicher Fehler.

Die manuelle Konfiguration beim Wechsel zwischen den RZ ist eine potentielle Fehlerquelle und birgt das Risiko die Ausfallzeit zu verlängern. Die geplante Automatisierung dieses Prozesses ist daher dringend erforderlich, um die Wiederherstellungszeiten zu verkürzen und die Zuverlässigkeit des Notfallumschaltungs-Prozesses zu verbessern.

Die Verbesserung der Teamverfügbarkeit, die Automatisierung kritischer Aufgaben und eine klare Dokumentation der Prozesse sind entscheidende Faktoren, um im Ernstfall ein schnelles und zuverlässiges

Failover zu ermöglichen. Beim Wechsel zwischen Rechenzentren müssen zudem technische, organisatorische und konfigurationsspezifische Vorgaben beachtet und regelmässig getestet werden.

Basisdienste, die eine niedrigere Verfügbarkeitsklasse aufweisen, stellen ein erhebliches Risiko für die Verfügbarkeit des gesamten eIAM-Systems dar. Da sie das schwächste Glied in der Kette bilden, besteht die Gefahr, dass Ausfälle oder Störungen in diesen Diensten die Funktionsfähigkeit des eIAM beeinträchtigen und somit die Erreichung der angestrebten Verfügbarkeitsziele gefährden. Insgesamt führt die mangelnde Konsistenz der Verfügbarkeitsstufen zwischen dem eIAM und seinen Basisdiensten zu einer erhöhten Anfälligkeit des Systems.

Die Entscheidung bei jedem Release einen Test auf der Referenzumgebung für die eIAM-Kernkomponenten durchzuführen, ist grundsätzlich positiv zu bewerten. Regelmässige Failover-Tests sind entscheidend, um die Ausfallsicherheit und Verfügbarkeit der Systeme sicherzustellen und potenzielle Schwachstellen frühzeitig zu identifizieren. Die bewusste Ausklammerung der RP-PEP-Integrationen aus diesen Tests stellt jedoch ein Risiko dar. Die RP-PEP Integrationen spielen eine zentrale Rolle in der Authentifizierungs- und Zugriffskontrollstruktur des eIAM-Systems. Ein Ausfall oder eine Fehlkonfiguration in diesen Komponenten könnte schwerwiegende Auswirkungen auf den Zugang zu kritischen Anwendungen und Diensten haben. Indem die RP-PEPs nicht getestet werden, bleibt ein potenziell wichtiger Teil der Infrastruktur ungetestet, was im Ernstfall zu unvorhergesehenen Problemen führen kann.

EMPFEHLUNG 2 — PRIORITÄT 2

Die EFK empfiehlt dem BIT, die Verfügbarkeitsanforderungen der Basisdienste zu überprüfen und, wo erforderlich und ökonomisch sinnvoll, auf die Verfügbarkeitsklasse 3 anzuheben, um die angestrebte Systemverfügbarkeit vollständig zu gewährleisten.

STELLUNGNAHME DES BIT

Die Empfehlung ist akzeptiert.

Das BIT wird die Basisdienste gemäss den Anforderungen der Verfügbarkeitsklasse 3 analysieren. Hierbei berücksichtigt das BIT die Abhängigkeiten zwischen den Basisdiensten und eIAM. Für Basisdienste, die mindestens eine dieser Anforderungen unterschreiten und die Verfügbarkeit von eIAM gefährden, wird das BIT Massnahmen bewerten zur Erfüllung respektive zur Reduktion der Abweichung von der Verfügbarkeitsklasse 3.

EMPFEHLUNG 3 — PRIORITÄT 1

Die EFK empfiehlt dem Bereich DTI in Zusammenarbeit dem BIT, die Machbarkeit regelmässiger und umfassender Failover-Tests, welche alle kritischen Komponenten, einschliesslich RP-PEP, abdecken zu prüfen. Dabei sollen die Verantwortlichen der relevanten Anwendungen entsprechend integriert werden, um eine ganzheitliche Testabdeckung der RP-PEP-Integrationen zu gewährleisten.

STELLUNGNAHME DES BEREICHS DTI

Die Empfehlung ist akzeptiert.

Es werden bereits heute Failover-Tests mit Einbezug von Anwendungen durchgeführt. Bei Failover-Tests wird ein Umschalten von einem Rechenzentrum zum anderen für das Vorkommen eines

unvorhergesehenen Störfalls geübt. Der Bereich DTI der Bundeskanzlei wird das BIT beauftragen, zu prüfen, wie die Tests regelmässig, insbesondere auch mit Anwendungen mit einer RP-PEP-Integration erweitert werden können.

Die Detailkonzepte werden im Verlauf 2025 erarbeitet. Die Umsetzung bis Mitte 2026 erfolgt unter Beizug eines spezialisierten Dritten, da Failover-Test auch erhebliche Ausfallrisiken mit sich bringen können.

3.3 Notfallpläne im Krisenfall sind nicht vorhanden

Es existieren Notfall- und Neustartpläne für die Rechenzentren, in welchen eIAM betrieben wird. Der Neustartplan für den Dienst eIAM wird auf Ebene des LE und unter der Leitung der Verantwortlichen für das Business Continuity Management (BCM) geregelt. eIAM ist Teil des Programms zur Dienstkontinuität des BIT. Aus diesem Grund hat das BIT ein Dokument für den Neustart von eIAM formalisiert. Dieses Dokument befindet sich derzeit in der internen Validierung. Die aktuelle Version betrifft vorerst nur das RZ «Primus» in Bern. Dennoch ist der Wechsel vom RZ «Primus» zum RZ «Campus» dokumentiert und wird unter der Leitung des BCM BIT durchgeführt.

Für einen möglichen Ausfall beider RZ existieren zum Prüfzeitpunkt keine konkreten Pläne.

BEURTEILUNG

Die Prüfung zeigt, dass bereits wichtige Massnahmen zur Sicherstellung der Dienstkontinuität für eIAM, insbesondere im Bereich des Neustartplans, ergriffen wurden. Die Existenz eines formalisierten Neustartplans für das Rechenzentrum «Primus» in Bern sowie die dokumentierte Möglichkeit, im Falle eines Ausfalls auf das Rechenzentrum «Campus» zu wechseln, sind positive Ansätze, um die Dienstverfügbarkeit aufrechtzuerhalten.

Jedoch gibt es wesentliche Lücken, die adressiert werden müssen. Die Tatsache, dass für den gleichzeitigen Ausfall beider Rechenzentren aktuell keine konkreten Notfallpläne existieren, stellt ein Risiko dar.

EMPFEHLUNG 4 — PRIORITÄT 2

Die EFK empfiehlt dem Bereich DTI in Zusammenarbeit mit dem BIT, Notfallpläne für den gleichzeitigen Ausfall beider Rechenzentren zu prüfen.

STELLUNGNAHME DES BEREICHS DTI

Die Empfehlung ist akzeptiert.

Der eIAM-Service ist redundant aufgebaut. Bei einem Ausfall des primären Rechenzentrum-Standorts kann der Betrieb innerhalb weniger Stunden im zweiten Rechenzentrum wieder aufgenommen werden. Die Wahrscheinlichkeit eines gleichzeitigen Ausfalls beider Rechenzentren des Bundes stuft der Bereich DTI als tief ein. Da AGOV auch Leistungen zu Gunsten der Kantone erbringt, ist es trotzdem sinnvoll, die bestehenden Notfallpläne mit diesem Szenario zu erweitern. DTI wird zusammen mit dem BIT mögliche Lösungen – insbesondere bezüglich der zeitlichen und finanziellen Rahmenbedingungen – erarbeiten und die Umsetzung prüfen.

ANHANG 1 – RECHTSGRUNDLAGEN

RECHTSTEXTE

Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG), SR 128
Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV), SR 128.1
Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der Bundesverwaltung (Verordnung über die digitale Transformation und die Informatik, VDTI), SR 172.010.58
Weisungen zur Steuerung und Führung der Standarddienste gemäss VDTI

ANHANG 2 – ABKÜRZUNGEN

AGOV	Authentifizierungsdienst der Schweizer Behörden (siehe Glossar)
BCM	Business Continuity Management
BIT	Bundesamt für Informatik und Telekommunikation
BK	Bundeskanzlei
BTB	Bundes Trustbroker (siehe Glossar)
DTI	Bereich Digitale Transformation und IKT-Lenkung
eIAM	Electronic Identity and Access Management
E-ID (e-ID, eID)	Elektronische Identität, elektronischer Identitätsnachweis, digitale Identität
EFK	Eidgenössische Finanzkontrolle
IAM	Identitäts- und Accessmanagement (siehe Glossar)
ISDS	Informationssicherheits- und Datenschutzkonzept
RP-PEP	Reverse Proxy- Policy Enforcement Point (siehe Glossar)
RZ	Rechenzentrum
SD	Standarddienst (siehe Glossar)
VK	Verfügbarkeitsklasse

ANHANG 3 – GLOSSAR

Aktiv-Aktiv-Betrieb	In diesem Zusammenhang bezeichnet eine Aktiv/Aktiv-Konfiguration eine gesicherte Ressource, wie beispielsweise eine Datenbank, die auf allen Clusterknoten gleichzeitig aktiv ist. Fällt ein Knoten aus, übernehmen die verbleibenden Knoten die Aufgaben des ausgefallenen Knotens, wodurch praktisch keine Ausfallzeit entsteht. Allerdings kann die Performance stark beeinträchtigt werden, da die verbleibenden Systeme die gesamte Last tragen müssen.
Authentifizierungsdienst der Schweizer Behörden	Ein Vorhaben der Digitalen Verwaltung Schweiz. AGOV ist das Behörden-Login der Schweiz. Es kann beim Bund sowie bei kantonalen und kommunalen Behörden eingesetzt werden.
Availability Zones	Beim Cloud Computing ist eine Verfügbarkeitszone eine Teilmenge eines IT-Infrastruktursystems, die keine dienstkritischen Komponenten mit anderen Verfügbarkeitszonen teilt.
Bundes Trustbroker	Der Bundes Trustbroker (BTB) ist eine zentrale Vertrauensstelle innerhalb der IT-Infrastruktur der öffentlichen Verwaltung in der Schweiz. Er ermöglicht den sicheren Austausch von Daten zwischen verschiedenen Behörden, Organisationen und Systemen, indem er die Authentifizierung und Autorisierung der beteiligten Akteure sicherstellt. Der BTB sorgt dafür, dass nur berechtigte Nutzer auf bestimmte Dienste und Informationen zugreifen können und stellt sicher, dass die Identitäten und Rechte der Benutzer verlässlich geprüft werden. Dies trägt zur Sicherheit und Effizienz in der digitalen Verwaltung bei.
Identitäts- und Accessmanagement	Identitäts- und Accessmanagement Systeme (IAM-Systeme) wie eIAM erfüllen die Aufgaben der (Wieder-)Erkennung von Benutzern (Identität) und optional der Übermittlung von Aussagen zu deren Berechtigungen in den Zielapplikationen (Access).
Policy Enforcement Point	Dies ist ein Punkt in einem Netzwerk, an dem Richtlinien (Policies) erzwungen werden. Der PEP prüft, ob ein Nutzer oder ein System die notwendigen Berechtigungen hat, um auf eine bestimmte Ressource zuzugreifen.
Reverse Proxy - Policy Enforcement Point	Hierbei handelt es sich um eine Komponente innerhalb eines Identity- und Access-Management-Systems (IAM), die oft im Zusammenhang mit Zugriffskontrollen und Authentifizierungsmechanismen eingesetzt wird. Somit übernimmt ein RP-PEP die Funktion, eingehende Anfragen zu überprüfen und sicherzustellen, dass sie den festgelegten Sicherheitsrichtlinien entsprechen, bevor sie an die geschützten Backend-Systeme weitergeleitet werden.
Reverse Proxy	Ein Reverse Proxy ist eine Art Server, der Anfragen von Clients (z.B. Webbrowser) entgegennimmt und diese an einen internen Server weiterleitet. Dabei fungiert er als Vermittler zwischen dem Client und dem Backend-System. Im Kontext von eIAM-Systemen dient ein Reverse Proxy oft dazu, externe Zugriffe zu kontrollieren und zu schützen.
Single Point of Failure	Ein Single Point of Failure (dt. einzelner Ausfallpunkt) bezeichnet einen Bestandteil eines technischen Systems, dessen Ausfall den gesamten Systembetrieb beeinträchtigt.
Standarddienst	Informatikleistungen, welche die Verwaltungseinheiten des Bundes in gleicher oder ähnlicher Funktionalität und Qualität benötigen, werden als so genannte IKT-Standarddienste zentral für die ganze Bundesverwaltung geführt und zum Bezug angeboten.