INFORMATIKPROJEKTE

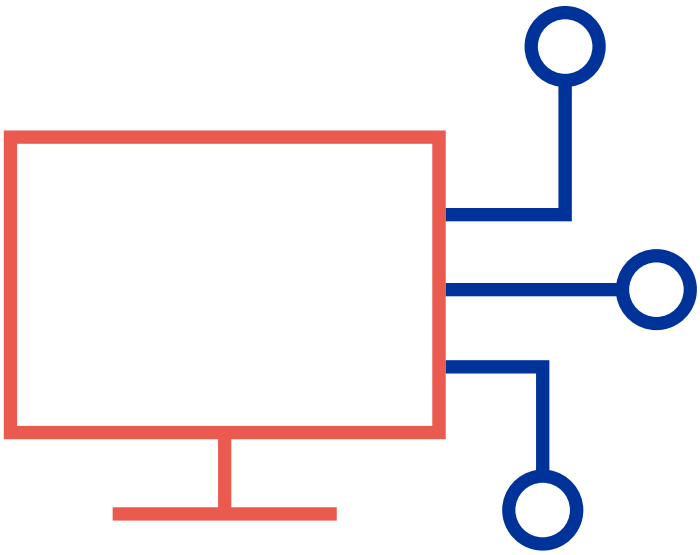
Prüfung des Schlüsselprojektes E-ID

Bundesamt für Justiz
Bundesamt für Polizei fedpol
Bundesamt für Informatik und Telekommunikation

EFK-25277

VERSION INKL. STELLUNGNAHMEN

19.12.2025



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

402.25277

ZUSÄTZLICHE INFORMATIONEN
COMPLÉMENT D'INFORMATIONS
INFORMAZIONI COMPLEMENTARI
ADDITIONAL INFORMATION

www.efk.admin.ch
info@efk.admin.ch
+ 41 58 463 11 11

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

PRÜFUNG

Prüfung des Schlüsselprojektes E-ID

Bundesamt für Justiz
Bundesamt für Polizei fedpol
Bundesamt für Informatik und Telekommunikation

DAS WESENTLICHE IN KÜRZE

Die EFK hat zum zweiten Mal das Programm Elektronischer Identifikationsnachweis (E-ID) geprüft. In dieser Prüfung beurteilte die EFK die Projekte «E-ID Ausstellung» und «Vertrauensinfrastruktur» und die technische Ausgestaltung der IT-Sicherheit der Schweizer E-ID. Für die Umsetzung dieser Projekte sind das Bundesamt für Justiz (BJ), das Bundesamt für Polizei fedpol sowie das Bundesamt für Informatik und Telekommunikation (BIT) zuständig. Als Vertrauensinfrastruktur wird die technische Plattform bezeichnet, die für die Prozesse beim Einsatz einer Schweizer E-ID vom Bund zur Verfügung gestellt wird. Die Vertrauensinfrastruktur ist offen gestaltet, so dass auch andere elektronische Nachweise darin abgebildet werden können.

Für die Entwicklung und den Betrieb der Vertrauensinfrastruktur, die Ausstellung der E-ID sowie die Pilotprojekte wurden Aufwände in Höhe von rund 182 Mio. Franken bewilligt. Nach Projektabschluss wird mit jährlichen Betriebsaufwänden von rund 25 Mio. gerechnet. Das Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz) ist zum Prüfungszeitpunkt Gegenstand der eidgenössischen Abstimmung vom 28. September 2025. Die Testversion der E-ID «Public Beta» und die Mobiltelefonanwendung (App) «swiyu» laufen seit Ende März 2025. Mit swiyu kann man elektronische Nachweise wie z. B. die E-ID speichern und im Rahmen einer Transaktion digital vorweisen.

Bis zum frühestmöglich geplanten Start der E-ID im 3. Quartal 2026 hat das Programm noch einige wesentliche Aufgaben vor sich. Die EFK ist angesichts der Zahl der noch offenen Themen im Programm besorgt. Sie sieht das Risiko, dass die zum Ende geplante Stabilisierungsphase als Zeitreserve für ungeplante Entwicklungs- bzw. Korrekturarbeiten zweckentfremdet werden könnte. Da bei der E-ID Fehlerfreiheit und Reife des Produktes aus Risikoüberlegungen höher zu gewichten sind als eine termingerechte Einführung, empfiehlt die EFK, an der Stabilisierungsphase am Ende in voller Länge festzuhalten. Dies auch, wenn sich die Einführung der E-ID dadurch verschieben würde.

Für die E-ID ist keine Überprüfung von legitimen Abfragezwecken geplant

Die Schweizer Vertrauensinfrastruktur für die E-ID und andere elektronische Nachweise ist noch im Aufbau. Kernelemente davon sind das Basisregister und das Vertrauensregister: Im Basisregister sind die widerrufenen Nachweise und alle registrierten Teilnehmenden hinterlegt. Ausstellerinnen oder Verifikatorinnen, die den Nutzenden besonderes Vertrauen vermitteln wollen, können ihre Identität durch das BJ freiwillig tiefergehend prüfen lassen. Ist das Ergebnis positiv, erfolgt ein entsprechender Eintrag in das zweite, sogenannte Vertrauensregister. Die swiyu-App, die von allen Nutzenden für elektronische Nachweise verwendet werden kann, zeigt bei einer Transaktion an, wenn die Identität des Gegenübers positiv in das Vertrauensregister eingetragen ist.

Darüber hinaus werden die notwendigen rechtlichen und technischen Vorkehrungen getroffen, um über die Identität der Teilnehmenden hinaus auch die Legitimation einer Verifikatorin zur Abfrage der E-ID tiefergehend prüfen zu können. Das Programm plant jedoch derzeit, vom Einsatz positiver Vertrauensregistereinträge für überprüfte Verifikationszwecke abzusehen. Dies, um den Einsatz der E-ID nicht durch behördliche Prüfungen zu erschweren, den Teilnehmern Kosten und Aufwand zu ersparen und die Wahrnehmung zu vermeiden, dass einzelne Teilnehmer vertrauenswürdiger seien als andere.

Die EFK erachtet es aber als wichtig für das im E-ID-Gesetz vorgesehene Vertrauensregister, dass legitime Abfragezwecke der E-ID als solche dargestellt werden. Sie empfiehlt dem Programm daher, einen freiwilligen

Prozess zur Überprüfung der legitimen Abfragezwecke von Verifikatorinnen und die entsprechenden positiven Vertrauensregistereinträge bei der E-ID vorzusehen und anzuwenden.

Die Verschlüsselung der Nutzdaten ist noch nicht fertig konzipiert und integriert

Die Kommunikation der verschiedenen Beteiligten am Ökosystem der Schweizer E-ID läuft mittels gängiger technischer Methoden verschlüsselt ab. Jedoch sind diese nicht in allen Fällen ausreichend sicher gegen Angriffe von Unbekannten, insbesondere aufgrund der nicht vertrauenswürdigen Strukturen moderner anonymer Datentransportnetze. Es ist daher notwendig und auch vom Programm geplant, die zwischen den Teilnehmern übermittelten Nutzdaten der E-ID auch Ende-zu-Ende zu verschlüsseln. Die EFK begrüsst diese Massnahme, ist jedoch überrascht, dass die entsprechende Konzeption der Nutzdatenverschlüsselung bei der E-ID noch nicht abgeschlossen ist und deren Entwicklung im Projekt Vertrauensinfrastruktur noch aussteht. Die Planungsunterlagen sehen vor, dass diese Aufgabe bis Ende 2025 abgeschlossen sein soll.

Die Testversion «Public Beta» entspricht nur zu Teilen der späteren E-ID

Die laufende Testversion «Public Beta» beinhaltet speziell für Demonstrationszwecke entwickelte Prozesse einer «Beta ID». Die späteren Prozesse der E-ID sollen die Grundlagen der Beta ID berücksichtigen, befinden sich aber noch in der Entwicklung. Ein wesentliches noch offenes Thema hierbei ist die Fertigstellung und Integration der E-ID Ausstellungsprozesse des fedpol (während eine Beta ID auf Knopfdruck erstellt werden kann, erfolgt bei der E-ID ein Ausstellungsprozess).

Das Projekt Vertrauensinfrastruktur konzentriert sich in der aktuellen Phase auf Entwickler- und Integrationstests. Darüber hinaus werden alle neu entwickelten Funktionen vor Freigabe zunächst durch Penetrationstests überprüft. Ein Konzept für Ende-zu-Ende-Tests der E-ID liegt bereits vor, die konkreten Testfälle müssen jedoch noch erstellt werden. Diese Benutzertests sind vor allem ab Frühjahr 2026 vorgesehen.

Der produktive Betrieb muss noch vorbereitet und ausreichend erprobt werden

Im Sommer 2026 plant das Programm eine Phase zur Stabilisierung und finalen Abnahme des Gesamtsystems der E-ID. Spätestens in dieser Phase muss auch der produktive Betrieb aufgebaut sein. Es ist sinnvoll, die Anforderungen an den Betrieb vorher zu erheben und Massnahmen bereits in der Public Beta möglichst breit zu erproben. Dies erhöht jedoch neben der abzuschliessenden Entwicklung und den noch aufzubauenden Ende-zu-Ende-Tests den allgemeinen Zeitdruck auf das Programm.

Während dies in gewissem Umfang zu normalem Projektgeschäft gehört, sieht die EFK hier das Risiko, dass die zur Stabilisierung geplante Zeit im Sommer 2026 zu Gunsten ausstehender Entwicklungen oder Fehlerbehebungen umgenutzt werden könnte. Die EFK empfiehlt dem BJ daher, in der Programmplanung dafür zu sorgen, dass ausreichend Budget, Zeit und Personal für eine wirksame Stabilisierungsphase und zum Aufbau des Betriebs zur Verfügung steht. Dies kann in Konsequenz bedeuten, dass der Start der E-ID später als geplant erfolgen könnte.

AUDIT

Audit du projet clé e-ID

Office fédéral de la justice

Office fédéral de la police fedpol

Office fédéral de l'informatique et de la télécommunication

L'ESSENTIEL EN BREF

Le Contrôle fédéral des finances (CDF) a examiné pour la deuxième fois le programme d'identité électronique (e-ID). Au cours de cet examen, il a évalué les projets « Délivrance de l'e-ID » et « Infrastructure de confiance », ainsi que les aspects techniques de la sécurité informatique de l'e-ID suisse. La mise en œuvre de ces deux projets relève de la compétence de l'Office fédéral de la justice (OFJ), de l'Office fédéral de la police fedpol ainsi que de l'Office fédéral de l'informatique et de la télécommunication (OFIT). L'infrastructure de confiance désigne la plateforme technique fournie par la Confédération pour les procédures liées à l'utilisation d'une e-ID suisse. Sa conception ouverte lui permet d'accueillir également d'autres moyens de preuves électroniques.

Des dépenses de près de 182 millions de francs ont été approuvées pour le développement et l'exploitation de l'infrastructure de confiance, pour la délivrance de l'e-ID et les projets pilotes. À la fin du projet, des charges d'exploitation annuelles de l'ordre de 25 millions de francs sont à prévoir. La loi fédérale sur l'identité électronique et d'autres moyens de preuves électroniques (LeID) a fait l'objet d'une votation fédérale le 28 septembre 2025, soit pendant l'audit. La version d'essai de l'e-ID « Public Beta » et l'application mobile « swiyu » sont opérationnelles depuis la fin mars 2025. swiyu permet d'enregistrer des moyens de preuves électroniques comme l'e-ID et de les présenter sous forme numérique lors d'une transaction.

Le programme devra encore venir à bout de plusieurs tâches essentielles avant le lancement de l'e-ID, prévu au troisième trimestre 2026 au plus tôt. Le CDF s'inquiète du nombre de questions restées en suspens. Selon lui, il est à craindre que la phase de stabilisation planifiée à la fin du programme ne soit détournée de sa finalité initiale au profit d'activités de développement ou de corrections tardives. Même si l'introduction de l'e-ID devait s'en trouver retardée, le CDF recommande de maintenir dans son intégralité la phase de stabilisation finale prévue, car, pour des considérations liées aux risques, l'absence de défaut et la maturité du produit doivent primer sur l'introduction de l'e-ID à la date prévue au départ.

Absence de vérification prévue de la légitimité des consultations effectuées de l'e-ID

L'infrastructure de confiance suisse destinée à l'e-ID et à d'autres moyens de preuves électroniques est encore dans sa phase de mise en place. Elle comprend essentiellement un registre de base et un registre de confiance : le registre de base renferme les moyens de preuves révoqués et tous les participants enregistrés. Les émetteurs ou les vérificateurs souhaitant renforcer la confiance des utilisateurs peuvent, de leur plein gré, faire vérifier plus en détail leur identité par l'OFJ. En cas de résultat positif, une entrée figurera dans le deuxième registre, soit le registre de confiance. L'application swiyu, dont chacun peut faire usage pour ses moyens de preuves électroniques, indique à chaque transaction si l'identité de la contrepartie est enregistrée ou non dans le registre de confiance.

En outre, les dispositions légales et techniques nécessaires ont été émises pour permettre de vérifier en détail, au-delà de l'identité des participants, la légitimité d'un vérificateur à consulter l'e-ID. Le programme prévoit toutefois à l'heure actuelle de ne pas exiger des vérificateurs qu'ils figurent dans le registre de confiance attestant de la pertinence de leurs consultations. Il s'agit de ne pas compliquer l'utilisation de l'e-ID par des contrôles administratifs, d'éviter aux participants des coûts et des efforts inutiles, et de ne pas donner l'impression que certains participants sont plus dignes de confiance que d'autres.

Le CDF juge toutefois important, pour le registre de confiance prévu dans la LeID, d'indiquer comme tels les motifs légitimes de consultation de l'e-ID. Il recommande donc au programme de prévoir et d'utiliser pour l'e-ID une procédure à caractère facultatif de vérification de la légitimité des motifs de consultation des vérificateurs et d'inscrire les résultats positifs obtenus dans le registre de confiance.

Phase de conception et d'intégration du cryptage des données utiles pas encore terminée

La communication entre les protagonistes de l'écosystème de l'e-ID suisse repose sur les méthodes usuelles de chiffrement des données. Or ces méthodes sont loin de toujours offrir une sécurité suffisante face à des agresseurs inconnus, en raison notamment du manque de fiabilité des structures des réseaux anonymes servant à l'heure actuelle au transport des données. Il est par conséquent nécessaire, comme le prévoit le programme, de crypter de bout en bout les données utiles de l'e-ID transmises entre les participants. Le CDF approuve une telle mesure, tout en s'étonnant que la phase de conception du cryptage de ces données ne soit pas encore terminée et que les développements correspondants se fassent encore attendre dans le projet d'infrastructure de confiance. Selon la feuille de route, cette tâche devrait être terminée d'ici la fin de 2025.

Version d'essai Public Beta partiellement conforme à l'e-ID à venir

La version d'essai en cours Public Beta comprend des procédures spécialement développées à des fins de démonstration pour une Beta ID. Les procédures subséquentes de l'e-ID, qui tiendront compte des bases de la Beta ID, sont en cours de développement. Un point essentiel est encore ouvert dans ce contexte, à savoir la finalisation et l'intégration des procédures de fedpol spécifiques à l'émission de l'e-ID (alors qu'une Beta ID peut être créée en un clic, l'e-ID fera l'objet d'une procédure d'émission).

Le projet d'infrastructure de confiance se concentre, dans sa phase actuelle, sur des tests de développement et d'intégration. En outre, toute nouvelle fonctionnalité développée est d'abord soumise à des tests de pénétration avant d'être validée. Bien qu'un plan de tests de bout en bout de l'e-ID existe déjà, il reste à définir les cas concrets à tester. Les tests auprès des utilisateurs sont principalement prévus à partir du printemps 2026.

Nécessité de préparatifs et de tests suffisants avant l'exploitation productive

Le programme prévoit pour l'été 2026 une phase de stabilisation et de réception finale de l'ensemble du système e-ID. Ce sera le dernier moment pour mettre en place l'exploitation productive. Il serait donc judicieux de passer d'abord en revue les exigences relatives à l'exploitation et de tester de manière aussi large que possible les mesures prévues dès la version Public Beta. Il est vrai que ces activités, en venant s'ajouter aux travaux de développement à terminer et aux tests de bout en bout à mettre au point, ne feront qu'accroître la pression en termes de délais à laquelle le programme est soumis.

Bien qu'il s'agisse jusqu'à un certain point d'un phénomène courant en gestion de projet, le CDF voit un réel risque que le temps prévu pour la stabilisation durant l'été 2026 serve plutôt à des activités de développement restées en souffrance ou à des corrections tardives. Le CDF recommande donc à l'OFJ de veiller, dans sa planification du programme, à prévoir un budget adéquat, assez de temps et les ressources en personnel nécessaires à une phase de stabilisation efficace ainsi qu'à la mise en place de l'exploitation. Il pourrait en résulter un report de la date actuellement prévue pour le lancement de l'e-ID.

VERIFICA

Verifica del progetto chiave e-ID

Ufficio federale di giustizia

Ufficio federale di polizia fedpol

Ufficio federale dell'informatica e della telecomunicazione UFIT

L'ESSENZIALE IN BREVE

Il Controllo federale delle finanze (CDF) ha esaminato per la seconda volta il programma per la prova elettronica dell'identità (e-ID). Nell'ambito della presente verifica, il CDF ha valutato i progetti «Emissione e-ID» e «Infrastruttura di fiducia» nonché la configurazione tecnica della sicurezza IT dell'e-ID svizzera. L'attuazione di questi progetti è di competenza dell'Ufficio federale di giustizia (UFG), dell'Ufficio federale di polizia fedpol e dell'Ufficio federale dell'informatica e della telecomunicazione (UFIT). Per «infrastruttura di fiducia» si intende la piattaforma tecnica messa a disposizione dalla Confederazione per i processi relativi all'utilizzo di un'identità elettronica svizzera. L'infrastruttura di fiducia è di tipo aperto, affinché possano essere integrate anche altre prove elettroniche.

Per lo sviluppo e la gestione dell'infrastruttura di fiducia, il rilascio dell'e-ID e i progetti pilota, sono stati approvati stanziamenti pari a circa 182 milioni di franchi. Una volta concluso il progetto, si prevedono spese di gestione annuali pari a circa 25 milioni. Al momento della verifica, la legge del 20 dicembre 2024 sull'Id-e è oggetto della votazione federale del 28 settembre 2025. La versione di prova dell'e-ID «Public Beta» e l'applicazione (app) per telefoni cellulari «swiyu» sono operative dalla fine di marzo 2025. Con swiyu è possibile salvare mezzi di autenticazione elettronici come l'e-ID e presentarli in formato digitale al momento di una transazione.

Fino al lancio dell'e-ID, previsto non prima del terzo trimestre del 2026, il programma prevede ancora alcuni compiti importanti da portare a termine. Il CDF si dice preoccupato per il numero di questioni ancora aperte e ritiene vi sia il rischio che la fase di stabilizzazione prevista alla fine del programma possa essere utilizzata in modo improprio come riserva di tempo per lavori di sviluppo o di correzione non pianificati. Dal momento che sotto il profilo del rischio l'assenza di errori e la maturità del prodotto sono più importanti della tempestività della sua introduzione, il CDF raccomanda di mantenere nella sua interezza la fase finale di stabilizzazione, anche se dovesse comportare un rinvio dell'introduzione dell'e-ID.

Non è prevista alcuna verifica delle finalità legittime di consultazione

L'infrastruttura di fiducia svizzera per l'e-ID e altri mezzi di autenticazione elettronici è ancora in fase di sviluppo. Suoi elementi centrali sono il registro di base e il registro di fiducia. Nel primo sono archiviati i mezzi di autenticazione revocati e tutti i partecipanti registrati. Gli emittenti o i verificatori che desiderano trasmettere particolare fiducia agli utenti possono sottoporre volontariamente la propria identità a una verifica approfondita da parte dell'UFG. Se il risultato è positivo, viene effettuata una registrazione nel registro di fiducia. L'app swiyu, che può essere utilizzata da tutti gli utenti per i mezzi di autenticazione elettronici, indica durante una transazione se l'identità della controparte è stata registrata positivamente nel registro di fiducia.

Inoltre, vengono adottate le misure giuridiche e tecniche necessarie a verificare in modo approfondito, oltre all'identità dei partecipanti, anche la legittimazione di un verificatore a consultare l'e-ID. Tuttavia, il programma prevede attualmente di rinunciare all'utilizzo di registrazioni positive nel registro di fiducia per finalità di consultazione verificate. Ciò al fine di non complicare l'utilizzo dell'e-ID con verifiche amministrative, di risparmiare costi e oneri ai partecipanti e di evitare la percezione che alcuni partecipanti siano più affidabili di altri.

Il CDF ritiene tuttavia importante per il registro di fiducia previsto dalla legge sull'Id-e che le finalità legittime di consultazione dell'e-ID siano presentate come tali. Raccomanda quindi che nel programma sia previsto e

applicato un processo volontario di verifica delle finalità legittime di consultazione dei verificatori e delle corrispondenti registrazioni positive nel registro di fiducia dell'e-ID.

La crittografia dei dati utente non è ancora completata né integrata

La comunicazione tra i diversi attori dell'ecosistema dell'e-ID svizzero avviene in forma crittografata utilizzando metodi tecnici comuni. Tuttavia, questi non sono sempre sufficientemente sicuri contro gli attacchi di sconosciuti, in particolare a causa delle strutture inaffidabili delle moderne reti di trasporto dati anonime. È quindi necessario, come previsto dal programma, crittografare i dati utili dell'e-ID trasmessi tra i partecipanti anche end-to-end. Il CDF accoglie con favore questa misura, ma è sorpreso dal fatto che la concezione della crittografia dei dati utili nell'e-ID non sia ancora stata portata a termine e che il suo sviluppo nel progetto «Infrastruttura di fiducia» sia ancora in sospeso. La documentazione relativa alla pianificazione prevede che questo compito sia completato entro la fine del 2025.

La versione di prova Public Beta corrisponde soltanto in parte alla futura e-ID

La versione di prova Public Beta attualmente in uso comprende processi di Beta-ID sviluppati appositamente a scopo dimostrativo. I processi successivi dell'e-ID terranno conto dei principi fondamentali della Beta-ID, ma sono ancora in fase di sviluppo. Una questione fondamentale ancora aperta sono il completamento e l'integrazione dei processi di emissione dell'e-ID da parte di fedpol (mentre una Beta-ID può essere creata con un semplice clic, l'e-ID richiede un processo di emissione).

Nella fase attuale, il progetto «Infrastruttura di fiducia» si concentra sui test di sviluppo e di integrazione. Inoltre, tutte le nuove funzionalità sviluppate vengono sottoposte a test di penetrazione prima del rilascio. È già disponibile un piano per i test end-to-end dell'e-ID, ma i casi di test concreti devono ancora essere creati. Questi test utente sono previsti prevalentemente a partire dalla primavera del 2026.

La messa in produzione deve ancora essere preparata e sufficientemente testata

Il programma prevede nell'estate del 2026 una fase di stabilizzazione e collaudo finale dell'intero sistema di identificazione elettronica. Al più tardi in questa fase dovrà essere avviata anche la messa in produzione. È opportuno definire in anticipo i requisiti operativi e testare nel modo più ampio possibile le misure già nella versione Public Beta. Tuttavia, insieme allo sviluppo da completare e ai test end-to-end ancora da realizzare, ciò fa sì che la pressione sulla tempistica del programma cresca.

Sebbene in una certa misura questo rientri nella normale attività di progetto, il CDF ritiene vi sia il rischio che il periodo per la stabilizzazione previsto nell'estate del 2026 possa essere utilizzato per completare gli sviluppi in sospeso o correggere errori. Il CDF raccomanda quindi all'UFG di garantire, nella pianificazione del programma, che vengano messi a disposizione budget, tempo e personale a sufficienza per garantire una fase di stabilizzazione efficace e la messa in produzione. Ciò significa che l'introduzione dell'e-ID potrebbe avvenire più tardi del previsto.

AUDIT

Audit of the key project e-ID

Federal Department of Justice

Federal Office of Police fedpol

Federal Office of Information Technology, Systems and Telecommunication

KEY FACTS

The SFAO audited the electronic proof of identity (e-ID) programme for the second time. In this audit, the SFAO assessed the "e-ID issuance" and "trust infrastructure" projects, and the technical design of the Swiss e-ID's IT security. The Federal Office of Justice (FOJ), the Federal Office of Police fedpol and the Federal Office of Information Technology, Systems and Telecommunication (FOITT) are responsible for implementing these projects. The trust infrastructure refers to the technical platform provided by the federal government for the processes associated with the use of a Swiss e-ID. The trust infrastructure is designed to be open so that other electronic proofs of identity can also be integrated into it.

Approximately CHF 182 million was approved for developing and operating the trust infrastructure, issuing the e-ID and pilot projects. Once the project is complete, annual operating costs of around CHF 25 million are expected. At the time of the audit, the Federal Act on Electronic Identity and Other Electronic Credentials (e-ID Act) was subject to a federal popular vote on 28 September 2025. The test version of the "Public Beta" e-ID and the "swiyu" mobile phone app have been running since the end of March 2025. Swiyu allows users to store electronic credentials such as e-IDs and present them digitally when making transactions.

The programme still has a number of key tasks to complete before the earliest possible launch of the e-ID in the third quarter of 2026. The SFAO is concerned about the number of issues still outstanding in the programme. It sees a risk that the stabilisation phase planned for the end of the programme could be misused as a time reserve for unplanned development or corrective work. Since, for risk reasons, the error-free nature and maturity of the product are more important than its timely introduction, the SFAO recommends that the stabilisation phase at the end be maintained in full. This should be done even if it means postponing the introduction of the e-ID.

There are no plans to verify the legitimacy of e-ID checks

The Swiss trust infrastructure for the e-ID and other electronic credentials is still under development. Its core elements are the basic register and the trust register: the basic register contains revoked proofs and all registered participants. Issuers and verifiers who want to instil a high level of trust in users can voluntarily have their identity checked in more detail by the FOJ. If the result is positive, a corresponding entry is made in the second register, known as the trust register. The swiyu app, which can be used by all users for electronic credentials, indicates during a transaction when the identity of the other party has been positively entered in the trust register.

In addition, the necessary legal and technical precautions are being taken to enable in-depth verification of the identity of not only the participants but also the legitimacy of a verifier to check the e-ID. However, the programme currently plans to refrain from using positive trust register entries for verified authentication purposes. This is to avoid complicating the use of the e-ID through official checks, to save participants costs and effort, and to avoid the perception that individual participants are more trustworthy than others.

However, the EFK considers it important that the trust register established under the e-ID Act clearly indicates which purposes for checking the e-ID are legitimate. It therefore recommends that the programme provide for and apply a voluntary process for checking the legitimate purposes of verifiers and the corresponding positive trust register entries for the e-ID.

The encryption of user data has not yet been fully designed and integrated

Communication between the various parties involved in the Swiss e-ID ecosystem is encrypted using standard technical methods. However, these are not always sufficiently secure against attacks by unknown parties, in particular due to the untrustworthy structures of modern anonymous data transport networks. It is therefore necessary, and also planned as part of the programme, to end-to-end encrypt the e-ID user data transmitted between participants. The EFK welcomes this measure, but is surprised that the relevant concept for e-ID user data encryption has not yet been finalised and that its development is still pending in the trust infrastructure project. The plans stipulate that this task should be completed by the end of 2025.

The Public Beta test version only partially reflects the future e-ID

The current Public Beta test version includes Beta ID processes developed specifically for demonstration purposes. The future e-ID processes will incorporate the principles of the Beta ID, but are still under development. A key issue that remains unresolved is the completion and integration of fedpol's e-ID issuance processes (unlike a beta ID, which can be created at the touch of a button, the e-ID requires an issuance process).

In its current phase, the trust infrastructure project is focusing on developer and integration tests. Furthermore, all newly developed functions are first checked using penetration tests before being released. A concept for end-to-end testing of the e-ID is already in place, but the specific test cases still need to be created. These user tests are primarily planned for spring 2026 onwards.

Productive operation still needs to be prepared and sufficiently tested

The programme envisages a phase for stabilising and finally approving the overall e-ID system in summer 2026. Productive operation must also be in place by this phase at the latest. It makes sense to identify the operational requirements in advance and to test measures as extensively as possible in the Public Beta version. However, in addition to the development work that still needs to be completed and the end-to-end tests that have yet to be set up, this increases the general time pressure on the programme.

While this is to a certain extent part of any normal project, the SFAO sees a risk here that the time planned for stabilisation in summer 2026 could be reallocated in favour of ongoing development work or troubleshooting. The EFK therefore recommends that the FOJ ensure that sufficient budget, time and personnel are made available in the programme planning for an effective stabilisation phase and for setting up operations. As a consequence, this may mean that the e-ID could be launched later than planned.

GENERELLE STELLUNGNAHME DES BUNDESAMTES FÜR JUSTIZ

Das Bundesamt für Justiz BJ bedankt sich für die sorgfältige Durchführung der zweiten Prüfung des Programms E-ID. Die Zusammenarbeit war wiederum konstruktiv, und wir begrüssen grundsätzlich die von der EFK aufgezeigten Optimierungsmöglichkeiten für das Programm E-ID. Diese waren für die noch anstehenden Umsetzungsarbeiten bereits eingeplant. Für das BJ ist es – auch aus Sicht des Programmauftraggebers – ein bewährtes Vorgehen in einem agilen Vorhaben, dass rund ein Jahr vor Betriebsaufnahme verschiedene Punkte zwar geplant, aber noch nicht umgesetzt sind.

GENERELLE STELLUNGNAHME DES BUNDESAMTES FÜR POLIZEI

Fedpol verzichtet auf eine eigene generelle Stellungnahme und beteiligt sich bei der generellen Stellungnahme des FF-Amtes.

GENERELLE STELLUNGNAHME DES BUNDESAMTES FÜR INFORMATIK UND TELEKOMMUNIKATION

Das BIT bedankt sich bei der EFK für die Prüfung des Programms E-ID.

Das BIT nimmt Berichte und Empfehlungen der EFK zum Anlass, sich stetig zu verbessern. Wenn die EFK im Programm E-ID Sachverhalte bemängelt, die Teil eines planmässigen Vorgehens sind und keine Anhaltspunkte für Abweichungen von diesem Vorgehen bestehen, weisen solche Erkenntnisse der EFK aus Sicht des BIT einen eingeschränkten Mehrwert auf und führen zu einer inadäquaten Darstellung der Risikosituation. Verschiedene Risiken werden von der EFK aufgeführt, die zum Prüfzeitpunkt keine sind, da sie durch den Programmverlauf planmässig adressiert werden.

Die E-ID ist noch nicht in der Betriebsphase. Die von der EFK bemängelten Punkte sind offene Aspekte eines agilen Vorhabens und werden planmässig umgesetzt. So ist beispielsweise die sichere verschlüsselte Übermittlung der Nutzdaten zum Prüfzeitpunkt der EFK ordnungsgemäss konzipiert und eingeplant gewesen und wird per Ende 2025 abgeschlossen sein. Das Programm E-ID hat der EFK die Spezifikation der sicheren Nutzdatenverschlüsselung zum Prüfzeitpunkt im Entwurf vorgelegt. Zudem ist es ein bewährtes Vorgehen, dass die Ergebnisse der End-Zu-End-Tests während des Prüfzeitpunkts noch nicht vorlagen. Denn zuerst müssen die Entwicklungs- und Integrationstests durchgeführt werden. Die End-Zu-End-Tests waren zum Prüfzeitpunkt der EFK bereits eingeplant.

Auch das BIT setzt konsequent das «DevSecOps» Verfahren ein, welches vorgibt, dass die Sicherheit ein integraler, automatisierter und kontinuierlicher Bestandteil des gesamten Entwicklungs- und Betriebsprozesses von Software ist.

Die EFK bemängelt zudem, dass der SIEM-Prozess (Security Incident und Event Monitoring Prozess) zur Erkennung von Sicherheitsvorfällen noch aufgebaut werden muss. Dies entspricht nicht den Tatsachen: eingesetzt wird der bewährte SIEM-Prozess vom BIT CSIRT gemäss den Vorgaben des Bundesamtes für Cybersicherheit BACS, wie er planmässig im vorliegenden Sicherheitskonzept spezifiziert wurde.

Die Stellungnahmen wurden unverändert und unkommentiert in den Bericht übernommen.

1 AUFTRAG UND VORGEHEN

1.1 Ausgangslage

Am 7. März 2021 wurde das Bundesgesetz über elektronische Identifizierungsdienste an der Urne mit 64 Prozent Nein-Stimmen abgelehnt. Am 10. März 2021 sind sechs inhaltlich gleiche Motionen mit dem Titel «Vertrauenswürdige staatliche E-ID» von allen Fraktionen eingereicht worden. Im Mai 2021 erklärte der Bundesrat, dass er rasch eine neue Lösung für den elektronischen Identitätsnachweis vorlegen wolle, die den Anliegen der Motionen Rechnung trägt. Er beauftragte das Bundesamt für Justiz (BJ) mit der Initialisierung des Programms E-ID.

Mit der Botschaft vom 22. November 2023 wurde der Entwurf des E-ID Gesetzes sowie Ressourcen in Höhe von rund 182 Mio. Franken zur Entwicklung der Vertrauensinfrastruktur, der Ausstellung der E-ID und dazugehörige Pilotprojekte bewilligt. Nach Projektabschluss wird mit einem Aufwand für den Betrieb von jährlich rund 25 Mio. gerechnet.

Ab August 2024 wurde das Programm E-ID zur Umsetzung beauftragt. Dieses hat zum Ziel, dass sich Nutzerinnen und Nutzer der elektronischen Identität des Bundes (E-ID) zukünftig sicher, schnell und unkompliziert digital ausweisen können. Die E-ID soll vom Bund herausgegeben werden, den grösstmöglichen Schutz der persönlichen Daten gewährleisten, sowie kostenlos und freiwillig sein. Die E-ID Infrastruktur soll auch von kantonalen und kommunalen Behörden sowie von Privaten für die Ausstellung von elektronischen Nachweisen genutzt werden können. Das BJ nimmt im Programm die Rolle des Auftraggebers wahr.

Die E-ID soll, vorbehaltlich des Terminplanes zur Inkraftsetzung der Rechtsgrundlage für die E-ID, dem Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz), frühestens im 3. Quartal 2026 eingeführt werden. Das Programm befindet sich zum Zeitpunkt der Prüfung in der Realisierung.

Die EFK prüft das Vorhaben zum zweiten Mal. Nachdem in der ersten Prüfung im Jahr 2023 die Programm- und Projektgouvernanz beurteilt wurde, steht im vorliegenden Prüfauftrag die konkrete Ausgestaltung und technische Umsetzung der E-ID im Vordergrund.

1.2 Prüfungsziel und -fragen

Ziel der Prüfung war die Beurteilung der Projekte Ausstellung E-ID (fedpol) und Vertrauensinfrastruktur (BIT) im Hinblick auf die technische Umsetzung, die EU-Kompatibilität und die IT-Sicherheit. Die folgenden Fragen werden beantwortet:

- Können Vertraulichkeit, Verfügbarkeit und Integrität der Daten bei der Ausstellung der E-ID entsprechend den angewendeten Vorgaben und Standards sichergestellt werden?
- Verfügen E-ID-Portal und Wallet über angemessene Sicherheitsmechanismen zur Erkennung und Behandlung von unautorisierten internen und externen Zugriffen?
- Werden ausreichende Massnahmen ergriffen, um die Interoperabilität der Schweizer E-ID mit EU-Systemen gewährleisten zu können?

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Martin Scheid (Revisionsleiter) und Warren Paulus vom 4. August bis 9. September 2025 durchgeführt. Sie erfolgte unter der Federführung von Martina Moll. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach der Prüfungsdurchführung.

1.4 Unterlagen und Auskunftserteilung

Die notwendigen Auskünfte wurden der EFK von den Geprüften umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen sowie die benötigte Infrastruktur standen dem Prüfteam vollumfänglich zur Verfügung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 13. November 2025 statt. Teilgenommen haben von Seiten Bundesamt für Justiz der Direktor, der Chef E-ID und der Programmkoordinator E-ID; von Seiten Bundesamt für Polizei der Chef Polizeisysteme und Identifikation, der Projektleiter E-ID Ausstellung und der CIO; von Seiten ISC-EJPD der Stellvertretende Leiter; von Seiten des Bundesamtes für Informatik und Telekommunikation der Leiter Interne Revision, der Business Owner Resources, Foreign Affairs und Defense und der Projektleiter Vertrauensinfrastruktur sowie von Seiten EFK die Mandatsleiterin, die Federführende und der Revisionsleiter.

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

EIDGENÖSSISCHE FINANZKONTROLLE

2 FUNKTIONALE AUSGESTALTUNG

2.1 Ohne überprüfte Verifikationszwecke leidet die Vertrauensfähigkeit

Die Vertrauensinfrastruktur besteht aus:

- den beiden vom Bund entwickelten Mobiltelefonanwendungen zur Speicherung der E-ID (die Wallet swiyu) und deren Verifikation, sowie
- Verzeichnissen der widerrufenen elektronischen Nachweise und der registrierten Teilnehmenden (sog. «Basisregister») sowie tiefergehend geprüfter Ausstellerinnen und Verifikatorinnen («Vertrauensregister»).

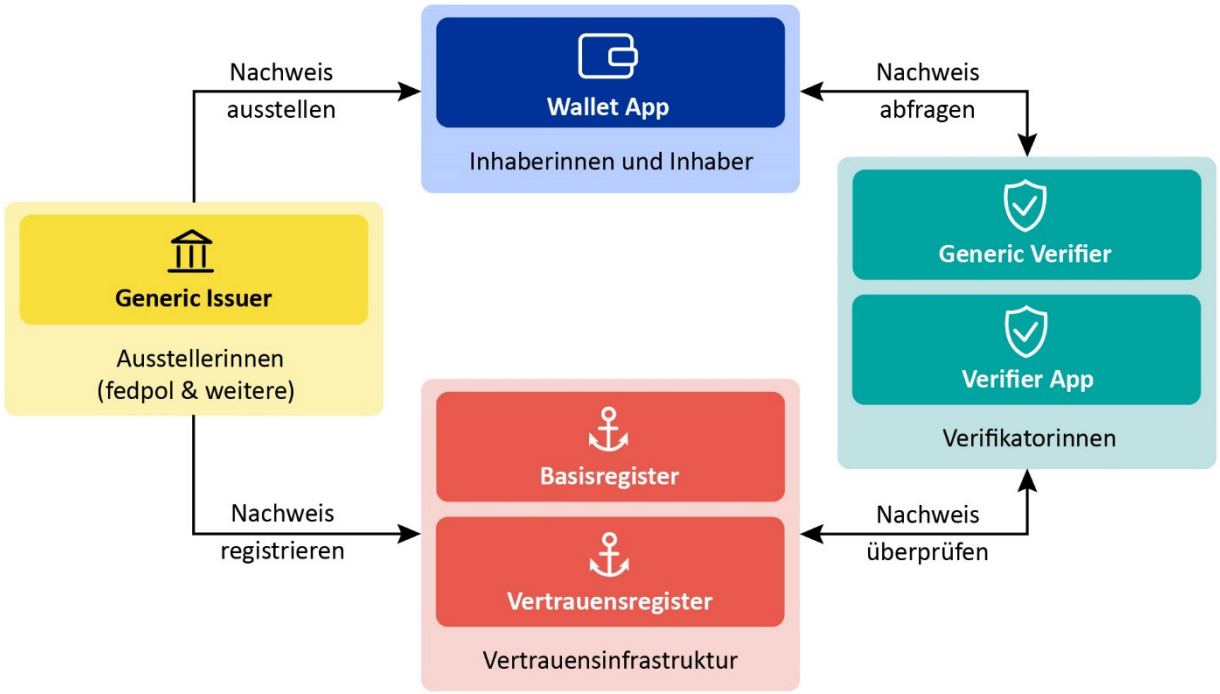


Abb. 1: Zusammenspiel der Akteure im Ökosystem der E-ID, Darstellung: EFK

Die Schweizer E-ID und andere elektronische Nachweise werden im Rahmen eines Ausstellungsprozesses von festgelegten Ausstellerinnen erstellt. So ist die Ausstellerin der E-ID analog zu den physischen Ausweisdokumenten in der Schweiz das Bundesamt für Polizei fedpol. Die Ausstellerinnen liefern ihre elektronischen Nachweise an die Wallet-Apps der Inhaberinnen und Inhaber aus.

Inhaberinnen und Inhaber erhalten Anfragen zur Überprüfung ihrer elektronischen Nachweise von den Verifikatorinnen. Eine Verifikatorin kann dabei jede berechtigte Stelle sein, die im Rahmen einer behördlichen Überprüfung oder privatrechtlichen Transaktion die Daten eines elektronischen Nachweises, z. B. der E-ID, abfragt. Die angefragten Daten werden nach erfolgter Freigabe von der Wallet-App an die Verifikatorin übermittelt. Die Echtheit der vorgewiesenen E-ID wird dabei durch Abfrage des Basisregisters durch die Verifikatorin festgestellt.

Die Programmcodes des E-ID Ökosystems werden entsprechend den Vorgaben des EMBAG[1] veröffentlicht. Damit stehen den Teilnehmenden staatliche Anwendungen oder Programmcodes für die weitere Verwendung zur Verfügung. Dies bedeutet, dass durch Verwendung der beiden staatlichen Anwendungen oder Einbau der Programmcodes in eigene Anwendungen jede und jeder am Ökosystem der elektronischen Nachweise teilnehmen kann. Durch diese Offenheit soll eine weitreichende Akzeptanz in Wirtschaft und Verwaltung erreicht werden.

[1] EMBAG: Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben

Der Staat hält sich dabei als Akteur zurück: Der Austausch von Informationen eines elektronischen Nachweises, z. B. einer E-ID, stellt eine Wechselbeziehung zwischen Wallet der Inhaberinnen und Inhaber sowie einer Verifikationsanwendung dar. Der Bund nimmt daran nicht teil und erhält davon keine Kenntnis. Diese Systematik entspricht dem Grundsatz der schweizerischen E-ID als «selbst-souverän».

Diese Selbstsouveränität gilt nicht nur für Inhaberinnen und Inhaber der E-ID, sondern auch für teilnehmende Unternehmen. Behörden benötigen Rechtsgrundlagen, in denen explizit festgelegt wird, für welche amtlichen Zwecke die Identität von Einwohnern festgestellt werden darf. Unternehmen entscheiden hingegen selbst, für welche Vorgänge sie die E-ID einverlangen. Sie entscheiden auch selbst, ob und wie sie die durch die Abfragen erhaltenen Daten weiterverwenden. Dies ist rechtens, solange die Bestimmungen des schweizerischen Datenschutzgesetzes und die spezifischen Einschränkungen des E-ID-Gesetzes eingehalten sind. D. h. die abgefragten Daten müssen zwingend notwendig für die Prozesse des Unternehmens sein, oder diese sind für die Zuverlässigkeit der Transaktion unbedingt erforderlich, insbesondere um Missbrauch und Identitätsdiebstahl zu verhindern.

Zwischen Unternehmen und ihren Kunden besteht im Rahmen einer geschäftlichen Transaktion jedoch ein grundsätzliches Ungleichgewicht und eine Situation, die für viele technisch wenig überschaubar wirkt. Potenzielle Kunden ersuchen darum, Produkte oder Dienstleistungen von den jeweiligen Anbietern zu beziehen. Wenn zum Erwerb eines Produktes oder einer Dienstleistung eine starke Identifikation, heute z. B. mittels Videoident-Verfahren, notwendig ist, muss dieses erfolgreich abgeschlossen werden. Auch mit der E-ID wird ein solcher Vorgang nur dann erfolgreich durchgeführt werden können, wenn die angefragten Daten freigegeben werden. Eine Verweigerung der Datenfreigabe führt zum Abbruch des Vorgangs.

Exkurs: Erkenntnisse zu Altersverifikationen aus dem Ausland

Am Beispiel des Vereinigten Königreiches können seit dem Inkrafttreten zwingend erforderlicher Altersverifikationen im Internet Erkenntnisse zur Beliebtheit privater Dienstleister für Identitätsverifikationen gewonnen werden. Für viele Unternehmen ist es nicht wirtschaftlich, eigene Dienstleistungen zur Verifikation der Identität ihrer Kunden aufzubauen. Insbesondere nicht, wenn diese Verifikation nur einen Teil des Abschluss- oder Einkaufsprozesses darstellt (oder, wie im Vereinigten Königreich, als «Türöffner» für den Zugang zum Internetauftritt dient). Die Identitätsverifikation wird daher möglicherweise ausgelagert. Diese Leistung kann von spezialisierten Dienstleistungsunternehmen in der Schweiz, ebenso aber auch aus dem Ausland erbracht werden, wo Schweizer Datenschutzgesetze nicht gelten. Wollen Schweizer Einwohner ein Produkt oder eine Dienstleistung erwerben, bleibt ihnen dennoch keine Wahl: Ihre Daten sind auch diesen Dienstleistern freizugeben, wenn der Prozess fortgesetzt werden soll.

In der Europäischen Union beabsichtigt man, der Bevölkerung für den Umgang mit Verifikatorinnen weitere Hilfestellung zu geben. So sollen sich am europäischen Ökosystem teilnehmende Identitätsverifikatorinnen vorab bei einer staatlichen Stelle registrieren. Im Rahmen dieses Prozesses sollen auch die zur Abfrage beabsichtigten Datenfelder der elektronischen Identität behördlich bekannt gegeben. Bei jeder daraufhin stattfindenden Abfrage zwischen Wallets und Verifikatorinnen in der EU sollen die vorab registrierten Datenfelder mit den tatsächlich angeforderten abgeglichen werden. Stimmen diese nicht überein, würde die Wallet App die Übermittlung blockieren.

Die Vertrauensinfrastruktur in der Schweiz kennt analog hierzu ein Konzept sogenannter *Identity-, Issuer- und Verifier-Trust Statements*. *Trust Statements* werden von der Fachstelle E-ID des BJ für Ausstellerinnen bzw. Verifikatorinnen ausgegeben, die sich freiwillig einer Prüfung unterzogen haben. Die Prüfung soll für interessierte Teilnehmende feststellen, wer hinter den digitalen Identifikatoren der Teilnehmenden wirklich steckt und in spezifischen Fällen, ob es sich um eine legitimierte Ausstellerin (*Issuer-Trust Statement*) oder eine legitimierte Verifikatorin (*Verifier-Trust Statement*) für einen bestimmten Nachweis-Typ handelt. In der swiyu-App wird positiv ausgewiesen, welche Ausstellerinnen und Verifikatorinnen *Trust Statements* erhalten haben.

Während dieses Konzept in der schweizerischen Vertrauensinfrastruktur zwar technisch umgesetzt wird, sollen *Verifier-Trust Statements* für Verifikatorinnen der E-ID jedoch nicht genutzt werden. Das Programm

E-ID begründet dies damit, dass man einzelne Teilnehmende nicht anderen gegenüber hervorheben wolle. Vielmehr solle die Bevölkerung selbst-souverän entscheiden, ob sie einem Gegenüber ihre E-ID Daten anvertrauen kann oder nicht.

BEURTEILUNG

Da die Akzeptanz der E-ID durch die Bevölkerung auf Vertrauen basieren muss, sieht die EFK in der Realisierung des Konzeptes der *Verifier-Trust Statements* auch für Verifikatorinnen der E-ID ein bislang ungenutztes Potenzial.

Die visuelle Hervorhebung in der swiyu Wallet als E-ID Verifikatorin mit legitimem Abfragezweck ist eine vertrauensbildende Massnahme des Bundes als Treuhänder der E-ID, zu deren Erlangung die Verifikatorin zusätzlichen Aufwand auf sich genommen hat.

EMPFEHLUNG 1 — PRIORITÄT 1

Die EFK empfiehlt dem BJ, das Konzept der *Verifier-Trust Statements* auch in die Prozesse beim Einsatz der E-ID zu integrieren. Darüber hinaus sollte im Programm geprüft werden, ob das Konzept der *Trust Statements* für Verifikatorinnen so erweitert werden kann, dass es möglich wird, die abzufragenden Datenfelder freiwillig zu registrieren. Dies, um in der swiyu Wallet auch ausweisen zu können, wenn keine Differenzen zwischen vorab von der Verifikatorin registrierten und in einer Transaktion abgefragten Datenfeldern der E-ID bestehen.

STELLUNGNAHME DES BUNDESAMTES FÜR JUSTIZ

Die Empfehlung ist akzeptiert.

Im Nachgang zur Referendumsabstimmung vom 28. September 2025 wird im Programm E-ID aktuell geprüft, wie die Freiwilligkeit der E-ID, der Datenschutz und die Sicherheit und Vertrauenswürdigkeit für Inhaberinnen sowie Ausstellerinnen und Verifikatorinnen weiter und nachhaltig gestärkt werden können. Diese Prüfung hat zum Ziel, die Akzeptanz der neuen staatlichen E-ID weiter zu stärken. Dazu werden auch die Ausführungsbestimmungen zum E-ID-Gesetz nach der Vernehmlassung, die bis zum 15. Oktober 2025 dauerte, entsprechend überarbeitet.

Die Prüfung umfasst auch eine Erweiterung des Konzeptes der Trust Statements für Verifikatorinnen, wie dies von der EFK empfohlen wird.

2.2 Die Offenheit des Ökosystems wird von der technischen Realität vorgegeben

Mit der Veröffentlichung der Programmcodes (siehe Kapitel 2.1) ist es technisch möglich, dass Dritte diese beziehen und an ihre Bedürfnisse anpassen. Dies etwa, um daraus eine eigene Anwendung zu erstellen, die ebenfalls in der Lage ist die E-ID technisch zu verarbeiten. Als Voraussetzung für die Ausstellung der E-ID in Wallets von Drittanbietern hat das Programm E-ID festgelegt, dass die Speicherung auch hier nachvollziehbar im sicheren Bereich, sog. «Secure Element», des empfangenden Mobiltelefons erfolgen muss.

Die sichere Speicherung der E-ID könnte in diesem Fall nur anhand von manueller Durchsicht der Programmcodes solcher Drittanbieteranwendungen bestätigt werden. Das E-ID-Gesetz sieht für diesen Fall vor, dass der Bund eine Zertifizierungspflicht für Drittanbieteranwendungen zur Verarbeitung der E-ID einführen kann. Ein solcher Zertifizierungsschritt ist in der zum Prüfungszeitpunkt in Vernehmlassung befindlichen Verordnung zum E-ID-Gesetz jedoch noch nicht vorgesehen.

Gemäss dem Programm E-ID seien die zur Zertifizierung für Wallets von Dritten notwendigen Prozesse ab Anfang 2026 zur Spezifizierung vorgesehen. Sie sollen dann in der ersten Revision der E-ID-Verordnung festgeschrieben werden, welche jedoch nicht vor 2028 erlassen wird. Wallets von Dritten sollen daher zur Speicherung der E-ID bis dahin nicht zugelassen werden.

Unklar verbleibt jedoch, auf welche Weise (zertifizierte oder nicht zertifizierte) Wallets überhaupt erkannt werden können. Dies insbesondere, wenn ihre Programmcodes entweder weitgehend von swiyu abgeleitet sind oder die Funktionen von swiyu im Rahmen der E-ID-Ausstellung exakt nachbilden.

BEURTEILUNG

Das Programm E-ID wird zeitnah eine Lösung finden müssen, wie Wallets von Dritten zuverlässig systematisch erkannt und bei Notwendigkeit vom Empfang der E-ID ausgeschlossen werden können. Dies insbesondere dann, wenn deren Programmcode und das Verhalten dieser Anwendungen von swiyu abgeleitet ist oder diesem sogar 1:1 entspricht.

Ohne Überprüfung der Programmcodes kann zum Prüfungszeitpunkt nicht sichergestellt werden, dass eine Wallet von Dritten nicht trotz Speicherung der E-ID in einem «Secure Element» unlautere Zwecke mit den erhaltenen Daten verfolgt und diese z. B. an andere Stellen ausleitet.

Die EFK begrüsst daher die Absicht des Programms E-ID, Wallets von Drittanbietern erst dann zuzulassen, wenn der entsprechende Zertifizierungsprozess etabliert ist. Sie verzichtet daher auf eine Empfehlung.

2.3 Das E-ID-Gesetz ist die Grundlage zur Klärung internationaler Fragestellungen

Erst mit Inkrafttreten des E-ID-Gesetzes gibt es in der Schweiz eine Rechtsgrundlage, um Gespräche zur internationalen Anerkennung der E-ID aufzunehmen. Ein offizielles Mandat besteht heute weder auf Seite der Europäischen Union noch in der Schweiz. Dennoch unterhält das Programm E-ID informelle Austausche mit der EU-Kommission sowie mit einzelnen EU-Mitgliedsstaaten und verfolgt die dortigen Entwicklungen eng.

Die Schweizer Implementierung der E-ID stützt sich zur Erreichung der technischen Interoperabilität darauf ab, die verwendeten Protokolle standardkonform umzusetzen. Diese sind teilweise jedoch noch in internationalen Gremien in Erarbeitung bzw. Finalisierung und somit als vorläufig zu verstehen. Dies erfordert gelegentliche Nacharbeiten des Programms, da finale Protokolle teils erst im Laufe des Entwicklungsprozesses vorliegen werden.

Die internationale Anerkennung der E-ID ist jedoch primär ein politischer, nicht ein technischer Prozess. Sobald eine politische Einigung vorliegt, gibt es grundsätzlich verschiedene Möglichkeiten, das Beschlossene technisch umzusetzen. Das Programm E-ID hat hierbei auf technischer Ebene bereits zwei mögliche Wege vorgesehen, wie die technische Interoperabilität sichergestellt werden könnte: Die Bereitstellung der Schweizer E-IDs in einem konkreten, politisch festgelegten internationalen Austauschformat oder der Aufbau von «Schweizer Knoten» innerhalb ausländischer Vertrauensinfrastrukturen, in welchen die gültigen E-IDs analog zur Schweizer Vertrauensinfrastruktur bekannt gegeben werden.

Darüber hinaus ist mit der EU jedoch noch grundsätzlich zu klären, wie mit von der EU abweichenden Funktionsprinzipien des Schweizer E-ID Ökosystems umgegangen werden soll. Dies betrifft z. B. den Umgang mit allfälligen Wallets von Drittanbietern aus der Schweiz: In der EU sind nur staatlich anerkannte Wallets geplant. Unter Umständen muss die Schweiz daher international auch für Wallets von lokalen Drittanbietern dereinst deren Sicherheit garantieren.

Zu diesen offenen Themen zählt auch, wie mit den per EU-Verordnung geforderten Sicherheitsniveaus umgegangen wird. Die EU definiert in ihrer eIDAS-Verordnung[2] vier Sicherheitsniveaus und fordert, dass

[2] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

für elektronische Identitätsnachweise das höchste dieser Niveaus anzustreben ist. Gemäss Analyse des Programms E-ID erreicht die Schweizer Implementierung der E-ID das Sicherheitsniveau «substanziell» und liegt somit eine Stufe tiefer als eIDAS fordert. Dieses niedrigere Sicherheitsniveau resultiert aus der Verwendung nicht quelloffener Mobiltelefone und ihrer Betriebssysteme, auf denen die Wallet läuft. Der Bund kann hier nicht bis auf die Hardware der verwendeten Geräte analysieren und zertifizieren, was mit den auf die Mobiltelefone ausgestellten Daten passiert. Hierfür bräuchte es analog dem z. B. seit 2010 in Deutschland ausgestellten elektronischen Personalausweis separate, zertifizierte Hardware, was jedoch die Verbreitung der E-ID bei der Bevölkerung hemmen würde.

BEURTEILUNG

Die EFK begrüsst, dass zwischen dem Programm E-ID und mehreren EU-Mitgliedsstaaten bereits informelle Austausche stattfinden. Themen wie der internationale Umgang mit Schweizer Drittanbieter Wallets und unterschiedlichen Funktionsweisen der Systeme in der Schweiz und der EU sind jedoch zunächst politisch zu klären. Dann kann für die technische Interoperabilität gesorgt werden.

Da technisch mehrere Ansätze denkbar sind, ist von Wichtigkeit, dass die Rechtsgrundlage für ein konkretes Mandat zeitnah in Kraft tritt, um das Thema Internationalisierung der Schweizer E-ID überhaupt offiziell angehen zu können. Da dies primär ein politischer Prozess ist, der vom Programm nicht gesteuert werden kann, verzichtet die EFK an dieser Stelle auf eine Empfehlung.

3 TECHNISCHE SICHERHEIT

3.1 Bei der Vertrauensinfrastruktur hat das Programm wesentliche Teile des Plans noch vor sich

Die beiden durch den Bund zur Verfügung gestellten Mobiltelefonanwendungen, die Wallet swiyu und die Verifikationsanwendung, greifen auf zentrale Dienste der staatlichen Vertrauensinfrastruktur zu. Diese vom Bund zentral zur Verfügung gestellten Dienste umfassen die Ausstellung der E-ID, ein Portal zur Registrierung von Teilnehmenden (Ausstellerinnen und Verifikatorinnen) sowie das Basis- und das Vertrauensregister zur Erfassung des aktuellen Zustands der gültigen elektronischen Nachweise und der Teilnehmenden.

Neben den Prozessen zur Ausstellung, Speicherung und Verarbeitung der E-ID ist die Vertrauensinfrastruktur so offen gestaltet, dass ebenfalls andere elektronische Nachweise darauf ausgestellt und verarbeitet werden können. So wird z. B. als weiterer Hauptprozess der elektronische Lernfahrausweis der Schweiz (eLFA) über die Vertrauensinfrastruktur in die swiyu-App ausgestellt. Der eLFA wird ab Ende 2025 in der gesamten Schweiz zur Verfügung stehen.

Neben der E-ID auf der Vertrauensinfrastruktur umgesetzte und in Zukunft noch folgende Hauptprozesse werden jeweils auf Basis ihrer eigenen Rechtsgrundlage in das Ökosystem integriert. Sollte eine dieser Rechtsgrundlagen nach einem Referendum abgelehnt oder wesentlich abgeändert werden, wirkt sich dies lediglich auf die betroffenen Funktionsbereiche aus. Der Fortbestand des Ökosystems als Ganzes ist davon jedoch nicht betroffen. Die EFK behandelt in der vorliegenden Prüfung die Hauptprozesse der E-ID mit ihrer Rechtsgrundlage, dem E-ID-Gesetz.

Die Vertrauensinfrastruktur befindet sich im Stadium einer «Public Beta». Die Beta ID ist ein der E-ID ähnlicher elektronischer Nachweis, der zwar in Teilen bereits die Funktionsweise der E-ID vorwegnimmt, jedoch noch nicht die spätere Schweizer E-ID darstellt. Die Hauptprozesse der tatsächlichen E-ID befinden sich zum Prüfungszeitpunkt noch in der Entwicklung.

Dem Programm verbleiben bis zum geplanten Start der E-ID ab frühestens 3. Quartal 2026 wesentliche Herausforderungen, die erfolgreich gelöst werden müssen.

Die Verschlüsselung der Nutzdaten ist noch nicht fertig konzipiert und integriert

Der Datenaustausch zwischen Ausstellerinnen, Verifikatorinnen und swiyu findet über verschlüsselte Kommunikation statt. Eine Verschlüsselung der ausgetauschten Nutzdaten selbst findet zwischen Verifikatorin und swiyu hingegen noch nicht statt: Die Spezifikation der Nutzdatenverschlüsselung ist noch nicht abgeschlossen. Das sogenannte «DevSecOps» Verfahren (siehe Glossar), welches vorgibt, dass die Sicherheit ein integraler, automatisierter und kontinuierlicher Bestandteil des gesamten Entwicklungs- und Betriebsprozesses von Software sein soll, nicht ein nachträglicher Schritt, wird spezifisch an dieser Stelle im Projekt Vertrauensinfrastruktur nicht konsequent eingehalten.

Die noch fehlende Sicherheitsfunktionalität soll bis Ende 2025 integriert werden und dann Gegenstand spezieller Testszenarien werden. Das Programm hat während der Prüfung die Spezifikation der Nutzdatenverschlüsselung im Entwurf vorgelegt.

Die Prozesse der E-ID-Ausstellung sind noch nicht fertig entwickelt und getestet

Die derzeit umgesetzten Prozesse der Beta ID sind in der Lage, einen elektronischen Nachweis auf Knopfdruck zu generieren. Dies wird bei der E-ID grundlegend anders funktionieren. An dieser Stelle sind die Prozesse zur Ausstellung einer E-ID zu integrieren. Diese Prozesse umfassen eine automatisierte Gesichtsüberprüfung der Antragstellenden sowie bei Notwendigkeit oder explizitem Wunsch die Vereinbarung eines persönlichen Termins in einem lokalen Passbüro.

Bei erfolgreichem Antrag wird die E-ID von fedpol ausgestellt und an das oder die Mobiltelefone der Antragstellenden ausgeliefert. Die funktionalen Abläufe der Ausstellungs- und Identitätsprüfungsvorgänge sind fertig spezifiziert, müssen in fedpol-Systemen und der swiyu-App aber noch implementiert werden. Die Anwendung zur Identitätsprüfung für die E-ID wurde extern beschafft und soll bis Ende 2025 integriert und abgenommen sein.

Sämtliche fertig entwickelten Komponenten werden vor der Freigabe funktional getestet und einem Penetrationstest unterzogen. Allfällige dabei auffallende Fehler müssen bis zum geplanten Start der E-ID behoben werden.

Ende-Zu-Ende-Tests müssen noch aufgebaut und durchgeführt werden

Da sich die Prozesse der Ausstellung und Verifikation der E-ID noch in der Entwicklung befinden, verfügt das Programm noch nicht über spezifische Ende-Zu-Ende-Tests für die E-ID. Zum Zeitpunkt der Prüfung liegt der Schwerpunkt auf Entwickler- und Integrationstests. Ein Konzept für Ende-Zu-Ende-Tests besteht, dessen Umsetzung ist jedoch noch hängig. Eine konsolidierte Liste von geplanten Testfällen liegt ebenfalls noch nicht vor.
Das Programm beabsichtigt für die E-ID insbesondere Ende-Zu-Ende-Testfälle mit verschiedenen Arten von physischen Dokumenten (Identitätskarte, Reisepass, Aufenthaltsgenehmigung) vorzusehen, sowie technische Szenarien (z. B. unterbrochene oder unvollständige Datenübertragung). Darüber hinaus sollen Situationen, in denen die automatisierte Gesichtsüberprüfung fehlschlägt und manuelle Überprüfung erforderlich wird, sowie der manuelle Export von Archivdaten, z. B. zur Beweissicherung, getestet werden.

Das Programm entwickelt die E-ID in agilem Vorgehen. Die genannten offenen Themen sind auf einer Roadmap eingeplant. Die Entwicklung findet in jeweils 10 Wochen dauernden «Programm Inkrements» (PI, siehe Glossar) statt. Die Entwicklung neuer Funktionalitäten soll bis April 2026 abgeschlossen werden. Bis zum vorgesehenen frühestmöglichen Start der E-ID im 3. Quartal 2026 soll ein weiteres PI zur Stabilisierung und finalen Abnahme der entwickelten Prozesse genutzt werden.

BEURTEILUNG

Die EFK ist auch unter Berücksichtigung des agilen Umsetzungsvorgehens überrascht, dass im Programm noch derart viele Arbeiten an der E-ID offen sind. Die EFK hätte beispielsweise erwartet, dass die Konzeption der Sicherheitsfunktionen zum Prüfungszeitpunkt bereits vollständig abgeschlossen wäre. Bei der Verschlüsselung der Nutzdaten ist dies noch nicht der Fall, womit das Risiko besteht, dass Aspekte der Sicherheit an das System «angebaut» werden müssen.

Die EFK begrüsst das nach Abschluss der Entwicklungsarbeiten geplante PI zur Stabilisierung. Basierend auf Erfahrungswerten aus anderen Programmen sieht sie jedoch die Gefahr, dass dieses PI stattdessen zu Gunsten offener Entwicklungen oder ausstehender Fehlerbehebungen genutzt wird. Damit würde die notwendige Stabilisierung verkürzt oder sogar ganz gestrichen. Dies ist zu vermeiden. Das Vorhaben E-ID stellt national und international ein Reputationsrisiko für den Bund dar. Sicherheit und Stabilität der E-ID sind daher in diesem Programm über Termineinhaltung für den Start zu gewichten.

EMPFEHLUNG 2 PRIORITÄT 1

Die EFK empfiehlt dem BJ, in der Planung und Budgetierung des Programms E-ID dafür Sorge zu tragen, dass ausreichend Zeit und Ressourcen zur Stabilisierung vor dem Start der E-ID zur Verfügung stehen, auch wenn hierfür die Programmlaufzeit verlängert werden müsste.

STELLUNGNAHME DES BUNDESAMTES FÜR JUSTIZ

Die Empfehlung ist akzeptiert.

Die EFK bemängelt, dass die geplante Stabilisierungsphase als Zeitreserve für ungeplante Entwicklungsarbeiten zweckentfremdet werden könnte. Dies entspricht nicht der Planung zum Prüfzeitpunkt der EFK sowie nicht der Absicht des Programms. Vielmehr plant das Programm E-ID noch ein zweites Stabilisierungs-PI (Product Increment) einzuschieben.

Für das BJ haben Sicherheit und Stabilität der E-ID oberste Priorität. Eine Verlängerung der Programmlaufzeit und damit ein erhöhter Ressourcenbedarf werden bewusst in Kauf genommen.

3.2 Technische Zugriffe der Ausstellerinnen sind nur schwach gesichert

Die Schweizer E-ID wird ausschliesslich von fedpol ausgestellt werden. Für andere elektronische Nachweise sind jedoch auch weitere Behörden oder Private als Ausstellerinnen möglich. So wird z. B. der eLFA von den kantonalen Strassenverkehrsämtern ausgestellt.

Die Ausstellerinnen liefern periodisch eine kryptographisch verkettete Liste ihrer publizierten Schlüssel und eine signierte Liste der widerrufenen elektronischen Nachweise an das Basisregister. Die Verifikationsanwendungen konsumieren diese Listen, um die Gültigkeit eines vorgezeigten elektronischen Nachweises festzustellen.

Zugriffe der Ausstellerinnen auf die Vertrauensinfrastruktur zur Einlieferung ihrer Listen erfolgen jedoch mittels Benutzername und Passwort anstelle einer modernen Absicherung technischer Zugriffe. Die Zugangsdaten werden allen Ausstellerinnen kommuniziert werden müssen. Sollte der Zugang auf diesem Wege auch Unbefugten bekannt werden, wird für diese unter Umständen ein Löschungsangriff auf die Vertrauensinfrastruktur durchführbar.

Exkurs: Der Bund verfügt bereits über Konzepte zur Förderung sicherer Softwareentwicklung

Bei den IKT-Leistungserbringenden im Bund werden über die verbreitete «DevSecOps» Vorgehensweise hinaus teilweise bereits Konzepte angewendet, die dafür sorgen sollen, dass Software von vornherein sicher entwickelt wird. Diese sehen beispielsweise vor, dass in agilen Entwicklerteams jeweils mindestens ein Mitglied, genannt «Security Champion», vertreten ist, welches spezifisch in Sicherheitsthemen ausgebildet ist.

Damit soll gefördert werden, dass die in diesem Team entstehenden Programmcodes möglichst direkt auf sichere Art und Weise geschrieben werden. Sicherheitslücken sollen so nicht erst in Penetrationstests auffallen und teure oder zeitaufwändige Nacharbeiten nach sich ziehen.

Das Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements (ISC-EJPD) als IKT-Leistungserbringer für fedpol und das BIT wenden ein solches Konzept bei Eigenentwicklungen bereits generell als Teil des Standardvorgehens an.

Für alle neu entwickelten Funktionalitäten der Vertrauensinfrastruktur und der Mobiltelefonanwendungen ist jeweils vor Freigabe ein Penetrationstest verpflichtend vorgesehen. Im Projekt Vertrauensinfrastruktur steht den Entwicklern neben dem Sicherheitsarchitekten ein Sicherheitsberater für Fragen zur sicheren Softwareentwicklung zur Verfügung. Dieser soll darüber hinaus sicherstellen, dass z. B. im

Rahmen von Penetrationstests aufgefallene Probleme in der Entwicklung teamübergreifend kommuniziert werden, um die Wiederholung bekannter Fehler zu vermeiden.

BEURTEILUNG

Der Zugriff für technische Benutzer der Ausstellerinnen mittels Benutzername und Passwort gilt als technisch unsicher und nicht mehr zeitgemäss. Das Konzept entspricht zwar dem derzeitigen Standard des BIT für technische Benutzerzugriffe, ist für ein derart kritisches System jedoch nicht ausreichend.

Positiv wird jedoch bewertet, dass das BIT mit der Rolle des zusätzlichen Sicherheitsberaters bereits dafür gesorgt hat, dass das Programm Massnahmen zur Stärkung der Sicherheit vorsieht. In diesem Zuge sind auch die verpflichtenden generellen Penetrationstests vor Freigabe von neuen Funktionalitäten sinnvoll und stellen ein wichtiges Mittel dar, um Problemen bei der Sicherheit vorzubeugen.

EMPFEHLUNG 3 — PRIORITÄT 2

Die EFK empfiehlt dem BJ, für den Zugriff der Ausstellerinnen der E-ID auf die Vertrauensinfrastruktur ein sicheres Login-Verfahren mit individuellem Zugang zu fordern, z. B. zertifikatsbasiert oder mittels API-Key. Dieses soll auch die Möglichkeit der Sperrung des Zugangs durch die Ausstellerin beinhalten, z. B. beim Verdacht auf unberechtigte Zugriffe Dritter.

STELLUNGNAHME DES BUNDESAMTES FÜR JUSTIZ

Die Empfehlung ist akzeptiert.

Die EFK bemängelt den Zugriff für technische Benutzer der Ausstellerinnen mittels Benutzername und Passwort als technisch unsicher und nicht mehr zeitgemäss (die Schweizer E-ID wird ausschliesslich von fedpol ausgestellt und der Zugriff auf die Vertrauensinfrastruktur ist sicher; die Empfehlung der EFK wollte wohl auf die Ausstellerinnen anderer elektronischer Nachweise abzielen). Es handelt sich hierbei um Dienstkonti. Das Programm E-ID hält sich an die offiziellen Vorgaben des Grundschutzes des BACS bezüglich der Authentifikationsmethode für Dienstkonti. Die Realisierbarkeit und der damit zusammenhängende Sicherheitsgewinn einer anderen Authentifizierungsmethode konnten von der EFK dem Programm E-ID nicht aufgezeigt werden. Bei Verdacht auf Missbrauch kann der Zugriff unabhängig von der Authentifizierungsmethode entzogen werden.

Das BJ wird prüfen, ob ein anderes Login-Verfahren mit individuellem Zugang für die Ausstellerinnen anderer elektronischer Nachweise (z. B. zertifikatsbasiert oder mittels API-Key) möglich und angemessen wäre und würde dessen Umsetzung gegebenenfalls einfordern.

3.3 Wichtige betriebliche Themen werden in der Public Beta noch nicht getestet

Vor der Aufnahme des produktiven Betriebs der Vertrauensinfrastruktur muss das Programm auch betriebliche Themen vorbereiten. Das Ökosystem muss ab dem ersten Tag mit voller Sicherheit und Zuverlässigkeit im Betrieb zur Verfügung stehen. Die betrieblichen Prozesse und Abläufe müssen daher vorab erprobt werden, weshalb das Programm E-ID die Public Beta durchführt. Zur Steuerung der Sicherheit des Gesamtsystems baut das Programm ein Informationssicherheits-Managementsystem auf. Darüber hinaus ist geplant, nach Abschluss des Programms die Bewirtschaftung von Informationssicherheits-Risiken im Betrieb durch eine dedizierte Risikomanagement-Rolle fortzuführen.

Es gibt jedoch Themenbereiche, die vom Programm zusätzlich zur normalen Planung der Betriebsaufnahme noch adressiert werden müssen. In der Public Beta wurden die Arbeiten hieran noch nicht aufgenommen.

Prozesse zur Erkennung von Sicherheitsvorfällen müssen noch aufgebaut werden

Das BIT plant, für die Vertrauensinfrastruktur einen Prozess zur Erkennung und Bearbeitung von Sicherheitsvorfällen (Security Information and Event Management, SIEM) einzuführen. Dieser sollte zum Prüfungszeitpunkt bereits im Entwurf konzipiert sein, konnte aufgrund von Verzögerungen jedoch noch nicht vorgelegt werden. Der SIEM-Prozess soll vom betriebsverantwortlichen Team des BIT ausgeführt werden, welches auch die Weiterentwicklung der E-ID übernimmt.
Darüber hinaus plant das ISC-EJPD als IKT-Leistungserbringer für die Prozesse der E-ID Ausstellung bei fedpol, in 2026 eine Sicherheitsbetriebszentrale (Security Operations Center, SOC) einzuführen.

Ein Inventar der verwendeten Softwarekomponenten wird noch nicht erstellt

Bei der Übersetzung der Programmcodes für die Vertrauensinfrastruktur und die Mobiltelefonanwendungen des Bundes werden bei einzelnen intern erstellten Komponenten bereits Software-Stücklisten (Software Bill of Materials, SBOM) generiert. Diese werden heute jedoch noch nicht systematisch verwendet und z. B. mit verwendeten Drittanbieterkomponenten und Abhängigkeiten angereichert, um für jede aktuelle Version der Vertrauensinfrastruktur eine vollständige Lieferkette der Software nachweisen zu können.

Insbesondere diejenigen Teilnehmenden, die von der Vertrauensinfrastruktur abhängige Programme erstellen, z. B. Ausstellerinnen elektronischer Nachweise oder Hersteller von Wallet-Apps, sind auf ein solches detailliertes Inventar aller verwendeten Softwarekomponenten angewiesen. Dies dient ihrem technologischen Risikomanagement, der Compliance z. B. zu den verwendeten Lizenzen und fördert die Transparenz bei allfälligen Sicherheitslücken.

Im Basisregister sind keine regelmässigen Kontrollen der Teilnehmerdaten vorgesehen

Während diejenigen Teilnehmenden, die auf eigenen Wunsch im Vertrauensregister eingetragen werden wollen, vorab einen Prüfungsprozess durchlaufen müssen, sind im Basisregister aller registrierter Teilnehmender keine Kontrollen geplant. Sobald ein Teilnehmender in der Portalanwendung der Vertrauensinfrastruktur registriert ist und die notwendigen Gebühren entrichtet hat, kann der Zugang genutzt werden. Zur Registrierung sind nur wenige Daten verpflichtend anzugeben, und die erfassten Daten unterliegen keinen Kontrollen. Das Programm E-ID begründet dies damit, dass die im Basisregister erfassten Daten der Teilnehmenden ohnehin an keiner weiteren Stelle zur Verwendung kommen: Anfragen zur Verifikation einer E-ID enthalten Informationen zur absendenden Stelle nur in den Transaktionsdaten, die Vertrauensinfrastruktur wird hierfür nicht abgefragt.

BEURTEILUNG

Die EFK begrüsst die Absicht des Programms E-ID, die Bewirtschaftung von Informationssicherheits-Risiken im Betrieb fortzuführen. Ebenso positiv wird bewertet, dass von Seiten ISC-EJPD und BIT bereits geplant ist, einen SIEM-Prozess bzw. ein SOC einzuführen. Die EFK verzichtet daher auf deren Empfehlung.

Es ist üblich, dass der konkrete Aufbau des Betriebs erst gegen Ende eines Projektes oder Programms angegangen wird. Dennoch erachtet die EFK es als notwendig, bei den offenen betrieblichen Themen bereits jetzt die Arbeiten aufzunehmen. Dies, um einige der einzuführenden Massnahmen, insbesondere die umfassende Erstellung und Publikation der Software-Stückliste (SBOM), allenfalls noch in der Public Beta zu beüben. Dies hilft dem Programm sicherzustellen, dass das Ökosystem zum Start der Schweizer E-ID ab dem ersten Tag für einen zuverlässigen und sicheren Produktivbetrieb bereitsteht.

Zur Erlangung des Vertrauens der Schweizer Bevölkerung in diese vom Bund bereitgestellte Lösung wird es keine zweite Chance geben. Zentral ist daher, dass der Zeitplan und dessen Risiken vor dem Hintergrund der offenen Massnahmen für den Aufbau des produktiven Betriebs weiterhin konsequent überwacht und allen Beteiligten transparent kommuniziert werden. Die EFK verweist in diesem Zusammenhang auf Empfehlung Nr. 2 in Kapitel 3.1.

EMPFEHLUNG 4 — PRIORITÄT 3

Die EFK empfiehlt dem BJ in Zusammenarbeit mit dem BIT, fortlaufend ein aktuelles Inventar (Software-Stückliste) der Bestandteile der E-ID zu veröffentlichen, damit den Teilnehmenden bekannt ist, welche Komponenten, Abhängigkeiten und Lizenzen verwendet werden. Dieses Inventar sollte möglichst frühzeitig eingeführt werden, um Prozesse zu seiner Erstellung und Aktualisierung ausreichend üben zu können.

STELLUNGNAHME DES BUNDESAMTES FÜR JUSTIZ

Die Empfehlung ist akzeptiert.

Für das Programm E-ID ist ein transparenter Umgang mit den verschiedenen Teilnehmenden am E-ID Ökosystem von zentraler Bedeutung. Deshalb wird die technische Dokumentation laufend auf GitHub veröffentlicht und gepflegt, so auch ein Inventar der Softwarekomponenten.

Das BJ wird diese Empfehlung im ersten Quartal 2026 umsetzen. Bis zur Betriebsaufnahme besteht damit genügend Zeit, um die Prozesse zur Erstellung und Aktualisierung des Inventars einzuführen und falls notwendig anzupassen.

ANHANG 1 – RECHTSGRUNDLAGEN UND PARLAMENTARISCHE VORSTÖSSE

RECHTSTEXTE

Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) vom 20. Dezember 2024, BBl 2025 20
Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG) vom 17. März 2023, SR 172.019

PARLAMENTARISCHE VORSTÖSSE

21.3124	Motion, Gerhard Andrey	«Vertrauenswürdige staatliche E-ID», 26. Mai 2021
21.3125	Motion, Franz Grüter	«Vertrauenswürdige staatliche E-ID», 26. Mai 2021
21.3126	Motion, Min Li Marti	«Vertrauenswürdige staatliche E-ID», 26. Mai 2021
21.3127	Motion, Jörg Mäder	«Vertrauenswürdige staatliche E-ID», 26. Mai 2021
21.3128	Motion, Simon Stadler	«Vertrauenswürdige staatliche E-ID», 26. Mai 2021
21.3129	Motion, FDP-Liberale Fraktion	«Vertrauenswürdige staatliche E-ID», 26. Mai 2021

VERNEHMLASSUNGSVERFAHREN

2025/54	Verordnung zum Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Verordnung, VEID) vom 20. Juni 2025

ANHANG 2 – ABKÜRZUNGEN

BIT	Bundesamt für Informatik und Telekommunikation
BJ	Bundesamt für Justiz
EFK	Eidgenössische Finanzkontrolle
E-ID	Elektronischer Identitätsnachweis für natürliche Personen
eLFA	Elektronischer Lernfahrausweis
EMBAG	Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben
ISC-EJPD	Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartements
PI	Programm Inkrement, siehe Glossar
SBOM	Software Bill of Materials, siehe Glossar
SIEM	Security Information and Event Management, siehe Glossar
SOC	Security Operations Center, siehe Glossar

ANHANG 3 – GLOSSAR

DevSecOps	Development, Security and Operations (deutsch: «Entwicklung, Sicherheit und Betrieb») DevSecOps ist ein Ansatz in der Softwareentwicklung, bei dem Sicherheit von Anfang an in alle Phasen des Softwarelebenszyklus integriert wird. Statt die Sicherheit als separaten Schritt am Ende zu betrachten, wird sie in gemeinsamer Verantwortung von Entwicklungs- (*Dev*), Sicherheits- (*Sec*) und Betriebsteams (*Ops*) zu einem integralen Bestandteil des Prozesses. Ziel ist es, Schwachstellen frühzeitig zu erkennen und zu beheben, was zu schnelleren, sichereren und kostengünstigeren Entwicklungsprozessen führen soll.
PI	Programm Inkrement Ein Programm Inkrement beschreibt einen festen Zeitraum (üblicherweise zwischen acht und zwölf Wochen), in dem agile Teams einen zuvor gemeinsam geplanten und festgelegten Fortschritt in der Softwareentwicklung zu erreichen beabsichtigen. Das Inkrement beinhaltet dabei die vollständigen notwendigen Aufwände zur Planung, Entwicklung, Test und Demonstration des festgelegten Fortschritts.
SBOM	Software Bill of Materials (deutsch: «Software-Stückliste») Ein detailliertes Inventar von verwendeten (Drittanbieter-) Komponenten, Bibliotheken und Abhängigkeiten, die in einer Software enthalten sind oder für deren Ausführung benötigt werden. Eine SBOM hilft dem Anwender bzw. Konsumenten einer Software, Transparenz über allfällige Sicherheitslücken, verwendete Lizenzen oder Abhängigkeiten in der Software-Lieferkette zu identifizieren und unterstützt so dessen Risikomanagement und Compliance.
SIEM	Security Information and Event Management (deutsch: «Sicherheitsinformations- und Ereignisverwaltung») Ein SIEM-Prozess hilft bei der Erkennung, Überwachung und Meldung von sicherheitsrelevanten Ereignissen. Das Ziel ist, einen zentralen Überblick über den Zustand der verwendeten IT-Infrastruktur zu erlangen, und Einblicke in die darin ablaufenden Aktivitäten zu gewinnen. Der SIEM-Prozess wird durch spezielle Cybersicherheitssysteme unterstützt, die Daten aus den verschiedenen Quellen sammeln. Dies, um in Echtzeit Bedrohungen und Anomalien zu erkennen und eine schnelle Reaktion darauf zu ermöglichen.
SOC	Security Operations Center (deutsch: «Sicherheitsbetriebszentrale») Ein SOC ist eine zentrale Funktion oder Einheit in einer Organisation, welche für die Cybersicherheit zuständig ist. Das SOC überwacht die Systeme, Netzwerke und Anwendungen (z. B. im Rahmen eines SIEM-Prozesses) rund um die Uhr. Erkannte potenzielle Bedrohungen werden vom SOC analysiert, um darauf reagieren zu können. Ziel ist die Verbesserung der Sicherheitslage der Organisation und deren Schutz vor Cyberbedrohungen.