Dateinummer: 2022-0941
KLASSIFIKATIONS-ID: 3.2.3

Der Vertrauensrahmen

Schwedische E-Identifizierung

Version 04.10.2022

1. Hintergrund und Zweck

Der Vertrauensrahmen für die schwedische E-Identifikation zielt darauf ab, gemeinsame Anforderungen für Aussteller von elektronischen IDs festzulegen, die von der schwedischen Agentur für digitale Verwaltung (DIGG) überprüft und genehmigt wurden. Die Anforderungen sind in verschiedene Schutzklassen – Vertrauensstufen – unterteilt, die verschiedenen Graden der technischen und betrieblichen Sicherheit des Ausstellers und verschiedenen Graden der Überprüfung entsprechen, dass die Person, für die ein elektronischer Identitätsnachweis ausgestellt wird, diejenige ist, die sie vorgibt zu sein.

Die Anforderungen dieses Vertrauensrahmens gelten für die Vertrauensniveaus 2 bis 4, wobei Niveau 4 dem höchsten Schutzniveau entspricht.

Die Einhaltung ist wie folgt zu interpretieren:

(a) wenn das Sicherheitsniveau nicht festgelegt ist, muss die Anforderung auf allen Niveaus erfüllt werden, und

(b) wenn die Zuverlässigkeitsstufe festgelegt ist, so ist die Einhaltung zumindest auf dem entsprechenden Level sicherzustellen.

Anforderungen, die für ein niedrigeres Niveau als das entsprechende festgelegt wurden, bleiben unberücksichtigt.

2. Organisation und Governance

Allgemeine betriebliche Anforderungen

K2.1 Aussteller von schwedischen eID, die keine öffentlichen Einrichtungen sind, müssen als registrierte juristische Personen tätig sein und die für das Unternehmen erforderlichen Versicherungen abschließen und aufrechterhalten.

K2.2 Aussteller von schwedischen eID müssen ein etabliertes Unternehmen sein, in allen in diesem Dokument genannten Bereichen voll einsatzfähig sein, und mit den rechtlichen Anforderungen vertraut sein, die an sie als Aussteller von schwedischen eID gestellt werden.

K2.3 Aussteller von schwedischen eID müssen in der Lage sein, das Haftungsrisiko für Schäden zu tragen, und über ausreichende finanzielle Mittel verfügen, um ihre Geschäfte mindestens ein Jahr lang durchführen zu können.

Informationssicherheit

K2.4 Aussteller von schwedischen eID müssen für die Teile ihrer Tätigkeiten, die vom Vertrauensrahmen betroffen sind, ein Informationssicherheitsmanagementsystem (ISMS) eingerichtet haben, das gegebenenfalls auf ISO/IEC 27001 oder gleichwertigen Grundsätzen für die Verwaltung und Kontrolle der Arbeit im Bereich der Informationssicherheit beruht, einschließlich der folgenden:

(a) Alle sicherheitskritischen administrativen und technischen Prozesse müssen dokumentiert werden und auf einer formalen Grundlage beruhen, auf der Rollen, Verantwortlichkeiten und Befugnisse klar definiert sind.

(b) Die Aussteller von schwedischen eID stellen sicher, dass sie jederzeit über ausreichende personelle Ressourcen verfügen, um ihren Verpflichtungen nachzukommen.

(c) Die Aussteller von schwedischen eID richten einen Risikomanagementprozess ein, der in geeigneter Weise kontinuierlich oder mindestens alle 12 Monate Bedrohungen und Schwachstellen im Unternehmen analysiert und durch die Einführung von Sicherheitsmaßnahmen die Risiken auf ein akzeptables Maß abwägt.

(d) Die Aussteller von schwedischen eID müssen einen Vorfallmanagementprozess einrichten, der systematisch die Qualität des Dienstes sicherstellt, die Formen der Weitermeldung festlegt und sicherstellt, dass geeignete reaktive und präventive Maßnahmen ergriffen werden, um Schäden, die sich aus solchen Ereignissen ergeben, zu mindern oder zu verhindern.

(e) Die Aussteller von schwedischen eID erstellen und testen regelmäßig einen Kontinuitätsplan, der die Zugänglichkeitsanforderungen des Unternehmens erfüllt, indem sie in der Lage sind, kritische Prozesse im Falle einer Krise oder schwerwiegender Vorfälle wiederherzustellen.

(f) Die Aussteller von schwedischen eID bewerten regelmäßig die Arbeit im Bereich der Informationssicherheit und führen Verbesserungsmaßnahmen im Managementsystem ein.

K2.5 Umfang und Reifegrad des Managementsystems:

Level 4: Das Informationssicherheitsmanagementsystem muss der SS-ISO/IEC 27001:2017 oder gleichwertigen nachfolgenden oder internationalen Versionen der Norm entsprechen und im Rahmen dieser Norm alle Anforderungen umfassen, die Aussteller von schwedischen eID auferlegt werden.

Bedingungen für Unteraufträge

K2.6 Ein Aussteller von schwedischen eID, der die Durchführung eines oder mehrerer sicherheitskritischer Prozesse an eine andere Partei ausgelagert hat, legt vertraglich fest, für welche kritischen Prozesse der Unterauftragnehmer verantwortlich ist und welche Anforderungen auf diese anwendbar sind, und präzisiert das Vertragsverhältnis in der Ausstellererklärung.

Rückverfolgbarkeit, Löschung und Speicherung von Dokumenten

K2.7 Die Aussteller von schwedischen eID speichern:

(a) Antragsunterlagen und Unterlagen im Zusammenhang mit der Ausstellung, dem Empfang oder der Sperrung von eID;

(b) Verträge, Strategiepapiere und Ausstellererklärungen; und

(c) Verarbeitungsverlauf und andere Unterlagen, die erforderlich sind, um die Einhaltung der Anforderungen an Aussteller von schwedischen eID nachzuweisen, und die Folgemaßnahmen zu ermöglichen, die belegen, dass die sicherheitskritischen Prozesse und Kontrollen vorhanden und wirksam sind.

K2.8 Die Speicherdauer beträgt mindestens fünf Jahre, und das Material muss während dieses Zeitraums in lesbarer Form vorliegen können, es sei denn, eine Löschung ist aus Sicht des Datenschutzes erforderlich und wird durch Gesetze oder andere Vorschriften gestützt.

Überprüfung und Nachverfolgung

K2.9 Die Aussteller von schwedischen eID richten eine interne Revisionsfunktion ein, welche die Ausgabetätigkeiten regelmäßig überprüft. Der interne Prüfer ist bei der Wahrnehmung seiner Aufgaben in einer Weise unabhängig, die eine objektive und unparteiische Überprüfung gewährleistet, und verfügt über die für die Wahrnehmung seiner Aufgaben erforderliche Kompetenz und Erfahrung. Der interne Prüfer plant die Durchführung der Prüfung unabhängig und dokumentiert dies in einem Prüfplan für einen Zeitraum von drei Jahren. Die Prüfungselemente werden auf der Grundlage einer Risiko- und Wesentlichkeitsanalyse ausgewählt und basieren auf den Beschreibungen der Vorgänge, welche die Aussteller der Agentur für digitale Verwaltung vorgelegt hat.

Level 3 und 4: Die interne Revision erfolgt auf der Grundlage anerkannter Prüfungsstandards.

3. Physische, administrative und personenorientierte Sicherheit

K3.1 Die zentralen Teile des Betriebs sind physisch vor Schäden infolge von Umweltereignissen, unbefugtem Zugang oder anderen äußeren Störungen zu schützen. Die Zugangskontrolle ist so durchzuführen, dass der Zugang zu vertraulichen Bereichen auf befugtes Personal beschränkt ist, Informationsträger sicher aufbewahrt und entsorgt werden und der Zugang zu diesen Schutzbereichen kontinuierlich überwacht wird.

K3.2 Bevor eine Person eine der gemäß K2.4 Buchstabe a genannten und für die Sicherheit besonders wichtigen Rollen übernimmt, hat der Aussteller von schwedischen eID Hintergrundüberprüfungen durchgeführt, um sicherzustellen, dass die Person als zuverlässig angesehen werden kann und dass die Person über die Qualifikationen und Schulungen verfügt, die erforderlich sind, um die sich aus der Rolle ergebenden Aufgaben sicher und geschützt zu erfüllen.

K3.3 Die Aussteller verfügen über Verfahren, mit denen sichergestellt wird, dass nur speziell befugtes Personal Zugang zu den gemäß K2.7 erhobenen und gespeicherten Daten hat.

K3.4 **Level 3 und 4:** Die Aussteller stellen in der gesamten Kette des Ausstellungsverfahrens sicher, dass die Aufgabentrennung so angewandt wird, dass keine einzelne Person in der Lage ist, eine eID im Namen einer anderen Person zu erhalten.

4. Technische Sicherheit

K4.1 Die Aussteller von schwedischen eIDs stellen sicher, dass die vorhandenen technischen Kontrollen ausreichen, um das Schutzniveau zu erreichen, das in Bezug auf Art, Umfang und andere Umstände des Geschäfts als notwendig erachtet wird, und dass diese Kontrollen funktionieren und wirksam sind.

K4.2 Elektronische Kommunikationsmittel, die bei der Übermittlung vertraulicher Daten verwendet werden, sind vor Abhören, Manipulation und Wiederholung zu schützen.

K4.3 Vertrauliches kryptografisches Schlüsselmaterial, das zur Ausstellung von eID, zur Identifizierung von Inhabern und zur Ausstellung von Identitätszertifikaten verwendet wird, ist so zu schützen, dass Folgendes eingehalten wird:

(a) der Zugang ist logisch und physisch auf die unbedingt erforderlichen Rollen und Anwendungen beschränkt

(b) das Schlüsselmaterial darf niemals im Klartext auf persistenten Speichermedien gespeichert werden

(c) das Schlüsselmaterial wird durch die Verwendung eines kryptografischen Hardwaremoduls mit aktiven Sicherheitsmechanismen geschützt, die sowohl physischen als auch logischen Versuchen, das Schlüsselmaterial zu kompromittieren, entgegenwirken

(d) die Sicherheitsmechanismen für den Schutz von Schlüsselmaterial sind transparent und beruhen auf anerkannten und etablierten Normen und

(e) **Niveau 3 und 4:** Die Aktivierungsdaten für den Schlüsselmaterialschutz werden über eine Mehrpersonensteuerung verwaltet.

K4.4 Die Aussteller müssen über dokumentierte Verfahren verfügen, um sicherzustellen, dass das erforderliche Schutzniveau in der einschlägigen IT-Umgebung im Laufe der Zeit und im Zusammenhang mit Änderungen aufrechterhalten werden kann, einschließlich regelmäßiger Schwachstellenbewertungen und angemessener Vorbereitung auf sich ändernde Risikoniveaus und auftretende Vorfälle.

5. Anwendung, Identifizierung und Registrierung

Informationen zu den Bedingungen

K5.1 Die Aussteller von schwedischen eID müssen verbundenen Nutzern, Anbietern elektronischer Dienste und anderen Personen, die sich auf den Dienst des Ausstellers verlassen können, Informationen über Verträge, Geschäftsbedingungen sowie damit zusammenhängende Informationen und Einschränkungen der Nutzung des Dienstes zur Verfügung, bereitstellen.

K5.2 Ein Aussteller von schwedischen eID muss sich eindeutig auf die Geschäftsbedingungen beziehen und die Verfahren so gestalten, dass die Geschäftsbedingungen dem Antragsteller im Ausstellungsverfahren zur Verfügung gestellt werden.

K5.3 Aussteller von schwedischen eID legen eine Ausstellererklärung vor, die Folgendes enthält:

(a) Identität und Kontaktdaten des Ausstellers

(b) kurze Beschreibungen der vom Aussteller erbrachten Dienstleistungen und Lösungen, einschließlich angewandter Methoden für die Beantragung, Ausgabe und Sperrung

(c) Bedingungen im Zusammenhang mit der erbrachten Dienstleistung, einschließlich der Verpflichtungen des Nutzers zum Schutz seiner elektronischen ID, der Verpflichtungen und Verantwortlichkeiten des Ausstellers, etwaiger Garantien und zugesagter Verfügbarkeit

(d) Informationen über die Verarbeitung personenbezogener Daten und die Art und Weise, in der sie durchgeführt wird und

(e) Vorkehrungen zur Änderung der Bedingungen oder sonstigen Konditionen der erbrachten Dienstleistung, einschließlich der Maßnahmen, die zu ergreifen sind, um den Dienst kontrolliert einzustellen.

K5.4 **Level 3 und 4:** Die Aussteller von schwedischen eID legen auf Anfrage der Agentur für digitale Verwaltung (DIGG) oder einer anderen Vertragspartei, die sich auf die vom Aussteller erbrachten Dienstleistungen stützt, Informationen darüber vor, wie das Unternehmen im Besitz ist und geführt wird.

K5.5 Ein Aussteller von schwedischen eID, der seine Tätigkeit einstellt, muss einen im Voraus festgelegten Plan zur Einstellung des Dienstes befolgen. Der Plan umfasst die Unterrichtung aller Nutzer des Dienstes und der DIGG. Der Aussteller hat archiviertes Material nach Einstellung gemäß K2.7 und K2.8 weiterhin zur Verfügung zu halten.

Anwendung

K5.6 Eine schwedische eID darf nur auf Antrag des Antragstellers oder im Rahmen eines anderen gleichwertigen Anerkennungsverfahrens und erst dann ausgestellt werden, wenn der Antragsteller über die Bedingungen, unter denen sie ausgestellt wird, und die ihm obliegende Verantwortung unterrichtet wurde.

Die Ausstellung einer eID, die ein gültiges oder kürzlich gesperrtes eID-Dokument ersetzt oder ergänzt, das zuvor von demselben Aussteller ausgestellt wurde, kann jedoch ohne vorheriges Antragsverfahren erfolgen.

K5.7 Ein Antrag auf eine schwedische eID ist mit einer persönlichen Identitätsnummer oder Koordinierungsnummer sowie mit den Informationen zu verknüpfen, die der Aussteller ansonsten benötigt, um eine solche eID bereitzustellen.

Feststellung der Identität des Antragstellers

K5.8 Die Aussteller von schwedischen eID müssen sich vergewissern, dass die mit dem Antrag verknüpften Informationen vollständig sind, und den in einem amtlichen Register eingetragenen Informationen entsprechen.

K5.9 Werden die in einem amtlichen Register zu überprüfenden Informationen als vertraulich gekennzeichnet („geschützte Identität"), so können die erforderlichen Kontrollen auf andere gleichwertige Weise durchgeführt werden.

K5.10 Identifizierung des Antragstellers bei einem persönlichen Besuch:

Aussteller von schwedischen eID können die Identität des Antragstellers während eines persönlichen Besuchs auf die gleiche Weise überprüfen wie bei der Ausstellung eines Standardausweises.

K5.11 Fernidentifizierung des Antragstellers in der bestehendenBeziehung:

Level 3: Aussteller von schwedischen eID, die den Antragsteller bereits in einer Beziehung identifiziert haben, die wirtschaftlich oder rechtlich bedeutsame Transaktionen umfasst, und bei denen der Antragsteller durch andere zuverlässige Mittel, die den Anforderungen der Stufe 3 des schwedischen eID-Gütezeichens gleichwertig sind, aus der Ferne identifiziert werden kann, können diese Methode verwenden, um die Identität des Antragstellers festzustellen.

Level 4: Nicht zutreffend.

K5.12 Identifizierung über schwedische eID:

Ein Aussteller von schwedischen eID kann den Antragsteller mittels einer bestehenden gültigen schwedischen eID, die mindestens der gleichen Sicherheitsstufe wie die auszustellende entspricht, aus der Ferne identifizieren, wenn er diese Identifizierung ohne vertragliche Hindernisse als Grundlage für die Ausstellung einer neuen eID verwenden kann.

Level 4: Die Gültigkeitsdauer der neu ausgestellten eID ist darauf beschränkt, die Gültigkeitsdauer der bestehenden eID nicht zu überschreiten.

K5.13 Fernidentifizierung des Antragstellers:

Level 2: Aussteller von schwedischen eID können zuverlässige Bildaufzeichnungen eines gültigen Standardausweises und des Gesichts des Antragstellers als Grundlage für die Feststellung der Identität des Antragstellers aus der Ferne verwenden, wenn der Vergleich keine Zweifel an der wahren Identität des Antragstellers aufkommen lässt.

Level 3: Die Aussteller von schwedischen eID können durch sicheres Auslesen eines gültigen Standardausweises, der elektronisch gespeicherte biometrische

Daten enthält, die Identität des Antragstellers aus der Ferne auf der Grundlage dieser Daten feststellen, wenn die entsprechenden biometrischen Daten der zu identifizierenden Person so sicher erhoben werden können, dass ein Vergleich mit gleicher Zuverlässigkeit wie bei einem persönlichen Besuch durchgeführt werden kann, und wenn der Abgleich keine Zweifel an der wahren Identität des Antragstellers aufkommen lässt.

Level 4: Nicht zutreffend.

Registrierung

K5.14 Die Aussteller von schwedischen elektronischen Identitätsnachweisen führen unter Berücksichtigung der geltenden Vorschriften zum Schutz personenbezogener Daten ein Register der verbundenen Nutzer und der zugewiesenen elektronischen Identifizierungsdokumente und halten dieses Register auf dem neuesten Stand.

6. Ausstellung und Sperrung der eID

Gestaltung technischer Mittel

K6.1 „Technisch“ bedeutet:

Level 2 und 3: Die technischen Mittel für die elektronische Identifizierung mittels eID mit dem schwedischen eID-Gütezeichen werden nach dem Zwei-Faktor-Prinzip konzipiert, wobei ein Teil aus elektronisch gespeicherten Informationen besteht, die der Nutzer besitzen muss, und der andere Teil aus dem, was der Nutzer zur Aktivierung der eID verwenden muss.

Level 4: Technische Mittel für die elektronische Identifizierung mittels eID mit dem schwedischen eID-Gütezeichen werden nach dem Zwei-Faktor-Prinzip konzipiert, wobei ein Teil aus einem persönlichen Sicherheitsmodul besteht, das der Nutzer besitzen muss, und der andere Teil aus dem, was der Nutzer zur Aktivierung des Sicherheitsmoduls verwenden muss.

K6.2 Der Aktivierungsmechanismus und der personalisierte Code müssen so gestaltet sein, dass es unwahrscheinlich ist, dass Dritte den Schutz, auch mit mechanischen Mitteln, verletzen.

Level 3 und 4: Der Schutz umfasst Mechanismen zur Verhinderung der Vervielfältigung und Manipulation des elektronischen Identifizierungsdokuments.

K6.3 Nutzer von eID mit dem schwedischen eID-Gütezeichen können von sich aus innerhalb der Gültigkeitsdauer der eID kostenlos und ohne nennenswerte Unannehmlichkeiten einen neuen persönlichen Code austauschen oder anfordern und durch Anleitung oder automatische Erstellung dabei unterstützt werden, die Anforderungen von K6.2 aufrechtzuerhalten.

Wenn die eID so gestaltet ist, dass ein personalisierter Code nicht ausgetauscht werden kann, sollte der Benutzer stattdessen unter den gleichen Bedingungen umgehend eine neue eID mit einem neuen personalisierten Code erhalten können, der den vorherigen über ein Sperrverfahren ersetzt.

K6.4 Die Aussteller von schwedischen eID stellen sicher, dass die für die elektronische Identifizierung der Inhaber registrierten Daten den Antragsteller eindeutig repräsentieren und der betreffenden Person bei der Ausstellung des eID-Dokuments zugeordnet werden.

K6.5 Die Gültigkeitsdauer der ausgestellten eID wird unter Berücksichtigung der Sicherheitsmerkmale des eID-Dokuments und der Missbrauchsrisiken begrenzt. Die maximale Gültigkeitsdauer der eID beträgt fünf Jahre.

Bereitstellung des eID-Dokuments

K6.6 Fernbereitstellung:

Level 2: Ein Aussteller von schwedischen eID stellt das e-ID-Dokument in einer Weise bereit, welche die im amtlichen Register gespeicherten Kontaktdaten oder die im Zusammenhang mit dem elektronischen Verfahren gemäß K5.13 Stufe 2 aufgezeichneten Informationen bestätigt.

Level 3: Ein Aussteller von schwedischen eID, der eine eID über ein elektronisches Verfahren gemäß K5.11 Level 3, K5.12 Level 3 oder K5.13 Level 3 bereitstellt, hat bei Neuausstellung unabhängig von der Sicherheitsvorkehrung sicherzustellen, dass der Nutzer darüber informiert wird, dass ein solches e-ID-Dokument übergeben wurde, oder durch andere Maßnahmen ein gleichwertiges Maß an Kontrolle sicherzustellen, dass die Person im Zusammenhang mit der Bereitstellung auf das Risiko eines Identitätsdiebstahls hingewiesen wird.

Level 4: Ein Aussteller von schwedischen eID, der eine eID über ein elektronisches Verfahren gemäß K5.12 Stufe 4 bereitstellt, muss bei der Neuausstellung, getrennt und unabhängig von der Sicherheitsvorkehrung, sicherstellen, dass der Nutzer darüber informiert wird, dass ein solches eID-Dokument übergeben wurde.

K6.7 Bereitstellung während eines persönlichen Besuchs:

Ein Aussteller von schwedischen eID stellt während eines persönlichen Besuchs und nach einer Identitätsprüfung gemäß K5.10 das elektronische Identifizierungsdokument gegen unterzeichneten Empfang zur Verfügung und stellt ferner den Teil zur Verfügung, den der Nutzer verwenden muss, um die eID getrennt und unabhängig von der Bereitstellung des eID-Dokuments in Bezug auf die Sicherheit auf der Grundlage der in einem amtlichen Register geführten Kontaktdaten oder anderer Informationen von gleichwertiger Glaubwürdigkeit zu aktivieren.

Sperrdienst

K6.8 Die Aussteller von schwedischen eID stellen einen Sperrdienst bereit, der für den Nutzer gut zugänglich ist, damit er seine eID sperren kann.

K6.9 Aussteller von schwedischen eID müssen Blockierungsanfragen umgehend und sicher bearbeiten und ausführen und Maßnahmen ergreifen, um einen systematischen Missbrauch des Blockierungsdienstes oder andere vorsätzliche Maßnahmen zu verhindern,die zu einer weitverbreiteten Sperrung elektronischer Identifizierungsdokumente führen, und sicherstellen, dass die eID der Nutzer bei Bedarf zur Verfügung stehen.

7. Überprüfung der elektronischen Identitäten der Inhaber

K7.1 Die Aussteller von schwedischen eID stellen sicher, dass bei der Überprüfung der Identität des Inhabers zuverlässige Kontrollen der Echtheit und Gültigkeit des eID-Dokuments durchgeführt werden.

K7.2 Die Aussteller von schwedischen eID stellen sicher, dass bei der Überprüfung der elektronischen Identitäten der Inhaber technische Sicherheitskontrollen durchgeführt wurden, sodass es unwahrscheinlich ist, dass Dritte durch Erraten, Abhören, Wiedergeben oder Manipulation des Prozesses gegen die Schutzmechanismen verstoßen können.

8. Ausstellung von Identitätsbescheinigungen

Aussteller von schwedischen elektronischen Identitätsnachweisen, die einen Dienst für die Ausstellung von Identitätszertifikaten für vertrauende elektronische Dienste erbringen, müssen auch die Bestimmungen dieses Abschnitts einhalten.

K8.1 Die Aussteller von schwedischen eID stellen sicher, dass der Dienst für die Ausstellung von Identitätszertifikaten gut zugänglich ist und dass der Ausstellung von Identitätszertifikaten eine zuverlässige Identifizierung gemäß Abschnitt 7 vorausgeht.

Level 4: Die Zertifikate enthalten einen Verweis auf kryptografisches Schlüsselmaterial, das sich nach Prüfung durch den Aussteller im alleinigen Besitz des Inhabers befindet.

K8.2 Eingereichte Identitätszertifikate sind nur so lange gültig, wie dies erforderlich ist, um dem Benutzer den Zugriff auf den angeforderten e-Service zu ermöglichen, und müssen so geschützt sein, dass die Informationen nur vom vorgesehenen Empfänger gelesen werden können und dass die Echtheit der Zertifikate von den Empfängern der Zertifikate überprüft werden kann.

K8.3 Die Aussteller von schwedischen eID begrenzen unter Berücksichtigung der Risiken eines Missbrauchs des Zertifizierungsdienstes den Zeitraum, innerhalb dessen einem bestimmten Inhaber mehrere aufeinanderfolgende Identitätszertifikate ausgestellt werden können, bevor der Inhaber gemäß den Bestimmungen von Abschnitt 7 erneut identifiziert wird.