

eCH-0170 – Qualitätsmodell zur Authentifizierung von Subjekten

Name	Qualitätsmodell zur Authentifizierung von Subjekten
eCH-Nummer	eCH-0170
Kategorie	Standard
Reifegrad	Implementiert
Version	2.0.1
Status	Genehmigt
Beschluss am	2025-09-03
Ausgabedatum	2017-10-09
Ersetzt Version	2.0.0 – Minor Change
Voraussetzungen	---
Beilagen	Beil1_d_2017-06-02_eCH-0170_V2.0_Hilfsmittel_Vergleich-v1.0-und-v2.0.xlsx BEIL2_d_2017-06-02_eCH-0170_V2.0_Hilfsmittel_Vertrauensstufen-Rechner.xlsx
Sprachen	Deutsch (Original), Französisch (Übersetzung)
Fachgruppe	IAM
Herausgeber / Vertrieb	Verein eCH, Räfelstrasse 20, 8045 Zürich T 044 388 74 64 / info@ech.ch / www.ech.ch

Zusammenfassung

Der Standard *eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten* dient der qualitativen Einstufung und dem Vergleich der Authentifizierung von natürlichen und juristischen Personen. Der Standard ist damit bei der Schaffung einer gemeinsamen Vertrauensbasis in föderierten, organisationsübergreifenden IAM-Systemen von grosser Bedeutung und kann als Ausgangspunkt für die Zertifizierung der IAM-Dienstleister verwendet werden.

Das in diesem Standard beschriebene Qualitätsmodell definiert **4 Vertrauensstufen**. Diese 4 Vertrauensstufen setzen sich aus den folgenden vier Teilmodellen zusammen:

- Qualitätsmodell der Authentifizierung: Definiert die Vertrauensstufen der Authentifizierung (VSA) basierend auf der Stärke und möglichen Zertifizierungen eines Authentifizierungsmittels.
- Qualitätsmodell der Registrierung: Definiert die Vertrauensstufen der Registrierung (VSR), dabei wird zwischen natürlichen und juristischen Personen unterschieden. Die Qualität der Registrierung natürlicher Personen wird durch die Stärke der Identifikation der Person sowie der Übergabe und Verlängerung der Authentifizierungsmittel bestimmt. Die Registrierung juristischer Personen wird durch die Stärke der Registrierung der zugehörigen natürlichen Person, der Identifizierung der juristischen Person sowie der Verknüpfung der beiden Personen bestimmt.
- Qualitätsmodell der Steuerung: Definiert die Vertrauensstufen der Steuerung (VSS) basierend auf den Kriterien Aufsicht, Haftung und Maturität.
- Qualitätsmodell der Föderierung: Definiert die Vertrauensstufen der Föderierung (VSF) basierend auf der Authentizität, dem Vertraulichkeitsschutz, der Übermittlungsform und dem Nachweis des Besitzes der Authentifizierungsbestätigung.

Um eine Vertrauensstufe des Gesamtmodells zu erfüllen, müssen alle Teilmodelle den aufgeführten Stufen entsprechen. Die geringste Stufe bei einem Teilmodell bestimmt somit die Stufe des Gesamtmodells.

Jedem Teilmodell sind Qualitätskriterien zugeordnet, die detailliert mit Beispielen beschrieben sind. Die Qualitätskriterien enthalten Ausprägungen, die erfüllt werden müssen. Dadurch erhalten sie eine Bewertungsstufe. Die Vertrauensstufe der Teilmodelle wird dann jeweils durch die tiefste Stufe der Kriterien bestimmt.

Die folgende Tabelle zeigt im Überblick die wesentlichen Ausprägungen pro Teilmodell und deren Komposition zu den vier Vertrauensstufen. Die detaillierte und vollständige Beschreibung und Bewertung dieser Eigenschaften erfolgen in den Kapiteln 4 bis 8.

Vertrauensstufe	Bezeichnung	VSA	VSR	VSS	VSF
1	Kein oder minimales Vertrauen	Single Factor Authentisierung (SFA)	Selbst deklarierte Angaben	Keine Prüfung, keine Haftung des CSP	authentisierte Bestätigung
2	Geringes Vertrauen	Multi Factor Authentisierung (MFA)	Überprüfung der Beweismittel, online Anwesenheit, sichere Übergabe des Auth.mittels	Interne Regelungen und Standards, beschränkte Haftung	+ verschlüsselte Bestätigung
3	Beträchtliches Vertrauen	HW-MFA	Validierung anerkannter Beweismittel, online Anwesenheit, persönliche Übergabe des Auth.mittels	Regelungen und Standards extern überprüft, Haftung nach Gesetz	
4	Hohes Vertrauen	Zertifizierte HW-MFA	Staatlich anerkannte Beweismittel, Dokumentation der Anwesenheit (physisch oder Virtual-in-Person), eigenhändige Übergabe des Auth.mittels	Standards durch amtlich akkreditierte Stelle überprüft, automatisierte Prozesse, Haftung und Konventionalstrafe	+ Authentisierung des Überbringers (HoK)

Zu Abschluss wird das Qualitätsmodell den internationalen Standards der eIDAS-Verordnung 910/2014 [1], ISO/IEC 29115 [2], NIST SP 800-63-3 [3] gegenübergestellt (siehe Kapitel 8).

Inhaltsverzeichnis

1	Einleitung	9
1.1	Status.....	9
1.2	Überblick	9
1.3	Ziel des Dokuments	9
1.4	Nutzer des Standards	12
1.5	Abgrenzung.....	12
1.6	Informationsarchitektur.....	13
1.7	Abstützung.....	14
1.7.1	STORK.....	14
1.7.2	eIDAS.....	14
1.7.3	ISO.....	15
1.7.4	NIST.....	15
1.7.5	ZertES/VZertES	15
1.8	Vorteile	15
1.9	Schwerpunkte	15
1.10	Normativer Charakter der Kapitel	16
2	Terminologie	16
2.1	Authentifikator	16
2.2	Authentifizierung	17
2.3	Authentifizierungsbestätigung	17
2.4	Authentifizierungsfaktor.....	17
2.5	Authentifizierungsmittel.....	18
2.6	Beweismittel.....	20
2.7	Biometrisches Merkmal.....	20
2.8	Certificate Authority/Certification authority (CA)	21
2.9	Client Plattform	21
2.10	Credential	21
2.11	Credential Service Provider (CSP).....	22
2.12	E-Identity	22
2.13	Elektronisches Identifizierungsmittel.....	22

2.14	Elektronisches Identifizierungssystem	22
2.15	Definitionszeit	23
2.16	Föderierung / Federation	23
2.17	Identifizierung	24
2.18	Identitätsdokument.....	24
2.19	Identity Provider (IdP).....	24
2.20	Juristische Person.....	24
2.21	Körperliches Merkmal	24
2.22	Laufzeit	24
2.23	Registrierungsstelle/Registration Authority (RA).....	25
2.24	Subjekt.....	25
2.25	UID-Einheit	26
2.26	Verlässliche Quelle	26
2.27	Verwaltung	26
3	Qualitätsmodell	27
3.1	Vertrauensstufen	28
3.2	Komposition der Vertrauensstufen	30
3.3	Verwendung zur Einstufung von IAM-Diensteanbietern	31
3.3.1	Einstufung einer RA	31
3.3.2	Einstufung eines IdP	31
3.3.3	Einstufung eines CSP	31
3.4	Qualitätskriterien	32
3.5	Vorbedingungen	32
4	Qualitätsmodell der Authentifizierung.....	35
4.1	Vertrauensstufen der Authentifizierung (VSA)	35
4.2	Kriterien der Authentifizierung	36
4.2.1	Authentifizierungsmittel	36
4.2.2	Zertifizierung des Authentifizierungsmittel	37
4.2.3	Re-Authentifizierung.....	38
5	Qualitätsmodell der Registrierung.....	39
5.1	Vertrauensstufen der Registrierung (VSR)	39

5.1.1	Für natürliche Personen	39
5.1.2	Für juristische Personen.....	40
5.2	Kriterien der Registrierung	41
5.2.1	Faktoren zur Identifikation	41
5.2.1.1	Faktor Anwesenheit	41
5.2.1.2	Faktor Beweismittel.....	42
5.2.1.3	Faktor Validierung der Angaben.....	44
5.2.1.4	Faktor Nichtabstreitbarkeit	45
5.2.1.5	Faktor Vollmacht	46
5.2.2	Identifikation natürlicher Personen	47
5.2.3	Identifikation juristischer Personen	49
5.2.4	Verknüpfung natürliche und juristische Person.....	50
5.2.5	Übergabe Authentifizierungsmittel.....	51
5.2.6	Verlängerung/Ersetzung Authentifizierungsmittel	54
6	Qualitätsmodell der Steuerung	56
6.1	Vertrauensstufen der Steuerung (VSS)	56
6.2	Kriterien der Steuerung.....	57
6.2.1	Aufsicht	57
6.2.2	Haftung	58
6.2.3	Maturität.....	59
7	Qualitätsmodell der Förderierung	61
7.1	Vertrauensstufen der Förderierung (VSF)	61
7.2	Kriterien der Förderierung.....	62
7.2.1	Nachweis des Besitzes der Authentifizierungsbestätigung	62
7.2.2	Authentizität der Authentifizierungsbestätigung	63
7.2.3	Vertraulichkeitsschutz der Authentifizierungsbestätigung	63
7.2.4	Übermittlungsform der Authentifizierungsbestätigung.....	64
8	Vergleich mit internationalen Standards.....	65
8.1	Qualitätsmodell der Authentifizierung	66
8.2	Qualitätsmodell der Registrierung	67
8.2.1	Registrierung für natürliche Personen	67

8.2.2	Registrierung von juristischen Personen	67
8.3	Qualitätsmodell der Steuerung	68
8.4	Qualitätsmodell der Föderierung	68
9	Haftungsausschluss/Hinweise auf Rechte Dritter	69
10	Urheberrechte	69
Anhang A - Referenzen & Bibliographie		70
Anhang B - Mitarbeit & Überprüfung		72
Anhang C - Abkürzungen und Glossar		72
C.1	Abkürzungen	72
C.2	Glossar	73
Anhang D - Änderungen gegenüber Vorversion		76
Anhang E - Abbildungsverzeichnis		78
Anhang F - Tabellenverzeichnis		79
Anhang G - Prozesse		81
G.1	Subjekt authentifizieren und Identität föderieren	81
G.1.1	Subjekt authentifizieren	81
G.1.2	Identität föderieren	82
G.2	Subjekt registrieren	84
G.2.1	Identität überprüfen natürliche Person	85
G.2.2	Identität überprüfen juristische Person	85
G.2.3	Authentifizierungsmittel festlegen	86
G.3	IAM steuern	87
G.3.1	Vertrauensstufen festlegen	87
G.3.2	Dienstanbieter festlegen	88
G.3.3	Steuerungsprozesse festlegen	88
G.3.4	Risiko einschätzen und behandeln	89
Anhang H - Anforderungen an Authentifizierungsmittel		90
H.1	Memorized Secrets	90
H.2	Look-Up Secrets	90
H.3	Out of Band Authenticators	91
H.4	OTP Devices	91

H.5 Single Factor Cryptographic Devices.....	92
H.6 Multi-Factor Cryptographic Software	92
H.7 Multi-Factor Cryptographic Devices.....	92
Anhang I - Anforderungen an den Faktor Validierung der Angaben	93

Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

1 Einleitung

1.1 Status

Genehmigt: Das Dokument wurde vom Expertenausschuss genehmigt. Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

1.2 Überblick

Unter dem Standard eCH-0107 [4] positionieren sich die Konzepte und ergänzende Hilfsmittel für föderierte IAM-Lösungen.

Beim vorliegenden Standard eCH-0170 handelt es sich um ein Qualitätsmodell und gehört damit zusammen mit dem Standard eCH-0171 [5] zur Gruppe der ergänzenden Hilfsmittel (siehe auch Abbildung 1).

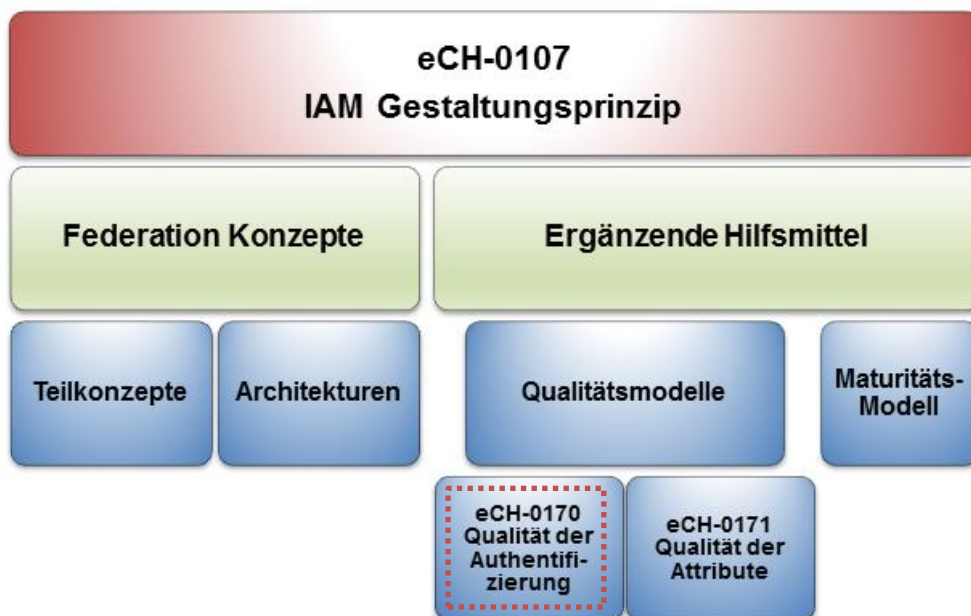


Abbildung 1: Einordnung des eCH-0170 Standards

1.3 Ziel des Dokuments

Ziel des Standards ist es, den Stakeholdern im IAM (entsprechend der Definition der Stakeholder im eCH-0107 [4]) eine Vorgabe zur qualitativen Einstufung und zum Vergleich der Authentifizierung von Subjekten zu geben. Damit können Stakeholder besser einschätzen, wie sicher es ist, dass sich ein Subjekt, welches in einem gegebenen IAM-System authentifiziert wird, wirklich das ist, als welches es sich ausgibt.

Wie aus Abbildung 2 ersichtlich ist, werden vor allem föderierte, organisationsübergreifende IAM-Systeme in diesem Standard betrachtet. D.h. in einem typischen föderierten IAM-System gehören Identity Provider (IdP) und Relying Party (RP) zu verschiedenen Organisationen. So befinden sich Subjekte und Ressourcen in verschiedenen Domänen. In einem föderierten IAM-System besteht eine logische und physische Trennung von IdP und RP und die Informationen über die Authentifizierung und das Subjekt werden über ein Netzwerk übertragen.

Allerdings ist es ohne weiteres möglich, das Qualitätsmodell für nicht föderierte oder organisationsinterne IAM-Systeme anzuwenden. Insbesondere sollten Stakeholder, die ggf. später in ein föderiertes Identitätssystem integriert werden sollen, frühzeitig beginnen, die in diesem Zusammenhang an sie gestellten Anforderungen umzusetzen. Die EU strebt selbst einen digitalen Einheitsmarkt an. Der eCH-0170 Standard berücksichtigt die internationalen Anforderungen und die der EU, um dazu beizutragen, dass Schweizer Lösungen, die zu diesem Standard konform sind, auch international und europäisch interoperabel sind.

Dieser Standard ist nicht nur eine Vorgabe zur Bewertung der IAM-Dienstleister, sondern kann auch als Ausgangspunkt für die Zertifizierung von IAM-Dienstleister beigezogen werden.

In Abbildung 2 sind die Kernelemente, die zur Bestimmung der Qualität der Authentifizierung eines Subjekts notwendig sind, dargestellt. Darin, wie auch bei weiteren Modellen im Dokument, wird die Farbverwendung aus Tabelle 1 verwendet.

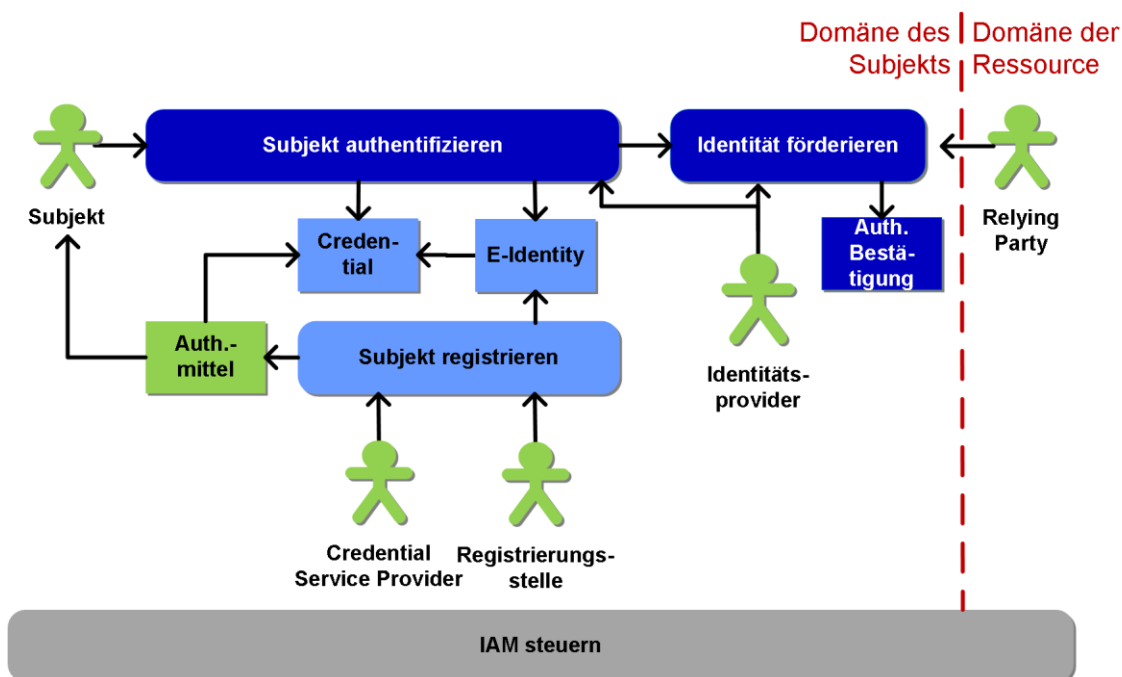


Abbildung 2: Prozessmodell Authentifizierung eines Subjektes

Im Zentrum steht die Authentifizierung des Subjektes zur Laufzeit (Prozess *Subjekt authentifizieren*). Ziel des Vorganges ist es - nebst der Authentifizierung des Subjekts – die Zugriffssteuerung auf eine Ressource durch eine Relying Party (RP) zu ermöglichen. Die Zugriffssteuerung wird in diesem Standard nicht behandelt.

Bei der Authentifizierung verwendet das Subjekt ein Authentifizierungsmittel, das einen oder mehrere

Authentifizierungsfaktoren unterstützt. Bei der Authentifizierung wandelt ein Authentifikator mit Hilfe eines Geheimnisses - welches nur ihm zugänglich ist - mögliche Authentifizierungsfaktoren in einen Ausgabewert um.

Der authentifizierende Dienst (IdP) prüft den Ausgabewert des Authentifikators mit Hilfe des Credentials, das die Verbindung zwischen Authentifikator und der E-Identity bildet (siehe auch Kapitel 2.5). Ist die Prüfung positiv, ist die Authentifizierung erfolgreich und die behauptete E-Identity wird bestätigt.

Erfolgt die Authentifizierung des Subjekts in einem föderierten IAM-System, wird nach der primären Authentifizierung des Subjekts gegenüber dem IdP das Ergebnis dieses Vorgangs in Form einer Authentifizierungsbestätigung vom IdP an die RP übertragen (Prozess *Identität föderieren*).

Bevor sich ein Subjekt zur Laufzeit authentisieren kann, muss es bei einer Registrierungsstelle (RA) registriert werden. Die RA überprüft die Identität des Subjektes und erstellt eine E-Identity mit einem eindeutigen Identifikator für das Subjekt. Der Credential Service Provider (CSP) stellt für diese E-Identity ein neues Authentifizierungsmittel aus oder verbindet ein vorhandenes mit dieser E-Identity. Im Credential wird die Verbindung zwischen der E-Identity und dem Authentifizierungsmittel abgelegt. Das Authentifizierungsmittel kann ein oder mehrere Authentifikationsfaktoren unterstützen.

Die RA und der IdP können integraler Teil des CSP sein, oder von diesem beauftragt werden.

Alle beteiligten Stakeholder müssen im Voraus gemeinsam auf die notwendigen Vorgaben und Rahmenbedingungen für den Betrieb des IAM-Systems geeinigt haben (Prozess *IAM steuern*).

grau	Grau visualisiert in diesem Dokument Elemente, die bereits vor der Definitionszeit aktiv sind (z.B. Governance).
hellblau	Die hellblaue Farbe wird in diesem Dokument konsequent für die Definitionszeit verwendet, während der alle Informationen den Informationselementen zugeordnet (also definiert) werden.
dunkelblau	Die dunkelblaue Farbe wird durchgehend für die Laufzeit verwendet. Zur Laufzeit wird eine Eigenschaft auf der Basis der Informationselemente bestätigt.
hellgrün	Die hellgrüne Farbe wird in diesem Dokument konsequent für Realweltobjekte verwendet.

Tabelle 1: Farbverwendung im Dokument

1.4 Nutzer des Standards

Dieser Standard kann von den grundlegenden Stakeholdern in einer Identitätsföderation (siehe auch eCH-0107 [4]) unterschiedlich verwendet werden:

- Das beschriebene Qualitätsmodell hilft den **Subjekten** die Anforderungen an unterschiedliche Authentifizierungsmittel sowie an die Registrierungsprozesse besser zu verstehen.
- **Relying Parties** können mit diesem Standard die Leistungen der IAM-Dienstleister bewerten und vergleichen.
- **IAM-Dienstleister** können den Standard zur Spezifikation und Bewertung ihrer eigenen Leistungen verwenden.

Regulatoren erlangen ein konzeptionelles Verständnis der Anknüpfungspunkte für die Festlegung von Regeln.

1.5 Abgrenzung

In diesem Kapitel wird aufgezeigt, welche Teile in die Bestimmung des Qualitätsmodells einfließen bzw. behandelt werden und welche nicht.

- In diesem Standard wird nur die Authentifizierung von natürlichen Personen und von juristischen Personen nach Art. 52 ff ZGB sowie gemäss den einschlägigen Bestimmungen des Gesellschaftsrechtes des OR behandelt.
- Natürliche Personen, die im Auftrag einer Organisation (z.B. in der Verwaltung), eines Unternehmens oder einer UID-Einheit handeln, werden bei der Authentifizierung von natürlichen Personen, die im eigenen Namen handeln, nicht unterschieden und sollten bei der Definition von Zugriffsrechten entsprechend behandelt werden (z.B. durch Vergabe von Rollen oder das Zuweisen von Attributen).
- Die Authentifizierung von Services und Objekten (z.B. Sensorknoten im Internet der Dinge oder die Maschinen-zu-Maschinen Kommunikation zwischen Servern) wird aufgrund von fehlenden internationalen Standards¹ in dieser Version nicht betrachtet.
- Dieser Standard definiert die Qualitätskriterien für die Authentifizierung von natürlichen und juristischen Personen in föderierten und nicht föderierten IAM-Systemen. Die speziellen Anforderungen von IAM-Systemen mit zentraler Vermittlungsinfrastruktur oder Interfederation sind nicht berücksichtigt und müssen ggf. ergänzt werden.

¹Erste Versuche zur Standardisierung findet man z.B. auf: <https://kantarainitiative.org/confluence/display/IDoT/Home>

1.6 Informationsarchitektur

Die Informationsarchitektur in Abbildung 3 stellt eine Ergänzung der Informationsarchitektur von eCH-0107 [4] dar.

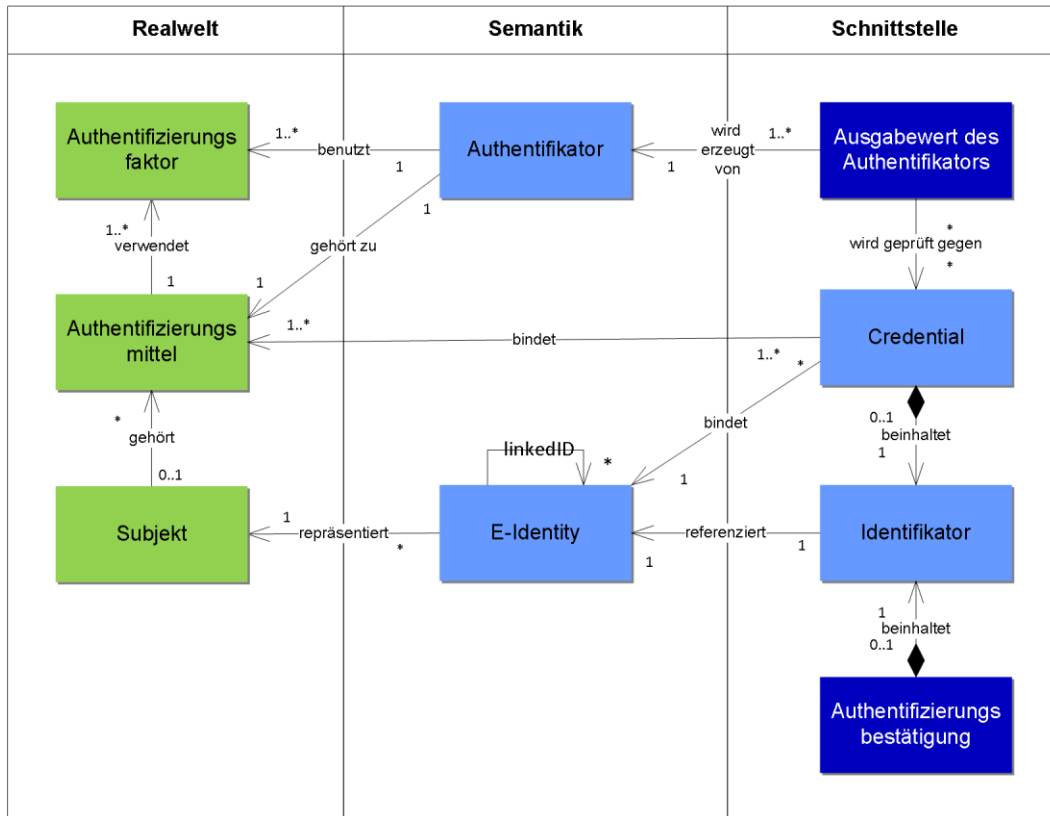


Abbildung 3: Informationsarchitektur

In der Informationsarchitektur (siehe Abbildung 3) wird der Unterschied zwischen Authentifizierungsfaktor (siehe Kapitel 2.4), Authentifizierungsmittel (siehe Kapitel 2.5), Authentifikator (siehe Kapitel 2.1) und Credential (siehe Kapitel 2.9) deutlich. Das Authentifizierungsmittel und die von ihm verwendeten Authentifizierungsfaktoren sind Objekte der Realwelt. Der Authentifikator wird im Authentifizierungsprozess verwendet, um die Authentifizierungsfaktoren in einen Ausgabewert umzuwandeln.

Im Credential wird mittels Identifikator zur Definitionszeit die Verbindung zwischen einem Authentifizierungsmittel und der E-Identity gebildet und abgelegt. Während der Laufzeit wird mit Hilfe des Credentials der Ausgabewert des Authentifikators überprüft. Ist die Prüfung positiv, war die Authentifizierung erfolgreich und die behauptete E-Identity wird bestätigt.

Beispiel

Im Fall einer SuisseID ist das Crypto Device (die Smartcard) inklusive Driver und Middleware das Authentifizierungsmittel. Dieses Authentifizierungsmittel beinhaltet zwei Authentifizierungsfaktoren: Hardware-Token mit privatem Schlüssel (Besitz) und die PIN (Wissen). Durch die Eingabe der PIN wird auf der SuisseID der zweite Authentifizierungsfaktor (der private Schlüssel) freigeschaltet, um mit der Authentifizierungsfunktion (Signatur) einen Ausgabewert zu berechnen, welcher dem authentifizierenden Dienst (IdP) übermittelt wird. Mit dem mitgelieferten Credential (Zertifikat), das den Identifikator (SuisseID Nummer) enthält, wird vom SuisseID IdP (oder auch direkt von einer Web-Applikation) der Ausgabewert auf Echtheit und Gültigkeit hin geprüft. Das Ergebnis dieser Prüfung wird an die Relying Party (oder intern in einer Applikation) als Authentifizierungsbestätigung weitergegeben.

1.7 Abstützung

Die Version 1.0 des Standards eCH-0170 basierte vorwiegend auf dem STORK Quality Authentication Assurance Framework [6]. Die vorliegende Version bezieht andere europäische und internationale Qualitätsmodelle mit ein, die im Folgenden kurz vorgestellt werden.

1.7.1 STORK

STORK war ein EU-Projekt in zwei Phasen, welches Ende 2015 beendet wurde. Das Ziel des Projekts war es, eine europäische Interoperabilitäts-Plattform für elektronische Identitätslösungen zu schaffen, welche es einem EU-Bürger erlaubt, seine nationale elektronische Identität (eID) grenzübergreifend zu verwenden. Im Rahmen des STORK-Projektes wurde ein Qualitätsmodell, das Quality Authentication Assurance Framework [6], zur Bewertung und zum Vergleich von elektronischen Identitäten definiert. Dieses Qualitätsmodell wurde als Grundlage für den eCH-0170 Version 1.0 verwendet.

Dieses Qualitätsmodell wurde später bei der Ausarbeitung der eIDAS-Verordnung 910/2014 [1] mit einbezogen.

1.7.2 eIDAS

eIDAS stützt sich auf die EU Verordnung Nr. 910/2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt [1] und EU Durchführungsverordnung 2015/1502 [7] ab. Ziel ist es, unter den Mitgliedstaaten ein grenzübergreifendes, föderiertes Identitätssystem zu etablieren. Die Anforderungen dieser EU-Verordnung gelten für notifizierte elektronische Identifizierungsmittel, die nach einem notifizierten elektronischen Identifizierungssystem ausgestellt wurden. Dabei wurden Konzepte und Methoden des STORK Projektes übernommen und zum Teil angepasst.

Das Qualitätsmodell für elektronische Identifizierungssysteme von eIDAS wird in Sicherheitsniveaus unterteilt, dabei werden die Stufen „niedrig“, „substanziell“ und „hoch“ unterschieden. eIDAS schränkt die Anwendung dieser Sicherheitsniveaus auf notifizierte elektronische Identifizierungssysteme ein. Es wird zwischen natürlichen und juristischen Personen unterschieden.

Die eIDAS Verordnungen sind für die Schweiz nicht bindend, aber bei einer möglichen Zusammenarbeit voraussichtlich für die Akzeptanz von schweizerischen elektronischen Identitäten fundamental. Das Qualitätsmodell von eIDAS ist daher eine der Grundlagen bei der Erarbeitung dieses Standards.

1.7.3 ISO

Die International Organization for Standardization (ISO) hat den Standard ISO/IEC 29115 [2] ausgearbeitet. Der Standard beschreibt 4 „levels of entity authentication assurance“, oder kurz LoA. Diese wurden bei der Ausarbeitung der eIDAS Verordnung 910/2014 [1] berücksichtigt.

1.7.4 NIST

Das NIST (National Institute of Standards and Technology) hat mit der Special Publication „Digital Authentication Guideline“ NIST SP 800-63-3 [3] in mehreren Versionen einen umfassenden Standard als Richtlinie für die Implementierung digitaler Authentifizierungssysteme in staatlichen Behörden der USA erarbeitet. Für die Definition von Begriffen wird für dieses Dokument soweit sinnvoll auf NIST SP 800-63-3 [3] zurückgegriffen. Insbesondere das im Dokument NISTIR 7298 Revision 2 erstellte Glossar [8] wurde für diesen Standard verwendet.

1.7.5 ZertES/VZertES

ZertES [9] ist das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03) in der Schweiz. VZertES [10] ist die zum ZertES gehörende Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032).

1.8 Vorteile

Mit dem in diesem Standard definierten Qualitätsmodell können föderierte und nicht föderierte IAM-Systeme bewertet und verglichen werden. Der Standard bietet eine Richtlinie, welche Anforderungen erfüllt werden müssen, um eine entsprechende Qualität zu erlangen.

Da sich das Qualitätsmodell auch an eIDAS orientiert, kann dieser mit europäischen Identitätslösungen verglichen werden und bietet damit eine Grundlage für künftige Interoperabilität mit europäischen und internationalen Lösungen.

1.9 Schwerpunkte

Kapitel 2 definiert die im Dokument verwendeten Begriffe.

In Kapitel 3 wird das Qualitätsmodell mit seinen vier Vertrauensstufen und die Komposition in vier Teilmodelle beschrieben. Zudem wird die Verwendung des Qualitätsmodells zur qualitativen Einordnung verschiedener IAM-Dienstleister betrachtet. Es wird ein Überblick aller zugrundeliegenden Qualitätskriterien gegeben und die Vorbedingungen für deren Einsatz aufgelistet.

In den folgenden Kapiteln werden Kriterien und deren Komposition zur Bestimmung der Vertrauensstufen für die 4 Teilmodelle beschrieben:

- Kapitel 4: Qualitätsmodell der Authentifizierung,
- Kapitel 5: Qualitätsmodell der Registrierung,
- Kapitel 6: Qualitätsmodell der Steuerung.
- Kapitel 7: Qualitätsmodell der Förderierung

Kapitel 8 vergleicht die definierten Vertrauensstufen mit den wichtigsten internationalen Qualitätsmodellen.

1.10 Normativer Charakter der Kapitel

Die Kapitel des vorliegenden Standards sind von normativem oder auch deskriptivem Charakter. Tabelle 2 definiert die Einordnung der Kapitel.

Kapitel	Beschreibung
1 Einleitung	Deskriptiv
2 Terminologie	Normativ
3 Qualitätsmodell	Normativ, ausser 4.5
4 Qualitätsmodell der Authentifizierung	Normativ
5 Qualitätsmodell der Registrierung	Normativ
6 Qualitätsmodell der Steuerung	Normativ
7 Qualitätsmodell der Förderierung	Normativ
8 Vergleich mit internationalen Standards	Deskriptiv

Tabelle 2: Übersicht des normativen Charakters der Kapitel

Anhang A, C und H sind ebenfalls normativ. Alle anderen Anhänge dieses Standards sind deskriptiv.

2 Terminologie

Der vorliegende Standard eCH-0170 verwendet grundsätzlich die Begrifflichkeiten aus eCH-0107 [4]. Zusätzlich werden weitere Begriffe, die zum Verständnis dieses Dokumentes notwendig sind, in einer abweichenden Bedeutung gebraucht werden oder ergänzt wurden, im Folgenden alphabetisch aufgeführt.

2.1 Authentifikator

Der **Authentifikator** ist das funktionale Abbild des *Authentifizierungsmittels* der Realwelt. Mit der Funktion eines Authentifikators wird in der Regel aus einem Eingabewert (Challenge) und einem geheimen Wert ein Ausgabewert erzeugt. Je nach Ausprägung muss der geheime Wert durch einen zweiten Faktor (PIN) aktiviert werden.

Synonym: Authentifizierungsfunktion, engl. Authenticator

2.2 Authentifizierung

Authentifizierung ist der Vorgang der Überprüfung einer behaupteten *E-Identity* eines *Subjekts* nach bestimmten Vorgaben. Das angestrebte Sicherheitsniveau der Authentifizierung bestimmt diese Vorgaben.

Synonym: Authentifikation

Spezialfall eIDAS: dynamische Authentifizierung (kein SSO)

2.3 Authentifizierungsbestätigung

Die **Authentifizierungsbestätigung** ist der Nachweis, welcher vom *Identity Provider* nach einer erfolgreichen Authentifizierung des Subjektes ausgestellt wird. Die Authentifizierungsbestätigung ist für einen bestimmten Zeitraum gültig und hat eine der in diesem Dokument beschriebenen Vertrauensstufen.

Beispiele

Bei Security Assertion Markup Language (SAML) [11] ist die Authentifizierungsbestätigung die „Authentication Assertion“ und wird vom (SAML) Identity Provider ausgestellt.

Bei OIDC [12] ist die Authentifizierungsbestätigung das sogenannte „ID Token“ und wird vom „Authorization Server“ ausgestellt.

Bei Kerberos ist die Authentifizierungsbestätigung ein „Ticket Granting Ticket“ (TGT) und wird vom Kerberos Distribution Center (KDC) ausgestellt.

2.4 Authentifizierungsfaktor

Authentifizierungsfaktoren sind Informationen und/oder Prozesse, die zur Authentifizierung eines Subjektes verwendet werden können. Authentifizierungsfaktoren können auf vier verschiedenen Merkmalen oder auch Kombinationen davon beruhen:

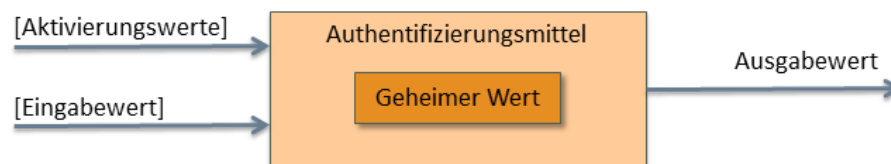
- **besitzabhängiger Authentifizierungsfaktor:** beruht auf Besitz (etwas, das das Subjekt besitzt, z.B. Zertifikat, Hardware-Token mit privatem Schlüssel, elektronischer Pass oder ID-Karte),
- **kenntnisabhängiger Authentifizierungsfaktor:** beruht auf Wissen (etwas, das das Subjekt weiss, z.B. Passwort, PIN),
- **inhärenter Authentifizierungsfaktor:** beruht auf einem *biometrischen Merkmal* (etwas, das das Subjekt ist, wie Iris, Netzhaut, Fingerabdruck),
- **verhaltensbasierter Authentifizierungsfaktor:** beruht auf Verhalten (etwas, das welches das Subjekt typischerweise macht, z.B. dynamisches Unterschriftsmuster).

Synonym: Authentifizierungsmerkmal

2.5 Authentifizierungsmittel

Ein **Authentifizierungsmittel** ist etwas, das ein Subjekt besitzt und das es unter seiner Kontrolle hat (typischerweise ein kryptographischer Schlüssel, ein Geheimnis oder ein biometrisches Merkmal). Ein Authentifizierungsmittel muss nicht unbedingt in Hardwareform vorliegen, sondern kann auch ein Soft-Token oder eine Software-Komponente sein. Ein Authentifizierungsmittel kann einen (*single-factor authenticator*) oder auch mehrere unabhängige Authentifizierungsfaktoren (*multi-factor authenticator*) benutzen (für Beispiele siehe Anhang H).

Der vom Authentifizierungsmittel generierte Ausgabewert (engl. *Authenticator output* oder *authenticator response*) wird durch eine mathematische Funktion (*Authentifikator* oder Authentifizierungsfunktion) aus einem geheimen Wert (z.B. privater Schlüssel), einem oder mehreren optionalen Aktivierungswerten (z.B. PIN oder biometrischer Informationen), und einem oder mehreren optionalen Eingabewerten (z.B. Zufallswerten oder Challenges) generiert. Im Trivialfall kann das Authentifizierungsmittel der geheime Wert selbst sein (z.B. im Fall eines Passworts). Siehe Tabelle 3 für weitere Beispiele.



$$\text{Ausgabewert} = \text{Authentifizierungsfunktion}(\text{geheimer Wert}, [\text{Aktivierungswerte}], [\text{Eingabewerte}])$$

Abbildung 4: Schematische Funktionsweise eines Authentifizierungsmittels

	Passwort	Strichliste	SMS	OTP	Mobile-ID	SuisseID
Typ	SFA	SFA	SFA	(HW-)MFA	HW-MFA	HW-MFA
Eingabewert	-	Index	gesendeter Code	Seed	gesendeter Code	Nonce
Geheimer Wert	Passwort	(alpha-) numerischen Wert	-	Device Key	Private Key	Private Key
Aktivierungswert	-	-	-	-	PIN	PIN

	Passwort	Strichliste	SMS	OTP	Mobile-ID	SuisseID
Authentifikator	-	Liste der (alpha-) numerischen Werte	Handy	Device	SIM-Karte	Crypto-Device
Authentifizierungsfunktion	Keine oder Hash-Fkt.	Selektion	Lesen und Schreiben des gesendeten Codes	HMAC	Signatur	Signatur
Ausgabewert	Passwort, Hash des Passworts	(alpha-) numerischen Wert	gesendeter Code	Code	Sign (gesendeter Code)	Sign (Nonce)
Credential²	Passwort, Hash des Passworts	Liste der (alpha-) numerischen Werte	Mobile-Nr.	Device-Nr./ Seed	SIM-Karte mit Mobile-Nr./ Public Key	Certificate

Tabelle 3: Beispiele für Authentifizierungsmittel und zugehörigem Credential

Synonyme:

- Authenticator (siehe NIST 800-63-3 [3]), früher bei NIST 800-63-2 [13] als **Token** bezeichnet.
- Bei STORK als *identity token* bzw. *authentication token* bezeichnet

² Zum Credential gehört immer auch der Identifier, z.B. der Name des Benutzers.

2.6 Beweismittel

Ein **Beweismittel** für die Identitätsüberprüfung ist ein Dokument oder Objekt, aus einer verlässlichen Quelle, das Angaben zum Antragsteller enthält.

Ein Beweismittel muss den Namen des Antragsstellers enthalten. Es kann zusätzlich einen eindeutigen Identifikator, körperliche und biometrische Merkmal aber auch beliebige andere Angaben des Antragstellers enthalten. Es sollte Sicherheitsmerkmale enthalten, die ein Reproduzieren erschweren.

Beispiele:

- Beglaubigte Urkunde,
- Kreditkarten,
- Fahrausweis,
- Identitätsdokumente.

2.7 Biometrisches Merkmal

Ein **biometrisches Merkmal** ist ein *körperliches Merkmal* eines Menschen, das es erlaubt, diesen hinreichend von anderen zu unterscheiden, welches also zu dessen Identifizierung verwendet werden kann. Ein biometrisches Merkmal sollte sich im Laufe der Zeit wenig ändern. Kombinationen mehrere Merkmale sind dabei möglich, z.B. Erfassung des Gesichtes kombiniert mit Stimmerkennung. Ein entscheidender Nachteil bei der Verwendung von biometrischen Merkmalen bei der Authentifizierung ist, dass sie im Fall einer Kompromittierung nicht für ungültig erklärt bzw. neu erzeugt werden können.

Zu den wichtigsten biometrischen Merkmalen gehören:

- Fingerprint,
- (dynamische) Unterschrift,
- Gesichtsgeometrie,
- Gesichtsbild (Foto),
- Irismuster,
- Retina (Netzhaut),
- Handgeometrie,
- Fingergeometrie,
- Ohrform,
- Stimme (Klangfarbe),
- DNA,
- Geruch,
- Tastenanschlag.

Zur Identifizierung von natürlichen Personen werden zurzeit meist nur

- Fingerprint,
- Iris,
- Retina,
- Gesichtsgeometrie,
- Gesichtsbild (Foto)

verwendet.

Biometrische Merkmale können bezüglich Funktion, Sicherheit, Fälschbarkeit und Anwendungsfreundlichkeit ebenfalls klassifiziert werden. Das NIST hat mit ihrer Online-Dokumentation „Strength of Function for Authenticators – Biometrics“ [14], kurz SOFA-B, dazu einen ersten Beitrag geleistet.

2.8 Certificate Authority/Certification authority (CA)

Eine **Certificate Authority** ist ein spezieller Credential Service Provider (CSP), der digitale Zertifikate (Public Key Zertifikate, e.g. X.509) als Authentifizierungsmittel ausgibt, erneuert und revoziert.

Synonyme: Certification Service Provider, Trust Service Provider (TSP)

Synonym deutsch: Zertifizierungsstelle für digitale Zertifikate, Vertrauensdiensteanbieter

2.9 Client Plattform

Die **Client Plattform** ist das System oder Gerät, von welchem das Subjekt einen Authentisierungsprozess anstösst. Dies kann beispielsweise ein Browser auf einem PC oder eine Applikation auf einem mobilen Gerät sein.

2.10 Credential

Ein **Credential** stellt eine Menge von Daten (keine Hardware oder andere physische Container) dar, mit der eine elektronische Identität (*E-Identity*) an ein Authentifizierungsmittel gebunden wird, welches vom Subjekt besitzt und kontrolliert wird.

Das Credential wird zusammen mit dem Ausgabewert des Authentifizierungsmittel zum Nachweis der behaupteten E-Identity verwendet. Je nach verwendeten Authentifizierungsfaktoren kann dies z.B. der Hash eines Passwortes, ein Abbild eines biometrischen Merkmals oder ein Zertifikat sein (siehe auch Tabelle 3), das zur Definitionszeit von einem CSP an eine E-Identity gebunden wurde.

Ein Credential muss immer auf Authentizität und Vertrauenswürdigkeit überprüft werden, bevor es verwendet wird.

(siehe auch ISO 29115 [2], Annex B und NIST SP 800-63B [15], Kap 3).

Synonym: Identitätsnachweis

2.11 Credential Service Provider (CSP)

Ein **Credential Service Provider** ist eine Entität, die als vertrauenswürdiger Herausgeber von digitalen Zertifikaten und anderer Sicherheits-Tokens (Authentifizierungsmitteln) agiert.

Der CSP kann eine eigene Registration Authorities (RA) enthalten und Dienste zur Authentifizierung (Identity Provider, siehe Kapitel 2.19) umfassen. Ein CSP kann als öffentliche Instanz auftreten oder als Dienst in eine abgeschlossene Domäne integriert sein.

Synonym: Wird im NIST 800-63-3 [3] auch als Identity Provider (IdP) bezeichnet.

2.12 E-Identity

Eine **E-Identity** ist die Repräsentation eines *Subjekts*. Eine *E-Identity* hat einen *Identifikator* (eindeutiger Name), meist zusammen mit einer Menge von zusätzlichen *Attributen*, welche innerhalb eines Namensraumes eindeutig einem *Subjekt* zugewiesen werden können. Ein *Subjekt* kann mehrere *E-Identities* haben.

Eine **notifizierte E-Identity** ist eine E-Identity, die alle in eIDAS 910/2014 [1] Artikel 7 aufgeführten Voraussetzungen erfüllt muss.

2.13 Elektronisches Identifizierungsmittel

Begriff aus eIDAS 910/2014 [1]: „*Elektronisches Identifizierungsmittel*“ ist eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird.

Ein **elektronisches Identifizierungsmittel** enthält Authentifizierungsfaktoren, Attribute für Personen und hat eine Gültigkeit. Bei einer (dynamischen) Authentifizierung wird der gesamte Prozess *Subjekt authentifizieren* vom elektronischen Identifizierungsmittel abgewickelt. Es umschliesst daher sowohl Authentifizierungsmittel, Credential und IdP. Das Ergebnis einer Authentifizierung mit einem elektronischen Identifizierungsmittel ist eine Authentifizierungsbestätigung, mit der die Identität des Subjekts und die erfolgreiche Authentifizierung bestätigt werden.

Beispiele für elektronische Identifizierungsmittel sind der neue deutsche Personalausweis (nPA) inkl. Middleware (AusweisApp) oder die gesamte SuisselD Infrastruktur bestehend aus SuisselD Token, Middleware (Gerätetreiber) und SuisselD IdP.

2.14 Elektronisches Identifizierungssystem

Begriff aus eIDAS 910/2014 [1] : „*Elektronisches Identifizierungssystem*“ ist ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden.

Ein **notifiziertes** elektronisches Identifizierungssystem muss alle in eIDAS 910/2014 [1] Artikel 7 aufgeführten Voraussetzungen erfüllen.

2.15 Definitionszeit

In der **Definitionszeit** wird das IAM-System eingerichtet und konfiguriert. Zusätzlich werden die elektronischen Identitäten etabliert. Die Definitionszeit umfasst damit die Prozesse zur Bereitstellung aller notwendigen Informationen für alle beteiligten Komponenten sowie der Komponenten selbst.

2.16 Föderierung / Federation

Eine Identitäts-**Föderierung** ist eine Zusammenarbeit verschiedener Entitäten eines IAM-Systems über Organisations- und Systemgrenzen hinweg, ohne Duplikation oder Replikation der dazu notwendigen Benutzerdaten (*E-Identities*).

Eine Föderierung von Identitäten erlaubt es, Informationen über eine Authentifizierung eines Subjektes und optional Identitätsinformationen zu diesem Subjekt über ein Netzwerk zu übermitteln.

Wie in Abbildung 5 dargestellt, besteht ein föderiertes Identitätssystem aus den drei Entitäten Subjekt, Relying Party (RP) und einem Identity Provider (IdP). Je nach Ausprägung des verwendeten Protokolls ist die Abfolge der Informationen anders. Das Subjekt kommuniziert dabei aber immer mit dem IdP, wie auch mit der RP. Das Subjekt authentifiziert sich gegenüber dem IdP in einem primären Authentifizierungsverfahren mit einem bestimmten Authentifizierungsmittel (Authenticator). Dieses Ereignis wird dann in Form einer Authentifizierungsbestätigung an die vertrauende Partei über das Netzwerk weitergegeben. Der IdP kann dieser Authentifizierungsbestätigung noch weitere (Personen-)Attribute zum authentisierten Subjekt beifügen.

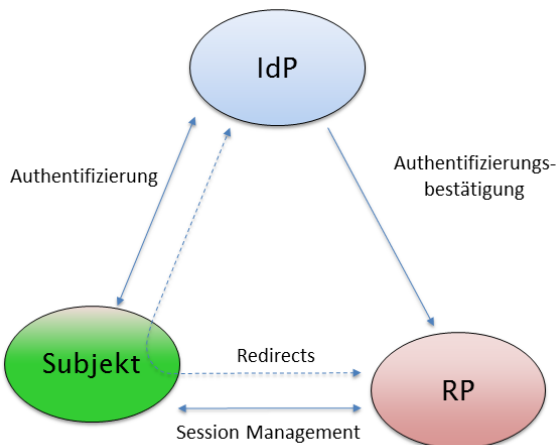


Abbildung 5: Modell einer Identity Federation

Synonyme: föderiertes Identitätssystem, föderiertes IAM-System

2.17 Identifizierung

Identifizierung ist ein Vorgang zur Definitionszeit, bei welchem die Identität des Subjekts meist mit Hilfe von Beweismitteln überprüft wird. Die Identifizierung wird meist durch eine Registration Authority (RA) durchgeführt.

Synonym: Identitätsfeststellung

2.18 Identitätsdokument

In der Schweiz gelten die folgenden Dokumente als **Identitätsdokumente**:

- Reisepass,
- Schweizer Identitätskarte,
- eine für die Einreise in die Schweiz anerkannte Identitätskarte.

2.19 Identity Provider (IdP)

Entität, die zur Laufzeit die E-Identity des Subjekts überprüft. Dazu wird der Besitz bzw. die Kontrolle des Subjektes über die Authentifizierungsmittel und die Verbindung des Subjektes zu den verwendeten Authentifizierungsmittel mit Hilfe der Credentials überprüft.

Ein IdP stellt einen Authentication Service und meist auch einen Attribute Assertion Service zur Verfügung.

Synonym: Authorization Provider (bei OIDC [12]), Verifier (im NIST 800-63-3 [3])

2.20 Juristische Person

Juristische Personen sind Organisationen nach Art. 52 ff ZGB sowie gemäss den einschlägigen Bestimmungen des Gesellschaftsrechtes des OR definiert.

Juristische Personen können **nur** durch natürliche Personen handeln und sind daher immer an eine natürliche Person gebunden (siehe Abbildung 6).

2.21 Körperliches Merkmal

Ein **körperliches Merkmal** ist ein Merkmal eines Menschen, wie Körpergrösse und Augenfarbe. Spezielle körperliche Merkmale sind die *biometrischen Merkmale* (siehe Kap. 2.7).

2.22 Laufzeit

Zur **Laufzeit** finden die elektronischen Prozesse statt, mit denen ein Subjekt – im Erfolgsfall - Zugang und Zugriff auf die Ressourcen einer Relying Party erhält.

Synonym: Ausführungszeit

2.23 Registrierungsstelle/Registration Authority (RA)

Eine **Registrierungsstelle** ist eine Entität, die genügend Informationen zu einem Subjekt erfasst und überprüft, um dessen Identität überprüfen zu können.

Die RA kann ein integraler Bestandteil eines CSP sein oder als eigener Dienst im Auftrag des CSP handeln.

2.24 Subjekt

Ein **Subjekt** ist eine natürliche Person, eine *juristische Person*, ein Service oder Objekt, das auf eine *Ressource* zugreift oder zugreifen möchte. Ein **Subjekt** wird durch *E-Identities* repräsentiert.

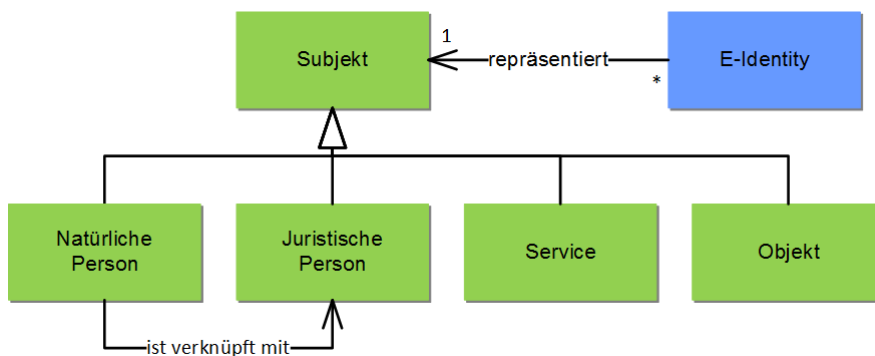


Abbildung 6: Definition *Subjekt*

Ein **Abonnent** (engl. *Subscriber*, siehe NIST 800-63-3A [16]) ist ein *Subjekt*, welches nach erfolgreich abgeschlossenem Registrationsprozess (Prozess *Subjekt registrieren*) ein Authentifizierungsmittel von einem CSP erhalten hat. Damit wird das Subjekt zu einem autorisierten Teilnehmer in der Identity Federation Community.

Ein **Antragsteller** (engl. *Applicant*, siehe NIST 800-63-3A [16]), ist ein *Subjekt*, das in die Identity Federation Community aufgenommen werden möchte und dazu den Prozess *Subjekt registrieren* durchläuft. Wurde dieser erfolgreich abgeschlossen, wird aus dem *Antragsteller* ein *Abonnent*.

Ein **Überbringer** (engl. *Bearer*) ist ein *Subjekt*, das eine vom IdP ausgestellte Authentifizierungsbestätigung an die RP übergibt.

2.25 UID-Einheit

UID-Einheiten sind nach Art. 3.c des Bundesgesetzes über die Unternehmens-Identifikationsnummer [17] festgelegt,

Bei **UID-Einheiten** handelt es sich um alle Unternehmen und Institutionen, die eine UID erhalten. Im UID-System ist der Unternehmensbegriff weit gefasst. Unter UID-Einheit versteht man somit nicht nur alle in der Schweiz tätigen Unternehmen im eigentlichen Sinn, sondern alle «Kundinnen und Kunden der öffentlichen Verwaltung», die Charakteristiken eines Unternehmens aufweisen oder die zu rechtlichen, administrativen oder statistischen Zwecken identifiziert werden.³

Synonym: Unternehmen

2.26 Verlässliche Quelle

Eine **verlässliche Quelle** ist eine beliebige Informationsquelle, welche bezogen auf eine konkrete Situation als vertrauenswürdig betrachtet wird.

eIDAS 2015/1502 [7]: „*Verlässliche Quelle*“ ist eine beliebige Informationsquelle, die auf verlässliche Weise präzise Daten, Informationen und/oder Beweismittel bereitstellt, die zum Identitätsnachweis verwendet werden können.

Verlässliche Quellen können viele verschiedene Formen haben, z.B. Register, Urkunden, Stellen usw.

2.27 Verwaltung

Verwaltung bezeichnet ein Gemeinwesen (Ämter und Behörden, allenfalls mit solchen Aufgaben beauftragte Private), welches gesetzlich übertragene Staatsaufgaben besorgt.

Der Begriff Verwaltung ist ein organisatorischer Begriff, der ausserhalb der juristischen Definition von natürlicher und juristischer Person steht.

³ Siehe auch: <https://www.bfs.admin.ch/bfs/de/home/register/unternehmensregister/unternehmens-identifikationsnummer/uid-einheiten-unternehmen.html>

3 Qualitätsmodell

Das Qualitätsmodell zur Authentifizierung von Subjekten wird in Stufen bzw. Niveaus aufgeteilt. In diesem Standard wird der Begriff **Vertrauensstufen (VS)** verwendet.

Das Qualitätsmodell zur Authentifizierung von Subjekten besteht aus vier Teilen (siehe Tabelle 4). Jedem dieser Teilmodelle ist ein Prozess zugeordnet. Die Prozesse sind in Abbildung 2 und im Anhang G beschrieben.

Qualitätsmodell	Prozess	Vertrauensstufen (VS)
Qualitätsmodell der Authentifizierung	Subjekt authentifizieren	Vertrauensstufen der Authentifizierung (VSA)
Qualitätsmodell der Registrierung	Subjekt registrieren	Vertrauensstufen der Registrierung (VSR)
Qualitätsmodell der Steuerung	Registrierung und Authentifizierung steuern	Vertrauensstufen der Steuerung (VSS)
Qualitätsmodell der Föderierung	Identität föderieren	Vertrauensstufen der Föderierung (VSF)

Tabelle 4: Teile des Qualitätsmodells und die dazugehörigen Vertrauensstufen

Die Teilmodelle werden je nach Art des IAM-Systems komponiert (siehe Kapitel 3.2) oder können auch einzeln für die Einstufung der IAM-Dienstleister verwendet werden (siehe Kapitel 3.3). So kann z.B. das Qualitätsmodell der Registrierung zur qualitativen Bewertung einer RA verwendet werden.

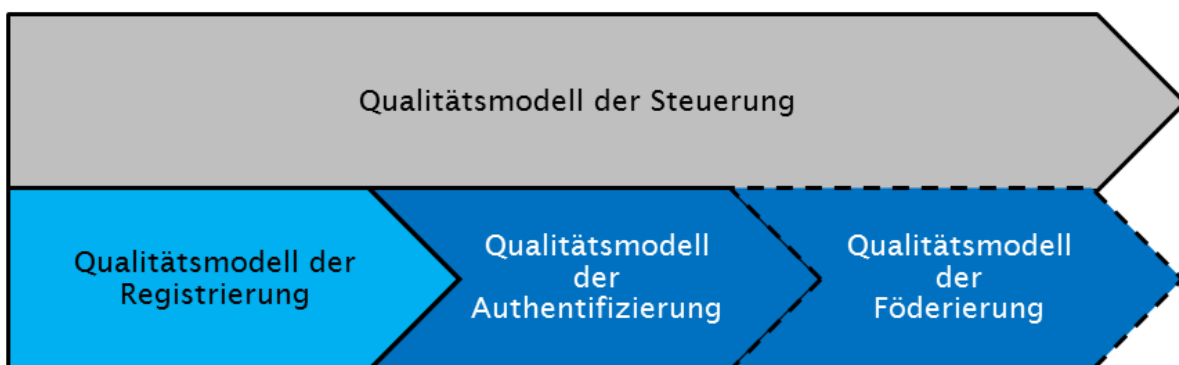


Abbildung 7: Komposition des Qualitätsmodells

Jedem Teilmodell bzw. jedem Prozess sind Qualitätskriterien zugeordnet. Die Qualitätskriterien enthalten Ausprägungen, die erfüllt werden müssen. Dadurch erhalten sie eine Bewertungsstufe. Diese Bewertungsstufen werden auf der Prozessebene zusammengefasst und ergeben die Prozessbewertungsstufe. Auf der Gesamtbewertungsebene werden die Prozessbewertungsstufen zusammengefasst und ergeben die Gesamt-Qualität der Authentifizierung von Subjekten.

3.1 Vertrauensstufen

Im Qualitätsmodell zur Authentifizierung von natürlichen und juristischen Subjekten sind vier Vertrauensstufen definiert. Vertrauensstufe 1 ist die niedrigste und bedeutet, dass sie seitens Relying Party am wenigsten Vertrauen genießt. Vertrauensstufe 4 ist die höchste Stufe und genießt seitens Relying Party am meisten Vertrauen. In Tabelle 5 sind alle 4 Vertrauensstufen mit ihren Merkmalen beschrieben. Die Qualität wird durch die Farben Rot (wenig Vertrauen) bis Grün (Hohes Vertrauen) unterstrichen.

Vertrauensstufen	Bezeichnung	Beschreibung
1	Kein oder minimales Vertrauen	Die Vertrauensstufe 1 ist die niedrigste Stufe.
		VSA: Die Authentifizierung erfordert nur einen Authentifizierungsfaktor, mit dem mit geringer Gewissheit sichergestellt werden kann, dass einem Subjekt beim wiederholten Zugriff auf eine RP dieselbe E-Identität zugeordnet werden kann.
		VSR: Alle vorhandenen Informationen zur E-Identität des Subjektes sind selbst deklariert und wurden nicht überprüft. [Nur für juristische Personen: Die Verknüpfung zwischen natürlichen Person und juristischen Person ist selbst deklariert.]
		VSS: Die beteiligten IAM-Dienstleister verwenden Prozesse, unterliegen aber keinerlei Aufsicht und schliessen, soweit zulässig, die Haftung aus.
		VSF: Die Datenherkunft und -integrität einer Authentifizierungsbestätigung muss einwandfrei feststellbar sein.

Vertrauensstufen	Bezeichnung	Beschreibung
2	Geringes Vertrauen	VSA: Bei der Vertrauensstufe 2 muss sich das Subjekt mit mindestens 2 verschiedenen Single-Factor Authenticators oder mit einem Multi-Factor Authenticator anmelden, damit wird die Gewissheit erhöht, dass einem Subjekt beim wiederholten Zugriff auf eine RP dieselbe E-Identität zugeordnet werden kann.
		VSR: Bei der Registrierung wurden die Angaben des Antragstellers mit Hilfe von Beweismitteln überprüft. Das Subjekt muss dazu mindestens online anwesend sein. [Nur für juristische Personen: Die Verknüpfung zwischen natürlicher und juristischer Person wurde hergestellt.] Das Authentifizierungsmittel wurde sicher übergeben.
		VSS: Die beteiligten IAM-Dienstleister verwenden interne Regelungen und Standards um ihre Prozessqualität sicherzustellen. Die Prozesse sind definiert und kommuniziert. Es besteht eine beschränkte Haftung.
		VSF: Eine Authentifizierungsbestätigung muss zusätzlich bezüglich Vertraulichkeit genügend geschützt werden.
3	Beträchtliches Vertrauen	VSA: Bei der Vertrauensstufe 3 muss sich das Subjekt mit einem hardware-basierten Multi-Factor Authenticator anmelden.
		VSR: Bei der Registrierung wurden die Angaben des Antragstellers mit Hilfe von Beweismitteln stark validiert und die Kopie eines Beweismittels mit körperlichen Merkmalen erstellt. Das Subjekt muss dazu mindestens online anwesend sein. [Nur für juristische Personen: Die Verknüpfung zwischen natürlicher und juristischer Person wurde überprüft.] Das Authentifizierungsmittel wurde persönlich ausgeliefert oder übergeben.
		VSS: Die beteiligten IAM-Dienstleister verwenden Standards, um ihre Prozessqualität sicherzustellen. Die Prozesse werden überwacht und gemessen. Die Einhaltung der Standards wird durch eine externe Stelle überprüft. Die beteiligten Dienstleister übernehmen Haftung nach Gesetz.
		VSF: Eine Authentifizierungsbestätigung muss zusätzlich bezüglich Vertraulichkeit genügend geschützt werden.

Vertrauensstufen	Bezeichnung	Beschreibung
4	Hohes Vertrauen	Vertrauensstufe 4 ist die höchste Stufe. Diese bietet ein sehr hohes Mass an Vertrauen an die beanspruchte E-Identität des Subjekts.
		VSA: Bei der Authentifizierung muss sich das Subjekt mit einem hardware-basierten Multi-Factor Authenticator, welcher zertifiziert sein muss, anmelden.
		VSR: Bei der Registrierung muss das Subjekt physisch oder Virtual-in-Person anwesend sein. Diese Präsenz wird dokumentiert. Die Beweismittel müssen staatlich anerkannt sein und biometrische Merkmale enthalten, die – soweit möglich – überprüft werden müssen. [Nur für juristische Personen: Die Verknüpfung zwischen natürlicher und juristischer Person wurde mittels Handelsregisterauszug überprüft und eine Zustimmungserklärung liegt vor.]
		Das Authentifizierungsmittel muss eigenhändig übergeben werden. Bei der Verlängerung des Authentifizierungsmittels muss wiederum ein staatlich anerkanntes Beweismittel vorgelegt und validiert werden.
		VSS: Die beteiligten IAM-Dienstanbieter verwenden Standards um ihre Prozessqualität sicherzustellen. Die Prozesse sind optimiert und automatisiert. Die Einhaltung wird durch eine amtlich akkreditierte Stelle überprüft. Die beteiligten Dienstanbieter übernehmen Haftung nach Gesetz. Die der Durchsetzung von Schadensersatzansprüchen wird durch Konventionalstrafen erleichtert.
		VSF: Der Überbringer einer Authentifizierungsbestätigung muss sich zusätzlich als Inhaber authentisieren können.

Tabelle 5: Vertrauensstufen des Qualitätsmodells zur Authentifizierung von Subjekten

3.2 Komposition der Vertrauensstufen

Die Vertrauensstufen des Qualitätsmodells zur Authentifizierung von Subjekten setzen sich aus 4 Teilmodellen zusammen. Diese Zusammensetzung ist in Tabelle 6 beschrieben.

Um eine Vertrauensstufe zu erfüllen, müssen alle Teilmodelle den aufgeführten Stufen entsprechen. Die geringste Stufe bei den Teilmodellen VSA, VSR und VSS bestimmt somit die Stufe des Gesamtmodells.

Für das Teilmodell mit den Vertrauensstufen der Registrierung (VSR) kommt je nach Art des Subjektes das Modell für natürliche (VSRN) bzw. das Modell für juristische Personen (VSRJ) zum Einsatz.

Das Teilmodell mit den Vertrauensstufen der Föderierung (VSF) kommt nur für föderierte IAM-Systeme zum Einsatz und wird bei nicht föderierten Systemen bei der Komposition weggelassen.

Vertrauensstufe	Bezeichnung	VSA	VSR VSRN/VSRJ	VSS	VSF
1	Kein oder minimales Vertrauen	1	1	1	1
2	Geringes Vertrauen	2	2	2	2
3	Beträchtliches Vertrauen	3	3	3	2
4	Hohes Vertrauen	4	4	4	3

Tabelle 6: Komposition der Vertrauensstufen aus den Stufen der Teilmodelle

3.3 Verwendung zur Einstufung von IAM-Diensteanbietern

Die in diesem Standard vorgeschlagenen Teilqualitätsmodelle lassen sich auch zur qualitativen Einstufung einzelner IAM-Diensteanbieter verwenden.

3.3.1 Einstufung einer RA

Bei der Einstufung einer RA kommt das Qualitätsmodell der Registrierung (VSR) und das der Steuerung (VSS) zum Einsatz. Dabei werden beim Qualitätsmodell der Steuerung die Kriterien nur auf den betrachteten Diensteanbieter angewendet.

3.3.2 Einstufung eines IdP

Bei der Einstufung eines IdP kommt das Qualitätsmodell der Authentifizierung (VSA) und das der Steuerung (VSS) zum Einsatz. Dabei werden beim Qualitätsmodell der Steuerung die Kriterien nur auf den betrachteten Diensteanbieter angewendet. Soll der IdP weiter zur Föderierung der Identitäten eingesetzt werden, muss zusätzlich noch das Qualitätsmodell der Föderierung (VSF) in die Bewertung einbezogen werden.

3.3.3 Einstufung eines CSP

Bei der Einstufung eines CSP, inklusive IdP, kommt das Qualitätsmodell der Authentifizierung (VSA), das der Registrierung (VSR) und das der Steuerung (VSS) zum Einsatz. Das Qualitätsmodell der Föderierung ist optional. Die Stufen entsprechen den Vertrauensstufen des Gesamtmodells (siehe Tabelle 5 und Tabelle 6).

Bei der Einstufung der Qualität der Steuerung werden die Kriterien nur auf den betrachteten Dienstleister angewendet. Hat der CSP die Registrierungsprozesse an eine RA ausgelagert, muss auch diese in die Bewertung (VSR und VSS) einbezogen werden.

3.4 Qualitätskriterien

Die drei Ebenen der Qualitätsdefinition der Authentifizierung eines Subjektes sind in Abbildung 8 ersichtlich. Die Bezeichnung in der Grafik bezieht sich immer auf die Qualität des entsprechenden Elements.

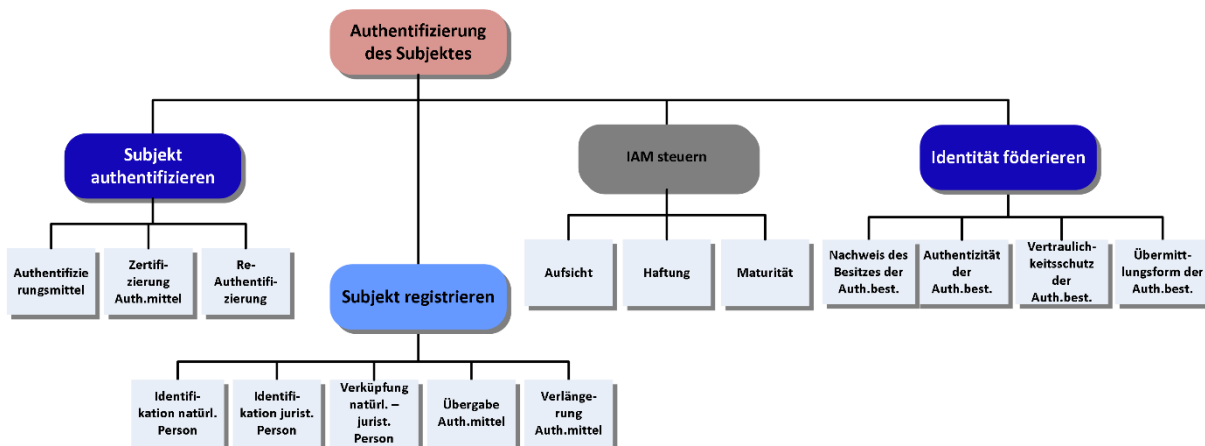


Abbildung 8: Übersicht aller Kriterien

Die Qualitätskriterien und ihre Ausprägungen werden in den Kapiteln 4 bis 6 zusammen mit den Qualitätsmodellen, in denen sie verwendet werden, beschrieben.

3.5 Vorbedingungen

Die folgenden Vorbedingungen (Tabelle 7) werden für die hier behandelten Qualitätskriterien von Identity Federation Systemen als gegeben betrachtet. Eine Verletzung dieser Vorbedingungen kann negativen Einfluss auf das gesamte IAM-System haben und damit auch die Qualität der Authentifizierung absenken.

Nr.	Vorbedingungen	Beschreibung
A1	Verifizierung der Authentifizierungsstufe	Die RP muss die Authentifizierungsstufe des Subjekts in der ihr vorgelegten Authentifizierungsbestätigung überprüfen. (NIST 800-63-3 [3] Kap. 4.4.2)
A2	Autorisierung der RP	Wenn notwendig, muss ein IdP im Vorfeld der Ausstellung einer Authentifizierungsbestätigung prüfen, ob der Empfänger (RP) berechtigt ist, eine solche anzufordern. (NIST 800-63-3 [3] Kap. 4.1)

Nr.	Vorbedingungen	Beschreibung
A3	Einverständnis des Subjekts (User consent)	Bei persönlichen Identitätsinformationen muss ein IdP vor der Ausstellung einer Authentifizierungsbestätigung an eine bestimmte RP dem Subjekt die zu übermittelnde Identitätsinformationen zur Freigabe vorlegen. ⁴ (NIST 800-63-3 [3] Kap. 4.1)
A4	Zeitbasis	Der IdP muss eine verlässliche Zeitbasis für die Ausstellung der Authentifizierungsbestätigung verwenden (z.B. öffentlicher Zeitdienst oder staatlich anerkannte Zeitstempel). Es ist zudem wichtig, dass RP und IdP über eine möglichst synchrone Zeit verfügen. (NIST 800-63-3 [3] Kap. 4.4.1)
A5	Sicherer Kommunikationskanal	Die Kommunikation zwischen IdP, Client Plattform und RP muss abgesichert sein (z.B. mit TLS). ⁵ (NIST 800-63-3 [3] Kap. 7.1)
A6	Vertrauenswürdige Kommunikationsendpunkte	Die Kommunikationsendpunkte müssen vertrauenswürdig (z.B. mittels Zertifikaten und einem Trust Anchor) sein und dies kann zur Laufzeit überprüft werden. (NIST 800-63-3 [3] Kap. 4.4.1)
A7	Sichere Client Plattform	Es kann davon ausgegangen werden, dass die Umgebung der Client Applikation gegen Schadsoftware möglichst gut geschützt ist, einen möglichst aktuellen System- und Sicherheitsstatus aufweist und nicht im Administrator-Modus betrieben wird. ^{6 7}

⁴ Ein User Consent ist z.B. nicht notwendig, wenn es sich um ein Enterprise-IAM handelt (siehe auch eCH-0168 [25], Kap. 3.11).

⁵ Siehe auch eIDAS 2015/1502 [7] Kap. 2.4.6. Technische Kontrollen: „Elektronische Kommunikationswege, die zur Übermittlung personenbezogener oder sensibler Informationen verwendet werden, müssen gegen Abhören, Manipulation und Replay geschützt sein.“

Entspricht der Special Publication (SP) 800-52 [26], welche vom NIST veröffentlicht wurde.

⁶ Die Anforderung A7 kann nur vollständig erfüllt werden, wenn die Client-Plattform unter der Kontrolle des Gesamt-IAM-Systems ist, z.B. in einem Verwaltungs- oder Enterprise-Umfeld. Aber besonders in einem offenen Umfeld, z.B. mit Bürgern als Endbenutzer, muss bei der Konzeption des Gesamt-Systems berücksichtigt werden, welchen Schaden z.B. ein infiziertes Endgerät auslösen kann und wie man durch die Wahl von geeigneten Authentifizierungsmittel zusammen mit entsprechender Aufklärung/Schulung das Schadenspotential senken kann.

⁷ Software-Komponenten zu Hardware Authentifizierungsmittel sollten auf dem aktuellsten Stand gehalten werden. Der Endbenutzer sollte darauf hingewiesen werden, wenn Aktualisierungen verfügbar sind.

Nr.	Vorbedingungen	Beschreibung
A8	Sichere Server Umgebung	Die im föderierten Identitätssystem beteiligten Server-Umgebungen können gegen bekannte Verwundbarkeiten möglichst zeitnah geschützt werden. (NIST 800-63-3 [3] Kap. 2.2)
A9	Kryptoparameter	In allen beteiligten Systemen kommen heute empfohlene kryptographische Algorithmen und Schlüssellängen zur Anwendung. Für den Einsatz adäquater Parameter wird auf diese Quellen ⁸ verwiesen. (NIST 800-63B [15] Kap. A2)
A10	Adäquate Gültigkeit der Authentifizierungsbestätigung	Die Authentifizierungsbestätigungen dürfen nur eine sinnvoll begrenzte Zeit gültig sein, um die Wiederverwendung (assertion reuse) zu reduzieren. (NIST 800-63C [18] Kap. 8.1)
A11	Revozierung	Das Subjekt und der CSP müssen jederzeit die Möglichkeit haben eine E-Identity zu revozieren, bzw. die E-Identity für ungültig zu erklären. (NIST 800-63B [15] Kap. 6.4)
A12	Berücksichtigung von Gefahren und Sicherheitsaspekte	Mögliche Gefahren und Gegenmassnahmen gegen Angriffe auf das Authentifizierungsmittel müssen berücksichtigt werden. (NIST 800-63B [15] Kap. 8.1, NIST 800-63B [15] Kap. 8.2)

Tabelle 7: Vorbedingungen für Identity Federation Systeme

Zusätzlich gibt es für die am häufigsten eingesetzten Technologie, meist zusätzliche technische Mindestanforderungen, so siehe z.B. für SAML: https://www.owasp.org/index.php/SAML_Security_Cheat_Sheet.

⁸ BlueKrypt: www.keylength.org

ETSI: http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf

Bundesamt für Sicherheit in der Informatik: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile

4 Qualitätsmodell der Authentifizierung

Das Qualitätsmodell der Authentifizierung wird durch Bewertung der Kriterien des Prozesses *Subjekt authentifizieren* bestimmt (siehe Anhang G.1.1 für eine Beschreibung des Prozesses).

4.1 Vertrauensstufen der Authentifizierung (VSA)

Die Vertrauensstufen der Authentifizierung (VSA) werden aus den folgenden 3 Kriterien abgeleitet (siehe Abbildung 9):

- Authentifizierungsmittel (Kapitel 4.2.1),
- Zertifizierung des Authentifizierungsmittel (Kapitel 4.2.2),
- Re-Authentifizierung (Kapitel 4.2.3).

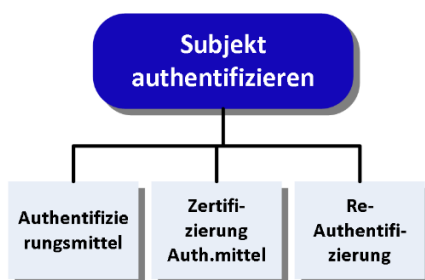


Abbildung 9: Kriterien für das Qualitätsmodell der Authentifizierung

Die Vertrauensstufe der Authentifizierung (VSA) wird hierbei durch die tiefste Ausprägung der Kriterien bestimmt. Die Qualität wird durch die Farben Rot (wenig Vertrauen) bis Grün (hohes Vertrauen) unterstrichen.

Beim Kriterium Authentifizierungsmittel wird zwischen der regulären Authentifizierung und einer einmaligen Authentifizierung nach einer erfolgreichen Online-Identifizierung der entsprechenden Stufe unterschieden. Die einmalige Authentifizierung nach Online-Identifizierung wird vor allem beim Erstkontakt des Antragstellers mit der Ressource verwendet.

Vertrauensstufe der Authentifizierung (VSA)	Authentifizierungsmittel		Zertifizierung Auth.mittel	Re-Authentifizierung
	Reguläre Authentifizierung	Einmalige Authentifizierung nach Online-Identifikation		
1	SFA	IDN1	keine	ReAuth1
2	MFA	IDN2	keine	ReAuth2
3	HW-MFA	IDN3	keine	ReAuth3
4	HW-MFA	IDN4	Zertifizierung	ReAuth4

Tabelle 8: Vertrauensstufen der Authentifizierung (VSA)

4.2 Kriterien der Authentifizierung

4.2.1 Authentifizierungsmittel

Fragen:	<p>Kann das Authentifizierungsmittel nur unter der Kontrolle oder im Besitz des Subjektes, dem es gehört, verwendet werden?</p> <p>Bietet das Authentifizierungsmittel Schutz vor Duplizierung und Fälschung durch Dritte?</p> <p>Ist das Authentifizierungsmittel so gestaltet, dass es vom Subjekt zuverlässig vor einer Benutzung durch andere geschützt werden kann?</p>
---------	--

Bemerkungen:

- Die Ausprägungen SFA, MFA und HW-MFA entsprechen der Liste der *permitted authenticator types* für die 3 Authenticator Assurance Level (AAL) aus NIST SP 800-63B [15].
- Die Ausprägungen SFA, MFA und HW-MFA entsprechen den 3 Stufen der „Merkmale und Gestaltung elektronischer Identifizierungsmittel“ aus eIDAS 2015/1502 [7].
- Im Anhang H sind die Anforderungen an die verschiedenen erwähnten Authentifizierungsmittel (SFA, MFA und HW-MFA) mit Beispielen erwähnt.

Ausprägungen		Beschreibung
Reguläre Authentifizierung	Single-Factor Authentication (SFA)	<p>Das Authentifizierungsmittel verfügt über mindestens einen Authentifizierungsfaktor (Single-Factor Authenticator). Es können die folgenden Arten unterschieden werden:</p> <ul style="list-style-type: none"> • Memorized Secret (z.B. Passwort, PIN), • Look-Up Secret (z.B. Strichliste), • Out of Band Authenticator (z.B. Bestätigung über SMS), • Single Factor OTP Device (z.B. Google Authenticator).
	Multi-Factor Authentication (MFA)	<p>a) Das Authentifizierungsmittel ist ein Multi-Factor Authenticator, wie z.B.</p> <ul style="list-style-type: none"> • Multi-Factor Software Cryptographic Authenticator, • Multi-Factor OTP Software Authenticator <p>oder</p> <p>b) Die Authentifizierung basiert auf der Kombination von 2 verschiedenen Single-Factor Authenticator als Authentifizierungsmittel, die auf unterschiedlichen Authentifizierungsfaktoren beruhen müssen.</p>
	Hardware based Multi-Factor Authentication (HW-MFA)	<p>Um grösstmöglichen Schutz vor Duplizierung und Fälschung zu bieten, sind nur die folgenden 3 Hardware-Devices erlaubt:</p> <ul style="list-style-type: none"> • Multi-Factor OTP Device, • Multi-Factor Cryptographic Device, • Single-Factor Cryptographic Device mit Memorized Secret.

Ausprägungen	Beschreibung
Einmalige Authentifizierung nach Online-Identifikation	Direkt im Anschluss an eine erfolgreiche Online -Identifikation der natürlichen Person (siehe Kapitel 5.1.1) erhält das Subjekt einmaligen Zugriff auf die gewünschte Ressource. Dabei beeinflusst die Ausprägung der Identifikation die Vertrauensstufe der Authentifizierung (VSA).

Tabelle 9: Ausprägungen Kriterium *Authentifizierungsmittel*

Beispiel Einmalige Online-Identifikation:

Nach einer audiovisuellen Video-Identifikation und der Überprüfung von entsprechenden Beweismitteln wird der Antragsteller direkt (inkl. Personendaten) an das Zielsystem (RP) weitergereicht. Beispiele sind Prozesse, bei dem der Antragsteller zuvor noch keine Berührung mit dem Zielsystem hatte (z.B. Online Konto-Eröffnung oder Kreditbeantragung mit anschliessendem Signieren von Dokumenten).

4.2.2 Zertifizierung des Authentifizierungsmittel

Fragen:	Ist das Authentifizierungsmittel zertifiziert? Bietet das Authentifizierungsmittel bestmöglichen Schutz vor Angriffen?
---------	---

Bemerkungen:

- Entspricht der *FIPS 140 verification* für die 3 Authenticator Assurance Level (AAL) aus NIST SP 800-63B [15]
- Die Zertifizierung umfasst ebenfalls die eingebettete Software, Software-Komponenten (Treiber, Middleware), sowie das Betriebssystem gemäss FIPS 140-2 [19] Kapitel 4.6.1.

Ausprägungen	Beschreibung
Keine Zertifizierung	Das Authentifizierungsmittel ist nicht zertifiziert.
Zertifizierung	Das Authentifizierungsmittel ist mindestens nach FIPS 140-2 Level 3 bzw. Common Criteria EAL 4+ zertifiziert.

Tabelle 10: Ausprägungen Kriterium *Zertifizierung des Authentifizierungsmittel*

Beispiele:

- Ein hardware-basiertes Authentifizierungsmittel mit mehreren Faktoren (HW-MFA) **ohne** Zertifizierung ist zum Beispiel die Mobile ID.
- Ein hardware-basiertes Authentifizierungsmittel mit mehreren Faktoren (HW-MFA) **mit** Zertifizierung ist zum Beispiel die SuisseID.

4.2.3 Re-Authentifizierung

Frage:	Nach welcher Zeitdauer muss eine RP - unabhängig von ihrem eigenen Session Management - ein Subjekt erneut vom IdP authentifizieren lassen? Wie kann bei einer laufenden Sitzung sichergestellt werden, dass das Subjekt immer noch dasselbe ist, wie bei der initialen Authentifizierung durch den IdP?
--------	---

Bemerkungen:

- Entspricht dem *reauthentication requirement* für die 3 Authenticator Assurance Level (AAL) aus NIST SP 800-63B [15]
- Im Gegensatz zu den von der RP bestimmten Ereignissen, in welchen sich ein Subjekt erneut authentisieren muss, in etwa:
 - nach Inaktivität (z.B. 5 min)
 - nach einer maximal erreichten Zeit pro Session (z.B. 30 min)
 - durch anwählen einer bestimmten Aktion (z.B. Speicherung von Daten)
 stellt diese Re-Authentifizierungszeit die maximal erlaubte Zeit dar, in welcher eine RP ein aktives Subjekt immer erneut vom IdP authentifizieren lassen sollte.

Bei der Ausprägung *ReAuth2* und *ReAuth3* müssen jeweils alle Authentifizierungsfaktoren verwendet werden, die bei der initialen Authentifizierung verwendet wurden. Der Unterschied besteht darin, dass bei *ReAuth3*, die Authentifizierungsfaktoren in genau derselben Art und Weise wie bei der initialen Authentifizierung verwendet werden müssen.

Ausprägungen	Beschreibung
ReAuth1	Das Subjekt muss nach einer adäquaten Zeitspanne (z.B. 30 Tage) erneut vom IdP authentifiziert werden.
ReAuth2	Das Subjekt muss nach maximal 18 Stunden erneut authentifiziert vom IdP werden, unabhängig von der Nutzungsaktivität. Ein Authentifizierungsfaktor ist ausreichend bei der Re-Authentifizierung.
ReAuth3	Das Subjekt muss nach maximal 12 Stunden erneut vom IdP authentifiziert werden. Die Re-Authentifizierung muss alle Authentifizierungsfaktoren berücksichtigen, die bei der initialen Authentifizierung verwendet wurden.
ReAuth4	Das Subjekt muss nach maximal 30 Minuten erneut vom IdP authentifiziert werden. Die Re-Authentifizierung muss alle Authentifizierungsfaktoren in der genau gleichen Art und Weise anwenden, wie bei der initialen Authentifizierung.

Tabelle 11: Ausprägungen Kriterium *Re-Authentifizierung*

Beispiel:

- Stufe ReAuth1
 - Bei OAuth [20] empfiehlt sich, dass Refresh Tokens nicht unbeschränkt verwendet und nach definierten Kriterien erneuert werden (z.B. nach 50maliger Verwendung zur Erstellung von Access Token). Danach muss auch hier eine Re-Authentifizierung am OAuth-Server erzwungen werden oder es werden Massnahmen definiert, welche den Missbrauch von Refresh Tokens entgegenwirkt (z.B. untypisch viele Anfragen für Access Tokens).
- Stufe ReAuth3
 - Bei *ReAuth3* ist das Caching eines wissensbasierten Faktors möglich, so wie dies bei der aktuellen Implementierung der SuisseID der Fall ist.
- Stufe ReAuth4
 - Bei der SuisseID würde der Benutzer mit allen Authentifizierungsfaktoren in der gleichen Reihenfolge authentifiziert werden (Erkennung des HW-Device, sowie Eingabe des PINs). Der wissensbasierte Faktor (PIN) darf nicht gecached werden.

5 Qualitätsmodell der Registrierung

Das Qualitätsmodell der Registrierung wird durch Bewertung der Kriterien des Prozesses *Subjekt registrieren* bestimmt (siehe Anhang G.2 für eine Beschreibung des Prozesses).

Das Qualitätsmodell der Föderierung enthält 5 Kriterien (siehe Abbildung 10).

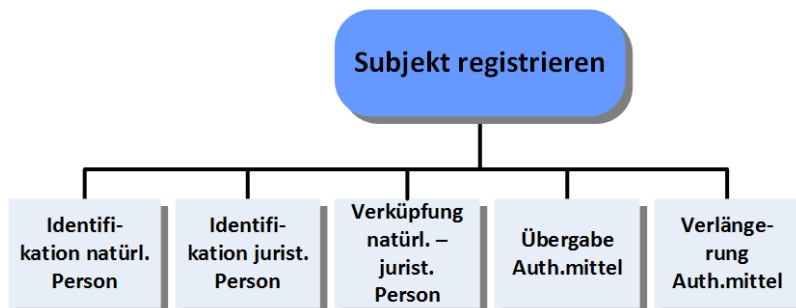


Abbildung 10: Kriterien für das Qualitätsmodell der Registrierung

5.1 Vertrauensstufen der Registrierung (VSR)

Die Vertrauensstufen der Registrierung (VSR) für den Prozess *Subjekt registrieren* werden je nach Art des Subjektes unterschiedlich bestimmt.

5.1.1 Für natürliche Personen

Die Vertrauensstufen der Registrierung (VSRN) für den Prozess *Subjekt registrieren* werden für natürliche Personen aus den folgenden 3 Kriterien abgeleitet:

- Identifikation natürlicher Personen (Kapitel 5.2.2),
- Übergabe Authentifizierungsmittel (Kapitel 5.2.5),
- Verlängerung/Ersetzung Authentifizierungsmittel (Kapitel 5.2.6).

Die Vertrauensstufe der Registrierung (VSRN) wird hierbei durch die tiefste Ausprägung der Kriterien bestimmt.

Vertrauensstufen der Registrierung (VSRN) für natürl. Personen	Identifikation natürl. Personen	Übergabe Auth.mittel ⁹	Verlängerung Auth.mittel
1	IDN1	1	CN1
2	IDN2	2	CN2
3	IDN3	3	CN3
4	IDN4	4a oder 4b	CN4

Tabelle 12: Bestimmung der VSR für natürliche Personen

5.1.2 Für juristische Personen

Die Vertrauensstufen der Registrierung (VSRJ) für den Prozess *Subjekt registrieren* für juristische Personen besteht aus den Vertrauensstufen der Registrierung für natürliche Personen und folgenden beiden zusätzlichen Kriterien:

- Identifikation juristischer Personen (Kapitel 5.2.3),
- Verknüpfung natürliche und juristische Person (Kapitel 5.2.4).

Die Vertrauensstufe der Registrierung (VSRJ) wird hierbei durch die tiefste Ausprägung der Vertrauensstufe für natürliche Personen (VSRN) und der der Kriterien bestimmt.

Im Bereich von öffentlichen Verwaltungen bestimmen sich die Vertretungsbefugnisse gemäss einschlägigen gesetzlichen Grundlagen auf Bundes-, Kantons- und Gemeindeebene, sowie internen Vorgaben der entsprechenden Behörden.

Beispiel auf Bundesebene:

Die Unterschriftsberechtigung wird auf höchste Kaderstufe gemäss Regierungs- und Verwaltungsorganisationsgesetz (RVOG) [21] vom Departementsvorsteher bestimmt. Die Direktoren der Gruppen und Ämter regeln für Ihren Bereich die Unterschriftsberechtigungen und delegieren allenfalls entsprechende Befugnisse weiter.

Vertrauensstufen der Registrierung (VSRJ) für juristische Personen	VSRN	Identifikation jurist. Personen	Verknüpfung
1	1	IDJ1	L1
2	2	IDJ2	L2
3	3	IDJ3	L3
4	4	IDJ4	L4

⁹ Das Kriterium kann entfallen, wenn der CSP ein Authentifizierungsmittel an die E-Identity des Subjektes bindet, das bereits im Besitz oder unter Kontrolle des Subjektes ist.

Tabelle 13: Bestimmung der VSR für juristische Personen

5.2 Kriterien der Registrierung

5.2.1 Faktoren zur Identifikation

Sowohl das Kriterium *Identifikation natürlicher Personen* als auch das Kriterium *Identifikation juristischer Personen* setzen sich aus mehreren Faktoren zusammen.

5.2.1.1 Faktor Anwesenheit

Der Faktor *Anwesenheit (Physical Presence, PP)* hält fest, ob der Antragsteller während der Registrierung physisch anwesend sein muss oder nicht. Der Faktor kann nur auf natürliche Personen angewendet werden.

Fragen:	In welcher Form ist der Antragsteller bei der Identifikation anwesend? Kann festgestellt werden, dass die natürliche Person existiert und persönlich anwesend ist?
---------	---

Bemerkungen:

- Bei der Registrierung muss der Antragsteller persönlich anwesend sein und kann nicht vertreten werden.
- Ist der Antragsteller nicht handlungsfähig nach Artikel 13 ZGB, d.h. nichtvolljährig oder urteilsunfähig, muss der gesetzliche Vertreter seine Zustimmung geben.
- Die Ausprägungen für den Faktor *Anwesenheit* entsprechen den Werten (*remote, in person* und *virtual in-person*) für *Presence Requirements* aus NIST 800-63-3A [16] – Kapitel 4.4 – 4.8.
- Für die Ausprägung *Virtual In-Person* kommt in der Schweiz die VZertES Verordnung Art 7.2 [10] zur Anwendung: *Die anerkannten Anbieterinnen können geregelte Zertifikate im Rahmen eines Verfahrens zur Personenidentifikation mittels audiovisueller Kommunikation in Echtzeit ausstellen, wenn das Verfahren den Anforderungen des Geldwäschereigesetzes vom 10. Oktober 1997 entspricht.*

Stufe	Ausprägungen	Beschreibung
PP.a	Keine Anwesenheit	Es ist keine Anwesenheit erforderlich.
PP.b	Online	Der Antragsteller ist online über ein Netzwerk (Internet, Telefon) anwesend.
PP.c	Virtual In-Person	Zusätzlich zu Stufe PP.b: Das verwendete System verfügt über genügend technologische und verfahrenstechnische Massnahmen, die es erlauben mittels audiovisueller Kommunikation in Echtzeit die Online-Präsenz, einer physischen Anwesenheit nahezu gleich zu setzen.

Stufe	Ausprägungen	Beschreibung
PP.d	In-Person (physisch)	Es ist die persönliche physische Anwesenheit des Antragstellers während der Registrierung erforderlich.

Tabelle 14: Ausprägungen Faktor Anwesenheit

Beispiel:

- Stufe PP.a
 - Registrierung per E-Mail oder Ticket-System
- Stufe PP.b
 - Online-Registrierung per Web-Anwendung oder Smartphone-App
 - Registrierung per Telefon durch fachspezifische oder personenbezogene Auskünfte (z.B. überprüfbare Angaben zur Person)
- Stufe PP.c
 - Video-Identifizierung gemäss den aufsichtsrechtlichen Rahmenbedingungen der FINMA
- Stufe PP.d
 - Der Antragsteller erscheint persönlich bei der RA.

5.2.1.2 Faktor Beweismittel

Der Faktor *Beweismittel (Identity Evidence, IE)* stuft die bei der Registrierung vorgelegten Beweismittel ihrer Qualität nach ein. Die RA ist für die Prüfung der Beweismittel auf Gültigkeit und Echtheit sowie deren Quelle zuständig.

Werden mehrere Beweismittel verwendet, muss das Kriterium für jedes Beweismittel einzeln bestimmt werden.

Fragen:	Ist das Beweismittel echt und gültig? Stammt das Beweismittel aus einer verlässlichen und anerkannten Quelle?
---------	--

Bemerkungen:

- Die Ausprägungen für den Faktor *Beweismittel* entsprechen den Werten (*unacceptable, weak/adequate, strong, superior*) für *Identity Evidence* aus NIST 800-63-3A [16] – Kapitel 5.3.1.1 (Identity Evidence).
- Die Stufen IE.b, IE.c und IE.d entsprechen den Anforderungen für die Sicherheitsniveaus *niedrig, substantiell* und *hoch* aus eIDAS 2015/1502 [7], Abschnitt 2.1.2.
- Für die höchste Stufe kommen in der Schweiz das ZertES (943.03), Art. 9 [9], sowie die VZertES (943.032), Art. 5 [10] zur Anwendung: Der Antragsteller muss in der Schweiz bei der RA einen Pass, eine CH-Identitätskarte oder eine für die Schweiz anerkannte Identitätskarte persönlich vorweisen.
- Im Bereich von öffentlichen Verwaltungen gelten die Bestimmungen gemäss einschlägigen gesetzlichen Grundlagen auf Bundes-, Kantons- und Gemeindeebene.

Stufe	Ausprägungen	Beschreibung
IE.a	Kein Beweismittel	Es wird kein Beweismittel vorgelegt. oder Die Beweismittel sind nicht aussagekräftig, da die ausstellende Stelle offensichtlich keine Identitätsprüfung vorgenommen hat.
IE.b	Beweismittel vorhanden	<i>Es kann davon ausgegangen werden, dass das Beweismittel echt ist oder laut einer verlässlichen Quelle existiert und dass das Beweismittel dem Anschein nach gültig ist.</i> ¹⁰ Das Beweismittel enthält mindestens einen Identifikator, der eindeutig das Subjekt identifiziert, dem es gehört. Der Ausgabe-Prozess für das Beweismittel ist so gestaltet, dass man davon ausgehen kann, dass es dem richtigen Subjekt zugestellt wurde. Das Beweismittel enthält Sicherheitsmerkmale, die nur mit Spezialwissen reproduziert werden können.
IE.c	Beweismittel anerkannt und überprüft	Zusätzlich zur Stufe IE.b muss eine der folgenden Alternativen erfüllt sein. 1) Das Beweismittel ist im gegebenen Kontext anerkannt und gültig. und Das Beweismittel ist geprüft worden, um seine Echtheit festzustellen, oder einer verlässlichen Quelle ist bekannt, dass es existiert und sich auf ein real existierendes Subjekt bezieht. 2) Ein gültiges Identitätsdokument wurde vorgelegt (im Original oder als Kopie) 3) Als Beweismittel gilt auch die Vorlage eines elektronischen Nachweises einer gültigen, qualitativ gleichwertigen oder höher notifizierten bzw. zertifizierten E-Identity.
IE.d	Beweismittel für körperliche Merkmale	Zusätzlich zur Stufe IE.c muss eine der folgenden Alternativen erfüllt sein. 1) Das Beweismittel muss staatlich anerkannt sein und im Original vorgelegt werden. Das Beweismittel muss den Vergleich eines oder mehrerer körperlicher Merkmale der Person (Foto oder biometrische Merkmale) unterstützen und diese müssen – soweit zugreifbar – überprüft werden. 2) Als Beweismittel gilt auch die Vorlage eines elektronischen Nachweises einer gültigen, qualitativ gleichwertig notifizierten bzw. zertifizierten E-Identity.

Tabelle 15: Ausprägungen Faktor Beweismittel

¹⁰ eIDAS 2015/1502 [7], Abschnitt 2.1.2. Sicherheitsniveau niedrig.

Beispiele:

- Stufe IE.a
 - Dokument unbekannter Quelle, ohne Stempel einer öffentlichen Einrichtung
- Stufe IE.b
 - Kreditkarte
 - Geburtsurkunde
 - SBB SwissPass
 - Versichertenkarte einer Krankenkasse
 - Studierenden- oder Mitarbeitendenausweis
- Stufe IE.c
 - SBB SwissPass und erfolgter Prüfung durch das Kontrollpersonal
 - Studierendenausweis mit Foto und Gültigkeit, ausgestellt von einer öffentlichen Einrichtung im Bildungssektor
 - Kopie eines staatlich anerkannten Identitätsdokuments
 - Fahrausweis
- Stufe IE.d
 - Staatlich anerkannte Identitätsdokumente

5.2.1.3 Faktor Validierung der Angaben

Der Faktor *Validierung der Angaben (Identity Validation, IV)* beschreibt mit vier Ausprägungen, wie die Korrektheit der bei der Antragstellung angegebenen Daten mit Hilfe der vorgelegten Beweismittel von der RA überprüft werden.

Frage:	<p>Kann die Verbindung zwischen dem Antragsteller (Subjekt), der die Beweismittel präsentiert, und der behaupteten Identität des Subjekts hergestellt werden?</p> <p>Stimmen die vom Antragsteller gemachten Angaben mit den Daten der vorgelegten Beweismittel überein?</p>
--------	--

Bemerkungen:

- Die Stufen für den Faktor *Validierung der Angaben* entsprechen den Werten (*unacceptable, weak/adequate, strong, superior*) aus NIST 800-63-3A [16] – Kapitel 5.4.1 (Identity Verification)
- Die Stufen IV.b, IV.c und IV.d entsprechen den Anforderungen für die Sicherheitsniveaus *niedrig, substantiell* und *hoch* aus eIDAS 2015/1502 [7], Abschnitt 2.1.2.
- Im Anhang I sind die zusätzlichen Anforderungen an die verschiedenen Arten der Validierung entsprechend der Anwesenheitsform des Antragstellers erwähnt.
- Je nach Anwendungsfall und Kontext können weitere nicht subjektidentifizierbare Attribute angefragt bzw. überprüft werden.

Stufe	Ausprägungen	Beschreibung
IV.a	Keine Validierung	Eine Überprüfung der Angaben ist nicht möglich oder nicht erwünscht.
IV.b	Adäquate Validierung	Der Antragsteller kann beweisen, dass er Zugriff auf die Beweismittel hat. Die Angaben des Antragstellers werden mit Hilfe der Daten der vorgelegten Beweismittel überprüft.
IV.c	Starke Validierung	Zusätzlich zu Stufe IV.b: Es wurden Vorkehrungen getroffen, um das Risiko zu mindern, dass die Identität des Antragstellers nicht mit der beanspruchten E-Identity übereinstimmt.
IV.d	Höchste Validierung	Zusätzlich zu Stufe IV.c: Ein Beweismittel muss körperliche Merkmale enthalten. und Die Verbindung zwischen dem Antragsteller und den Beweismitteln wurde durch einen Abgleich der Person und den zur Verfügung stehenden oder zugreifbaren biometrischen Angaben des stärksten Beweismittels hergestellt. und Die Verbindung des Antragstellers und der behaupteten E-Identität wurde mit Hilfe einer Postadresse überprüft.

Tabelle 16: Ausprägungen Faktor Validierung der Angaben

Beispiele:

- Stufe IV.c
 - Die Überprüfung von körperlichen Merkmalen oder anderen redundanten Angaben (fachliche Selbstauskunft) kann z.B. durch entsprechende Fragen am Telefon oder mit anderen elektronischen Hilfsmitteln (Fragebögen) durchgeführt werden.

5.2.1.4 Faktor Nichtabstreitbarkeit

Der Faktor *Nichtabstreitbarkeit* (*Nonrepudiation, NP*) beschreibt, ob und wie zum Zeitpunkt der Antragstellung biometrische Daten erhoben werden, um die Anwesenheit eines Subjektes zu einem späteren Zeitpunkt beweisen zu können.

Fragen:	Kann zu einem späteren Zeitpunkt (nach der Validierung der Identität) bewiesen werden, dass ein Antragsteller bei der Registrierung anwesend war? Kann verhindert werden, dass das Subjekt die Anwesenheit bei der Registrierung (und damit die Ausstellung eines Authentifizierungsmittels) abstreitet?
---------	---

Bemerkungen:

- Siehe auch NIST 800-63-3A [16] – Kapitel 4.6.7
- Für die höchste Stufe kommt in der Schweiz die VZertES Verordnung 943.032 Art 11.1 [10] zur Anwendung: Die Belege zur Identifizierung des Antragstellers müssen elf Jahre lang aufbewahrt werden.

Stufe	Ausprägungen	Beschreibung
NP.a	Keine Erhebung	Es werden keine biometrischen Daten während der Antragstellung erhoben.
NP.b	Kopie eines Identitätsdokuments	Es wird zum Zeitpunkt der Überprüfung der Identität eine Kopie eines echten und gültigen Beweismittels, das körperliche Merkmale enthält, erstellt.
NP.c	Erhebung biometrischer Daten	Es werden zum Zeitpunkt der Überprüfung der Identität biometrische Daten (z.B. Fingerabdrücke oder Gesichtsbilder) erhoben und gespeichert, um die Präsenz des Antragsstellers zu dokumentieren.

Tabelle 17: Ausprägungen Faktor Nichtabstreitbarkeit

Beispiele:

- Stufe NP.b
 - Kopie eines Identitätsdokumentes

5.2.1.5 Faktor Vollmacht

Frage:	Ist die natürliche Person berechtigt, im Namen der Organisation zu handeln?
--------	---

Bemerkungen:

- keine

Stufe	Ausprägungen	Beschreibung
PA.a	Keine Vollmacht	Es wird keine Vollmacht oder Zustimmungserklärung vorgelegt.
PA.b	Vollmacht	Nach VZertES [10], Artikel 5.2 muss eine Zustimmungserklärung vorgelegt werden: <ol style="list-style-type: none"> 1. Personen die im Handelsregister eingetragen sind haben gemäss dessen Eintrag Unterschriftsberechtigung (Einzel-, Kollektivunterschrift usw.). 2. Personen die nicht im Handelsregister eingetragen sind brauchen eine Zustimmungserklärung von den Unterschriftsberechtigte(n) Person(en) gemäss Handelsregistereintrag oder gemäss kaufmännische Stellvertretung gestützt auf OR Art 32ff. 3. Bei öffentlichen Verwaltungen: Gemäss einschlägigen gesetzlichen Grundlagen auf Bundes-, Kantons- und Gemeindeebene.

Tabelle 18: Ausprägungen Faktor *Vollmacht*

5.2.2 Identifikation natürlicher Personen

Das Kriterium *Identifikation natürlicher Personen* beschreibt, wie eine natürliche Person identifiziert wird. Es fasst, nach dem in Tabelle 19 dargestellten Schema die folgenden Faktoren zusammen (siehe auch Abbildung 11):

- Faktor Anwesenheit: Kapitel 5.2.1.1,
- Faktor Beweismittel: Kapitel 5.2.1.2,
- Faktor Validierung der Angaben: Kapitel 5.2.1.3,
- Faktor Nichtabstreitbarkeit: Kapitel 5.2.1.4.

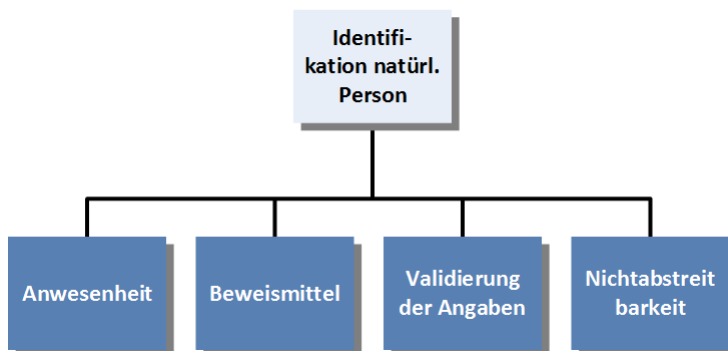


Abbildung 11: Faktoren zum Kriterium Identifikation natürlicher Personen

Fragen:	<p>Wie wurde die Identität einer natürlichen Person, welcher eine elektronische Identität ausgestellt wurde, überprüft?</p> <p>Nach welchen Gesichtspunkten wurden optionale Attribute verifiziert?</p>
---------	---

Bemerkungen:

- Die Stufen IDN2, IDN3 und IDN4 entsprechen den Sicherheitsniveaus *niedrig*, *substantiell* und *hoch* aus eIDAS 2015/1502 [7], Abschnitt 2.1.2 (Identitätsnachweis und -überprüfung (natürliche Person)).

Ausprägungen	Beschreibung	Anwesenheit	Beweismittel	Validierung der Angaben	Nichtabstreitbarkeit
IDN1	Alle Informationen zur Identität sind selbstdeklariert und nicht überprüft.	PP.a	IE.a	IV.a	NP.a
IDN2	Die Informationen zur Identität werden mit Hilfe anscheinend echter und gültiger Beweismittel überprüft. Der Antragsteller kann physisch oder online anwesend sein.	PP.b, PP.c oder PP.d	IE.b	IV.b	NP.a
IDN3	Zusätzlich zur Stufe IDN2: Die Beweismittel wurden stark validiert. Zum Zeitpunkt der Überprüfung wurde die Kopie eines Beweismittels mit körperlichen Merkmalen erstellt.	PP.b, PP.c oder PP.d	1x IE.c oder 2 x IE.b	IV.c	NP.b
IDN4	Zusätzlich zur Stufe IDN3: Der Antragsteller muss physisch oder „virtual in-person“ anwesend sein. Die biometrischen Angaben aus dem Beweismittel werden überprüft. Zum Zeitpunkt der Überprüfung wurde die Präsenz des Antragstellers dokumentiert.	PP.c oder PP.d	IE.d	IV.d	NP.c

Tabelle 19: Ausprägungen Kriterium *Identifikation natürlicher Personen*

5.2.3 Identifikation juristischer Personen

Frage:	Existiert die juristische Person? Wie wurde die Existenz der juristischen Person überprüft? Nach welchen Gesichtspunkten wurden Attribute verifiziert?
--------	---

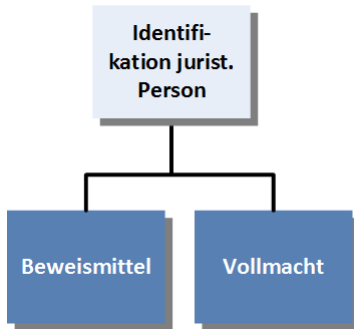


Abbildung 12: Faktoren zum Kriterium Identifikation juristischer Personen

Das Kriterium *Identifikation juristischer Personen* beschreibt, wie eine juristische Person (Organisation) identifiziert wird. Es beruht auf den Faktoren *Beweismittel* und *Vollmacht* (siehe auch Tabelle 18):

- Faktor Beweismittel: Kapitel 5.2.1.2
- Faktor Vollmacht: Kapitel 5.2.1.5

Bemerkungen:

- Die Stufe IDJ2 entspricht dem Sicherheitsniveau *niedrig* und IDJ3 entspricht dem Sicherheitsniveau *hoch* aus eIDAS 2015/1502 [7], Abschnitt 2.1.3 Identitätsnachweis und -überprüfung (juristische Person)).

Ausprägungen	Beschreibung	Beweismittel	Vollmacht
IDJ1 (selbstdeklariert)	Alle Informationen zur Identität sind selbstdeklariert und nicht überprüft.	IE.a	PA.a
IDJ2 (überprüft)	Die Informationen zur Identität entstammen einem gültigen Beweismittel und wurden validiert.	IE.b	PA.a
IDJ3 (anerkannt)	Zusätzlich zur Stufe IDJ2 muss das Folgende erfüllt sein: Die Informationen zur Identität entstammen gültigen und anerkannten Beweismitteln. Die Beweismittel wurden überprüft. Das Beweismittel muss einem eindeutigen Identifikator, den Namen und die Rechtsform der juristischen Person enthalten.	IE.c	PA.a

Ausprägungen	Beschreibung	Beweismittel	Vollmacht
IDJ4 (bevollmächtigt)	Zusätzlich zur Stufe IDJ3 muss das Folgende erfüllt sein: Das Beweismittel muss ein aktueller, beglaubigter Handelsregisterauszug sein. ¹¹ Eine Zustimmungserklärung muss vorgelegt werden.	IE.c	PA.b

Tabelle 20: Ausprägungen Kriterium *Identifikation juristischer Personen*

5.2.4 Verknüpfung natürliche und juristische Person

Frage:	Darf die natürliche Person für die juristische Person handeln? Wie genau wurde mit einer verlässlichen Quelle die Verknüpfung überprüft?
--------	---

Bemerkungen:

- Für Stufe L4 muss in der Schweiz ein Eintrag im Handelsregister existieren, siehe VZertES [10], Artikel 5.2
- eIDAS 2015/1502 [7], Abschnitt 2.1.4 regelt den Lebenszyklus einer Verknüpfung entsprechend den auf nationaler Ebene anerkannten Verfahren.
- Für die Verknüpfung braucht es weitere Attribute um die Funktion bzw. (Unter-)Organisation der natürlichen Person innerhalb der juristischen Person zu bestimmen.

Stufe	Ausprägungen	Beschreibung
L1	Keine Überprüfung	Die Verbindung zwischen natürlicher Person und juristischer Person wird nicht überprüft.
L2	Einfache Verknüpfung	Die Verknüpfung ist gemäss auf nationaler Ebene anerkannten Verfahren hergestellt worden.
L3	Verknüpfung mit Eintragung	Die Verknüpfung ist gemäss auf nationaler Ebene anerkannten Verfahren hergestellt worden, was zu einer Eintragung der Verknüpfung in einer verlässlichen Quelle geführt hat.
L4	Verknüpfung mit eindeutiger Kennung	Die Verknüpfung ist anhand einer im nationalen Umfeld verwendeten eindeutigen Kennung, die die juristische Person repräsentiert, sowie anhand von Informationen einer verlässlichen Quelle, die die natürliche Person eindeutig repräsentieren, überprüft worden.

¹¹ Nach VZertES [10], Artikel 5.2

Tabelle 21: Ausprägungen Kriterium *Verknüpfung natürliche und juristische Person*

5.2.5 Übergabe Authentifizierungsmittel

Fragen:	<p>Wie wird sichergestellt, dass nur das richtige Subjekt das Authentifizierungsmittel/-faktor erhält?</p> <p>Wie wird verhindert, dass Unberechtigte das Authentifizierungsmittel in ihren Besitz bringen können.</p> <p>Bei Auslieferung per Post:</p> <p>Ist die vom Antragsteller angegebene Post-Adresse gültig?</p> <p>Kann die Postadresse der behaupteten E-Identität zugeordnet werden?</p>
---------	--

Das Kriterium *Übergabe Authentifizierungsmittel* beschreibt, den Übergabeprozess für ein Authentifizierungsmittel bzw. für einen Authentifizierungsfaktor.

Das Kriterium kann entfallen, wenn der CSP ein Authentifizierungsmittel an die E-Identity des Subjektes bindet, das bereits im Besitz oder unter Kontrolle des Subjektes ist (z.B. ein Passwort).

Werden für eine Authentifizierung Authentifizierungsmittel mit mehreren Authentifizierungsfaktoren oder mehrere Authentifizierungsmittel verwendet, muss das Kriterium für jedes Authentifizierungsmittel bzw. für jeden -faktor einzeln bestimmt werden. Die Gesamt-Qualitätsstufe ergibt sich dann aus der tiefsten Stufe der einzelnen Bewertungen.

Das Kriterium hat eine Abhängigkeit zur *Adress-Überprüfung* (in Tabelle 22 dargestellt), wenn die Auslieferung per Post erfolgt. Dieser Faktor (siehe auch NIST 800-63-3A [16] – *Address Confirmation, AC*) beschreibt, ob und wie die Angaben zu einer Post-Adresse überprüft wurden.

Bemerkungen:

- Die Stufen 2, 3 und 4a, 4b entsprechen den Sicherheitsniveaus niedrig, substantiell und hoch aus eIDAS 2015/1502 [7], Abschnitt 2.2.2 (Ausstellung, Auslieferung und Aktivierung)
- Im ISO 29115 [2], Kap. 10.2.2.1 werden zusätzliche *Controls* zur *Credential Issuance* definiert.

Stufe	Ausprägungen	Beschreibung	Adress-Überprüfung ¹²
1	Einfache Auslieferung	Die Auslieferung garantiert eine bestimmte Gewissheit, dass das Authentifizierungsmittel dem richtigen Subjekt zugeordnet wird. Es sind Prozesse definiert und dokumentiert.	Keine Überprüfung: Die Adress-Angaben sind selbst deklariert und werden nicht überprüft.

¹² Die Adress-Überprüfung ist nur relevant, wenn die Auslieferung per Post erfolgt.

Stufe	Ausprägungen	Beschreibung	Adress-Überprüfung ¹²
2	Sichere Auslieferung	Zusätzlich zu Stufe 1: <i>Nach der Ausstellung wird das Authentifizierungsmittel auf eine Weise ausgeliefert, bei der davon ausgegangen werden kann, dass es nur das beabsichtigte Subjekt erreicht.</i> ¹³ Bei einer digitalen Auslieferung muss das Authentifizierungsmittel mit einer digitalen Signatur gegen Veränderungen (<i>tampering</i>) geschützt werden.	Keine Überprüfung: Die Adress-Angaben sind selbst deklariert und werden nicht überprüft.
3	Persönliche Auslieferung	Zusätzlich zu Stufe 2: <i>Nach der Ausstellung wird das Authentifizierungsmittel auf eine Weise ausgeliefert, bei der davon ausgegangen werden kann, dass es nur in den Besitz des Subjekts gelangt, dem es gehört.</i> ¹⁴ Wird das Authentifizierungsmittel nicht persönlich übergeben, muss die Existenz und die Zugehörigkeit der Adresse zum Subjekt überprüft werden.	Adäquate Validierung: Die Adress-Angaben werden einem geeigneten, gültigen Beweismittel entnommen.
4a	Mit Aktivierungsprozess für das Authentifizierungsmittel	Zusätzlich zu Stufe 3: <i>Im Aktivierungsprozess wird geprüft, dass das Authentifizierungsmittel nur in den Besitz des Subjekts gelangt ist, dem es gehört.</i> ¹⁵ Bei einer digitalen Auslieferung muss ein sicherer Kanal verwendet werden und das Subjekt (oder ein autorisierter Vertreter) muss den Empfang bestätigen. Der Aktivierungsprozess darf nur eine bestimmte Zeit aktiv sein (max. 10 min bei digitaler Auslieferung des Aktivierungs-codes; max. 7 Tage bei Auslieferung per Post im Inland; max. 21 Tage für Auslandspost).	Starke Validierung: Die Adress-Angaben werden einem geeigneten, gültigen Beweismittel entnommen und auf geeignete Art und Weise überprüft.

¹³ eIDAS 2015/1502 [7], Abschnitt 2.2.2. Sicherheitsniveau niedrig.

¹⁴ eIDAS 2015/1502 [7], Abschnitt 2.2.2. Sicherheitsniveau substantziell.

¹⁵ eIDAS 2015/1502 [7], Abschnitt 2.2.2. Sicherheitsniveau hoch.

Stufe	Ausprägungen	Beschreibung	Adress-Überprüfung ¹²
4b	Eigenhändige Übergabe	Das Authentifizierungsmittel wird dem persönlich physisch anwesenden Subjekt direkt von einer vom CSP autorisierten Stelle übergeben. Die Identität des Subjektes wird durch einen Vergleich körperlicher Merkmale mit einem geeigneten Beweismittel (starke Validierung IV.c) überprüft. Der Empfang wird quittiert.	-

Tabelle 22: Ausprägungen Kriterium *Übergabe Authentifizierungsmittel*

Beispiele:

- Stufe 1
 - Passwort (Authentifizierungsmittel) wird an die während der Registration genannte E-Mail Adresse versendet.
- Stufe 2
 - Benutzername (Identifikator) und Passwort (Authentifizierungsmittel) werden separat verschickt, wobei mindestens eines der beiden per Briefpost an die während der Registration genannte Adresse gesendet werden muss.
 - Ein Link zum Herunterladen des Authentifizierungsmittels, wird an die während der Registration genannte E-Mail-Adresse versendet. Der Gültigkeit des Links verfällt nach einer gewissen Zeit (z.B. 24 Stunden).
- Stufe 3
 - Als Beweismittel für die Adress-Angaben können Wohnsitzbestätigungen, Strom- oder Wasserrechnung verwendet werden
 - Authentifizierungsmittel wird per eingeschriebenen Brief an die während der Registration genannte und überprüfte Adresse gesendet.
 - Authentifizierungsmittel wird nach der Eingabe eines Passwortes, welches physisch bei der Registration übergeben wurde, heruntergeladen.
- Stufe 4a
 - Authentifizierungsmittel wird dem Subjekt per eingeschriebenen Brief an die während der Registration genannte und überprüfte Adresse gesendet und erst nach der Validierung deren E-Identität durch einen Aktivierungsprozess aktiviert.

- Stufe 4b
 - Authentifizierungsmittel wird dem Subjekt per eingeschriebenen Brief mit Zusatz „eigenhändig“ zugestellt¹⁶.
 - Authentifizierungsmittel wird dem Subjekt persönlich bei einer zuständigen Stelle übergeben (z.B. Übergabe Personalausweis durch die zuständige Personalausweisbehörde in Deutschland¹⁷).

5.2.6 Verlängerung/Ersetzung Authentifizierungsmittel

Fragen:	<p>Unter welchen Bedingungen kann ein noch gültiges Authentifizierungsmittel verlängert bzw. ein revoziertes Authentifizierungsmittel ersetzt werden?</p> <p>Wie kann bei der Verlängerung/Ersetzung garantiert werden, dass das Subjekt noch existiert und die gemachten Angaben (z.B. zur Adresse) noch stimmen?</p>
---------	--

Das Kriterium *Verlängerung/Ersetzung Authentifizierungsmittel* bewertet den Prozess,

- wie die Gültigkeit eines ablaufenden, aber noch gültigen Authentifizierungsmittels verlängert (siehe Spalte *Verlängerung* in Tabelle 23) oder
- ein revoziertes Authentifizierungsmittel ersetzt werden kann (siehe Spalte *Ersetzung* in Tabelle 23).

Werden für eine Authentifizierung mehrere Authentifizierungsmittel verwendet, muss das Kriterium für jedes Authentifizierungsmittel einzeln bestimmt werden. Die Gesamt-Qualitätsstufe ergibt sich dann aus der tiefsten Stufe der einzelnen Bewertungen.

Bemerkungen:

- Die Stufen CN1 und CN2 entsprechen den Sicherheitsniveaus niedrig und hoch aus eIDAS 2015/1502 [7], Abschnitt 2.2.4 (Verlängerung und Ersetzung)
- Die Anforderungen zum *CredentialSecureRenewal* aus ISO 29115 [2] Kapitel 10.2.2.1 wurden berücksichtigt.
- Die Erneuerung eines Passwortes mit Hilfe einer gültigen Email-Adresse ist ein Sonderfall der Ersetzung von Authentifizierungsmittel und entspricht der Stufe CN1.

¹⁶ Die Schweizer Post bietet einen entsprechenden Zusatzdienst für eingeschriebene Briefe an, bei der die Identität des Empfängers überprüft wird. Siehe <https://www.post.ch/de/geschaeflich/themen-a-z/zusatzleistungen/zusatzleistungen-briefe-inland/eigenhaendig> .

¹⁷ Siehe http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/eperso.pdf?__blob=publicationFile .

Stufe	Ausprägungen	Beschreibung	
		Verlängerung	Ersetzung
CN1	Verlängerung nach Vorweis/Einfache Ersetzung	Der CSP verfügt über definierte und dokumentierte Prozesse zur Verlängerung/Ersetzung der Authentifizierungsmittel.	
		Das noch gültige Authentifizierungsmittel wird bei der Beantragung der Verlängerung vorgewiesen. Ist das aktuelle Authentifizierungsmittel bereits abgelaufen, ist eine Verlängerung nicht mehr möglich. Alle Interaktionen müssen über sichere Kanäle ablaufen.	Beim Ersetzen wird ein neues Authentifizierungsmittel einfach ausgeliefert (siehe Kriterium <i>Übergabe Authentifizierungsmittel</i> Stufe 1).
CN2	Verlängerung nach Vorweis/ Sichere Ersetzung	Wie bei CN1.	Beim Ersetzen wird ein neues Authentifizierungsmittel sicher ausgeliefert (siehe Kriterium <i>Übergabe Authentifizierungsmittel</i> Stufe 2).
CN3	Verlängerung nach Vorweis/ Persönliche Ersetzung	Zusätzlich zur Stufe CN2: Das Subjekt muss nach IDN2 bzw. IDJ2 erneut identifiziert werden.	
		Wie bei CN2.	Beim Ersetzen wird ein neues Authentifizierungsmittel persönlich ausgeliefert (siehe Kriterium <i>Übergabe Authentifizierungsmittel</i> Stufe 3).

Stufe	Ausprägungen	Beschreibung	
		Verlängerung	Ersetzung
CN4	Verlängerung/Ersetzung nach Prüfung	Zusätzlich zur Stufe CN3: <i>Erfolgt die Verlängerung oder Ersetzung aufgrund eines gültigen elektronischen Identifizierungsmittels, so werden die Identitätsdaten anhand einer verlässlichen Quelle überprüft.¹⁸</i> Oder Für natürliche Personen, muss ein Beweismittel der Stufe IE.d vorgelegt und die Angaben nach Stufe IV.d validiert werden. Für juristische Personen muss zusätzlich die Verknüpfung zur natürlichen Person nach Stufe L4 überprüft werden.	
			Das ersetzte Authentifizierungsmittel wird eigenhändig übergeben (siehe Kriterium <i>Übergabe Authentifizierungsmittel</i> Stufe 4).

Tabelle 23: Ausprägungen Kriterium Verlängerung/Ersetzung Authentifizierungsmittel

6 Qualitätsmodell der Steuerung

Das Qualitätsmodell der Steuerung wird durch Bewertung der Kriterien des *IAM steuern* bestimmt (siehe Anhang G.3 für eine Beschreibung des Prozesses).

Das Qualitätsmodell der Steuerung enthält drei Kriterien (siehe Abbildung 16).

6.1 Vertrauensstufen der Steuerung (VSS)

Die Vertrauensstufen der Steuerung (VSS) werden aus den folgenden drei Kriterien abgeleitet (siehe Abbildung 13):

- Aufsicht (Kapitel 6.2.1),
- Haftung (Kapitel 6.2.2),
- Maturität (Kapitel 6.2.3).

¹⁸ eIDAS 2015/1502 [7], Abschnitt 2.2.4. Sicherheitsniveau hoch.

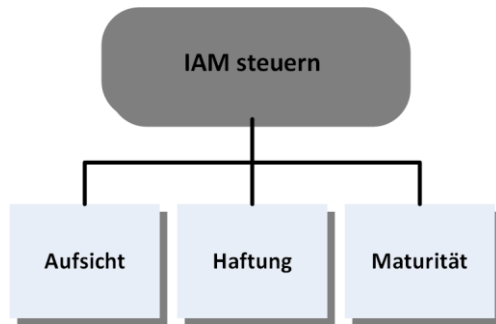


Abbildung 13: Kriterien für das Qualitätsmodell der Steuerung

Die Vertrauensstufe der Steuerung (VSS) wird hierbei durch die tiefste Ausprägung der Kriterien bestimmt.

Vertrauensstufe der Steuerung (VSS)	Aufsicht	Haftung	Maturität
1	Intern nach eigenem Standard oder gar nicht	Keine Haftung	Initial
2	Intern nach vordefinierten Regeln/Standards	Beschränkte Haftung	Definiert
3	Externes Audit	Haftung nach Gesetz	Verwaltet, gemessen
4	Audit durch akkreditierte Stelle	Haftung + Konventionalstrafe	Optimiert, integriert

Tabelle 24: Bestimmung der Vertrauensstufe der Steuerung (VSS)

6.2 Kriterien der Steuerung

6.2.1 Aufsicht

Fragen:	Wie vertrauenswürdig sind die Dienstleister? Wie gut ist die Prozessqualität der Dienstleister? Wie beaufsichtigt sind die Dienstleister?
---------	---

Die Prozesse zur Bereitstellung der Dienste sind unterschiedlich ausgeprägt und liegen in unterschiedlicher Qualität vor. Basieren die Prozesse auf Standards und wird die Prozessumsetzung zudem überprüft, so erhöht sich die Qualität der Prozesse der Dienstleister. Je höher die Qualität der internen Prozesse ist, desto kleiner ist das Risikopotential für Angriffe und Fehler.

Sind bei der Authentifizierung des Subjektes mehrere Dienstanbieter involviert, muss das Kriterium für jeden Dienstanbieter einzeln bestimmt werden. Die niedrigste Stufe bestimmt dann die Gesamtqualität dieses Kriteriums.

Bemerkungen:

- Die Stufen 2, 3 und 4 entsprechen den Sicherheitsniveaus niedrig, substantiell und hoch aus eIDAS 2015/1502 [7], Abschnitt 2.4.7 (Einhaltung und Prüfung)
- Für die Stufe 4 kommt in der Schweiz die VZertES Verordnung SR 943.032 [10] zur Anwendung.
- Die Stufen entsprechen dem Kriterium *Aufsicht Attribut-Autorität* aus dem Standard eCH-0171 [5], der aber nur die Aufsicht der Attribut-Autorität beschreibt.

Stufe	Ausprägungen	Beschreibung
1	Intern nach eigenem Standard oder gar nicht	Der Dienstanbieter richtet sich nach keinen oder selber entwickelten Standards. Die Überprüfung der Einhaltung wird nicht oder von einer internen Stelle durchgeführt.
2	Intern nach vordefinierten Regeln/Standards	Der Dienstanbieter richtet sich nach Standards, die öffentlich zugänglich sind und verbreitet angewendet werden. Die Überprüfung der Einhaltung der Standards lässt sie regelmässig durch eine interne Stelle durchführen.
3	Unabhängiges Audit	Der Dienstanbieter richtet sich nach Standards, die öffentlich zugänglich sind und verbreitet angewendet werden. Die Überprüfung der Einhaltung der Standards lässt sie regelmässig durch eine unabhängige Stelle durchführen.
4	Audit durch akkreditierte Stelle	Der Dienstanbieter richtet sich nach Standards, deren Einhaltung und Überprüfung eine amtlich akkreditierte Stelle durchführt. <i>Wird das System direkt von einer staatlichen Stelle verwaltet, so erfolgen die Prüfungen nach den nationalen Rechtsvorschriften.¹⁹</i>

Tabelle 25: Ausprägungen Kriterium *Aufsicht*

6.2.2 Haftung

Frage:	In welchem Umfang haftet der Dienstanbieter?
--------	--

Das Kriterium *Haftung des Dienstanbieters* zeigt, in welchem Umfang er verpflichtet ist, für die von ihm bereitgestellten Dienste zu haften. Je höher die Pflicht/Bereitschaft zu haften ist, desto höher ist die Qualität.

¹⁹ eIDAS 2015/1502 [7], Abschnitt 2.4.7. Sicherheitsniveau hoch.

Bemerkungen:

- Die Stufen entsprechen auch dem Kriterium *Haftung der Attribut-Autorität* aus dem Standard eCH-0171 [5], der aber nur die Haftung der Attribut-Autorität beschreibt.
- Für die Bundesverwaltung wird immer die Stufe 4 verwendet.

Stufe	Ausprägungen	Beschreibung
1	Keine Haftung	Jegliche Haftung wird durch Vertrag resp. AGB soweit gesetzlich zulässig wegbedungen.
2	Beschränkte Haftung	Die Haftung wird durch Vertrag resp. AGB soweit gesetzlich zulässig beschränkt.
3	Haftung nach Gesetz	Für die Haftung des Diensteanbieters sind die einschlägiger Haftungsbestimmung (Allgemeiner Teils des Obligationenrechts (Art. 97 ff.), nach ZertES [9], ...) anwendbar.
4	Haftung + Konventionalstrafe	Zusätzlich zu Stufe 3, wird die Durchsetzung von Schadenersatzansprüchen durch die Vereinbarung einer angemessenen kumulativen Konventionalstrafe nach Art. 163 ff. Obligationenrechts erleichtert.

Tabelle 26: Ausprägungen Kriterium *Haftung*

6.2.3 Maturität

Fragen:	<p>Wie reif ist das System der Registrierung und Authentifizierung?</p> <p>Wie gut ist der Diensteanbieter in der Lage eigene Erkenntnisse, wie z.B Sicherheitsvorfälle, zu erheben?</p> <p>Wie gut/schnell ist der Diensteanbieter in der Lage auf Grund von neuen Erkenntnissen (eigene oder externe) seine Prozesse anzupassen?</p>
---------	--

Prozessdefinitionen und deren Umsetzung zur Bereitstellung der Dienste sind pro Diensteanbieter unterschiedlich ausgeprägt und liegen in unterschiedlichen Detaillierungsgraden vor. Basieren die Prozesse auf Standards und wird die Prozessumsetzung zudem überprüft, so erhöht sich die Qualität der Prozesse der Diensteanbieter. Je höher die Qualität der internen Prozesse ist, desto kleiner ist das Risikopotential für Angriffe und Fehler. Je höher die Qualität der Änderungsfähigkeit dieser Prozesse ist, desto höher ist das Vertrauen in diesem Diensteanbieter.

Sind bei der Authentifizierung des Subjektes mehrere Diensteanbieter involviert, muss das Kriterium für jeden Diensteanbieter einzeln bestimmt werden. Die niedrigste Stufe bestimmt dann die Gesamtqualität dieses Kriteriums.

Die folgenden Stufen des Reifegrads aus dem Maturitätsmodell eCH-0172 [22] werden zur Definition der Stufen für das Kriterium *Maturität* verwendet:

- Reifegrad Stufe 1: Initiiert, Ad hoc und Reifegrad Stufe 2: Wiederholbar, entspricht der Stufe 1,
- Reifegrad Stufe 3: Definiert, entspricht der Stufe 2,
- Reifegrad Stufe 4: Verwaltet, gemessen, entspricht der Stufe 3,
- Reifegrad Stufe 5: Optimiert, integriert, entspricht der Stufe 4.

Falls bei der Einstufung eines Diensteanbieters die Beurteilung nicht durchführbar ist, darf man davon ausgehen, dass die Prozesse zumindest definiert sind, aber allenfalls nicht dokumentiert. Die Begründung für diese Annahme ist die Tatsache, dass es hier zum grössten Teil um automatisierte Abläufe handelt.

Stufe	Ausprägungen	Beschreibung
1	Initial	Prozesse sind ad-hoc und unorganisiert (Reifegrad 1) oder folgen bereits einem regelmässigen Muster (Reifegrad 2).
2	Definiert	Zusätzlich zu Stufe 1: Die Prozesse sind dokumentiert und kommuniziert. Es besteht ein Logging für die Registrierung- und Authentisierung-Vorgänge und es gibt Alarmvorgaben- und Prozesse für fehlgeschlagene Authentisierungen.
3	Verwaltet, gemessen	Zusätzlich zu Stufe 2: Die Prozesse sind überwacht und gemessen. Es bestehen Vorgaben zur Registrierung der Benutzerkategorien, zur Stärke der Authentisierung, abgeleitet vom Schutzbedarf der Ressource, Authentisierungs-Vorgaben für den Einsatz von Federated IAM.
4	Optimiert, integriert	Zusätzlich zu Stufe 3: Good Practices (die Vorgaben zur Bestimmung des Qualitätslevels gemäss einem Standard (STORK-QAA, eCH, ...)) werden angewandt, die Prozesse automatisiert (es besteht eine zentrale Directory-Infrastruktur für das Identifizieren und Authentisieren zur Runtime) und mit systematischen Prozesskontrollen verbessert.

Tabelle 27: Ausprägungen Kriterium *Maturität*

7 Qualitätsmodell der Föderierung

Das Qualitätsmodell der Föderierung wird durch Bewertung der Kriterien des Prozesses *Identität föderieren* bestimmt (siehe Anhang G.1.2. für eine Beschreibung des Prozesses).

7.1 Vertrauensstufen der Föderierung (VSF)

Die Vertrauensstufen der Föderierung (VSF) werden aus den folgenden 4 Kriterien abgeleitet (siehe Abbildung 14):

- Nachweis des Besitzes der Authentifizierungsbestätigung (Kapitel 7.2.1),
- Authentizität der Authentifizierungsbestätigung (Kapitel 7.2.2),
- Vertraulichkeitsschutz der Authentifizierungsbestätigung (Kapitel 7.2.3),
- Übermittlungsform der Authentifizierungsbestätigung (Kapitel 7.2.4).

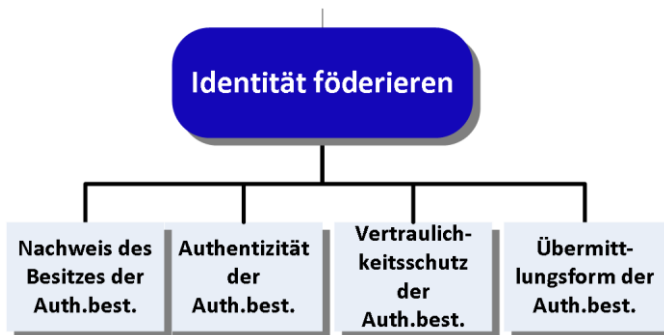


Abbildung 14: Kriterien für das Qualitätsmodell der Föderierung

Die Vertrauensstufe der Föderierung (VSF) wird hierbei durch die tiefste Ausprägung der Kriterien bestimmt.

Vertrauensstufen der Föderierung (VSF)	Nachweis des Besitzes der Auth. Best.	Authentizität	Vertraulichkeitsschutz	Übermittlungsform
1	Überbringer	Digitale Signatur	Keiner	Unabhängig
2	Überbringer	Digitale Signatur	Ver-schlüsse-lung	Front Channel
			Keiner	Back Channel
3	Überprüfbar durch RP	Digitale Signatur	Ver-schlüsse-lung	Unabhängig

Tabelle 28: Vertrauensstufen der Föderierung (VSF)

Beispiele:

- VSF1: SuisselD, Standard SAML Web SSO profile, OpenID Connect Implicit Client Profile
- VSF2:
 - (Front Channel): SwitchAAI
 - (Back Channel): SAML Artifact Binding, OpenID Connect ID Token
- VSF3:
 - SAML Holder of Key Profile

7.2 Kriterien der Föderierung

7.2.1 Nachweis des Besitzes der Authentifizierungsbestätigung

Fragen:	Kann die Authentifizierungsbestätigung das Subjekt genügend identifizieren? Repräsentiert die Authentifizierungsbestätigung sicher das referenzierte Subjekt (Abonnent)? Gibt es Schutz gegen Impersonation-Attacken? Ist der Überbringer der Authentifizierungsbestätigung auch der Abonnent (das sich zuvor authentifizierte Subjekt)?
---------	---

Bemerkung:

- Entspricht der *assertion possession category* aus NIST 800-63C [18]

Ausprägungen	Beschreibung
Überbringer - Bearer (B)	Die Identität des Subjekts wird nur durch die Authentifizierungsbestätigung bestätigt. Die RP muss davon ausgehen, dass die Authentifizierungsbestätigung für das überbringende Subjekt ausgestellt wurde. Dies stellt die schwächste Form einer Authentifizierungsbestätigung in einem föderierten Identitätssystem dar. Wenn ein Angreifer in der Lage ist, eine solche Authentifizierungsbestätigung abzufangen und selbst der RP vorzulegen, kann er sich damit mit einer falschen Identität Zugriff auf eine geschützte Ressource verschaffen.
Überprüfbar durch RP - Holder-of-Key (HoK)	Die Authentifizierungsbestätigung enthält eine Referenz auf ein Authentifizierungsmittel (Authentifikator), dessen Besitz das Subjekt zusätzlich identifiziert. Die RP kann somit den Überbringer auffordern, sich erneut zu authentisieren.

Tabelle 29: Ausprägungen Kriterium *Nachweis des Besitzes der Authentifizierungsbestätigung*

7.2.2 Authentizität der Authentifizierungsbestätigung

Fragen:	<p>Sind die Herkunft und die Unversehrtheit der Authentifizierungsbestätigung nachweisbar?</p> <p>Ist die Authentifizierungsbestätigung authentisch?</p> <p>Ist der Aussteller eindeutig identifizierbar?</p> <p>Kann der Aussteller abstreiten, die Authentifizierungsbestätigung ausgestellt zu haben?</p>
---------	--

Bemerkungen:

- Die Authentizität einer Authentifizierungsbestätigung wird in der Regel mit einer asymmetrischen, digitalen Signatur gewährleistet. Es sind auch andere Mittel denkbar (z.B. mit symmetrische Algorithmen), wenn dadurch die RP in der Lage ist, die Herkunft einer Authentifizierungsbestätigung genügend feststellen zu können. Aussagen zu konkreten Verfahren sind nicht Gegenstand dieses Standards.
- Die Authentizität ist Teil der *assertion protection category* aus NIST SP 800-63C [18].

Ausprägungen	Beschreibung
Keine Massnahmen	Es wurden keine Massnahmen ergriffen, um die Authentizität der Authentifizierungsbestätigung zu sichern.
Massnahmen zur Sicherung der Authentizität (Digitale Signatur)	Es wurden ausreichende Massnahmen ergriffen, um die Authentizität der Authentifizierungsbestätigung zu sichern.

Tabelle 30: Ausprägungen Kriterium Authentizität der Authentifizierungsbestätigung

Beispiele:

- Bei SAML ist die Authentifizierungsbestätigung (authentication assertion) mit einem privaten Schlüssel des IdP signiert. Der dazugehörige öffentliche Schlüssel ist publiziert und zugänglich für die RP.
- Bei Kerberos ist das Ticket symmetrisch mit einem Schlüssel verschlüsselt, der zuvor zwischen dem Empfänger Service (RP) und dem Key Distribution Center (IdP) ausgetauscht wurde.

7.2.3 Vertraulichkeitsschutz der Authentifizierungsbestätigung

Frage:	Ist die Authentifizierungsbestätigung so geschützt, dass unberechtigte Dritte die enthaltenen Informationen nicht einsehen können?
--------	--

Bemerkungen:

- Die Verschlüsselung ist Teil der *assertion protection category* aus NIST SP 800-63C [18]
- Die Verschlüsselung trägt zur Sicherheit bei. Die Daten können bei der Übermittlung gegenüber von Transitkomponenten geschützt werden (z.B. Browser)
- Aussagen zu konkreten Verfahren sind nicht Gegenstand dieses Standards.

Ausprägungen	Beschreibung
Keine Verschlüsselung	Die Authentifizierungsbestätigung ist nicht verschlüsselt.
Verschlüsselung	Der Payload der Authentifizierungsbestätigung wurde vom IdP mit dem öffentlichen Schlüssel der RP verschlüsselt. ²⁰

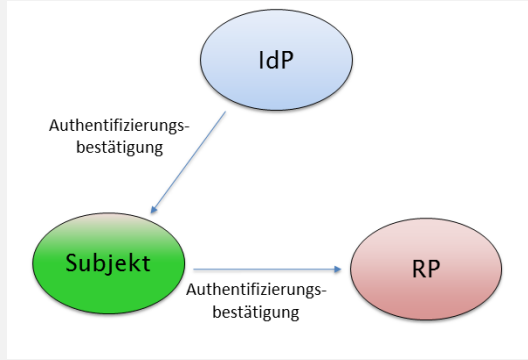
Tabelle 31: Ausprägungen Kriterium *Verschlüsselung der Authentifizierungsbestätigung*

7.2.4 Übermittlungsform der Authentifizierungsbestätigung

Frage:	Wird die Authentifizierungsbestätigung so übermittelt, dass unberechtigte Dritte die enthaltenen Informationen nicht einsehen können?
--------	---

Bemerkung:

- Die Übermittlungsform ist Teil der *assertion protection category* aus NIST SP 800-63C [18].

Ausprägungen	Beschreibung
Front Channel	<p>Bei der Übermittlung per Front Channel erstellt der IdP nach erfolgreicher primärer Authentifizierung eine Authentifizierungsbestätigung und sendet diese an das Subjekt (bzw. an dessen Client Applikation). Das Subjekt weist diese Assertion der RP vor, um sich ihr gegenüber zu authentisieren bzw. zu autorisieren.</p>  <p>Abbildung 15: Übermittlung per Front Channel</p>

²⁰ Aus Performance-Gründen wird bei der asymmetrischen Verschlüsselung nicht der gesamte Payload verschlüsselt, sondern eine hybride Verschlüsselung verwendet: Bei der hybriden Verschlüsselung generiert der Sender (IdP) einen zufälligen symmetrischen Schlüssel (Session-Key). Mit diesem Session-Key werden die zu schützenden Daten symmetrisch verschlüsselt. Anschliessend wird der Session-Key asymmetrisch mit dem öffentlichen Schlüssel des Empfängers (RP) verschlüsselt [27].

Ausprägungen	Beschreibung
Back Channel	<p>Bei der Übermittlung per Back Channel übergibt der IdP eine Referenz (z.B. in Form einer HTTP Redirect URL) an das Subjekt. Die Referenz selbst enthält <i>keine</i> Informationen über das Subjekt. Das Subjekt gibt diese Referenz an die RP weiter. Mit dieser Referenz kann die RP beim IdP innerhalb der erlaubten Zeitspanne und mit der entsprechenden Berechtigung die Authentifizierungsbestätigung über einen Back-Channel abholen.</p> <p>Abbildung 16: Übermittlung per Back Channel</p>

Tabelle 32: Ausprägungen des Kriteriums *Übermittlungsform der Authentifizierungsbestätigung*

8 Vergleich mit internationalen Standards

In diesem Kapitel werden die Modelle aus den internationalen Standards (NIST SP 800-63-3 [3], eIDAS Verordnung 910/2014 [1], ISO/IEC 29115 [2]) mit den Vertrauensstufen, die in diesem Standard definiert sind, verglichen.

Die in der Tabelle 33 dargestellte Vergleich dient als Übersicht, wie die Vertrauensstufen grob eingeordnet werden können.

Vertrauensstufe (VS)	NIST	eIDAS 910/2014	ISO/IEC 29115
VS1	AAL 1 IAL 1 FAL 1	-	LoA1
VS2	AAL 1 - FAL 2	niedrig ²¹	LoA2
VS3	AAL 2 IAL 2 FAL 2	substanziell	LoA3

²¹ eIDAS verlangt auf Stufe 'niedrig' nur einen Faktor für die Authentifizierung. Sowohl bei der Registrierung, wie bei der Steuerung verlangt eIDAS mind. ein Beweismittel bzw. ein internes Audit. Deshalb wird eIDAS 'niedrig' grob als VS2 eingestuft.

Vertrauensstufe (VS)	NIST	eIDAS 910/2014	ISO/IEC 29115
VS4	AAL 3 IAL 3 FAL 3	hoch	LoA4

Tabelle 33: Übersicht des Vergleichs der Vertrauensstufen

Nicht jeder internationale Standard deckt alle Teilmodelle, welche in diesem Standard definiert wurden, ab. Deshalb werden in den folgenden Kapiteln die verschiedenen Stufen gegenübergestellt und Unterschiede aufgezeigt. Dabei werden nur Kriterien erwähnt, die relevant für die qualitative Bewertung sind.

Die Vertrauensstufen werden ihrer Entsprechung aus den internationalen Standards gegenübergestellt. Abweichungen sind markiert (mit einem Sternchen *) und beschrieben.

8.1 Qualitätsmodell der Authentifizierung

Die eIDAS Sicherheitsniveaus und ISO/IEC 29115 Level of Assurance entsprechen den Vertrauensstufen der Authentifizierung, welche in diesem Standard definiert wurden, gemäss der Tabelle 34.

Vertrauensstufe der Authentifizierung (VSA)	NIST SP 800-63-3	eIDAS 910/2014	ISO/IEC 29115
VSA1	AAL 1	niedrig	LoA2
VSA2	AAL 1	substanziell	LoA3
VSA3	AAL 2	hoch	LoA3
VSA4	AAL 3	hoch	LoA4

Tabelle 34: Vergleich des Qualitätsmodells der Authentifizierung

8.2 Qualitätsmodell der Registrierung

8.2.1 Registrierung für natürliche Personen

Vertrauensstufe der Registrierung für natürl. Personen (VSRN)	NIST SP 800-63-3	eIDAS 910/2014	ISO/IEC 29115
VSRN1	IAL 1	-	LoA1
VSRN2	-	niedrig	LoA2*
VSRN3	IAL 2*	substanziell	LoA3
VSRN4	IAL 3*	hoch	LoA4

Tabelle 35: Vergleich des Qualitätsmodells der Registrierung natürlicher Personen

Abweichungen zu NIST SP 800-63B

NIST SP 800-63B unterstützt nur 3 Identity Assurance Level (IAL1, IAL2 und IAL3), die den Vertrauensstufen VSRN1, VSRN3 und VSRN4 entsprechen.

Die Unterschiede zwischen den Vertrauensstufen und den Identity Assurance Level beruhen hauptsächlich auf der Qualität und Anzahl der Beweismittel und wurden daher in diesem Standard auf die Gegebenheiten der Schweiz (Vorlage eines Identitätsdokumentes) angepasst.

Das NIST akzeptiert die Vorlage eines elektronischen Nachweises einer gültigen, qualitativ gleichwertigen oder höher notifizierten bzw. zertifizierten E-Identity nicht als Beweismittel.

Abweichungen zu ISO/IEC 29115

ISO erfordert bereits bei LoA2 ein Beweismittel mit einem Foto des Subjektes. Die Übergabe sollte gemäss Kriterium 5.2.5 Übergabe Authentifizierungsmittel auf Stufe 3 (Persönliche Übergabe) erfolgen.

8.2.2 Registrierung von juristischen Personen

Die Qualität der Registrierung von juristischen Personen wird nur in eIDAS abgehandelt und bewertet. Der Vergleich mit den Vertrauensstufen der Registrierung für juristische Personen ist in Tabelle 36 dargestellt.

Die im ISO/IEC 29115 beschriebenen Non-Person Entities (NPEs) sind nicht gleich zu setzen mit juristischen Personen.

Im NIST SP 800-63-3 werden juristische Personen nicht behandelt.

Vertrauensstufe der Registrierung für jurist. Personen (VSRJ)	NIST SP 800-63-3	eIDAS 910/2014	ISO/IEC 29115
VSRJ1	-	-	-
VSRJ2	-	niedrig	-
VSRJ3	-	hoch	-
VSRJ4	-	-	-

Tabelle 36: Vergleich des Qualitätsmodells der Registrierung juristischer Personen

8.3 Qualitätsmodell der Steuerung

Die eIDAS Sicherheitsniveaus und ISO 29115 Level of Assurance entsprechen den Vertrauensstufen der Steuerung (VSS), welche in diesem Standard definiert wurden (siehe Tabelle 37).

Im NIST SP 800-63-3 werden gemäss NIST SP 800-53 [23] Sicherheitsmassnahmen definiert, je nachdem wie schützenswert die zu verwaltenden Daten sind.

Vertrauensstufe der Steuerung (VSS)	NIST SP 800-63-3*	eIDAS 910/2014	ISO/IEC 29115
VSS1	-	-	LoA 1
VSS2	-	niedrig	LoA 2
VSS3	-	substanziell	LoA 3
VSS4	-	hoch	LoA 4

Tabelle 37: Vergleich des Qualitätsmodells der Steuerung

8.4 Qualitätsmodell der Föderierung

Vertrauensstufen der Föderierung (VSF) entsprechen den Federation Assurance Level (FAL) des NIST SP 800-63C [18] (siehe Tabelle 38).

Weder die eIDAS Verordnung 910/2014 [1] noch die ISO/IEC 29115 [2] betrachten die Qualität der Föderierung in einer Identity Federation als allein stehendes Qualitätsmodell. Es wird daher angenommen, dass diese bei eIDAS und ISO in der Authentifizierung integriert sind.

Vertrauensstufe der Föderierung (VSF)	NIST SP 800-63-3*	eIDAS 910/2014	ISO/IEC 29115
VSF1	FAL 1	-	-
VSF2	FAL 2	-	-
VSF3	FAL 3	-	-

Tabelle 38: Vergleich des Qualitätsmodells der Föderierung

Abweichungen zu NIST SP 800-63C

Im Unterschied zum NIST Standard wird in VSF2 zwischen Front-Channel und Back-Channel unterschieden. Bis zu dieser Vertrauensstufe erachten wir die verschlüsselte Übertragung einer Assertion über den Browser (Front Channel) und einer nicht-verschlüsselten Assertion über einen sicheren Kanal zwischen IdP und RP als äquivalent, bezüglich Vertraulichkeitsschutz.

9 Haftungsausschluss/Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellen oder welche **eCH** referenzieren, haben nur den Status von Empfehlungen. Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.

In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.

Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.

Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

10 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.

Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwickelt werden.

eCH-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.

Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

Anhang A - Referenzen & Bibliographie

- [1] D. A. S. Europ, I. Parlamentder, R. A. T. D. E. R. Europ, and I. Union, “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, (eIDAS),” 2015.
- [2] P. Editors, W. Fumy, M. De Soete, E. J. Humphreys, K. Naemura, and K. Rannenber, “ITU-T Recommendation X . 1254 | International Standard ISO / IEC DIS 29115 Information technology — Security techniques — Entity authentication assurance framework,” 2011.
- [3] J. L. F. Paul A. Grassi, “DRAFT NIST Special Publication 800-63-3,” 2017 [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63-3.html>. [Accessed: 22-Jun-2017]
- [4] R. Bernold, G. Hassenstein, A. Laube-Rosenpflanzler, A. Spichiger, and M. Topfel, “eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM),” version 2.0, 2013 [Online]. Available: <https://www.ech.ch/alfresco/s/ech/download?nodeid=5d5f74ed-77ae-4a68-af53-a4ff910dc89f>
- [5] M. Topfel, T. Jarchow, A. Spichiger, and R. Bernold, “eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID,” version 1.0, 2014 [Online]. Available: <https://www.ech.ch/alfresco/s/ech/download?nodeid=a26d17d1-fe03-4226-97ab-9beefef22856>
- [6] B. Hulsebosch, G. Lenzin, and H. Eertink, “STORK: D2.3 - Quality authenticator scheme,” version 1.6, 2009 [Online]. Available: https://www.eid-stork.eu/dmdocuments/public/D2.3_final_1.pdf
- [7] Europäische Union, “Durchführungsverordnung (EU) Nr. 2015/1502 der Kommission vom 8. September 2015,” no. September, 2012.
- [8] R. Kissel, “Glossary of Key Information Security Terms Glossary of Key Information Security Terms,” *Nist*, version NISTIR 729, no. Revision 2, 2013.
- [9] Schweizerische Eidgenossenschaft, “Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES),” 2016 [Online]. Available: <https://www.admin.ch/opc/de/classified-compilation/20131913/index.html>
- [10] Der Schweizerische Bundesrat, “Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate,” 2016 [Online]. Available: <https://www.admin.ch/opc/de/classified-compilation/20162168/index.html>
- [11] P. Madsen, E. Maler, S. Microsystems, T. Wisniewski, T. Nadalin, S. Cantor, and J. Hodges, “SAML V2.0 Executive Overview,” no. April, pp. 1–7, 2005.
- [12] Natsakimura, “OpenID Connect | OpenID.” [Online]. Available: <http://openid.net/connect/>. [Accessed: 10-Oct-2016]
- [13] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, W. E. Burr, D. F. Dodson, and R. A. Perlner, “NIST Special Publication 800-63-2 Electronic Authentication Guideline,” 2003 [Online]. Available: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>
- [14] NIST, “DRAFT Strength of Function for Authenticators - Biometrics.” [Online]. Available: <https://pages.nist.gov/SOFA/SOFA.html>. [Accessed: 03-Nov-2016]
- [15] J. P. R. Paul A. Grassi, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, James L. Fenton, “DRAFT NIST Special Publication 800-63B,” 2017 [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63b.html>. [Accessed: 22-Jun-2017]

- [16] J. L. F. Paul A. Grassi, Jamie M. Danker, William E. Burr, "DRAFT NIST Special Publication 800-63A," 2017 [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63a.html>. [Accessed: 22-Jun-2017]
- [17] D. Bundesversammlung and D. S. Eidgenossenschaft, *Bundesgesetz über die Unternehmens-Identifikationsnummer (UIDG)*. 2011 [Online]. Available: <https://www.admin.ch/opc/de/classified-compilation/20082601/index.html>
- [18] S. K. S. Paul A. Grassi, James L. Fenton, Justin P. Richer, "DRAFT NIST Special Publication 800-63C," 2017 [Online]. Available: <https://pages.nist.gov/800-63-3/sp800-63c.html>. [Accessed: 22-Jun-2017]
- [19] NIST, "FIPS 140-2 - Security Requirements for Cryptographic Modules," 2001 [Online]. Available: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>
- [20] E. D. Hardt, "The OAuth 2.0 Authorization Framework [RFC 6749]," 2012 [Online]. Available: <https://tools.ietf.org/html/rfc6749>
- [21] D. Bundesversammlung and D. S. Eidgenossenschaft, *Regierungs- und Verwaltungsorganisationsgesetz (RVOG)*. 2016 [Online]. Available: <https://www.admin.ch/opc/de/classified-compilation/19970118/index.html>
- [22] H. Häni and U. Kienholz, "eCH-0172 IAM-Maturitätsmodell," version 1.0, 2014 [Online]. Available: <https://www.ech.ch/alfresco/s/ech/download?nodeid=a26d17d1-fe03-4226-97ab-9beefef22856>
- [23] Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations [SP 800-53]," 2015.
- [24] NIST Information Technology Laboratory, "Measuring Strength of Identity Proofing," version 1, 2015 [Online]. Available: <https://www.nist.gov/sites/default/files/nstic-strength-identity-proofing-discussion-draft.pdf>
- [25] A. Laube-rosenpflanzer, G. Hassenstein, S. Agosti, M. Vinzens, U. Pfenninger, and D. Leiser, "eCH-0168 SuisseTrustIAM technische Architektur und Prozesse," version 1.0, 2014 [Online]. Available: <https://www.ech.ch/alfresco/s/ech/download?nodeid=31499686-813d-4589-b794-11015fbf2059>
- [26] T. Polk, K. Mckay, and S. Chokhani, "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations [SP 800-52]," 2014.
- [27] Wikipedia, "Hybride Verschlüsselung." [Online]. Available: https://de.wikipedia.org/wiki/Hybride_Verschl%C3%BCsslung. [Accessed: 22-Nov-2016]

Anhang B - Mitarbeit & Überprüfung

Buff Raffael	Abraxas Informatik AG
Gruoner Torsten	Bundesverwaltung – EFD – ISB
Hassenstein Gerhard	Berner Fachhochschule
Heerkens Marc	Bundesverwaltung – EFD – ISB
Kunz Marc	Berner Fachhochschule
Laube-Rosenpflanzler Annett	Berner Fachhochschule
Schlunegger Yves	CSC Switzerland GmbH
Selzam Thomas	Berner Fachhochschule
Spichiger Andreas	Berner Fachhochschule

Anhang C - Abkürzungen und Glossar

C.1 Abkürzungen

AAL	Authentication Assurance Level
CA	Credential Authority
CSP	Credential Service Provider
eIDAS	Verordnung (EU) Nr. 910/2014 über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
EU	Europäische Union
FAL	Federation Assurance
FIDO	Fast IDentity Online
HoK	Holder of Key
HTTP	Hypertext Transfer Protocol
HW-MFA	Hardware Multifactor Authentication
IAL	Identity Assurance Level
IAM	Identity and Access Management
IdP	Identity Provider
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KDC	Kerberos Distribution Center
LoA	Level of Assurance
MFA	Mult Factor Authentication

NIST	National Institute of Standards and Technology
nPA	neuer Personalausweis
OIDC	OpenID Connect
OTP	One-time Password
PIN	Persönliche Identifikationsnummer
RA	Register Authority / Registrierungsstelle
RP	Relaying Party
SAML	Security Assertion Markup Language
SFA	Single Factor Authentication
SMS	Short Message Service
SR	Systematische Rechtssammlung
SSO	Single Sign-on
STORK	Secure idenTity acrOss boRders linKed
TGT	Ticket Granting Ticket
TSP	Trust Service Provider
UID	Unique identifier
URL	Uniform Resource Locator
VS	Vertrauensstufe
VSA	Vertrauensstufe der Authentifizierung
VSF	Vertrauensstufe der Föderierung
VSR	Vertrauensstufe der Registrierung
VSRJ	Vertrauensstufe der Registrierung für juristische Personen
VSRN	Vertrauensstufe der Registrierung für natürliche Personen
VSS	Vertrauensstufe der Steuerung
ZGB	Schweizerisches Zivilgesetzbuch

C.2 Glossar

Authentifikator	Funktionales Abbild des Authentifizierungsmittels der Realwelt. Mit der Funktion eines Authentifikators wird aus einem Eingabewert und einem geheimen Wert ein Ausgabewert erzeugt.
Authentifizierung	Vorgang der Überprüfung einer behaupteten E-Identity.
Authentifizierungsbestätigung	Eine Bestätigung der erfolgreichen Authentifizierung eines Subjektes.

Authentifizierungsfaktor	Informationen und/oder Prozesse, die zur Authentifizierung eines Subjektes verwendet werden können. Authentifizierungsfaktoren können auf vier verschiedenen Merkmalen (besitzabhängig, kenntnisabhängig, inhärent oder verhaltensbasiert) oder Kombinationen davon beruhen.
Authentifizierungs-mittel	Etwas, das ein Subjekt besitzt und unter seiner Kontrolle hat (ein kryptographischer Schlüssel, ein Geheimnis oder ein biometrisches Merkmal).
Beweismittel	Dokument oder Objekt aus einer verlässlichen Quelle, das Angaben zum Antragsteller enthält.
Biometrisches Merkmal	Ein biometrisches Merkmal ist ein körperliches Merkmal eines Menschen, welches zur Identifizierung verwendet werden kann.
Certificate Authority / Certification authority (CA)	Eine Certificate Authority ist ein spezieller Credential Service Provider (CSP), der digitale Zertifikate (Public Key Zertifikate, e.g. X.509) als Authentifizierungsmittel ausgibt, erneuert und revoziert.
Client Plattform	Das System oder Gerät, von welchem das Subjekt einen Authentifizierungsprozess anstösst.
Credential	Ein Credential stellt eine Menge von Daten dar, mit der eine E-Identity an ein Authentifizierungsmittel gebunden wird, welches vom Subjekt besitzt und kontrolliert wird.
Credential Service Provider (CSP)	Eine Entität, die als vertrauenswürdiger Herausgeber von digitale Zertifikaten und anderer Sicherheits-Tokens (Authentifizierungsmitteln) agiert.
E-Identity	Repräsentation eines Subjekts. Eine E-Identity (digitale Identität) hat einen Identifikator (eindeutiger Name), meist zusammen mit einer Menge von zusätzlichen Attributen, welche innerhalb eines Namens-raumes eindeutig einem Subjekt zugewiesen werden können. Ein Subjekt kann mehrere E-Identities haben.
Elektronisches Identifizierungsmittel	Enthält Authentifizierungsfaktoren, Attribute für Personen und hat eine Gültigkeit. Bei einer Authentifizierung wird der gesamte Prozess Subjekt authentifizieren vom elektronischen Identifizierungsmittel abgewickelt. Es umschliesst daher sowohl Authentifizierungsmittel, Credential und IdP.
Elektronisches Identifizierungssystem	Begriff aus eIDAS 910/2014 [1] : „Elektronisches Identifizierungssystem“ ist ein System für die elektronische Identifizierung, in dessen Rahmen natürlichen oder juristischen Personen oder natürlichen Personen, die juristische Personen vertreten, elektronische Identifizierungsmittel ausgestellt werden. Ein notifiziertes elektronisches Identifizierungssystem muss alle in eIDAS 910/2014 [1] Artikel 7 aufgeführten Voraussetzungen erfüllen.

Definitionszeit	In der Definitionszeit wird das IAM-System eingerichtet und konfiguriert. Zusätzlich werden die elektronischen Identitäten etabliert. Die Definitionszeit umfasst damit die Prozesse zur Bereitstellung aller notwendigen Informationen für alle beteiligten Komponenten sowie der Komponenten selbst.
Föderierung / Federation	Eine Föderierung ist eine Zusammenarbeit verschiedener Entitäten eines IAM-Systems über Organisations- und Systemgrenzen hinweg, ohne Duplikation oder Replikation der dazu notwendigen Benutzerdaten (E-Identities).
Identifizierung	Identifizierung ist ein Vorgang zur Definitionszeit, bei welchem die Identität des Subjekts meist mit Hilfe von Beweismitteln überprüft wird.
Identitätsdokument	a) Reisepass, b) Schweizer Identitätskarte, c) eine für die Einreise in die Schweiz anerkannte Identitätskarte.
Identity Provider (IdP)	Entität, die zur Laufzeit die E-Identity des Subjekts überprüft. Dazu wird der Besitz bzw. die Kontrolle des Subjektes über die Authentifizierungsmittel und die Verbindung des Subjektes zu den verwendeten Authentifizierungsmittel mit Hilfe der Credentials überprüft.
Juristische Person	Juristische Personen sind Organisationen nach Art. 52 ff ZGB sowie gemäss den einschlägigen Bestimmungen des Gesellschaftsrechtes des OR definiert.
Körperliches Merkmal	Merkmal eines Menschen, wie Körpergrösse und Augenfarbe.
Laufzeit	Zur Laufzeit finden die elektronischen Prozesse statt, mit denen ein Subjekt Zugang und Zugriff auf die Ressourcen einer Relying Party erhält.
Registrierungsstelle / Registration Authority (RA)	Eine Entität, die genügend Informationen zu einem Subjekt erfasst, um dessen Identität überprüfen zu können.
Subjekt	Eine natürliche Person, Organisation (juristische Person) oder ein Service, die auf eine Ressource zugreift oder zugreifen möchte. Ein Subjekt wird durch E-Identities repräsentiert.
UID-Einheit	Bei UID-Einheiten handelt es sich um alle Unternehmen und Institutionen, die eine UID erhalten. UID-Einheiten sind nach Art. 3.c des Bundesgesetzes über die Unternehmens-Identifikationsnummer festgelegt.
Verlässliche Quelle	Beliebige Informationsquelle, welche bezogen auf eine konkrete Situation als vertrauenswürdig betrachtet wird.
Verwaltungen	Verwaltung bezeichnet ein Gemeinwesen (Ämter und Behörden, allenfalls mit solchen Aufgaben beauftragte Private), welche gesetzlich übertragene Staatsaufgaben besorgt.

Anhang D - Änderungen gegenüber Vorversion

Der vorliegende Standard ersetzt den Standard eCH-0170 v1.0. In die Überarbeitung sind wesentliche neue Erkenntnisse und Konzepte, insbesondere aus den Standards NIST SP 800-63-3 [3], eIDAS Verordnung 910/2014 [1] und ISO/IEC 29115 [2]) eingeflossen.

So wurde eCH-0170 in der Version 2.0 in wesentlichen Teilen von Grund auf neu erarbeitet. Die Unterschiede wurden in einem Hilfsmittel erarbeitet. Es zeigt auf, welche Kriterien von Version 1.0 mit der Version 2.0 vergleichbar sind. Nachfolgend werden die generellen Änderungen aufgeführt und auf die jeweiligen Inhalte in eCH-0170 Version 1.0 verwiesen.

Grundsätzliches:

- Der Aufbau der Kapitel wurde grundsätzlich geändert und der Struktur des eCH-0171 angeglichen. So wurde die Darstellung der Qualitätsmodelle vereinheitlicht, um die Lesbarkeit zu verbessern.
- V1.0 basierte rein auf den Erkenntnissen des EU-Projektes STORK. Diese flossen in die Erarbeitung der eIDAS Verordnung mit ein und sind deshalb auch in diesem Standard mitberücksichtigt.
- Zusätzlich zu der eIDAS Verordnung wurde auch der ISO/IEC 29155 und NIST 800-63-3 bei der Ausarbeitung dieses Standards berücksichtigt. Besonders die Unterteilung in Teilmodelle hat dort ihren Ursprung.
- V2.0 betrachtet neben der der Qualität der Authentifizierung von natürlichen Subjekten auch die von juristischen Subjekten.

Kapitel 2 Einleitung [eCH-0170 v1.00 Kapitel 1]

- Die Einleitung wurde komplett überarbeitet und auf das Prozess- und Informationsmodell des eCH-107 [4] abgestützt. Diese Modelle wurden dabei wesentlich erweitert.

Kapitel 3 Terminologie [neu]

- Die Terminologie wurde in Bezug auf den eCH-107 [4] deutlich erweitert und überarbeitet. Das entsprechende Glossar befindet sich in Anhang C.2.

Kapitel 4 Qualitätsmodell [eCH-0170 v1.00 Kapitel 3]

- Das neue Qualitätsmodell besteht aus Vertrauensstufen und wird aus 4 Teilmodellen komponiert.

Kapitel 5, 6, 7 und 8 [eCH-0170 v1.00 Kapitel 4]

- In diesen Kapiteln werden die Teilmodelle, die dazugehörigen Kriterien und deren Komposition zu den Vertrauensstufen beschrieben.

Kapitel 9 Vergleich mit internationalen Standards [neu]

- In diesem Kapitel wird das Qualitätsmodell den internationalen Standards eIDAS, ISO/IEC 29115 und NIST 800-63-3 gegenübergestellt.

Änderungen von Version 2.0 zu 2.01

Querverweisfehler (Fehler! Verweisquelle konnte nicht gefunden werden) in den Kapiteln 2.2, 2.5, 3.10, 4.4, 7.1, 8.1 und G1.2 wurden behoben

Überführung ins aktuelle Layout.

Anhang E - Abbildungsverzeichnis

Abbildung 1: Einordnung des eCH-0170 Standards	9
Abbildung 2: Prozessmodell Authentifizierung eines Subjektes.....	10
Abbildung 3: Informationsarchitektur	13
Abbildung 4: Schematische Funktionsweise eines Authentifizierungsmittels	18
Abbildung 5: Modell einer Identity Federation	23
Abbildung 6: Definition <i>Subjekt</i>	25
Abbildung 7: Komposition des Qualitätsmodells.....	27
Abbildung 8: Übersicht aller Kriterien	32
Abbildung 9: Kriterien für das Qualitätsmodell der Authentifizierung	35
Abbildung 10: Kriterien für das Qualitätsmodell der Registrierung.....	39
Abbildung 11: Faktoren zum Kriterium Identifikation natürlicher Personen	47
Abbildung 12: Faktoren zum Kriterium Identifikation juristischer Personen.....	49
Abbildung 13: Kriterien für das Qualitätsmodell der Steuerung	57
Abbildung 14: Kriterien für das Qualitätsmodell der Förderierung.....	61
Abbildung 15: Übermittlung per Front Channel	64
Abbildung 16: Übermittlung per Back Channel.....	65
Abbildung 17: Prozesslandkarte.....	81
Abbildung 18: Prozess <i>Subjekt authentifizieren</i>	81
Abbildung 19: Prozess <i>Identität fördern</i>	82
Abbildung 20: Prozess <i>Subjekt registrieren</i>	84
Abbildung 21: Prozess IAM steuern	87

Anhang F - Tabellenverzeichnis

Tabelle 1: Farbverwendung im Dokument.....	11
Tabelle 2: Übersicht des normativen Charakters der Kapitel.....	16
Tabelle 3: Beispiele für Authentifizierungsmittel und zugehörigem Credential.....	19
Tabelle 4: Teile des Qualitätsmodells und die dazugehörigen Vertrauensstufen.....	27
Tabelle 5: Vertrauensstufen des Qualitätsmodells zur Authentifizierung von Subjekten.....	30
Tabelle 6: Komposition der Vertrauensstufen aus den Stufen der Teilmodelle.....	31
Tabelle 7: Vorbedingungen für Identity Federation Systeme.....	34
Tabelle 8: Vertrauensstufen der Authentifizierung (VSA).....	35
Tabelle 9: Ausprägungen Kriterium <i>Authentifizierungsmittel</i>	37
Tabelle 10: Ausprägungen Kriterium <i>Zertifizierung des Authentifizierungsmittel</i>	37
Tabelle 11: Ausprägungen Kriterium <i>Re-Authentifizierung</i>	38
Tabelle 12: Bestimmung der VSR für natürliche Personen.....	40
Tabelle 13: Bestimmung der VSR für juristische Personen.....	41
Tabelle 14: Ausprägungen Faktor Anwesenheit.....	42
Tabelle 15: Ausprägungen Faktor Beweismittel.....	43
Tabelle 16: Ausprägungen Faktor Validierung der Angaben.....	45
Tabelle 17: Ausprägungen Faktor Nichtabstreitbarkeit.....	46
Tabelle 18: Ausprägungen Faktor <i>Vollmacht</i>	47
Tabelle 19: Ausprägungen Kriterium <i>Identifikation natürlicher Personen</i>	48
Tabelle 20: Ausprägungen Kriterium <i>Identifikation juristischer Personen</i>	50
Tabelle 21: Ausprägungen Kriterium <i>Verknüpfung natürliche und juristische Person</i>	51
Tabelle 22: Ausprägungen Kriterium <i>Übergabe Authentifizierungsmittel</i>	53
Tabelle 23: Ausprägungen Kriterium Verlängerung/Ersetzung Authentifizierungsmittel.....	56
Tabelle 24: Bestimmung der Vertrauensstufe der Steuerung (VSS).....	57
Tabelle 25: Ausprägungen Kriterium <i>Aufsicht</i>	58
Tabelle 26: Ausprägungen Kriterium <i>Haftung</i>	59

Tabelle 27: Ausprägungen Kriterium <i>Maturität</i>	60
Tabelle 28: Vertrauensstufen der Föderierung (VSF)	61
Tabelle 29: Ausprägungen Kriterium <i>Nachweis des Besitzes der Authentifizierungsbestätigung</i>	62
Tabelle 30: Ausprägungen Kriterium Authentizität der Authentifizierungsbestätigung	63
Tabelle 31: Ausprägungen Kriterium <i>Verschlüsselung der Authentifizierungsbestätigung</i>	64
Tabelle 32: Ausprägungen des Kriteriums <i>Übermittlungsform der Authentifizierungsbestätigung</i>	65
Tabelle 33: Übersicht des Vergleichs der Vertrauensstufen	66
Tabelle 34: Vergleich des Qualitätsmodells der Authentifizierung	66
Tabelle 35: Vergleich des Qualitätsmodells der Registrierung natürlicher Personen	67
Tabelle 36: Vergleich des Qualitätsmodells der Registrierung juristischer Personen.....	68
Tabelle 37: Vergleich des Qualitätsmodells der Steuerung	68
Tabelle 38: Vergleich des Qualitätsmodells der Föderierung	68
Tabelle 39: Anforderungen an die Übergabe der Authentifizierungsbestätigung.	84

Anhang G - Prozesse

Der Authentifizierungsprozess bedingt eine Vielzahl von Aktivitäten. Zur Bewertung der Qualität der Authentifizierung eines Subjektes werden nicht nur die eigentliche Bestätigung selber, sondern auch die mit der Erstellung verbundenen Prozesse berücksichtigt.

Abbildung 17 zeigt die Prozesse für die Ausführung, die Definition und die Steuerung einer Authentifizierung. Dabei werden nur die für eine qualitative Einstufung der Authentifizierung relevanten Prozesse berücksichtigt.

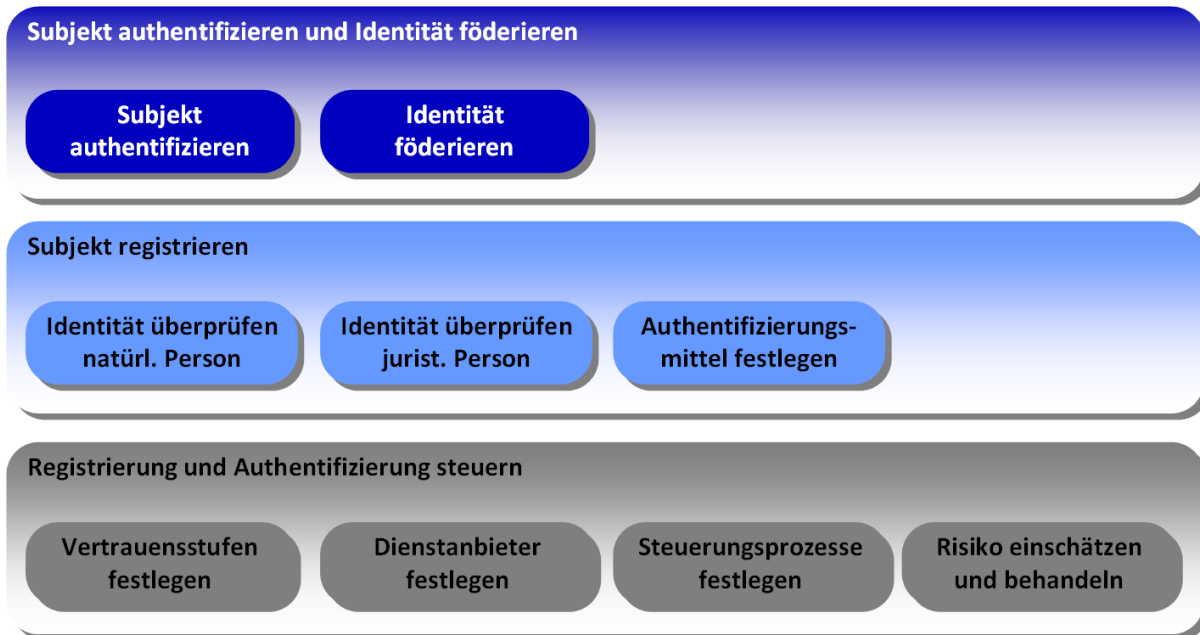


Abbildung 17: Prozesslandkarte

G.1 Subjekt authentifizieren und Identität fördern

G.1.1 Subjekt authentifizieren

Der Prozess *Subjekt authentifizieren* ermöglicht zur Ausführungszeit die zeitnahe Überprüfung der E-Identity eines Subjektes durch einen Identity Provider unter Verwendung eines Authentifizierungsmittels (siehe Abbildung 18).

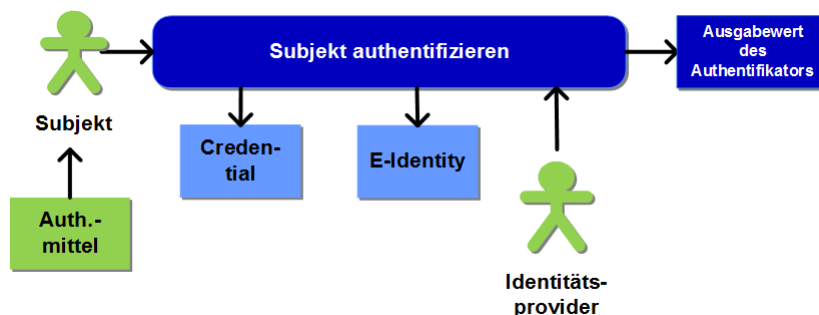


Abbildung 18: Prozess *Subjekt authentifizieren*

Dieser Prozess entspricht der *Entity Authentication Phase* bei ISO 29115 [2], der *Electronic Authentication Phase* (Elektronische Authentifizierungsphase) bei STORK [6], der Phase *Authentifizierung* bei eIDAS [7] und der *Digital Authentication* bei NIST SP 800-63B [15].

Subjekt authentifizieren	Überprüfung der behaupteten E-Identity eines Subjektes durch den Identity Provider.
--------------------------	---

Tätigkeiten:

- Das Subjekt verwendet ein ihm zur Verfügung gestelltes und unter seiner Kontrolle befindliches Authentifizierungsmittel.
- Das Authentifizierungsmittel generiert mit Hilfe des Authentifikators einen Ausgabewert aus den Eingaben des Subjekts (Geheimnis und optional anderen Eingabewerten).
- Das Authentifizierungsmittel sendet den generierten Ausgabewert an einen IdP zur Überprüfung.
- Der IdP prüft den generierten Ausgabewert mit dem Credential der behaupteten E-Identity. Ist die Prüfung positiv, ist die Authentifizierung erfolgreich.
- In Abhängigkeit der verlangten Sicherheitsstufe muss die RP das Subjekt nach einer bestimmten Zeitdauer (unabhängig von ihren eigenen Richtlinien) erneut durch den IdP authentifizieren lassen (Re-Authentifizierung).

Qualitätskriterien:

- Kapitel 4.2.1 Authentifizierungsmittel
- Kapitel 4.2.2 Zertifizierung des Authentifizierungsmittels
- Kapitel 4.2.3 Re-Authentifizierung

G.1.2 Identität fördern

Beim Prozess *Identität fördern* wird zur Ausführungszeit nach erfolgter Authentifizierung des Subjekts das Ergebnis in Form einer Authentifizierungsbestätigung vom IdP an die RP übertragen (siehe Abbildung 19).

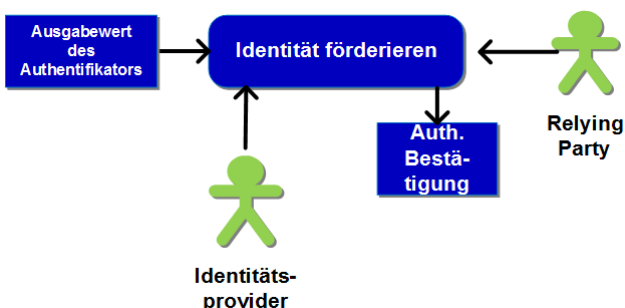


Abbildung 19: Prozess *Identität fördern*

Dieser Prozess wird im ISO 29115 [2], bei STORK [6] und bei eIDAS [7] nicht explizit erwähnt. Er entspricht dem *Federation Process* bei NIST SP 800-63C [18].

Identität fördern	Übergabe einer Authentifizierungsbestätigung vom IdP an die RP
-------------------	--

Tätigkeiten:

- Der IdP überprüft, ob die RP berechtigt ist, eine Authentifizierungsbestätigung anzufordern.
- (optional) IdP holt das Einverständnis des Subjekts ein, die Authentifizierungsbestätigung an den aufrufenden Service (RP) zu übermitteln.
- Der IdP erzeugt Authentifizierungsbestätigung mit Zeitstempel, Signatur und optionaler Verschlüsselung.
- Der IdP übergibt die Authentifizierungsbestätigung an die RP.
- Die RP überprüft die Aktualität und Authentizität der Authentifizierungsbestätigung.

In der folgenden Tabelle werden die hauptsächlichen Sicherheitsanforderungen aufgezeigt, welche zur Bemessung von Kriterien in Zusammenhang mit der Übermittlung einer Authentifizierungsbestätigung relevant sind.

Anforderung	Beschreibung	Mittel	Kriterien
Gesicherte Herkunft und Integrität einer Authentifizierungsbestätigung	Eine RP kann prüfen, ob eine Authentifizierungsbestätigung von einem vertrauenswürdigen IdP ausgestellt wurde, und ob diese zwischenzeitlich in irgendeiner Form manipuliert wurde.	Digitale Signatur wichtiger Informationen durch den Aussteller, welche eine vertrauende Partei (RP) bei Erhalt einer Authentifizierungsbestätigung prüfen kann.	Authentizität der Authentifizierungsbestätigung
Vertraulichkeit der übermittelten Authentifizierungsbestätigung und Identitätsinformationen	Die zu übermittelnden Authentifizierungs- und Identitätsinformationen müssen vor jeglichem Zugriff durch unberechtigte Dritte geschützt werden.	Durch kryptographische Mittel oder durch die Wahl einer gesicherten direkten Kommunikationsverbindung.	Vertraulichkeitsschutz der Authentifizierungsbestätigung Übermittlungsform der Authentifizierungsbestätigung

Anforderung	Beschreibung	Mittel	Kriterien
Überprüfung der Bindung des Abonnenten an die Authentifizierungsbestätigung	Eine RP soll die Möglichkeit haben zu prüfen, ob eine vorliegende Authentifizierungsbestätigung für den Abonnenten vom IdP ausgestellt wurde und damit der Überbringer auch der Abonnent ist.	Kryptographische Bindung einer Authentifizierungsbestätigung an ein Geheimnis, dass nur das sich zuvor authentifizierte Subjekt (Abonnent) als rechtmässiger Überbringer kennt.	Nachweis des Besitzes der Authentifizierungsbestätigung

Tabelle 39: Anforderungen an die Übergabe der Authentifizierungsbestätigung.

Qualitätskriterien:

- Kapitel 7.2.1 Nachweis des Besitzes der Authentifizierungsbestätigung
- Kapitel 7.2.2 Authentizität der Authentifizierungsbestätigung
- Kapitel 7.2.3 Vertraulichkeitsschutz der Authentifizierungsbestätigung
- Kapitel 7.2.4 Übermittlungsform der Authentifizierungsbestätigung

G.2 Subjekt registrieren

Der Prozess *Subjekt registrieren* umfasst alle Aktivitäten zur Überprüfung der Identität eines Subjektes und der Vergabe oder Zuordnung der Authentifizierungsmittel für eine E-Identity (siehe Abbildung 20). Der Prozess besteht aus 2 Teilprozessen: Der Prozess *Identität überprüfen*, bei dem zwischen der Überprüfung von natürlichen und juristischen Personen unterschieden wird, und dem Prozess *Authentifizierungsmittel festlegen*, der zeitlich erst nach erfolgreichem Abschluss des Prozesses *Identität überprüfen* gestartet wird.

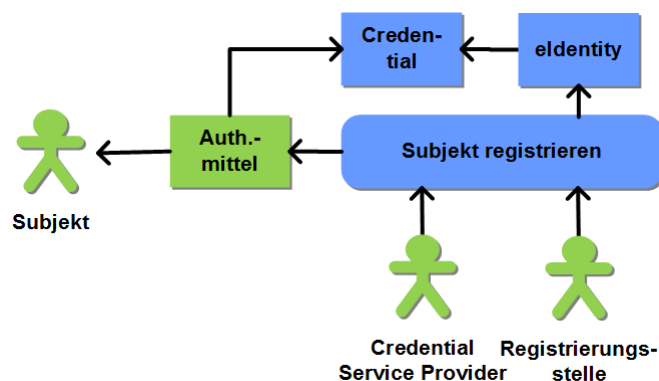


Abbildung 20: Prozess *Subjekt registrieren*

G.2.1 Identität überprüfen natürliche Person

Dieser Prozess entspricht der Phase *Identitätsnachweis und -überprüfung (natürliche Person)* bei eIDAS [7], Kap. 2.1.2.

Identität überprüfen natürliche Person	Überprüfung der Existenz des Subjektes, Feststellung der Identität und Validierung auf der Basis von Beweismitteln durch die RA
--	---

Tätigkeiten:

- Die RA erhebt die erforderlichen Personendaten und sichtet ggf. die Beweismittel.
- (optional) Die RA validiert die erhobenen Daten durch Abgleich mit den Angaben in den Beweismitteln.
- (optional) Die RA entnimmt Adress-Angaben einem geeigneten Beweismittel und überprüft diese.
- (optional) Die Anwesenheit des Subjektes während der Antragstellung werden protokolliert.

Qualitätskriterien:

- Kapitel 5.2.2 Identifikation natürlicher Personen.

G.2.2 Identität überprüfen juristische Person

Dieser Prozess entspricht der Phase *Identitätsnachweis und -überprüfung (juristische Person)* und Verknüpfung von elektronischen Identifizierungsmitteln natürlicher und juristischer Personen bei eIDAS [7], Kap. 2.1.3 und Kap. 2.1.4.

Identität überprüfen juristische Person	Überprüfung der Existenz des Subjektes, Feststellung der Identität und Validierung auf der Basis von Beweismitteln durch die RA, Verknüpfung der natürlichen mit der juristischen Person
---	--

Tätigkeiten:

- Die RA überprüft die Identität der natürlichen Person (siehe Kapitel G.2.1)
- Die RA erhebt die erforderlichen Daten für die juristische Person und sichtet ggf. die Beweismittel.²²
- (optional) Die RA validiert die erhobenen Daten durch Abgleich mit den Angaben in den Beweismitteln.
- (optional) Die RA überprüft die Verknüpfung der natürlichen und juristischen Person durch Abgleich mit Beweismitteln.

²² Werden mehrere natürliche Personen an eine juristische Person geknüpft, muss die Identifikation der juristischen Person nicht in jedem Fall wiederholt werden.

Qualitätskriterien:

- Kapitel 5.2.2 Identifikation natürlicher Personen
- Kapitel 5.2.3 Identifikation juristischer Personen
- Kapitel 5.2.4 Verknüpfung natürliche und juristische Person

G.2.3 Authentifizierungsmittel festlegen

Dieser Prozess entspricht den Phasen *Ausstellung, Auslieferung und Aktivierung* sowie *Verlängerung und Ersetzung* bei eIDAS [7], Kap. 2.2.2 und Kap. 2.2.4. Er wird nur nach erfolgreichem Abschluss des Prozesses *Identität überprüfen* gestartet.

Authentifizierungsmittel festlegen	Der CSP stellt auf der Grundlage der Identitätsprüfung durch die RA ein Authentifizierungsmittel aus und übergibt es dem Subjekt.
------------------------------------	---

Tätigkeiten:

- Der CSP stellt das Authentifizierungsmittel aus oder bindet ein vorhandenes an die E-Identity des Subjektes.
- (optional) Der CSP übergibt dem Subjekt das Authentifizierungsmittel. Diese Tätigkeit entfällt, wenn:
 - das Subjekt das Authentifizierungsmittel selbst bestimmt (z.B. Passwort),
 - das Authentifizierungsmittel von einer dritten Partei ausgestellt und an das Subjekt übergeben wird,
 - der CSP ein Authentifizierungsmittel an die E-Identity des Subjektes bindet, das bereits im Besitz oder unter Kontrolle des Subjektes ist.
- (optional) Das Subjekt aktiviert das Authentifizierungsmittel in einem Aktivierungsprozess.
- (optional) Das Subjekt kann vor Ablauf der Gültigkeit des Authentifizierungsmittels ein neues beim CSP beantragen.

Qualitätskriterien:

- (optional) Kapitel 5.2.5 Übergabe Authentifizierungsmittel
- Kapitel 5.2.6 Verlängerung/Ersetzung Authentifizierungsmittel

G.3 IAM steuern

Der Prozess *IAM steuern* beinhaltet Funktionen zu Führung, Governance, Risk und Compliance im Zusammenhang mit der Authentifizierung von Subjekten (siehe Abbildung 21).

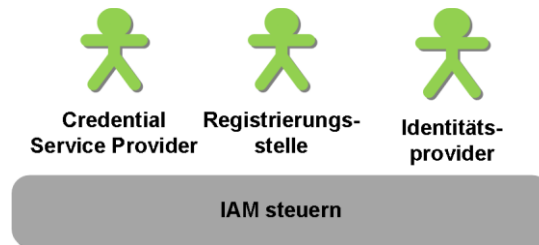


Abbildung 21: Prozess IAM steuern

G.3.1 Vertrauensstufen festlegen

Vertrauensstufen festlegen	Festlegen, wie die Qualität der Authentifizierung eines Subjektes bestimmt, überprüft und verglichen werden kann.
----------------------------	---

Tätigkeiten:

- Qualitätskriterien für das Qualitätsmodell festlegen.
- Qualitätsmodell für die Authentifizierung von Subjekten und dessen Unterteilung in Vertrauensstufen definieren.
- Festlegen, wie die Vertrauensstufen zwischen IdP und RP übermittelt werden.

Anmerkung:

- Der Standard eCH-0170 definiert sowohl Qualitätskriterien wie auch ein Qualitätsmodell mit seinen Vertrauensstufen. Der Standard dient damit als Grundlage für diesen Prozess.

Qualitätskriterien:

- keine

G.3.2 Dienstanbieter festlegen

Dienstanbieter festlegen	Festlegen der IAM-Dienstanbieter des IAM-Systems und Aufbau der Vertrauensbeziehungen zwischen diesen
--------------------------	---

Tätigkeiten:

- Festlegung der Organisation (Stakeholder) sowie ihrer Beziehung untereinander (Zusammenarbeit)
- Definieren der Vertrauensbeziehungen zwischen den Stakeholdern
- Pflege und Austausch der Metadaten

Qualitätskriterien:

- Kapitel 6.2.1 Aufsicht
- Kapitel 6.2.2 Haftung

G.3.3 Steuerungsprozesse festlegen

Steuerungsprozesse festlegen	Definition der Nachvollziehbarkeit aller Prozesse. Festlegen von Prozessen und Regeln für die Authentifizierung ergänzte Prozesse (Revozierung, Ersatz, etc.)
------------------------------	--

Tätigkeiten:

- Definition der Nachvollziehbarkeit der gesamten Prozessabläufe (z.B. das Ablegen der relevanten Dokumente) und deren Audit.
 - Festlegen der Aufbewahrungsfristen der relevanten Daten für jeden Prozessschritt (siehe auch ISO 29115 [2] Kapitel „Record-keeping/recording“)
- Festlegen der Prozesse und Regeln für Revozierung/Deprovisionierung von Authentifizierungsmitteln
- Festlegen der Prozesse und Regeln für den Ersatz von Authentifizierungsmitteln
- Festlegen der Verfügbarkeit (Service Level Agreements) der einzelnen Dienstanbieter
- Festlegen des Lebenszyklus einer Verknüpfung von natürlichen und juristischen Personen (z.B. Aktivierung, Aussetzung, Erneuerung, Widerruf) (siehe auch eIDAS 2015/1502 [7], Abschnitt 2.1.4)
- Maturitätsmodell und Maturitätsstufen festlegen

Anmerkung:

- Der Standard eCH-0172 [22] definiert IAM Maturitätsstufen für unter anderem die Einstufung für die Prozess-Maturität der Steuerung und wird ergänzt durch ein Hilfsmittel mit konkreten Fragen zur Bestimmung dieser Maturität. Es gibt auch andere Maturitätsmodelle die in Frage kommen könnten, aber die sind eher generisch, wie z.B. CMMI for Services v1.3 und die SCAMPI Beurteilung für dieses Modell.

Qualitätskriterien:

- Kapitel 6.2.1 Aufsicht
- Kapitel 6.2.3 Maturität

G.3.4 Risiko einschätzen und behandeln

Risiko einschätzen und behandeln	Definition der Abläufe zur Risikobehandlung (Risikoeinschätzung und -adressierung)
----------------------------------	--

Tätigkeiten nach eCH-0107 [4], Kap.6.3.2:

- Schutzbedarfsanalyse: Die Schutzbedarfsanalyse gewährleistet angepasste Sicherheitsanforderungen (so viel Sicherheit wie nötig, nicht so viel wie möglich).
- Durchführen und Festhalten einer Risikoanalyse.
- Erstellen eines Informations- und Datenschutzkonzepts.
- Kontinuierliche Verbesserung des Sicherheitskonzepts: wird in ISO 27001 definiert. Aufgrund der aktuellen Situation werden periodisch Massnahmen geplant, umgesetzt, überprüft und optimiert. Dieser Verbesserungsprozess ist ein bewährtes und effizientes Vorgehen und heute ein Kernelement von Best Practice.
- [OPTIONAL] Abstützung des Risikomanagements auf ein Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001.
- [OPTIONAL] Abstützung des Risikomanagements auf ein Framework wie COBIT.

Qualitätskriterien:

Kapitel 6.2.2 Haftung

Kapitel 6.2.3 Maturität

Anhang H - Anforderungen an Authentifizierungsmittel

In diesem Anhang werden die gängigsten Authentifizierungsmittel kurz beschrieben.

Jedes dieser Authentifizierungsmittel muss bestimmte Anforderungen erfüllen, um den Kriterien der Vertrauensstufen gerecht zu werden. Eine Definition dieser Anforderungen ist nicht in diesem Standard enthalten, dafür wird auf gängige Standards und Empfehlungen verwiesen.

Weitere Informationen wie die Authentifizierungsmittel angewendet werden können, befinden sich in NIST SP 800-63B [15] Kapitel 10.2.

H.1 Memorized Secrets

Typ: Single-Factor Authenticator

Synonym: gespeichertes Geheimnis

Memorized Secrets, im Allgemeinen als Passwort oder PIN bezeichnen, sind geheim gehaltene Werte, die meist vom Benutzer gewählt und in seinem Gedächtnis oder an einem anderen sicheren Aufbewahrungsort gespeichert werden. Sie müssen über eine genügend hohe Komplexität und Zufälligkeit verfügen, um von einem Angreifer nicht erraten oder auf sonstige Art und Weise berechnet werden können. *Passwort Policies* legen die Regeln zur Länge, Komplexität, Zeichenmix, Ablaufdauer und Wiederverwendung fest und bestimmen somit die Stärke des Memorized Secrets.

Beispiele: Passwort oder PIN

Detaillierte Anforderungen sind in den folgenden Quellen beschrieben:

- Siehe auch NIST SP 800-63B [15], Kapitel 5.1.1 und Appendix A.

H.2 Look-Up Secrets

Typ: Single-Factor Authenticator

Synonym: Nachschlagbares Geheimnis

Look-Up Secrets enthalten eine Liste von (alpha-)numerischen Werten, die zuvor zwischen dem Subjekt und dem Credential Service Provider (CSP) ausgetauscht wurden. Zur Authentifizierung muss der Benutzer einen bestimmten Wert aus dieser Liste angeben.

Die ausgetauschten Werte müssen zufällig generiert werden. Sie dürfen nur einmal benutzt werden und eine genügend hohe Entropie besitzen.

Beispiele: Strichlisten (engl. *tally sheet*) oder TAN-Blöcke

Detaillierte Anforderungen sind in den folgenden Quellen beschrieben:

- Siehe auch NIST SP 800-63B [15], Kapitel 5.1.2.

H.3 Out of Band Authenticators

Typ: Single-Factor Authenticator

Synonym: Externer Kanal

Out of Band ist ein physisches Gerät, welches eindeutig adressierbar sein muss und welches Geheimnisse, die vom CSP gewählt werden, zur einmaligen Verwendung empfangen kann.

Das Gerät ist im Besitz des Subjekts und sollte über einen eigenen, privaten Kanal angesprochen werden können, welcher unabhängig vom primären Kanal für den zweiten Authentifizierungsfaktor genutzt wird.

Der Out of Band Authenticator kann auf 2 verschiedene Arten funktionieren:

1. Das Subjekt präsentiert das Geheimnis, welches er über den zweiten Kanal erhalten hat dem authentifizierenden Dienst über den primären Kommunikationskanal.
2. Das Subjekt sendet dem authentifizierenden Dienst eine Antwort direkt über den zweiten Kommunikationskanal zurück.

Beispiele: Handy/Smartphone mit Mobilnummer und SMS-TAN-Verfahren

Detaillierte Anforderungen sind in den folgenden Quellen beschrieben:

- Siehe auch NIST SP 800-63B [15], Kapitel 5.1.3.

H.4 OTP Devices

Typ: je nach Implementierung: Single-Factor Authenticator oder (hardware based) Multi-Factor Authenticator

Synonym: Einmal-Passwort Generator

Ein Single-Factor OTP Device ist eine Software oder ein Gerät, welches nach einem bestimmten Algorithmus (pro Ereignis, Zeitbasiert) spontan ein Einmal-Passwort generiert.

Auf dem Gerät oder in der Applikation befindet sich ein eingebettetes Geheimnis (Schlüssel), welches für die Generierung des einmal verwendbaren Passwortes genutzt wird. Als Eingabewert kann die aktuelle Zeit oder ein sich inkrementierender Zähler dienen.

Beispiele: SecureID-Token, Google Authenticator, SafeNet mobilePass

Ein Multi-Factor OTP Device erfordert zur Aktivierung des Algorithmus einen zweiten Faktor (Wissen oder Eigenschaft) auf dem Gerät. Dieser zweite Authentifizierungsfaktor kann ein integriertes Keypad, ein biometrischer Sensor (z.B. Fingerabdruck) oder eine direkte Computer Schnittstelle (z.B. USB) sein.

Beispiele: SecureID-Token mit Keypad, HID ActivID Token

Detaillierte Anforderungen sind in den folgenden Quellen beschrieben:

- Siehe auch NIST SP 800-63B [15], Kapitel 5.1.4 (single-factor) und 5.1.5 (multi-factor).

H.5 Single Factor Cryptographic Devices

Typ: Single-Factor Authenticator

Synonym: Einfaktor Verschlüsselungsgeräte

Ein *single-factor cryptographic device* ist ein physisches Gerät, welches kryptographische Berechnungen anhand einer dem Gerät gegebenen Eingabe durchführt. Das Gerät benötigt dazu keine Aktivierung über einen zweiten Authentifizierungsfaktor. Das Gerät benutzt zur Generierung des Ausgabe-werts in ihm gespeicherte symmetrische oder asymmetrische Schlüssel. Die Authentifizierung wird durch den Besitznachweis des Gerätes vollbracht.

Ein *single-factor cryptographic device* enthält auch eingebettete Software. Der Credential Service Provider (CSP) ist für diese zuständig und kontrolliert die Art und Weise, wie die Software funktioniert.

Beispiel: Yubikey U2F

Detaillierte Anforderungen sind in den folgenden Quellen beschrieben:

- Siehe auch NIST SP 800-63B [15], Kapitel 5.1.6.

H.6 Multi-Factor Cryptographic Software

Typ: Multi-Factor Authenticator

Synonym: Multifaktor Verschlüsselungs-Software

Ein *multi-factor software cryptographic authenticator* ist ein kryptographischer Schlüssel, welcher auf einer Festplatte oder ähnlichem Medium gespeichert ist. Ein solcher Authenticator muss mit einem zweiten Authentifizierungsfaktor aktiviert werden. Die Authentifizierung wird durch den Besitznachweis und Kontrolle des kryptographischen Schlüssels vollbracht. Dieser Authenticator kombiniert 2 Authentifizierungsfaktoren: Besitz (kryptographischer Schlüssel) mit einem weiteren Geheimnis (Besitz oder Eigenschaft), das zur Aktivierung verwendet wird.

Beispiel: Soft-Token (PKCS#12 Datei)

Detaillierte Anforderungen sind in den folgenden Quellen beschrieben:

- Siehe auch NIST SP 800-63B [15], Kapitel 5.1.7.

H.7 Multi-Factor Cryptographic Devices

Typ: hardware based Multi-Factor Authenticator

Synonym: Multifaktor Verschlüsselungs-Geräte

Ein *multi-factor cryptographic device* ist ein physisches Gerät, welches einen geschützten kryptographischen Schlüssel enthält. Es muss mit einem zweiten Authentifizierungsfaktor (Wissen oder Eigenschaft) aktiviert werden. Die Authentifizierung wird durch den Besitznachweis und Kontrolle des kryptographischen Schlüssels vollbracht.

Ein *multifactor cryptographic device* enthält auch eingebettete Software. Der Credential Service Provider (CSP) ist für diese zuständig und kontrolliert die Art und Weise, wie die Software funktioniert.

Beispiele: SmartCard, SuisseID

Detaillierte Anforderungen sind in den folgenden Quellen beschrieben:

- Siehe auch NIST SP 800-63B [15], Kapitel 5.1.8.

Anhang I - Anforderungen an den Faktor Validierung der Angaben

In diesem Anhang werden die zusätzlichen Anforderungen an den Faktor *Validierung der Angaben* aufgeführt. Für detailliertere Anforderungen wird auf gängige Standards und Empfehlungen verwiesen.

Die Qualität der Validierung wird durch verschiedene Faktoren beeinflusst. Das sind u.a.:

- Ausbildungsstand der Überprüfer,
- Verfügbarkeit von gefälschten Dokumenten,
- Komplexität des Rechtsrahmens bei der Verwendung verschiedenster Dokumententypen,
- Verwendung von Geräten zur automatisierten Überprüfung von Dokumenten, z.B. bei elektronischen Reisepässen oder Identitätskarten.

Detaillierte Anforderungen sind in den folgenden Quellen beschrieben:

- NIST Measuring Strength of Identity Proofing [24], Kapitel 3.1.
- NIST 800-63A [16], Kapitel 5.4.3 detailliert die Anforderungen an die Überprüfung bei einer *virtual-in-person* Anwesenheit.
- eIDAS 2015/1502 [7] definiert in Kapitel 2.4.5 die Anforderungen an Einrichtungen und Personal, die für alle Sicherheitsniveaus gelten.