eCH-0170 Qualitätsmodell für elektronische Identitäten

Name	eID Qualitätsmodell
Standard-Nummer	eCH-0170
Kategorie	Standard
Reifegrad	experimentell; implementiert; verbreitet
Version	1.0
Status	Aufgehoben
Beschluss am	2017-09-06
Ausgabedatum	2017-09-13
Ersetzt Standard	
Sprachen	Deutsch (original), Französisch
Autoren	Fachgruppe IAM Martin Topfel, Berner Fachhochschule, martin.topfel@bfh.ch Thomas Jarchow, Berner Fachhochschule, thomas.jarchow@bfh.ch
Herausgeber / Vertrieb	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Zusammenfassung

Dieser Standard richtet sich an die Einführer der eID.

Das eID Qualitätsmodell bewertet eID Lösungen anhand von fünf Kriterien und drei Faktoren. Auf dieser Basis werden die eID Lösungen in vier Qualitätsstufen unterteilt. Mit der Einordung der eID Lösungen in vier Qualitätsstufen wird ersichtlich, wie viel Vertrauen diesen entgegengebracht werden kann. Die Kriterien des Qualitätsmodells lassen sich der Phase Registration der elektronischen Identität und der Phase der Anwendung zuordnen.

Als Grundlage für dieses Qualitätsmodell dient das Qualitätsmodell für elektronische Identitäten von STORK. Dadurch bleibt die Kompatibilität bestehen und europäische und schweizerische eID Lösungen können verglichen werden.

Inhaltsverzeichnis

1 Status des Dokuments

Aufgehoben: Das Dokument wurde von eCH zurückgezogen. Er darf nicht mehr genutzt werden.

2 Einleitung

2.1 Ausgangslage

Elektronische Identitäten spielen in der heutigen Gesellschaft eine immer wichtigere Rolle. Eine herausragende Rolle dabei haben die vertrauenswürdigen elektronischen Identitäten, da sich das Internet als bedeutende Plattform für geschäftliche Interaktionen zwischen Personen, Unternehmen und dem Staat etabliert hat.[1]

In Europa wurden bereits in vielen Staaten Lösungen zur elektronischen Identifizierung geschaffen. So gibt es beispielsweise die Bürgerkarte in Österreich, die SuisseID in der Schweiz, die carta d'identità elettronica in Italien, die BankID in Schweden, der elektronische Personalausweis in Deutschland, die ID-card in Estland oder die VITALE Carte und die Carte professionnelle de la Santé (CPS) in Frankreich. Die europäische Kommission hat diese fragmentierte Situation als problematisch erkannt und zur länderübergreifenden Identifizierung von Personen das Grossprojekt STORK ins Leben gerufen. Ziel von STORK ist es, die unterschiedlichen nationalen Lösungen miteinander kompatibel zu machen und so die Interoperabilität zwischen den verschiedenen europäischen eID-Lösungen zu ermöglichen. Dazu wurde unter anderem ein Qualitätsmodell mit vier Qualitätsstufen geschaffen. Es erlaubt verschiedene Lösungen hinsichtlich ihrer Qualitäten miteinander zu vergleichen. Ein solcher Vergleich erlaubt die grenzübergreifende Anerkennung und Anwendung von eID-Lösungen, weil damit qualifiziert wird, wie hoch die Qualität einer Authentifizierung, resp. wie vertrauenswürdig die einzelne eID Lösung ist.

Für die Schweiz wurde bis heute kein eID Qualitätsmodell definiert, das den strukturierten Vergleich der Güte verschiedener eID-Lösungen erlaubt. Es besteht daher Handlungsbedarf, ein solches Modell auch in der Schweiz zu etablieren.

Durch das Fehlen eines Qualitätsmodelles ist es in der Schweiz schwierig, eID-lösungen miteinander zu vergleichen. Ein Vergleich mit standardisierten Kriterien stiftet einerseits den Unternehmen und andererseits den Konsumenten einen Nutzen. Die Vergleichbarkeit unterstützt bei Entscheidungen, welche Lösung am besten zu den jeweiligen Anforderungen passt.

Ausserdem können Beteiligte mit einem ihnen bekannten und mit der EU kompatiblen Qualitätsmodell auch besser ausländische eID Lösungen beurteilen. Damit ist es für sie einfacher, fremde eIDs zu akzeptieren und damit ihren Absatzmarkt zu vergrössern.

Die Standardisierung des Qualitätsmodells erlaubt zudem, eigene Erkenntnisse, die für den Schweizer Markt wichtig sind, bei der Weiterentwicklung des Modells auf europäischer Ebene einzubringen und so einen gewissen Einfluss darauf zu nehmen.

---

[1] Im Folgenden wird der Begriff „elektronische Identität" verwendet, da er wesentlich anschaulicher ist, als der technisch korrekte Begriff der elektronischen Authentifizierung. Die heute üblichen virtuellen Verfahren erlauben lediglich die Authentifizierung und schliessen die Möglichkeit von Handlungen durch Stellvertretungen nicht aus, wozu die Stellvertretung natürlich über die nötigen Credentials verfügen muss.

2.2 Ziele

Der hier vorliegende eCH-Standard definiert ein eID-Qualitätsmodell (QM) zur Bewertung und Einstufung elektronischer Identitäten. Dazu werden die folgenden Ziele festgelegt:

- Beschreibung und Definition eines Qualitätsmodells zur Bewertung und zum Vergleich von elektronischen Identitätslösungen
- Beschreibung und Definition des Vorgehens, wie das Qualitätsmodell zu erstellen und einzusetzen ist
- Beschreibung und Definition der im Modell verwendeten Begriffe
- praxisrelevante und konkrete Beispiele für die Anwendung des Modelles
- Bewahrung der Kompatibilität mit den europäischen Standards, resp. klares Aufzeigen und Begründen von Abweichungen

2.3 STORK

Im Rahmen des Large Scale Pilot STORK wurde ein Qualitätsmodell zur Bewertung und zum Vergleich von elektronischen Identitäten definiert. Der hier vorliegende eCH-Standard basiert auf dem in STORK beschriebenen Quality of Authentication Assurance Model (QAA) und passt dieses an die Situation der Schweiz an.

2.4 Vorteile

Mit dem in diesem Standard vorgestellten Verfahren können elektronische Identitätslösungen hinsichtlich ihrer Qualität unterschieden und eingeteilt werden. Dabei wird ein strukturierter Kriterienkatalog zur Bewertung verwendet.

Da sich das CH angepasst Qualitätsmodell an der EU-Lösung STORK orientiert, sind resultierenden Bewertungen auch mit europäischen Identitätslösungen vergleichbar und dienen damit als Grundlage für künftige Interoperabilität.

Zudem kann auf der Erfahrung aus dem STORK Projekt profitiert und aufgebaut werden.

3 Qualitätsmodell

3.1 Qualitätsstufen

Ein Ausweis muss verschiedenen, durch seine Anwendung bestimmten Anforderungen genügen. So muss beispielsweise ein Reisepass die zuverlässige Identifikation seines Trägers ermöglichen, fälschungssicher sein, durch ein weltweit anerkanntes Vorgehen ausgestellt werden, eine bestimmte Aktualität haben usw. Diese Eigenschaften zusammen geben dem Reisepass eine gewisse Vertrauenswürdigkeit als Identifikationsmittel. Andere Ausweise und Ausweisformen müssen anderen Anforderungen genügen, was zu verschiedenen Qualitäten führt, die in verschiedene Qualitätsstufen kategorisiert werden.

Was für die physischen Ausweise gilt, gilt auch für virtuelle Ausweise. Dabei handelt es sich streng genommen um elektronische Verfahren zur Authentifizierung (und nicht der Identifizierung)[2].

Das QM erlaubt, die Qualität der Herstellung als auch die Verfahren beim Einsatz elektronischer Identitäten zu prüfen und zu bewerten. Damit schafft das QM ein Mass der Güte für elektronische Identifikationsverfahren, mit welchem das Vertrauen in die jeweiligen Verfahren beurteilt und somit gefördert werden kann. Das QM unterscheidet vier Qualitätsstufen (siehe Tabelle 1).

QM Stufe	Beschreibung
1	kein oder minimales Vertrauen
2	geringes Vertrauen
3	beträchtliches Vertrauen
4	hohes Vertrauen

Tabelle 1: Die 4 Qualitätsstufen des QM

Die QM Stufe 1 ist die niedrigste Qualitätsstufe, die beschrieben wird. In diese Kategorie fallen alle eID-Lösungen, die nur geringes oder kein Vertrauen in die Identität benötigen und daher aus Falschangaben keine negativen Konsequenzen folgen. Zudem ist es möglich, eine virtuelle Identität zu erstellen, hinter welcher man anonym bleibt.

Elektronische Identitäten, welche mit der QM Stufe 2 bewertet werden, haben eine minimal identifizierte Person als Grundlage. Es wird vorausgesetzt, dass eine sichere Art der Authentisierung möglich ist und dass Credentials einem Standard folgen.

QM Stufe 3 setzt voraus, dass die Identität so verifiziert wurde, dass die nachgewiesene elektronische Identität mit einer hohen Gewissheit das Subjekt repräsentiert. Institute, welche elektronische Identitäten der QM Stufe 3 ausstellen, müssen von einer Regierungsstelle überwacht und akkreditiert werden.

Die QM Stufe 4 beschreibt die höchste Vertrauensstufe, welche eine elektronische Identität erhalten kann. Das Subjekt, das hinter dieser Identität steht, muss sich mindestens einmal physisch identifizieren lassen. Zudem muss der ausgestellte Ausweis die höchstmögliche Sicherheit bieten, welche heute ein Hardware Zertifikat darstellt. Aussteller von Ausweisen dieser Stufe werden überwacht und akkreditiert und müssen die Vorgaben des Bundesgesetzes über die elektronische Signatur (ZertES) erfüllen.

[2] Der umgangssprachliche Ausdruck der digitalen Identifizierung wird durch den Umstand gerechtfertigt, dass im Alltag die äussere Identität eines Menschen nur von aussen her, durch sein „Umfeld“ bestätigt werden kann. Sobald der Mensch „ohne seine Papiere“ nicht mehr sagt, wer er ist, und ihn keiner erkennt, wird es kompliziert.

3.2 Struktur

Das QM unterscheidet die Phase der „Registrierung“, welche die Prozesse, Pflichten und Verfahren bei der Erstellung der eID bewertet und die Phase „Anwendung der eID“, welche die technischen und organisatorischen Prozesse bei der Anwendung der eID beschreibt.[3]

Die Kriterien der Registrierungsphase umfassen die Vorgänge bei Ausgabe und Erstellung der elektronischen Identität. Die Kriterien der Anwendungsphase bewerten die Verfahren, welche bei der Anwendung der elektronischen Identität zum Einsatz kommen (vgl. Abbildung 1).

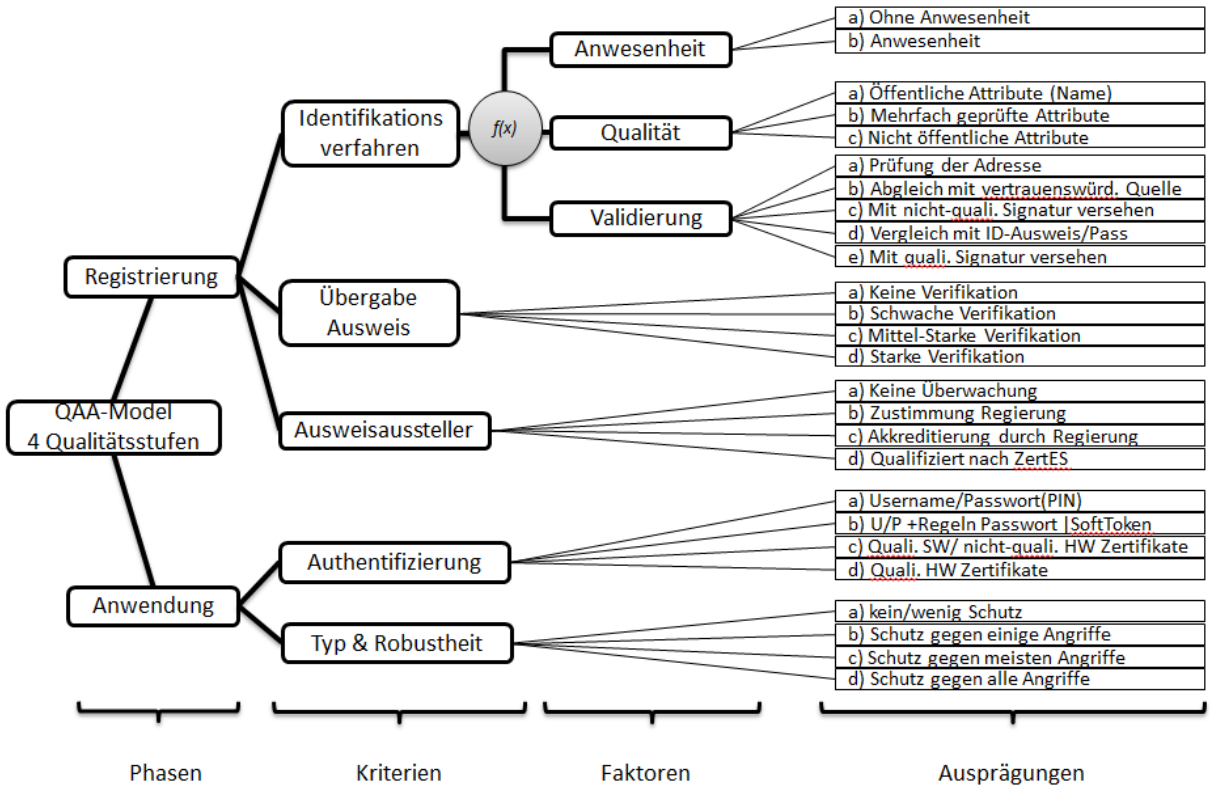

Abbildung 1: Phasen, Kriterien, Faktoren und Ausprägungen des QM

3.3 Regeln

Im QM wird die resultierende Qualitätsstufe immer durch die tiefste Ausprägung eines Kriteriums bestimmt. [MUST]

[3] Das Modell berücksichtigt zurzeit nicht, wie die Vorgänge bei der Wiederherstellung von Credentials organisiert sind (z.B. Passwort vergessen), diese müssen ähnlich stringent sein, wie bei der Erstellung der eID. Auch beschreibt das Modell nicht, wie verschiedene eID Lösungen interagieren und gegeneinander ausgespielt werden können, resp. welche Vorkehrungen bei partieller Identifizierung getroffen werden, damit verhindert wird wie aus mehrere partiellen eID nicht plötzlich eine ganze eID gemacht werden kann.

4 Beschreibung der Kriterien

Die in diesem Kapitel beschriebenen Anforderungen sind minimale Bedingungen an die QM Stufen und dürfen nicht unterschritten werden. [MUST]

Höhere Anforderungen sind erlaubt.

4.1 Identifikationsverfahren (Identification Procedure, ID)

Das Kriterium Identifkationsverfahren beschreibt, wie der Antragssteller identifiziert wird. Es fasst, nach dem in Tabelle 2 dargestellten Schema die drei Faktoren „Anwesenheit“ (Physical Presence, PP), „Qualität der Angaben“ (Quality of Assertion, QoA) und „Validierung der An-gaben“ (Validation of Assertion, VoA) zusammen.

Faktor	ID1	ID2	ID3	ID3	ID4
Anwesenheit	PP.a	PP.a	PP.b	PP.a	PP.b
Qualität der Angaben	QoA.a	QoA.b	QoA.b	QoA.c	QoA.c
Validierung der Angaben	VoA.a	VoA.b	VoA.c	VoA.d	VoA.d

Tabelle 2: Bestimmung der Ausprägung des Identifikationsprozederes aus den drei Faktoren

4.1.1 Faktor: Anwesenheit (Physical Presence, PP)

Der Faktor Anwesenheit (Physical Present, PP) hält fest, ob der Antragssteller während der Registrierung physisch anwesend sein muss oder nicht.

Ausprägung	Erklärung
PP.a	keine Anwesenheit erforderlich
PP.b	Anwesenheit während der Registrierung erforderlich

Tabelle 3: Ausprägungen des Faktors Anwesenheit

4.1.2 Faktor: Qualität der Angaben (Quality of Assertions, QoA)

Der Faktor Qualität der Angaben (Quality of Assertions, QoA) beschreibt die Öffentlichkeit und die Anzahl Quellen der vom Antragssteller angegebenen Daten.

Die Angabe von öffentlich bekannten und leicht zugänglichen Daten (z.B. Adresse aus Telefonbuch) trägt in geringerem Masse zur Identifizierung bei, als die Angabe von privaten Daten, welche nur dem Antragssteller oder einem eng eingegrenzten Personenkreis bekannt sind (z.B. Mädchenname der Mutter). Zudem kann man davon ausgehen, dass die Korrektheit der Angaben grösser wird, je mehr (unabhängige) Datenquellen den gleichen Sachverhalt bestätigen.

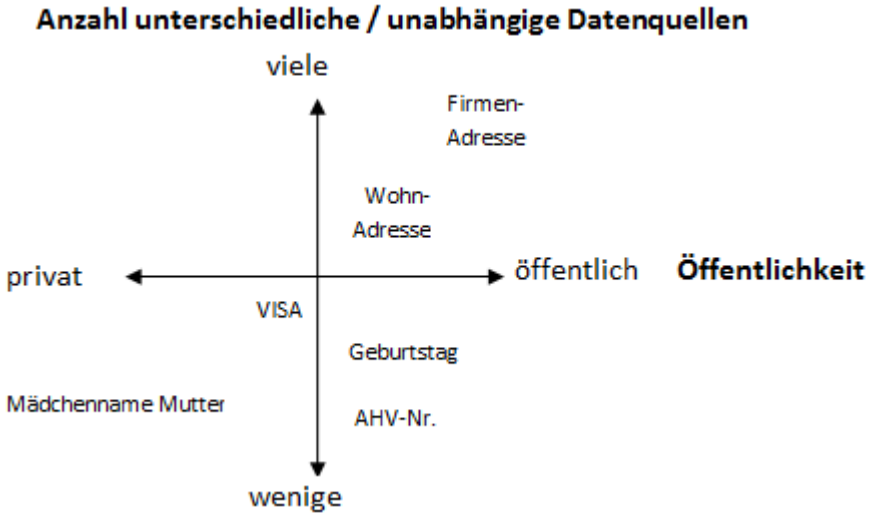

Abbildung 2: Dimensionen des Faktors Qualität der Angabe

Beispiele für die öffentliche Verfügbarkeit sind Name und Adresse, die in diesem Fall sehr wahrscheinlich öffentlich zugänglich sind, oder die Passnummer, welche üblicherweise nur die ausstellende Behörde und die besitzende Person kennen. Für diesen Faktor sind die Ausprägungen in Tabelle 5 dargestellt.

Kategorie	Erklärung
QoA.a	einmalige Erfassung von möglicherweise öffentlichen Daten, keine eindeutige Identifikation der Identität auf der Basis dieser Daten möglich
QoA.b	mehrmalige Erfassung von möglicherweise öffentlichen Daten, wie Namen, Vornamen oder Geburtstag, welche eine Identität eindeutigen identifizieren
QoA.c	mindestens eine Erfassung von nicht öffentlichen Daten, welche zu einer eindeutigen Identität führen

Tabelle 4: Ausprägungen des Faktors Qualität der Angabe

4.1.3 Faktor: Validierung der Angaben (Validation of Assertions, VoA)

Der Faktor Validierung der Angaben (Validation of Assertion, VoA) beschreibt mit fünf Ausprägungen, wie die Korrektheit der bei der Antragsstellung angegebenen Daten überprüft wird.

Kategorie	Erklärung
VoA.a	Die angegebene E-Mail Adresse wird auf ihre Existenz überprüft. Es erfolgt keine weitere Prüfung der Identität.
VoA.b	Die angegebenen Daten werden mit einer vertrauenswürdigen Quelle oder einer Identitätsdatenbank abgeglichen.
VoA.c	Die angegebenen Daten sind mindestens mit einer fortgeschrittenen elektronischen Signatur nach eCH-0048 signiert.
VoA.d	Die angegebenen Daten werden mit einem offiziellen Ausweisdokument abgeglichen (Reisepass, Identitätskarte, Führerausweis).
VoA.e	Die angegebenen Daten müssen mit einer qualifizierten digitalen Signatur versehen sein, welche von einem Certificate Service Provider (CSP) verifiziert ist.

Tabelle 5: Ausprägungen des Faktors Validierung der Angaben

4.2 Übergabe digitaler Ausweis (Credential Issuing Process, IC)

Das Kriterium Übergabe digitaler Ausweis (Credential Issuing Process, IC) bewertet, wie stark der Empfänger bei der Übergabe des elektronischen Ausweises verifiziert wird.[4]

Ein hoher IC Wert bedeutete, dass bei der Übergabe die tatsächliche Identität des Empfängers festgestellt wurde. Die entsprechenden Ausprägungen sind in Tabelle 6 beschrieben.

IC Stufe	Anforderungen
IC1	Keine Verifikation.
IC2	Leichte Verifikation des Empfängers: • Benutzername und Passwort 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 Ausweises, wird an die während der Registration genannte E-Mail Adresse versendet. Der Gültigkeit des Links verfällt nach einer gewissen Zeit (z.B. 24 Stunden).
IC3	Mittlere Verifikation des Empfängers: • Ausweis wird per eingeschriebenem Brief an die während der Registration genannte und überprüfte Adresse gesendet. • Ausweis wird direkt nach der Verifikation mittels qualifizierter Signatur (ID Phase) erstellt und von der antragstellenden Person heruntergeladen. • Ausweis wird nach der Eingabe eines Passwortes, welches physisch bei der Registration übergeben wurde, heruntergeladen.
IC4	Starke Verifikation des Empfängers: • Ausweis wird der Person persönlich übergeben. • Ausweis wird der Person zugesendet und erst nach der Validierung derer Identität aktiviert.

Tabelle 6: Ausprägungen des Kriteriums Übergabe digitaler Ausweis

[4] Der elektronische (oder digitale) Ausweis wird in diesem Dokument als Übersetzung des englischen Credentials verstanden. Ein elektronischer Ausweis besteht in einer einfachen Form aus Benutzername und Password, kann aber auch weitere oder andere Merkmale besitzen, wie z.B. ein OneTime Passwort, ein Zertifikat, Smartcard oder einen PIN.

4.3 Ausweisaussteller (Entity Issuing Credentials, IE)

Das Kriterium Ausweisaussteller (Entity Issuing Credential, IE) bewertet die Vertrauenswürdigkeit der Institution, welche den elektronischen Ausweis ausstellt und verwaltet.

IE Stufe	Anforderungen
IE1	keine Überwachung oder Akkreditierung durch eine Regierungsstelle
IE2	mit Zustimmung einer Regierungsstelle
IE3	mit Überwachung oder Akkreditierung einer Regierungsstelle
IE4	qualifiziert nach ZertES

Tabelle 7: Ausprägungen des Kriteriums Ausweisaussteller

4.4 Ausweisart (Type and Robustness of the Credential, RC)

Um zu bewerten, wie robust und von welchem Typ das angegebene Identitätsmerkmal ist, wird dieses in verschiedene Typenklassen unterteilt und den Qualitätsstufen von Type and Robustness of the Credential zugewiesen. Es gibt die in Tabelle 8 beschrieben Typen und RC Stufen.

RC Stufe	Typen	Beschreibung
RC1	Passwort oder PIN	Passwörter oder PINs ohne Vorgaben von Länge, Wiederverwendung, Zeichenmixtur etc.
RC2	Passwort oder PIN nach Vorgaben	Passwörter oder PINs mit Vorgaben an Länge, Wiederverwendung, Zeichenmixtur etc.
RC3	Software Zertifikate oder Einmalpasswort Geräte	kryptografischer Software Schlüssel (SoftToken), welcher durch den Besitz und das Kennen des dazugehörenden Kennworts überprüft werden kann (z.B. PKCS#12 Datei) Geräte, die ein einmaliges Kennwort (OTP – OneTime Password) generieren (z.B. RSA Secure-ID)
	Qualifizierte Software Zertifikate	Software Zertifikate, welche den Anforderungen von ZertES genügen
	Hardware Zertifikate	kryptografischer Hardware Schlüssel, welcher durch den Besitz und das Kennen des dazugehörenden Kennworts überprüft werden kann (z.B. Smartcard)
RC4	Qualifizierte Hardware Zertifikate	Hardware Zertifikate, welche den Anforderungen von ZertES genügen

Tabelle 8: Anforderungen des Qualitätskriteriums Ausweisart

Kriterien für die Einteilung der Identitätsmerkmale sind Massnahmen gegen das Kopieren des Identitätsmerkmals, das Benützen von verschiedenen Medienkanälen und die Konformität zum erwähnten Bundesgesetz.

4.5 Sicherheit des Authentifizierungsverfahrens (Security of the Authentication Mechanism, AM)

Das Kriterium Sicherheit des Authentifizierungsverfahrens (Security of the Authentication Mechanism, AM) bewertet die Absicherung des Identifikationsverfahrens gegen Identitätsdiebstahl. Dabei werden nur Angriffe berücksichtigt, die sich direkt auf das Authentisierungsverfahren richten (siehe Tabelle 9).

Angriff	Beschreibung
Raten (Guessing)	Passwörter, welche den Kommunikationskanal oder Zertifikate schützen, werden versucht zu erraten. Hilfsmittel sind dabei vordefinierte Listen (Dictionary Attack) und das Durchprobieren jeder Möglichkeit (Brute Force Attack).
Mithören (Eavesdropping)	Die Kommunikation wird mitgehört und analysiert. Anschliessend werden die Ergebnisse der Analyse für weitere Angriffe verwendet. Ziel ist meist das Mithören von Benutzernamen und Passwörter.
Entführen (Hijacking)	Entführen einer schon bestehenden Verbindung oder Kommunikation, um Zugriff auf sensible Daten zu bekommen
Wiederholen (Repeating)	Nachrichten werden wiederholt oder verspätet gesendet, um Zugriff auf sensible Daten zu bekommen
Weiterleiten (Man-in-the-middle)	Der Angreifer fängt jegliche Kommunikation von zwei Gesprächspartnern ab und leitet sie gegenseitig weiter. So hat er Zugriff auf alle Daten, die gesendet werden, ohne Wissen der Opfer.

Tabelle 9: Berücksichtigte Angriffe für Identitätsdiebstahl

Angriffe, die auf Social Engineering beruhen, wie zum Beispiel das Datensammeln in sozialen Netzwerken oder das Auswerten von Daten auf entsorgten Datenträgern, werden bei diesem Qualitätskriterium nicht berücksichtigt.

Da sich die Technik laufend weiterentwickelt, ist es wichtig zu wissen, dass die Bewertungen jeweils auf den momentanen Stand der Technik beruhen und somit nicht beliebig lange aktuell sind.

Um die Robustheit zu testen, gibt es zwei Möglichkeiten. Erstens, ein System besteht seit längerer Zeit, ohne dass ein Angriff bekannt geworden ist. Angriffe wie Entführen oder Weiterleiten sind jedoch sehr schwierig nachzuweisen oder überhaupt zu bemerken und werden daher von dieser „de facto“ Testmethode nicht abgedeckt.

Die zweite Möglichkeit besteht aus dem Testen und Belegen und somit dem Ausschliessen eines möglichen Angriffs. Nur auf Stufe AM4 wird die zweite Methode angewendet.

AM Stufe	Anforderungen
AM1	Authentisierungsverfahren bietet wenig oder keinen Schutz vor genannten Angriffen.
AM2	Authentisierungsverfahren bietet Schutz gegen einige der genannten Angriffe.
AM3	Authentisierungsverfahren bietet Schutz gegen die meisten der genannten Angriffe.
AM4	Authentisierungsverfahren bietet Schutz gegen alle genannten Angriffe. Vergleichbar mit EAL4+[5].

Tabelle 10: Anforderungen des Qualitätskriteriums Sicherheit des Authentifizierungsverfahrens

[5] (CCRA, 2012)

5 Phasen

Die in diesem Kapitel beschriebenen Anforderungen sind minimale Bedingungen an die QM Stufen und dürfen nicht unterschritten werden. [MUST]

Höhere Anforderungen sind erlaubt.

5.1 Registrationsphase (Registration Phase, RP)

Die Ausprägung der Registrationsphase (Registration Phase, RP) entspricht der minimalen Ausprägung in den Kriterien ID, IC oder IE. Zum Beispiel: Wenn die Kriterien ID4, IC4, IE1 auftreten, dann ergibt sich die Ausprägung RP1.

Kriterien	Ausprägung			
Identifikationsverfahren (ID)	ID1	ID2	ID3	ID4
Übergabe digitaler Ausweis (IC)	IC1	IC2	IC3	IC4
Ausweisaussteller (IE)	IE1	IE2	IE3	IE4
Registrationsphase (RP) (RP (ID, IC, IE))	RP1	RP2	RP3	RP4

Tabelle 11**: Erforderliche Qualitätsstufe zur Bewertung der Registrationsphase**

5.2 Elektronische Authentifizierungsphase (Electronic Authentication Phase, EA)

Die Elektronische Authentisierungsphase (Electronic Authentication Phase, EA) umschreibt die technische Sicht auf das Authentisierungsverfahren.

Die Ausprägung der Electronic Authentication Phase (Elektronische Authentisierungsphase) ergibt sich aus den Ausprägungen der Kriterien RC und AM gemäss Tabelle 12.

Speziell ist, dass trotz einer tiefen Ausprägung des AM (AM1 oder AM2) eine Gesamtausprägung von EA3 möglich ist. Die Gewichtung sagt aus, dass der Typ und die Robustheit eines Ausweises höher als der Schutz der angewendeten Authentifikationsverfahren vor Attacken gewertet werden.

Kriterien	Ausprägung			
Typ und Robustheit des Ausweises (RC)	RC1	RC2	RC3	RC4
Sicherheit des Authentifizierungsverfahrens (AM)	AM1-3			AM4

Elektronische Authentisierungsphase (EA) (EA (RC,AM))	EA1	EA2	EA3	EA4

Tabelle 12: Erforderliche Qualitätsstufe zur Bewertung der elektronischen Authentifizierungsphase

5.3 QM Stufen

Die Qualitätsstufe bestimmt sich aus den Ausprägungen von RP und EA nach Tabelle 13 (Minimum der Ausprägung von RP und EA führt zur Qualitätsstufe).

		Ausprägung elektronische Authentifizierungsphase			
		EA1	EA2	EA3	EA4
Ausprägung Registrations-phase	RP1	QM Stufe 1	QM Stufe 1	QM Stufe 1	QM Stufe 1
	RP2	QM Stufe 1	QM Stufe 2	QM Stufe 2	QM Stufe 2
	RP3	QM Stufe 1	QM Stufe 2	QM Stufe 3	QM Stufe 3
	RP4	QM Stufe 1	QM Stufe 2	QM Stufe 3	QM Stufe 4

Tabelle 13: Matrix der QM Stufen

Nachfolgend werden in der Tabelle 14 einige mögliche Beispiele von verschiedenen Qualitätsstufen dargestellt. Jede Zeile wird für sich selbst gelesen und beinhaltet alle Kriterien für die Bewertung sowie die resultierende Qualitätsstufe. Die jeweils rot schraffierten Felder zeigen, die für die Qualitätsstufe entscheidende Kriterien an; sie sind die Kriterien mit der tiefsten Bewertung.

Bsp.	ID	IC	IE	RP	RC	AM	EA	Resultat
1.	3	3	3	3	3	3	3	QM Stufe 3
2.	2	3	3	2	4	3	3	QM Stufe 2
3.	1	2	2	1	2	2	2	QM Stufe 1
4.	4	3	2	2	4	4	4	QM Stufe 2
5.	1	1	1	1	4	1	1	QM Stufe 1
6.	3	2	2	2	2	2	2	QM Stufe 2

Tabelle 14: Beispiel Stufenregel

6 Beschreibung der Qualitätsstufen

6.1 Allgemein

Die nachfolgenden Beschreibungen und Anwendungsfälle der QM Stufen stellen den Minimalfall dar und zeigen somit das Minimum für eine Einteilung in die entsprechende QM Stufe.

6.2 Qualitätsstufe 1

Die QM Stufe 1 ist die niedrigste Qualitätsstufe, die beschrieben wird. In diese Kategorie fallen alle eID-Lösungen, die nur geringes oder kein Vertrauen in die Identität benötigen und daher aus Falschangaben keine negativen Konsequenzen folgen. Zudem ist es möglich, eine virtuelle Identität zu erstellen, hinter welcher man anonym bleibt.

Kriterium	Beschreibung	
ID1	PP.a	keine Anwesenheit erforderlich.
	QoA.a	einmalige Erfassung von möglicherweise öffentlichen Daten, keine eindeutige Identifikation der Identität auf der Basis dieser Daten möglich
	VoA.a	Die E-Mail Adresse, welche angegeben wurde, wird auf ihre Existenz überprüft. Keine weitere Prüfung der Identität.
IC1	Es erfolgt keine Verifikation.	
IE1	keine Überwachung oder Akkreditierung durch eine Regierungsstelle	
RP1	Phasenkriteriumstufe (ID1;IC1;IE1) = RP1	
RC1	Passwort oder PIN	
AM1	Authentisierungsverfahren bietet wenig oder keinen Schutz vor genannten Angriffen.	
EA1	Phasenkriteriumstufe (RC1;AM1) = EA1	
QM1	(RP1;EA1) = QM1	

Tabelle 15: Kriterien der Qualitätsstufe 1

6.2.1 Beispiel Forum

Ein Autobesitzer tauscht in einem öffentlich zugänglichen Internetforum Informationen zu seiner Automarke mit Gleichgesinnten aus. Es können nur registrierte Benutzer Einträge erstellen, daher registriert sich der Autobesitzer. Das online Registrierungsformular wird direkt im Forum ausgefüllt. Darin werden Vorname, Name, E-Mail Adresse, Benutzername und Passwort eingetragen. Weder Benutzername noch Passwort sind durch Regeln oder Vorgaben eingeschränkt. Die eingegebenen Daten werden in der forumseigenen Datenbank ge-

speichert. Die angegeben Daten werden nicht weiter überprüft und auch nicht durch eine dritte Stelle bestätigt.

6.2.2 Wie kommt die Qualitätsstufe 1 zustande?

Kriterium	Beschreibung	
ID1	PP.a	Die Person registriert sich online.
	QoA.a	Die Person gibt Informationen an, die öffentlich verfügbar sind oder frei erfunden sind.
	VoA.a	Die angegebenen Informationen werden von keiner anderen vertrauenswürdigen Stelle überprüft.
IC1	Benutzername und Passwort sind sofort gültig und werden nicht verifiziert	
IE1	Der Betreiber des Forums wird von keiner dritten Stellt überwacht.	
RP1	Phasenkriteriumstufe (ID1;IC1;IE1) = RP1	
RC1	Der Benutzername und das Passwort können frei gewählt werden.	
AM1	Das Authentisierungsverfahren kann nicht überprüft werden und kann so nicht höher bewertet werden.	
EA1	Phasenkriteriumstufe (RC1;AM1) = EA1	
QM1	(RP1;EA1) = QM1	

Tabelle 16: Qualitätseinstufung Beispiel Forum

6.3 Qualitätsstufe 2

Elektronische Identitäten, welche mit der QM Stufe 2 bewertet werden, haben eine minimal identifizierte Person als Grundlage. Es wird vorausgesetzt, dass eine sichere Art der Authentisierung möglich ist und dass Credentials einem Standard folgen.

Kriterium	Beschreibung	
ID2	PP.a	keine Anwesenheit erforderlich
	QoA.b	Mehrmalige Erfassung von möglicherweise öffentlichen Daten, welche eine Identität eindeutigen identifizieren.
	VoA.b	Die angegebenen Daten werden mit einer vertrauenswürdigen Quelle oder einer Identitätsdatenbank abgeglichen.
IC2	Leichte Verifikation des Empfängers: • Benutzername und Passwort 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 Ausweises, wird an die während der Registration genannte E-Mail Adresse versendet. Der Link muss nach einer gewissen Zeit (z.B. 24 Stunden) ablaufen.	
IE2	mit Zustimmung einer Regierungsstelle	
RP2	Phasenkriteriumlevel (ID2;IC2;IE2) = RP2	
RC2	Passwort oder PIN nach Vorgaben	
AM2	Authentisierungsverfahren bietet Schutz gegen einige der genannten Angriffe.	
EA2	Phasenkriteriumlevel (RC2;AM2) = EA2	
QM2	(RP2;EA2) = QM2	

Tabelle 17: Kriterien der Qualitätsstufe 2

6.3.1 Beispiel Steuererklärung

Eine im Kanton Bern wohnhafte Person kann sich die Steuererklärung per Briefpost zusenden lassen oder die Steuererklärung online ausfüllen (www.taxme.ch). Um TaxMe nutzen zu können, werden die Codes benutzt, die mit der Steuererklärung und an die in der letzten Steuererklärung angegebene E-Mail Adresse verschickt werden[6]. Mit Hilfe der ZPV-Nummer,

[6] Der E-Mail Code wird derzeit nicht von TaxMe verwendet und wurde zur Vervollständigung des Beispiels hinzugefügt.

der Fallnummer, des ID-Codes und dem E-Mail Code kann sich eine Person auf dem TLS-geschützten Dienst von TaxMe einloggen und die Steuererklärung ausfüllen. Nach dem Einloggen ist zudem der Zugriff auf die Daten der letzten Steuererklärung möglich, sofern diese bereits online ausgefüllt wurde.

6.3.2 Wie kommt die Qualitätsstufe 2 zustande?

Kriterium	Beschreibung	
ID2	PP.a	Es ist keine Anwesenheit erforderlich, um den Ausweis, in diesem Fall die ZPV-Nummer, die Fallnummer und der ID-Code, zu erhalten.
	QoA.b	Durch die Erfassung der Daten bei der Gemeinde, dem Kanton und dem Bund führen die Daten zu einer eindeutigen Identität und werden gleichzeitig auch mit anderen Quellen verglichen. Wäre die Identität des Steuerpflichtigen einer dieser Quellen unbekannt, würde das bemerkt werden und zu Nachforschungen führen.
	VoA.b	Durch die Erfassung der Daten bei der Gemeinde, dem Kanton und dem Bund führen die Daten zu einer eindeutigen Identität und werden gleichzeitig auch mit anderen Quellen verglichen. Wäre die Identität des Steuerpflichtigen einer dieser Quellen unbekannt, würde das bemerkt werden und zu Nachforschungen führen.
IC2	Leichte Verifikation des Empfängers: • Benutzername und Passwort werden separat verschickt, wobei mindestens eines der beiden per Briefpost an die während der Registration genannte Adresse gesendet werden muss. Das Qualitätskriterium schreibt für die Stufe 2 eine Zustellung von Benutzernamen oder Passwort per Briefpost oder einer ähnlichen Verifizierung des Adressaten vor. Die Zugangsdaten für TaxMe Online erhält der Benutzer per Post und per Mail.	
IE2	Die Benutzung der ZPV-Nummer wird in der Verordnung zum Bundesgesetz über den Datenschutz geregelt. Es wird zwar eine Zustimmung des erstellenden Bundesorgans benötigt, aber keine Überwachung oder sogar Akkreditierung vorgeschrieben. Der Aussteller, in diesem Fall das KAIO (Kantonales Amt für Informatik und Organisation), gibt zwar die Zustimmung zur Nutzung durch die Finanzdirektion des Kantons Bern, aber es überwacht oder akkreditiert den Nutzer nicht, somit lässt sich das IE Qualitätskriterium mit der Stufe 2 bewerten.	
RP2	Phasenkriteriumstufe (ID2;IC2;IE2) = RP2	

RC2	Das Qualitätskriterium über die Art und Robustheit des Ausweises (RC) erreicht auch die Stufe 2. Der ID-Code, welcher automatisch generiert und vorgegeben wird, dient als Passwort oder PIN bei der Authentisierung des Benutzers. Dieser PIN erfüllt die Voraussetzung für eine Stufe 2 Einstufung, da die Länge (zehn Zeichen) sowie die Komplexität (grosse und kleine Buchstaben und Zahlen) die Vorgabe für starke Passwörter erfüllt.
AM2	Auch beim AM Qualitätskriterium kann die Stufe 2 vergeben werden, da die TLS geschützten Übertragung der Daten Schutz gegen einige der beschriebenen Angriffe gibt.
EA2	Phasenkriteriumstufe (RC2;AM2) = EA2
QM2	(RP2;EA2) = QM2

Tabelle 18: Qualitätseinstufung Beispiel Steuererklärung

6.4 Qualitätsstufe 3

QM Stufe 3 setzt voraus, dass die Identität so verifiziert wurde, dass die nachgewiesene elektronische Identität mit einer hohen Gewissheit das Subjekt repräsentiert. Institute, welche elektronische Identitäten der QM Stufe 3 ausstellen, müssen von einer Regierungsstelle überwacht und akkreditiert werden.

Kriterium	Beschreibung	
ID3	PP.b	Anwesenheit während der Registrierung erforderlich
	QoA.b	mehrmalige Erfassung von möglicherweise öffentlichen Daten wie Namen, Vornamen oder Geburtstag, welche eine Identität eindeutigen identifizieren
	VoA.c	Die angegebenen Daten müssen mit einer nicht qualifizierten digitalen Signatur signiert werden
		oder
	PP.a	keine Anwesenheit erforderlich.
	QoA.c	mindestens eine Erfassung von nicht öffentlichen Daten, welche zu einer eindeutigen Identität führen.
	VoA.d	Die angegebenen Daten werden mit einem offiziellen Ausweisdokument, wie zum Beispiel dem Pass, der Identitätskarte oder dem Führerausweis, verglichen.

IC3	Mittlere Verifikation des Empfängers: • Ausweis wird per eingeschriebenem Brief an die während der Registration genannte und überprüfte Adresse gesendet. • Ausweis wird direkt nach der Verifikation mittels qualifizierter Signatur (ID Phase) erstellt und von der antragstellenden Person heruntergeladen. • Ausweis wird nach der Eingabe eines Passwortes, welches physisch bei der Registration übergeben wurde, heruntergeladen.
IE3	mit Überwachung oder Akkreditierung durch eine Regierungsstelle
RP3	Phasenkriteriumlevel (ID3;IC3;IE3) = RP3
RC3	qualifizierte Software Zertifikate, Hardware Zertifikate
AM3	Authentisierungsverfahren bietet Schutz gegen die meisten der genannten Angriffe
EA3	Phasenkriteriumlevel (RC3;AM3) = EA3
QM3	(RP3;EA3) = QM3

Tabelle 19: Kriterien der Qualitätsstufe 3

6.4.1 Beispiel Bankkonto

Eröffnet eine Person ein Bankkonto, so muss sie dies persönlich in einer Geschäftsstelle tun. Sie gibt Name, Vorname, Adresse, Geburtstag und Mobiltelefonnummer an, identifiziert sich mit einem offiziellen Dokument wie z.B. der Identitätskarte und unterschreibt die nötigen Verträge. In jeweils separater Briefpost erhält sie einige Tage später ihre Konto-Karte, PIN (Einschrieben), Benutzername und Passwort. Der online Zugriff auf das Konto ist 2-Weg-authentifiziert, nach Eingabe von Benutzernamen und Passwort erhält die Person einen einmalig nutzbaren, 10 Minuten gültigen Code per SMS auf die bei der Registrierung angegebene Mobiltelefonnummer.

6.4.2 Wie kommt die Qualitätsstufe 3 zustande?

Kriterium	Beschreibung	
ID3	PP.b	Die Anwesenheit für die Eröffnung eines Bankkontos ist erforderliche. Diese führt zusammen mit QoA und VoA zu einer ID Stufe 4.
	QoA.b	Die erfassten Daten führen zu einer eindeutigen Identität und es werden nicht öffentliche Daten erfasst (z.B. Pass- oder ID-Nummer).
	VoA.c	Die angegebenen Daten werden mit einem offiziellen Ausweisdokument, wie zum Beispiel dem Pass, der Identitätskarte oder dem Führerausweis, verglichen.

IC3	Der Ausweis wird teilweise (Karte oder PIN) eingeschrieben an die während der Registrierung angegebene Adresse geschickt.
IE3	Das Qualitätskriterium IE erreicht im Anwendungsfall die Stufe 3, da es eine Regierungsstelle für die Überwachung und Akkreditierung von Banken gibt, nämlich die FINMA.
RP3	Phasenkriteriumstufe (ID3;IC3;IE3) = RP3
RC3	Das sogenannte OneTime Passwort (SMS Code gültig für 10 Minuten) erhöht die Sicherheit des Ausweises auf die Stufe 3.
AM3	Das Authentisierungsverfahren wird bei Banken auf alle genannten Angriffe hin überprüft und gewährt gegen alle genannten Angriffe Schutz. Dementsprechend wird die Stufe 4 erreicht.
EA3	Phasenkriteriumstufe (RC3;AM3) = EA3
QM3	(RP3;EA3) = QM3

Tabelle 20: Qualitätseinstufung Beispiel Bankkonto

6.5 Qualitätsstufe 4

Die QM Stufe 4 beschreibt die höchste Vertrauensstufe, welche eine elektronische Identität erhalten kann. Das Subjekt, das hinter dieser Identität steht, muss sich mindestens einmal physisch identifizieren lassen. Zudem muss der ausgestellte Ausweis die höchstmögliche Sicherheit bieten, welche heute ein Hardware Zertifikat darstellt. Aussteller von Ausweisen dieser Stufe werden überwacht und akkreditiert und müssen die Vorgaben des Bundesgesetzes über die elektronische Signatur (ZertES) erfüllen. Bei Missbrauch einer elektronischen Identität auf Stufe 4 entsteht ein grosser bis sehr grosser Schaden.

Kriterium	Beschreibung	
ID4	PP.b	Anwesenheit während der Registrierung erforderlich
	QoA.c	mindestens eine Erfassung von nicht öffentlichen Daten, welche zu einer eindeutigen Identität führen
	VoA.d	Die angegebenen Daten werden mit einem offiziellen Ausweisdokument, wie zum Beispiel dem Pass, der Identitätskarte oder dem Führerausweis, verglichen.
IC4	Starke Verifikation des Empfängers: • Ausweis wird der Person persönlich übergeben • Ausweis wird der Person zugesendet und erst nach der Validierung der Identität aktiviert.	
IE4	Qualifiziert nach ZertES	
RP4	Phasenkriteriumlevel (ID4;IC4;IE4) = RP4	

RC4	qualifizierte Hard Zertifikate
AM4	Authentisierungsverfahren bietet Schutz gegen alle genannten Angriffe. Vergleichbar mit EAL4+
EA4	Phasenkriteriumlevel (RC4;AM4) = EA4
QM4	(RP4;EA4) = QM4

Tabelle 21: Kriterien der Qualitätsstufe 4

6.5.1 Beispiel rechtsgültige elektronische Signatur

In der Schweiz kann eine Person mit der SuisseID rechtsgültige elektronische Signaturen erstellen. Um eine SuisseID zu erhalten, muss sich die antragstellende Person ein Antragsformular mit den Daten Name, Vorname, E-Mail Adresse, Land und Lieferadresse ausfüllen. Mit dem ausgefüllten Antragsformular geht sie auf eine Identitätsprüfstelle (Gemeindeverwaltung, Poststelle, Notariate, Botschaften und Konsulate) und lässt sich identifizieren. Dabei wird anhand eines Lichtbildausweises wie dem Pass oder der Identitätskarte die Identität der antragsstellenden Person überprüft und anschliessend eine Identitätsbestätigung ausgestellt. Das Antragsformular und die Identitätsbestätigung wird anschliessend einem SuisseID Anbieter eingeschickt.

Nach ca. zwei Wochen erhält die Antragsstellende Person die SuisseID und den nötigen Aktivierungscode persönlich[7] eingeschrieben per Post zugestellt. Die SuisseID kann dann mit dem Aktivierungscode aktivierte werden und nachfolgend mit einem selbst definierten PIN geschützt werden. Mit der aktivierten SuisseID können fortan rechtsgültige elektronische Signaturen erstellt werden und damit zum Beispiel Verträge unterzeichnet werden.

6.5.2 Wie kommt die Qualitätsstufe 4 zustande?

Kriterium	Beschreibung	
ID4	PP.b	Anwesenheit und sichere Identifizierung ist während der Registrierung erforderlich, um diesen Ausweis zu erhalten.
	QoA.c	Die erfassten Daten ergeben eine eindeutige Identität und enthalten nicht öffentlich zugängliche Informationen.
	VoA.d	Die angegebenen Daten werden mit einem offiziellen Ausweisdokument, wie dem Pass oder der Identitätskarte, verglichen.

[7] Zur Zeit wird die SuisseID nur eingeschrieben zugestellt.

IC4	Starke Verifikation des Empfängers durch die Zustellung via persönlich eingeschriebenen Brief, welcher als persönliche Übergabe gilt.
IE4	Die SuisseID Anbieter sind nach ZertES, dem Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur, akkreditiert[8].
RP4	Phasenkriteriumstufe (ID4;IC4;IE4) = RP4
RC4	Die SuisseID beinhaltet ein qualifiziertes Hardware Zertifikat, welches den Anforderungen des ZertES entspricht und folglich eine RC 4 Einstufung erhält.
AM4	Die SuisseID und die damit verbunden Authentifizierungsverfahren werden nach EAL4+ auf Schwachstellen hin geprüft und erhalten daher für das AM Qualitätskriterium die Stufe 4.
EA4	Phasenkriteriumstufe (RC4;AM4) = EA4
QM4	(RP4;EA4) = QM4

Tabelle 22: Qualitätseinstufung Beispiel Computergame

[8] In diesem Standard wird davon ausgegangen, dass die europäische Richtlinie 1999/93/EC mit dem Bundesgesetz über die elektronische Signatur (ZertES) kompatibel ist. Die Annahme wurde jedoch nicht juristisch überprüft.

7 Haftungsausschluss / Hinweise auf Rechte Dritter

eCH-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellt oder welche **eCH** referenziert, 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.

8 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

A-SIT. (29. 11 2012). www.buergerkarte.at. Abgerufen am 29. 11 2012 von Bürgerkarte: e-card aktivieren: http://www.buergerkarte.at/aktivieren-e-card.de.php

Bundesversammlung Schweiz. (2003). Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur. Schweizerische Eidgenossenschaft.

CCRA. (02. 05 2012). http://www.commoncriteriaportal.org. Abgerufen am 02. 05 2012 von Official CC/CEM versions: http://www.commoncriteriaportal.org/cc/

EU Parlament. (19. 01 2000). RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. EU. Abgerufen am 06. 04 2012 von http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett

Hulsebosch, B., Lenzini, G., & Eertink, H. (3. März 2009). D2.3 Quality authenticator scheme. Abgerufen am 13. 10 2011 von STORK Materials: https://www.eid-stork.eu/index.php?option=com_processes&act=list_documents&s=1&Itemid=60&id=312

Wikipedia. (28. 12 2012). PKCS 12. Abgerufen am 17. 01 2013 von www.wikipedia.org: http://en.wikipedia.org/wiki/PKCS_12

Wikipedia. (16. 01 2013). Social Engineering (Sicherheit). Abgerufen am 17. 01 2013 von www.wikipedia.org: http://de.wikipedia.org/wiki/Social_Engineering_%28Sicherheit%29

Anhang B – Mitarbeit & Überprüfung

Andreas Spichiger	Berner Fachhochschule
Thomas Jarchow	Berner Fachhochschule
Martin Topfel	Berner Fachhochschule

Anhang C – Abkürzungen

AM	Security oft he Authentication Mechanism
CSP	Certificate Service Provider
eID	Elektronische Identität
EA	Elektronische Authentifizierungsphase (Electronic Authentication Phase)
FINMA	Finanzmarktaufsicht
ID	Identifikationsverfahren (Identification Procedure)
IC	Übergabe digitaler Ausweis (Credential Issuing Process)
IE	Ausweisaussteller (Entity Issuing Credentials)
KAIO	Amt für Informatik und Organisation des Kantons Bern
OTP	OneTime Password
PP	Anwesenheit (Physical Presence)
PIN	Persönliche Identifikationsnummer
QM	eID-Qualitätsmodell
QAA	Quality of Authentication Assurance
QoA	Qualität der Angaben (Quality of Assertions)
RC	Ausweisart (Type and Robustness of the Credential)
RSA	Rivest, Shamir und Adleman
RP	Registrationsphase (Registration Phase)
RSa	Rückscheinbrief
STORK	Secure idenTity acrOss boRders linKed
TLS	Transport Layer Security
VoA	Validierung der Angaben (Validation of Assertions)
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur
ZPV	Zentrale Personenverwaltung

Anhang D – Glossar

Authentifizierung	gemäss Glossar eCH-107
Credential	gemäss Glossar eCH-107
PKCS#12	„In cryptography, PKCS #12 defines an archive file format commonly used to directly store a private key along with its X.509 certificate.“[9]
qualifiziertes Zertifikat	Bei einem Qualifizierten Zertifikat handelt es sich um ein Zertifikat, das nach speziell vorgegebenen Anforderungen (z.B. durch den Staat) erstellt wurde und denen entspricht.
Social Engineering	„Social Engineering nennt man zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhalten hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen.“[10]

[9] (Wikipedia, 2012)

[10] (Wikipedia, 2013)