eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID

Name	Qualitätsmodell der Attributwertbestätigung zur eID
Standard-Nummer	eCH-0171
Kategorie	Standard
Reifegrad	Definiert
Version	1.0
Status	Genehmigt
Genehmigt am	2014-09-03
Ausgabedatum	2014-09-04
Ersetzt Standard	-
Sprachen	Deutsch und Französisch
Autoren	Fachgruppe IAM Martin Topfel, Berner Fachhochschule, martin.topfel@bfh.ch Thomas Jarchow, Berner Fachhochschule, thomas.jarchow@bfh.ch Andreas Spichiger, Berner Fachhochschule, andreas.spichiger@bfh.ch Ronny Bernold, Berner Fachhochschule, ronny.bernold@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

Der Standard eCH-0171 Qualitätsmodell der Attributwertbestätigung zur eID wird genutzt, um die Qualität einer Attributwertbestätigung zu bewerten. Der Standard beschreibt die Grundlegenden Prozesse für das Anbieten von Attributwertbestätigungen und leitet von diesen die Qualitätskriterien für die Bewertung ab. Durch die definierten Ausprägungen der Qualitätskriterien wird eine Bewertung der Attributwertbestätigung ermöglicht. Mit Hilfe der Gesamtbewertung können verschiedene Anbieter von Attributwertbestätigungen verglichen werden.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Status des Dokuments

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

2 Einleitung

2.1 Überblick

In der realen Welt haben Subjekte (Personen, Organisationen oder Services) Eigenschaften, die sie beschreiben. In der digitalen Welt werden Abstraktionen dieser Eigenschaften Attribute genannt. Attribute sind ein wichtiger Bestandteil der digitalen Identitäten von natürlichen Personen, Organisationen und maschinellen Services.

Eine Schwierigkeit, die in der digitalen Welt auftritt, ist, dass die Person und die Belege für eine Eigenschaft nicht digital vorhanden sind und daher häufig nicht direkt belegt werden können. In vielen verschiedenen Prozessen des Alltags werden jedoch viele Eigenschaften digitalisiert und sind als Attribute für einen relativ kleinen Kreis jeweils verfügbar. So speichert ein Unternehmen die Personendaten der Mitarbeiter in einer HR-Datenbank oder das Einwohneramt erfasst auf ihrem System die Wohndaten ihrer Einwohner. Entlang der Forderung, eine Information einer Behörde den Behörden nur einmal angeben zu müssen, gibt es entsprechend Bestrebungen, diese Attribute breiter verfügbar zu machen. Es lassen sich Systeme entwickeln, welche die Möglichkeit bieten, Attribute von einer Quelle (Attribut-Autorität) bestätigen zu lassen. Die Attribut-Autoritäten haben zum Teil unterschiedliche Prozesse, um die Attribute zu erfassen, zu pflegen und zu bestätigen. Aufgrund der Heterogenität ist unklar, welche Qualität die Attributwertbestätigungen einer Attribut-Autorität haben. Für die Relying Party, die ein Attribut bestätigt haben will, ist es auf der Basis des Schutzbedarfs von zentraler Bedeutung, zum Beispiel bei der Unterzeichnung von Verträgen zu wissen, wer das Subjekt ist und ob das Subjekt zur Unterschrift berechtigt ist. Zur Authentifizierung von Subjekten gibt es unterschiedliche Lösungen, die mit eCH-0170 Qualitätsmodell für elektronische Identitäten bewertet werden. Der hier vorliegende Standard eCH-0171 erschliesst die Möglichkeit, zur eIdentity zugehörige Attribute mit einer Attributwertbestätigung (Attribute Assertion) nicht nur technisch zur Verfügung zu stellen, sondern diese Attributwertbestätigung auf der Basis des hier beschriebenen Qualitätsmodell zu bewerten.

2.1.1 Einführung Attributwertbestätigung

In Abbildung 1 werden die Kernelemente, die für eine vertrauenswürdige Attributwertbestätigung notwendig sind, dargestellt. Im Zentrum steht die Bestätigung von Eigenschaften eines Subjekts durch die Attribut-Autorität gegenüber der Relying Party. Die Begrifflichkeit folgt dabei eCH-0107 und werden in Kapitel 2.1.2 näher erklärt oder präzisiert.

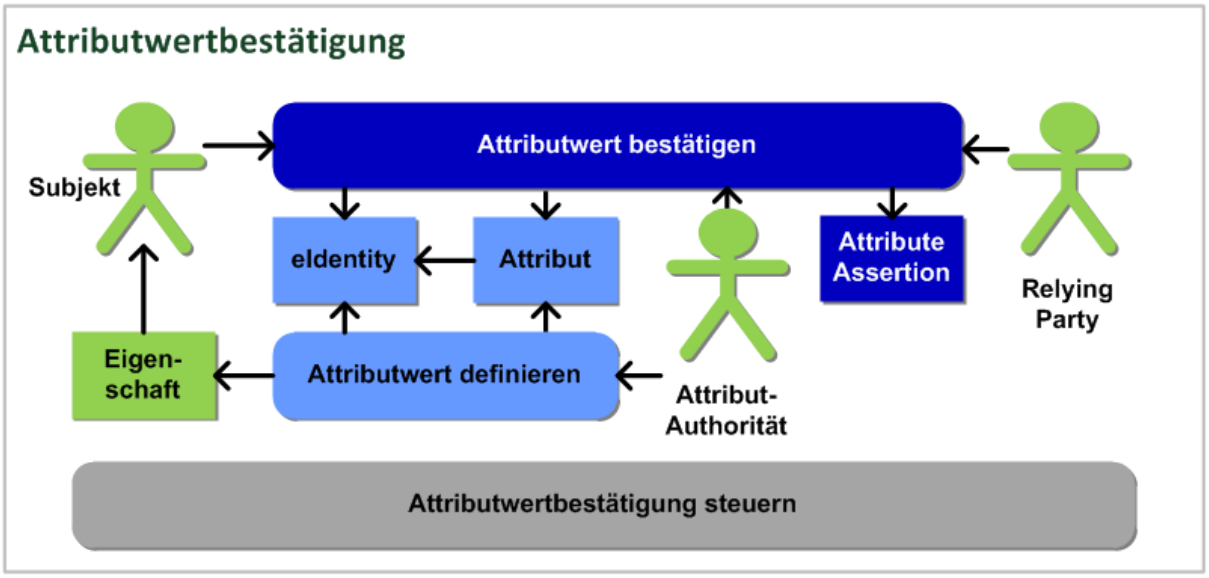

Abbildung 1: Attributwertbestätigung im Überblick

Zweck der im vorliegenden Standard beschriebenen Qualitätskriterien ist eine vertrauenswürdige Attributwertbestätigung (in Abbildung 1 durch das Schnittstellenelement *Attribute Assertion* repräsentiert) einer Attribut-Autorität an eine Relying-Party. Die *Attribut-Autorität* erstellt auf der Basis der *eIdentity* und deren *Attribute* die *Attribute Assertion* im Rahmen des Prozesses *Attributwert bestätigen.* Das Subjekt erhält im Rahmen des Prozesses allenfalls die Gelegenheit, der Übermittlung der *Attribute Assertion* an die *Relying Party* zuzustimmen[1].

eIdentity und *Attribute* werden durch die Attribut-Autorität im Rahmen des Prozesses *Attributwert definieren* auf der Basis der *Eigenschaften* eines *Subjekts* erhoben.

Das Zusammenspiel dieser Tätigkeiten wird im Rahmen des Prozesses *Attributwertbestätigung steuern* unter allen beteiligten Stakeholdern zusammen mit Regulatoren vereinbart.

Attributwert bestätigen ist Teil des Prozess *Zugriff kontrollieren* aus eCH-0107, kann aber auch zu anderen Zwecken als *eIdentity autorisieren* verwendet werden. *Attributwert definieren* entspricht dem Prozess *Attribut definieren* aus eCH-0107. Auf der Basis einer etwas differenzierteren Betrachtung der Thematik der Attributwertbestätigung wird im Rahmen dieses Standards konsequent vom Attributwert gesprochen. *Attributwertbestätigung steuern* ist Teil des Prozesses IAM steuern

[1] Attributwertbestätigungen einer verlinkten eIdentity werden in diesem Standard nicht berücksichtigt. Für eine Implementierung könnte die Verlinkung als Attribut verstanden und die Qualität der Verlinkung über den Prozess Attributwert bearbeiten bestimmt werden.

Die Elemente *Attributwert bestätigen* und *Attributwert definieren* stellen die Kernprozesse dar, welche vom Subjekt, der Attribut-Autorität und der Relying Party genutzt werden. Diese Kernprozesse werden zu unterschiedlichen Zeitpunkten verwendet, welche durch die hellblaue und dunkelblaue Farbe symbolisiert werden. Tabelle 1 definiert die Farbverwendung innerhalb dieses Dokuments.

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

2.1.2 Begriffe

Tabelle 2 definiert die wesentlichen Begriffe, die im Rahmen dieses Dokuments zur Beschreibung der Qualität der Attribut Assertion verwendet werden. Der hier vorliegende Standard richtet sich grundsätzlich nach den Begrifflichkeiten aus eCH-0107.

Begriff	Beschreibung
Attribut	Semantisches Abbild einer einem Subjekt zugeordneten Eigenschaft, die das Subjekt näher beschreibt. Der Identifikator und die Credentials sind ebenfalls Attribute. Ein Attribut setzt sich zusammen aus den Meta-Attributen Attributname (z.B. „Schuhgrösse“), Attributtyp (z.B. „Integer“) und Attributwert (z.B. „39“). [eCH-0107]
Attributwert	Ein Attributwert ist ein Teil eines Attributs und enthält den konkreten Wert, welcher dem Attribut zugeordnet ist.
Attribut-Autorität	Eine Attribut-Autorität ist ein Register oder sonstiges Verzeichnis mit einem Attribute Service zur Pflege von Attributwerten und einem Attribute Assertion Service zur Ausstellung von Attribute Assertions. (Präzisiert die Definition aus eCH-0107)
Attribute Assertion	Bestätigung eines Attributwertes durch eine Attribut-Autorität. Entspricht einer SAML 2.0 Attribute Assertion [angelehnt an eCH-0107]. (Präzisiert die Definition aus eCH-0107)

eIdentity	Repräsentation eines Subjekts. Eine digitale Identität (eIdentity) 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 digitale Identitäten haben. [eCH-0107]
Eigenschaft	Eigenschaften sind Charakteristika, Merkmale oder Verhalten eines Subjekts. [eCH-0107]
Subjekt	Eine natürliche Person, Organisation oder ein Service, die auf eine Ressource zugreift oder zugreifen möchte. Ein Subjekt wird durch digitale Identitäten beschrieben. [eCH-0107]

Tabelle 2: Definitionen der wesentlichen Begriffe

2.1.3 Informationsarchitektur

Die Informationsarchitektur in Abbildung 2 stellt einen Ausschnitt aus der Informationsarchitektur von eCH-0107 dar, welche sich am UML-Klassendiagramm orientiert.

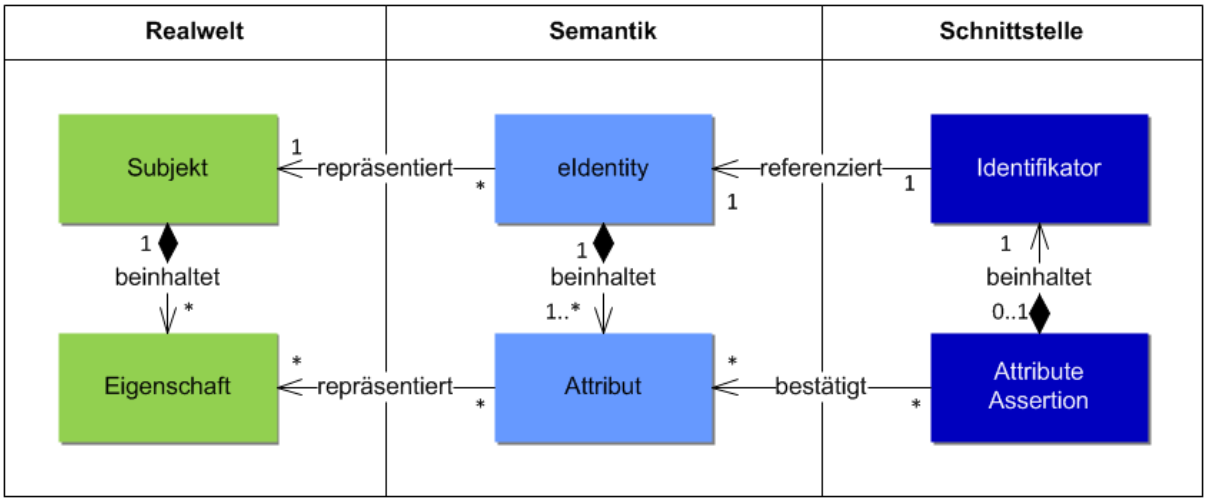

Abbildung 2: Informationsarchitektur

Durch die *Attribute Assertion* (Attributwertbestätigung) wird ein zu einer eIdentity zugehöriger Attributwert im Informationselement Attribut bestätigt. Der Attributwert einer eIdentity ist eine Abbildung des zum Subjekt gehörenden Eigenschaftswert im Informationselement Eigenschaft. Mittels dem Identifikator wird auf die eIdentity referenziert und Attributwerte der eIdentity zugeordnet.

2.2 Anwendungsgebiet

Der Standard eCH-0171 lässt sich in der IAM Standardisierungsarchitektur von eCH als ergänzendes Hilfsmittel einordnen und stellt ein Qualitätsmodell dar.

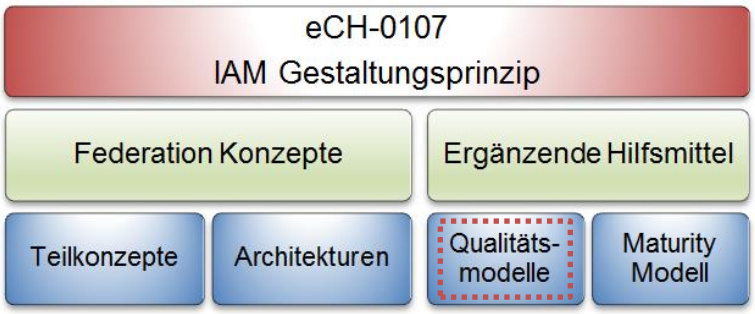

Abbildung 3: Einordung in IAM Standardisierungsarchitektur

Ziel dieses Standards ist die Definition eines Qualitätsmasses, das die Qualität der an die *Relying Party* übermittelten *Attribute Assertion* bezogen auf den Eigenschaftswert des durch die eIdentity repräsentierten Subjekts zum Zeitpunkt der Übermittlung beschreibt. Der Standard wird angewendet, wenn die Qualität einer Attributwertbestätigung einer Attribut-Autorität gemessen wird. Weitere Anwendungsmöglichkeiten bestehen beim Vergleich von mehreren Attribut-Autoritäten, die dasselbe Attribut anbieten. Dadurch kann entschieden werden, welches ausgehend vom Schutzbedarf für den jeweiligen Anwendungsfall die geeignete Attribut-Autorität ist.

Das Qualitätsmodell ist kontextunabhängig und kann daher für jede Art von Attributwertbestätigungen auch ausserhalb von IAM verwendet werden.

Credentials könnten mit dem Modell von eCH-0171 bewertet werden, wenn diese als Attribute verwendet werden. Da jedoch meist die Bewertung der gesamten Identität bei den Credentials im Vordergrund steht, wird empfohlen, dass der Standard eCH-0170 für die Bewertung von Credentials/Identitäten verwendet wird, welcher explizit für dieses Anwendungsfeld definiert wurde und entsprechende Qualitätskriterien enthält.

Als Grundlage zur Erarbeitung des hier vorliegenden Standards dienten die eCH-Standards eCH-0107 wie auch eCH-0170, wie auch der QAA Status Report aus dem Projekt STORK 2.0 [STORT D3.2].

2.3 Vorteile

Der hier vorliegende Standard eCH-0171 definiert ein Qualitätsmodell zur Bewertung und Einstufung von Attributwertbestätigungen. Dadurch werden folgende Vorteile erzielt:

- Das Qualitätsmodell für die Bewertung von Attributwertbestätigungen ist definiert.
- Die zum Qualitätsmodell gehörigen Qualitätskriterien sind definiert.
- Die Motivation für diese Qualitätskriterien ist auf der Basis der Prozesse zur Erstellung von Attributwertbestätigungen dokumentiert.

2.4 Schwerpunkte

Kapitel 3 beschreibt die Begrifflichkeiten und das Gesamtmodell der Qualität von Attributwertbestätigungen. Es werden die Qualitätsstufen und die Regeln für die Berechnung der Qualitätsstufen vorgestellt.

Kapitel 4 definiert die für Attributwertbestätigungen nötigen Prozesse und beschreibt diese. Durch die Prozesse werden die für die Bewertung notwendigen Qualitätskriterien sichtbar, ableitbar und definierbar.

Kapitel 5 definiert die Qualitätskriterien, anhand welcher Attributwertbestätigungen bewertet werden. Zu jedem Qualitätskriterium werden Fragen beschrieben, die beantwortet werden müssen, gefolgt von einer kurzen Beschreibung des Kriteriums. Anschliessen werden die möglichen Ausprägungen des Kriteriums aufgelistet und beschrieben.

2.5 Normativer Charakter der Kapitel

Die Kapitel des vorliegenden Standards sind von normativem oder auch deskriptivem Charakter. Tabelle 3 definiert die Einordnung der Kapitel.

Kapitel	Beschreibung
2 Einleitung	Deskriptiv
3 Qualitätsmodell	Normativ
4 Prozesse	Deskriptiv
5 Qualitätskriterien	Normativ
6 Bestimmen der Qualitätsstufe	Normativ
Anhang A – Referenzen & Bibliografie	Deskriptiv
Anhang B – Mitarbeiter & Überprüfung	Deskriptiv

Tabelle 3: Übersicht des normativen Charakters der Kapitel

3 Qualitätsmodell

3.1 Qualitätsstufen

Im Qualitätsmodell der Attributwertbestätigungen sind vier Stufen definiert. Stufe 1 ist die niedrigste und bedeutet, dass sie seitens Relying Party am wenigsten Vertrauen geniesst. Stufe 4 ist die höchste Stufe und geniesst seitens Relying Party am meisten Vertrauen. Diese Stufen basieren auf dem ISO/IEC Standard 29115 „Information technology - Security techniques - Entity authentication assurance framework“ [ISO29115].

Stufe	Beschreibung
1 – tief	Auf Stufe 1 besteht ein minimales Vertrauen in den behaupteten oder bestätigten Attributwert. Diese Vertrauensstufe wird genutzt, wenn ein minimales Risiko mit dem verwendeten Attributwert verbunden wird. Eine Vielzahl von Attribut-Autoritäten liefern Attributwertbestätigungen dieser Stufe und es werden keine bis sehr wenige Anforderungen an sie gestellt.
2 – mittel	Auf Stufe 2 besteht einiges Vertrauen in den behaupteten oder bestätigten Attributwert. Diese Vertrauensstufe wird genutzt, wenn ein mässiges Risiko mit dem verwendeten Attributwert verbunden wird. Es werden grundlegende Kontrollen und Prozesse eingehalten, jedoch findet keine generelle externe Überwachung der Attribut-Autorität statt. Attributwertbestätigungen dieser Stufe genügen, um einfache Geschäfte abzuwickeln.
3 – hoch	Auf Stufe 3 besteht ein hohes Vertrauen in den behaupteten oder bestätigten Attributwert. Diese Vertrauensstufe wird genutzt, wenn ein erhebliches Risiko mit dem verwendeten Attributwert verbunden wird. Es werden Kontrollen und Prozesse eingehalten, die von einer externen Stelle überwacht und überprüft werden. Attribute dieser Stufe genügen, um mittel-kritische Geschäfte abzuwickeln.
4 – sehr hoch	Auf Stufe 4 besteht ein sehr hohes Vertrauen in den behaupteten oder bestätigten Attributwert. Diese Vertrauensstufe wird genutzt, wenn ein hohes Risiko mit dem verwendeten Attributwert verbunden wird. Es werden Kontrollen und Prozesse eingehalten, die gesetzlich vorgeschrieben werden. Attributwertbestätigungen dieser Stufe genügen, um alle möglichen Geschäfte abzuwickeln.

Tabelle 4: Qualitätsstufen

3.2 Struktur

Die Gesamtstruktur des Qualitätsmodells besteht aus drei Ebenen: der Gesamtbewertung der Qualität der Attributwertbestätigung, der Bewertung der Qualität der Prozesse und den zu den Prozessen zugehörigen Qualitätskriterien. Die drei Ebenen sind beispielhaft in Abbildung 4 ersichtlich.

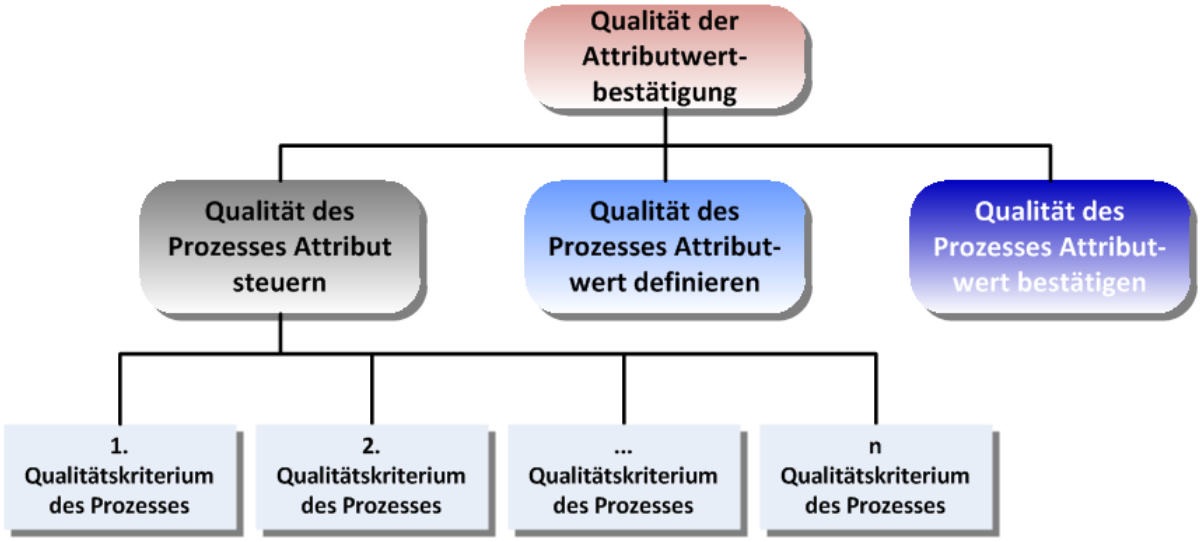

Abbildung 4: Aufbau Gesamtmodell

Die Qualitätskriterien enthalten Ausprägungen, die erfüllt werden müssen. Dadurch erhalten sie eine Bewertungsstufe. Diese Bewertungsstufe wird auf der Prozessebene zusammengefasst und ergeben die Prozessbewertungsstufe. Auf der Gesamtbewertungsebene werden die Prozessbewertungsstufen zusammengefasst und ergeben die Qualität der Attributwertbestätigung (vgl. auch Abbildung 6).

3.3 Regeln für die Stufenbestimmung

Im Qualitätsmodell für die Attributwertbestätigung wird die resultierende Qualitätsstufe immer durch die tiefste Ausprägung eines Kriteriums bestimmt. Somit kann durch eine sehr hohe Stufe eines Kriteriums nicht die Schwäche bei einem anderen Kriterium wettgemacht werden.

Beispiel: Wenn ein Kriterium Stufe 1 aufweist und alle anderen die Stufe 3 erreichen, so wird nur eine Gesamtqualität der Stufe 1 erreicht. Dasselbe gilt für die Prozessebene und die Gesamtbewertungsebene.

4 Prozesse

Die Attributwertbestätigung durch eine Attribut-Autorität bedingt eine Vielzahl von Aktivitäten. Zur Bewertung der Qualität einer Attributwertbestätigung werden nicht nur die eigentliche Bestätigung selber, sondern auch die mit der Erstellung verbundenen Prozesse berücksichtigt. Abbildung 5 zeigt die beteiligten Prozesse für die Ausführung, die Definition und die Steuerung einer Attributwertbestätigung. Weiter werden die identifizierten Qualitätskriterien den Prozessen zugeordnet.

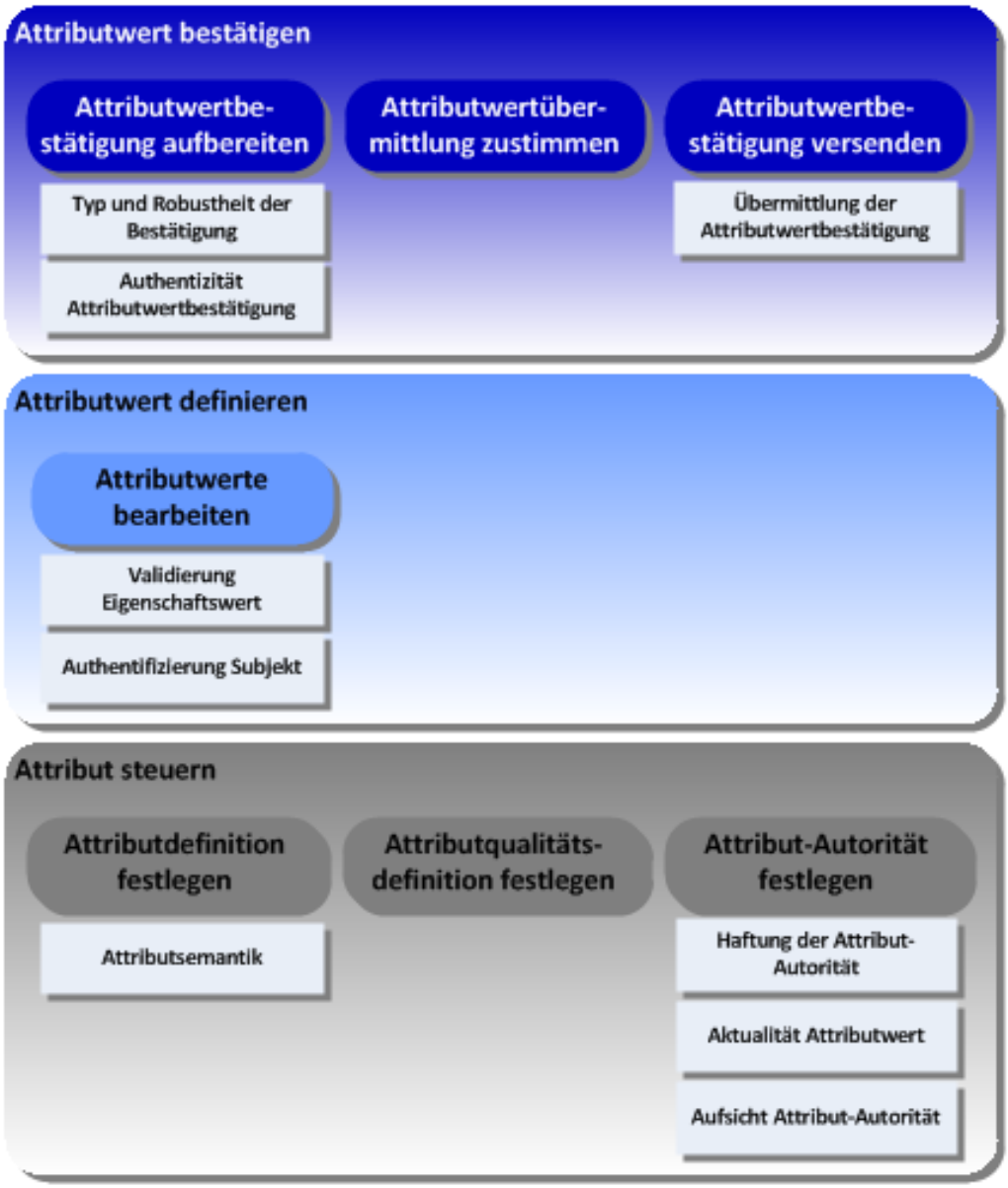

Abbildung 5: Prozesslandkarte und Zuordnung Qualitätskriterien

Anhand der definierten Prozesse werden die Qualitätskriterien abgeleitet. Nicht jeder Prozess bietet Kriterien, um die Qualität der Attributwertbestätigung zu messen. Die Prozesse werden aber, damit der Gesamtkontext berücksichtigt wird, trotzdem dargestellt. Qualitätskriterien in den Prozessen *Attribut steuern* und *Attributwert bestätigen* haben eine tiefere Ände-

rungsrate als welche aus dem Prozess *Attributwert definieren*. Sie werden daher im Rahmen der Governance einmal definiert und anschliessend in regelmässigen Abständen überprüft. Qualitätskriterien aus dem Prozess *Attribut definieren* können sich häufig ändern, da bei jeder Änderung des Attributwertes auch die Qualität ändern kann.

4.1 Attributwert bestätigen

Attributwert bestätigen umfasst alle Prozesse, die zur Ausführungszeit notwendig sind, um eine Attributwertbestätigung zu ermöglichen.

4.1.1 Attributwertbestätigung aufbereiten

Attributwertbestätigung aufbereiten	Aufbereitung der Attributwertbestätigung aus einem oder mehreren Attributen.

Tätigkeiten:

- Attributwert ermitteln oder aus bekannten Attributen berechnen.
- Die Attributwertbestätigung zu einer *eIdentity* erstellen.
- Attributwertbestätigung durch Attribut-Autorität signieren (inkl. Zeitstempel).

Qualitätskriterien:

- Kapitel 5.7 Typ und Robustheit der Bestätigung
- Kapitel 5.10 Authentizität der Attributwertbestätigung
-

4.1.2 Attributwertübermittlung zustimmen

Attributwertübermittlung zustimmen	Das Subjekt stimmt der Übermittlung der Attributwertbestätigung an die Relying Party zu.

Tätigkeiten:

- Subjekt wird für die Freigabe der Übermittlung an die Relying Party angefragt.
- Das Subjekt stimmt der Übermittlung der Bestätigung zu oder verweigert sie.

Anmerkung:

- Die Zustimmung durch das Subjekt erfolgt nur im benutzerzentrierten Ansatz.
- Die Zustimmung der Attributwertübermittlung hat aus Sicht Subjekt eine starke Auswirkung auf die Qualität von Datenschutz und Datenselbstbestimmung. Aus Sicht Relying Party ist sie jedoch irrelevant, da sie die Qualität durch eine nochmalige Kontrolle nur minimal erhöht und wird somit nicht im Qualitätsmodell berücksichtig.

Qualitätskriterien:

- keine

4.1.3 Attributwertbestätigung versenden

Attributwertbestätigung versenden	Die Attributwertbestätigung wird der Relying Party durch das Subjekt oder die Attribut-Autorität übergeben.

Tätigkeiten:

- Übergabe des Attributwerts oder der Attributaggregation an die Relying Party.

Anmerkung:

- Im benutzerzentrierten Ansatz muss die Übermittlung der Attributwertbestätigung von der Attribut-Autorität an das Subjekt mitberücksichtigt werden.

Qualitätskriterien:

- Kapitel 5.8 Übermittlung der Attributwertbestätigung

4.2 Attributwert definieren

Attributwert definieren stellt Funktionen zur Instanziierung und Pflege von Attributen zur Verfügung.

4.2.1 Attributwerte bearbeiten

Attributwerte bearbeiten	Vorgang der Attributwertebearbeitung. Dabei werden Attribute erstellt [Create], gelesen [Read], aktualisiert [Update] oder gelöscht [Delete].

Tätigkeiten:

- Das Subjekt authentisiert sich bei der Attribut-Autorität oder das Subjekt lässt sich durch die Attribut-Autorität identifizieren. Die Authentisierung kann auch über einen Broker geschehen.
- Eigenschaft auf der Basis eines Belegs validieren [Create, Update]
- Eigenschaft als Attribut speichern [Create, Update]
- Attribut einer eIdentity zuordnen [Create, Update]
- Attribut als inaktiv markieren [Delete]
- Attribut widerrufen [Delete]
- Attribut unwiderruflich löschen [Delete]
- Veränderung in einem Protokoll erfassen (minimal: Zeitstempel) [Create, Update, Delete]

Qualitätskriterien:

- Kapitel 5.6 Validierung Eigenschaftswert
- Kapitel 5.5 Authentifizierung Subjekt

4.3 Attributwertbestätigung steuern

Attributwertbestätigung steuern stellt Funktionen zu Governance, Risk und Compliance im Zusammenhang mit der Bestätigung von Attributwerten zur Verfügung.

4.3.1 Attributdefinition festlegen

Attributdefinition festlegen	Festlegung der (Meta-)Attribute und der Semantik eines Attributs.

Tätigkeiten:

- Definition der Informationsarchitektur zu Attributen
- Definition von Attributname und Attributtyp (Attributsschema festlegen)
- Festlegen und dokumentieren der Semantik des Attributs.

Qualitätskriterien:

- Kapitel 5.1 Attributsemantik

4.3.2 Attributqualitätsdefinition festlegen

Attributqualitäts-definition festlegen	Festlegen, wie Attributwertbestätigungen auf ihre Qualität hin überprüft werden können.

Tätigkeiten:

- Qualitätsmodell für Attributwertbestätigungen definieren
- Qualitätskriterien einer Attributwertbestätigung festlegen

Anmerkung:

- Durch die Definition des eCH-0171 Standards kann die Attributwertbestätigung auf ihre Qualität hin überprüft werden. Das Dokument eCH-0171 ist das Resultat aus dem Prozess *Attributqualitätsdefinition festlegen*.

Qualitätskriterien:

- keine

4.3.3 Attribut-Autorität festlegen

Attribut-Autorität festlegen	Die Zusammenarbeit wird etabliert. Dabei wird festgelegt, welche Attributwerte die Attribut-Autorität mit welcher Qualitätsstufe bestätigen darf.

Tätigkeiten:

- Zusammenarbeit zwischen Relying Party oder Broker mit Attribut-Autorität etablieren
- Einstufung der Attribut-Autorität bezüglich der Qualitätsstufe pro Attribut
- Einhaltung der Bedingungen für die Qualitätsstufe prüfen

Qualitätskriterien:

- Kapitel 5.2 Aufsicht Attribut-Autorität
- Kapitel 5.3 Aktualität Attributwert
- Kapitel 5.4 Haftung der Attribut-Autorität

5 Qualitätskriterien

Die drei Ebenen der Qualitätsdefinition der Attributwertbestätigung sind in Abbildung 6 ersichtlich. Die Bezeichnung in der Grafik bezieht sich immer auf die Qualität des entsprechenden Elements.

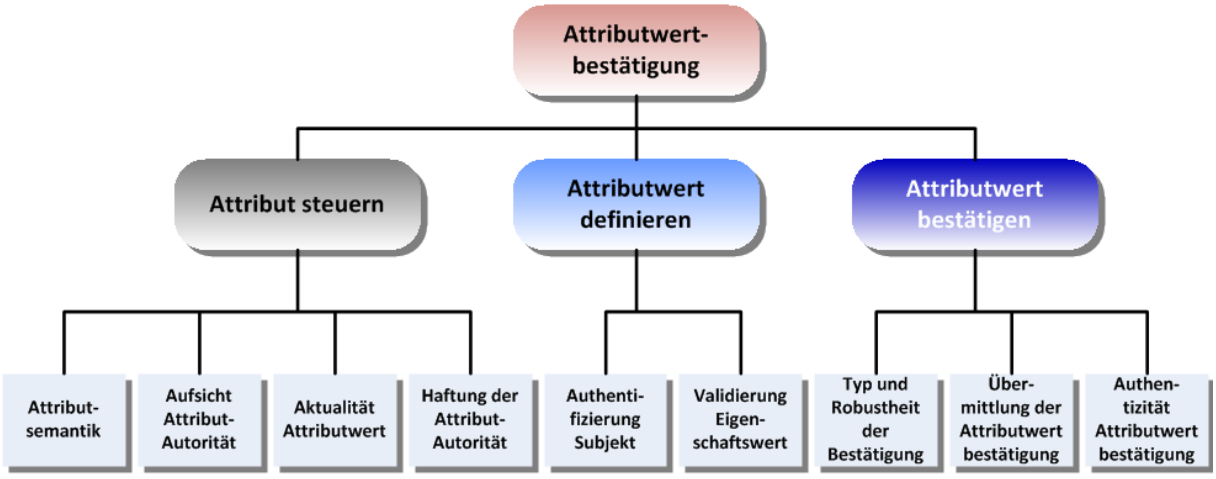

Abbildung 6: Übersicht Gesamtmodell

In den folgenden Unterkapiteln werden die Qualitätskriterien auf der untersten Ebene beschrieben und ihre Ausprägungen definiert.

5.1 Attributsemantik

Frage:	Wird der Attributname verstanden? Ist der Attributname kontextunabhängig?

Die Semantik der Attribute ist ein wichtiger Qualitätsfaktor, um die Anwendbarkeit und Benützung des Attributs zu bewerten. Mit Hilfe des Kriteriums Attributsemantik wird ausgedrückt, wie gut das Attribut definiert und verstanden wird. Ein Attribut kann je nach Kontext sehr unterschiedliche Bedeutungen aufweisen. Indem eine genaue und übergreifend genutzte Definition erstellt wird, kann die Qualität gesteigert werden.[2]

Stufe	Ausprägungen	Beschreibung
1	Keine Definition	Die Semantik ist nicht definiert und wird von Fall zu Fall neu verhandelt.
2	Allgemeine Definition	Die Definition ist allgemein bekannt, es besteht jedoch kein Standard.
3	Domänenstandard	In der Domäne ist man sich über die Semantik eines Attributs einig und hat einen entsprechenden Standard definiert.

[2] Falls das Attribut aus mehreren Attributen berechnet wird, die eine unterschiedliche Qualität aufweisen, dann wird die tiefere Qualität für das berechnete Attribut verwendet.

4	Regulatorischer Standard	Ein durch gesetzliche Regulation geforderter Standard definiert die Semantik eines Attributs.

Tabelle 5: Ausprägungen Attributsemantik

5.2 Aufsicht Attribut-Autorität

Frage:	Wie vertrauenswürdig ist die Attribut-Autorität? Wie gut ist die Prozessqualität der Attribut-Autorität?

Die Attribut-Autorität nimmt Prozesse während der Registrierung, der Definition und der Bestätigung von Attributwerten wahr. Die Prozesse sind in verschiedener Ausprägung vorhanden 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 Attribut-Autorität. Je höher die Qualität der internen Prozesse, desto kleiner muss das Risiko für Angriffe und Fehler via Social Engineering, Betrug, Fehleingaben, etc. sein.

Stufe	Ausprägungen	Beschreibung
1	Intern nach eigenem Standard oder gar nicht	Die Attribut-Autorität richtet sich nach keinen oder selber entwickelten Standards. Die Überprüfung der Einhaltung wird nicht oder von einer internen Stelle durchführt.
2	Intern nach vordefinierten Regeln/Standards	Die Attribut-Autorität richtet sich nach Standards, die öffentlich zugänglich sind und verbreitet angewendet werden. Die Überprüfung der Einhaltung der Standards lässt sie durch eine interne Stelle durchführen.
3	Externes Audit	Die Attribut-Autorität richtet sich nach Standards, die öffentlich zugänglich sind und verbreitet angewendet werden. Die Überprüfung der Einhaltung der Standards lässt sie durch eine externe Stelle durchführen.
4	Audit durch akkreditierte Stelle	Die Attribut-Autorität richtet sich nach Standards, deren Einhaltung und Überprüfung eine amtlich akkreditierte Stelle durchführt.

Tabelle 6: Ausprägungen Aufsicht Attribut-Autorität

5.3 Aktualität Attributwert

Frage:	Wie wird die Übereinstimmung von Attributwert und Eigenschaftswert sichergestellt? Welchen zeitlichen Wert der Eigenschaft enthält der Attributwert?

Eigenschaftswerte (in der realen Welt) ändern sich unabhängig von den Attributwerten (in einem System). Prozesse führen die zugehörigen Attributwerte nach, wenn sich die Eigenschaftswerte ändern. Dabei wird hier angenommen, dass sich Attributwerte selbst nicht

durch technische Störungen, etc. verändern. Die Qualität entsprechender Prozesse steigt, je zeitnäher die Anpassung erfolgt.

Stufe	Ausprägungen	Beschreibung
1	Unbekannt oder nicht definiert	Die aktuelle Übereinstimmung von Eigenschaftswert und Attributwert sind nicht bekannt.
2	Verzögerte Anpassung	Die Anpassung der Attributwerte folgt den Änderungen der Eigenschaftswerten verzögert.
3	Präventive Prüfung	Attributwerte werden auch ohne Änderungen der Eigenschaftswerte überprüft und allenfalls aktualisiert. (Um der Ineffizienz vorzubeugen, hilft ein grundlegendes Verständnis der Änderungsrate der Eigenschaftswerte).
4	Zeitnahe Anpassung	Die Änderung des Attributwerts folgt eng den Änderungen der zugehörigen Eigenschaftswerte. Die Änderung einer Eigenschaft führt automatisch oder mindestens sehr zeitnah zur Aktualisierung des abhängigen Attributwerts.

Tabelle 7: Ausprägungen Aktualität Attributwert

5.4 Haftung der Attribut-Autorität

Frage:	In welchem Umfang haftet die Attribut-Autorität?

Das Kriterium Haftung der Attribut-Autorität zeigt, in welchem Umfang die Quelle der Attributwertbestätigung bereit ist zu haften, falls sie Falschaussagen macht. Je höher die Bereitschaft zu haften, desto höher die Qualität.

Stufe	Ausprägungen	Beschreibung
1	Keine Haftung	Jegliche Haftung wird durch Vertrag resp. AGB wegbedungen.
2	Beschränkte Haftung	Die Haftung wird vertraglich beschränkt.
3	Normale vertragliche Haftung	Die Haftung der Organisation richtet sich nach den Grundsätzen des Allgemeinen Teils des Obligationenrechts (Art. 97 ff.).
4	Konventionalstrafe	Die Haftung wird durch Vereinbarung einer angemessenen kumulativen Konventionalstrafe nach Art. 163 ff. Obligationenrechts verschärft.

Tabelle 8: Ausprägung Haftung der Attribut-Autorität

5.5 Authentifizierung Subjekt

Frage:	Zu wem gehört der Attributwert?

Während der Bearbeitung des Attributwerts wird das Attribut einer eIdentity zugeordnet. Daher identifiziert die Attribut-Autorität das zugehörige Subjekt oder authentifiziert dieses elektronisch. Je besser die Qualität der Authentifizierung bzw. Identifizierung ist, desto stärker ist der Bezug zwischen Subjekt und eIdentity. Entsprechend stark ist schliesslich auch der Bezug zwischen Eigenschaft und Attribut. Damit die Qualitätsstufe der elektronischen Identität bestimmt werden kann, werden die Qualitätskriterien von eCH-0170 herangezogen. Das Resultat der Qualitätsbestimmung kann direkt für die Bestimmung der Qualität der Authentifizierung des Subjekts verwendet werden.

Stufe	Ausprägungen	Beschreibung
1	eCH-0170 Stufe 1, eCH-0170 ID-Stufe 1	Das Subjekt authentifiziert sich mit einer elektronischen Identität, die mit der eCH-0170 Stufe 1 bewertet wird. Falls der Eigenschaftswert am Schalter deklariert wird, muss die Identifizierung den Kriterien der eCH-0170 ID-Stufe 1 genügen.
2	eCH-0170 Stufe 2, eCH-0170 ID-Stufe 3	Das Subjekt authentifiziert sich mit einer elektronischen Identität, die mit der eCH-0170 Stufe 2 bewertet wird. Falls der Eigenschaftswert am Schalter deklariert wird, muss die Identifizierung den Kriterien der eCH-0170 ID-Stufe 2 genügen.
3	eCH-0170 Stufe 3, eCH-0170 ID-Stufe 3	Das Subjekt authentifiziert sich mit einer elektronischen Identität, die mit der eCH-0170 Stufe 3 bewertet wird. Falls der Eigenschaftswert am Schalter deklariert wird, muss die Identifizierung den Kriterien der eCH-0170 ID-Stufe 3 genügen.
4	eCH-0170 Stufe 4, eCH-0170 ID-Stufe 4	Das Subjekt authentifiziert sich mit einer elektronischen Identität, die mit der eCH-0170 Stufe 4 bewertet wird. Falls der Eigenschaftswert am Schalter deklariert wird, muss die Identifizierung den Kriterien der eCH-0170 ID-Stufe 4 genügen.

Tabelle 9: Ausprägungen Authentifizierung Subjekt

5.6 Validierung Eigenschaftswert

Frage:	Wie wird sichergestellt, dass die angegebenen Eigenschaftswerte zur Definitionszeit des Attributes stimmen?

Wenn der Eigenschaftswert während der Registrierung erfasst wird, wird überprüft, ob der Eigenschaftswert richtig ist. Je nachdem, welche Beweismittel zur Verfügung stehen, sind die Angaben der antragstellenden Person unterschiedlich vertrauenswürdig.

Stufe	Ausprägungen	Beschreibung
1	Selbstdeklaration	Der Eigenschaftswert wird ohne weitere Überprüfung aufgenommen.
2	Einfache Gegenprüfung	Der Eigenschaftswert wird mit Hilfe eines nicht amtlichen Ausweises, Zertifikats oder Dokuments überprüft.
3	Mehrfache Gegenprüfung	Der Eigenschaftswert wird mit Hilfe mehrerer nicht amtlichen Ausweisen, Zertifikaten oder Dokumenten überprüft.
4	Amtliches Dokument oder Datenbank	Der Eigenschaftswert wird mit Hilfe eines amtlichen Dokuments oder Datenbank überprüft.

Tabelle 10: Ausprägungen Validierung Eigenschaftswert

5.7 Typ und Robustheit der Bestätigung

Frage:	Wie stark ist die technische Absicherung der Assertion?

Mit diesem Qualitätskriterium wird gezeigt, wie gut eine Assertion gegen Veränderungen gesichert ist. Als Grundlage dient das Signieren einer Assertion. Können Assertions nicht signiert werden, dann bedeutet dies eine schlechte Qualität. Assertions die eine Signatur enthalten und höchstens mit einem privaten Zeitstempel versehen sind haben eine bessere Qualität. Die Qualität kann weiter gesteigert werden in dem die Uhr, mit der der Zeitstempel erstellt wird, öffentlich zugänglich ist und die Uhr akkreditiert wurde.

Stufe	Ausprägungen	Beschreibung
1	Keine Absicherung	Keine Absicherung
2	Private Uhr	Die Assertion wird von der Attribut-Autorität vor dem Versand signiert. Sie kann mit einem Zeitstempel versehen werden, der jedoch höchstens eine private Uhr als Zeitquelle hat.
3	Öffentliche Uhr	Die Assertion wird von der Attribut-Autorität vor dem Versand signiert. Sie ist mit einem Zeitstempel versehen, der eine öffentliche Uhr als Zeitquelle hat.
4	Akkreditierte öffentliche Uhr	Die Assertion wird von der Attribut-Autorität vor dem Versand signiert. Sie ist mit einem Zeitstempel versehen, der eine akkreditierte und öffentliche Uhr als Zeitquelle hat.

Tabelle 11: Ausprägungen Typ und Robustheit der Bestätigung

5.9 Übermittlung der Attributwertbestätigung

Frage:	Wie sicher ist die Übermittlung der Attributwertbestätigung?

Bei der Übermittlung einer Attributwertbestätigung können verschiedene Angriffe durchgeführt werden, um den Inhalt zu lesen oder zu verändern. Daher muss die Übermittlung von Attributwertbestätigung von der Attribut-Autorität zur Relying Party abgesichert werden. Die Angriffe auf die Kommunikation zwischen zwei Parteien, in diesem Fall zwischen Relying Party und Attribut-Autorität, werden in 7 Kategorien eingeteilt. [NIST 800-63-2, Kap. 8.2]

Angriff	**Beschreibung**
Online Guessing	Der Angreifer versucht durch wiederholtes Versuchen Passwörter zu erraten, welche den Kommunikationskanal oder Zertifikate schützen. Hilfsmittel sind dabei vordefinierte Listen (Dictionary Attack) und das Durchprobieren jeder Möglichkeit (Brute Force Attack).
Phishing	Die Relying Party wird mit Nachrichten, die eine Interaktion verlangen, zu einer gefälschten Attribut-Autorität gelockt oder weitergeleitet (z. B. Phishing-Mail), um ihre Credentials offenzulegen. Mit den erbeuteten Credentials ist es dem Angreifer möglich, sich als das Opfer des Angriffes auszugeben.
Pharming	Die Relying Party wird durch Manipulationen am Domain Name Service (DNS) oder Routing Tables zu einer gefälschten Attribut-Autorität geleitet, um ihre Credentials offenzulegen. Mit den erbeuteten Credentials ist es dem Angreifer möglich, sich als das Opfer des Angriffes auszugeben.
Eavesdropping	Die Kommunikation wird mitgehört und analysiert, um Informationen zu sammeln und Rückschlüsse auf den Inhalt zu machen. Anschliessend werden die Ergebnisse der Analyse für weitere Angriffe verwendet. Ziel ist meist das Mithören von Benutzernamen und Passwörter, um sich als das Opfer des Angriffes auszugeben.
Replay	Abgefangene Nachrichten werden zu einem späteren Zeitpunkt nochmals gesendet, um sich als das Opfer des Angriffes auszugeben.
Session Hijacking	Der Angreifer übernimmt eine bestehenden Verbindung oder Kommunikation (Session) zwischen Relying Party und Attribut-Autorität und gibt sich als Relying Party oder Attribut-Autorität aus.
Man-in-the-middle	Der Angreifer positioniert sich zwischen Relying Party und Attribut-Autorität und fängt jegliche Kommunikation zwischen den zwei Gesprächspartnern ab. Typischerweise gibt sich der Angreifer gegenüber der Relying Party als Attribut-Autorität aus und gegen über der Attribut-Autorität als Relying Party. So hat der Angreifer Zugriff auf alle Daten, die gesendet werden - ohne Wissen der Opfer.

Tabelle 12: Angriffsarten bei der Übermittlung der Attributwertbestätigung

Damit die Stufe der Qualität der Übermittlung der Attributwertbestätigung ermittelt werden kann, muss überprüft werden, wie resistent die verwendeten Authentifizierungsprotokolle gegen die aufgeführten Angriffsarten sind. Die Resistenz gegen die Angriffsarten wird in Tabelle 13 beschrieben. [NIST 800-63-2, Kap. 8.2.2]

Resistenz	**Beschreibung**
Online Guessing resistance	Online Guessing resistance wird erreicht, wenn es für den Angreifer praktisch unmöglich ist, mit den gegeben Wissen und Ressourcen die Credentials zu erraten.
Phishing and pharming resistance	Phishing and pharming resistance wird erreicht, wenn es praktisch unmöglich ist, dass die angegriffene Partei Informationen freigibt, welche die Imitierung der angegriffenen Partei ermöglicht.
Eavesdropping resistance	Eavesdropping resistance wird erreicht, wenn es für den Angreifer praktisch unmöglich ist, relevante Informationen abzuhören, welche für einen späteren Angriff notwendig sind. Protokolle, die Eavesdropping resistent sind, machen es dem Angreifer auch praktisch unmöglich, abgehörte Authentifikationsprotokolle lokal zu analysieren, um Informationen daraus zu gewinnen.
Replay resistance	Replay resistance wird erreicht, wenn es dem Angreifer nicht möglich ist, aufgezeichnete Nachrichten zu benutzen, um sich erfolgreich zu authentifizieren.
Session Hijacking resistance	Session Hijacking resistance wird erreicht, wenn verhindert wird, dass eine Verbindung (Session) übernommen werden kann, ohne dass dies bemerkt wird.
Man-in-the-middle resistance (weak)	Man-in-the-middle resistance (weak) wird erreicht, wenn die Relying Party sicher feststellen kann, mit welcher Attribut-Autorität sie sich verbindet.
Man-in-the-middle resistance (strong)	Man-in-the-middle resistance (strong) wird erreicht, wenn die Relying Party sicher feststellen kann mit welcher Attribut-Autorität sie sich verbindet und die Attribut-Autorität sicher feststellen kann, mit welcher Relying Party sie sich verbindet.

Tabelle 13: Resistenz gegen Angriffsarten

Die Qualitätsstufe ist abhängig von der Resistenz der Übermittlung der Attributwertbestätigung gegen die Angriffsarten. Je resistenter die Übermittlung gegen Angriffe desto höher die Qualität.

In der Tabelle 14 werden die Minimal-Anforderungen an die Resistenz für die Erreichung einer Qualitätsstufe für die Übermittlung der Attributwertbestätigung aufgezeigt.

Stufe	Online guessing resistance	Replay resistance	Session hijacking resistance	Eavesdropping resistance	Phishing/ pharming resistance	Man in the middle resistance

1	Ja	Ja	Nein	Nein	Nein	Nein
2	Ja	Ja	Ja	Ja	Nein	Weak
3	Ja	Ja	Ja	Ja	Ja	Weak
4	Ja	Ja	Ja	Ja	Ja	Strong

Tabelle 14: Anforderungen der Übermittlung der Attributwertbestätigung

5.10 Authentizität der Attributwertbestätigung

Frage:	Wie kann die Relying Party die Authentizität der Attributwertbestätigung überprüfen?

Dieses Qualitätskriterium definiert die Qualität der Authentizität der Attributwertbestätigung und stellt die Nachverfolgbarkeit sicher. Die dazu verwendeten Signaturen stellen die Integrität der Nachrichten sicher und können zudem auch zur Prüfung der Authentizität genutzt werden. Für die Verwendung von Signaturen werden Zertifikate verwendet, die in unterschiedlicher Qualität vorliegen können. Die Qualitätsbestimmung wird anhand der Klassifizierung der Zertifikatsklassen von eCH-0048 bestimmt. Je höher die Klasseneinordnung des genutzten Zertifikats, desto sicherer die Überprüfung und Überwachung der zertifikatsbesitzenden Organisation oder Person.

Stufe	Ausprägungen	Beschreibung
1	eCH-0048-Klasse 1 Zertifikat	Höchstens ein Zertifikat der Klasse 1 nach eCH-0048 wird von der Attribut-Autorität verwendet, um sich gegenüber dem Subjekt oder der Relying Party zu authentisieren.
2	eCH-0048-Klasse 2 Zertifikat	Ein Zertifikat der Klasse 2 nach eCH-0048 wird von der Attribut-Autorität verwendet, um sich gegenüber dem Subjekt oder der Relying Party zu authentisieren.
3	eCH-0048-Klasse 3 Zertifikat	Ein Zertifikat der Klasse 3 nach eCH-0048 wird von der Attribut-Autorität verwendet, um sich gegenüber dem Subjekt oder der Relying Party zu authentisieren.
4	Geregeltes Zertifikat	Ein geregeltes Zertifikat nach revidiertem ZertES[3] wird von der Attribut-Autorität verwendet, um sich gegenüber dem Subjekt oder der Relying Party zu authentisieren.

Tabelle 15: Ausprägungen Authentizität der Attributwertbestätigung

[3] Revision des ZertES ist zum Zeitpunkt der Dokumenterstellung (01.07.2014) noch in Erarbeitung.

6 Bestimmen der Qualitätsstufe

6.1 Qualität Attributwertbestätigung steuern

Die Qualitätsstufe des Prozesses *Attributwertbestätigung steuern* wird aus den vier Kriterien Attributsemantik, Aufsicht Attribut-Autorität, Aktualität Attributwert und Haftung der Attribut-Autorität abgeleitet. Die Qualitätsstufe wird hierbei durch die tiefste Ausprägung der Kriterien bestimmt. Die Qualität wird durch die Farben Rot (wenig Vertrauen) bis Grün (sehr hohes Vertrauen) unterstrichen.

Attributwertbestätigung steuern					
	Attributsemantik	1	2	3	4
	Aufsicht Attribut-Autorität	1	2	3	4
	Aktualität Attributwert	1	2	3	4
	Haftung der Attribut-Autorität	1	2	3	4
		S1	S2	S3	S4

Abbildung 7: Bestimmung Qualitätsstufe Attributwertbestätigung steuern

6.2 Qualität Attributwert definieren

Die Qualitätsstufe des Prozesses *Attributwert definieren* wird aus den zwei Kriterien Validierung Eigenschaftswert und Authentifizierung Subjekt abgeleitet. Die Qualitätsstufe wird hierbei durch die tiefste Ausprägung der Kriterien bestimmt.

Attributwert definieren					
	Validierung Eigenschaftswert	1	2	3	4
	Authentifizierung Subjekt	1	2	3	4
		D1	D2	D3	D4

Abbildung 8: Bestimmung Qualitätsstufe Attributwert definieren

6.3 Qualität Attributwert bestätigen

Die Qualitätsstufe des Prozesses *Attributwert bestätigen* wird aus den drei Kriterien Übermittlung der Attributwertbestätigung, Typ und Robustheit der Bestätigung und Authentifizierung der Attribut-Autorität abgeleitet. Die Qualitätsstufe wird hierbei durch die tiefste Ausprägung der Kriterien bestimmt.

Attributwert bestätigen					
	Übermittlung der Attributwertbestätigung	1	2	3	4
	Typ und Robustheit der Bestätigung	1	2	3	4
	Authentizität der Attributwertbestätigung	1	2	3	4
		B1	B2	B3	B4

Abbildung 9: Bestimmung Qualitätsstufe Attributwert bestätigen

6.4 Qualität Attributwertbestätigung

Um die Qualität der Attributwertbestätigung zu bestimmen, sind drei Dimensionen nötig, die durch die Prozessbewertungsstufen *Attributwertbestätigung steuern*, *Attributwert definieren* und *Attributwert bestätigen* symbolisiert werden. Die Qualitätsstufe der Attributwertbestätigung wird durch die tiefste Ausprägung der Prozessbewertungsstufen bestimmt.

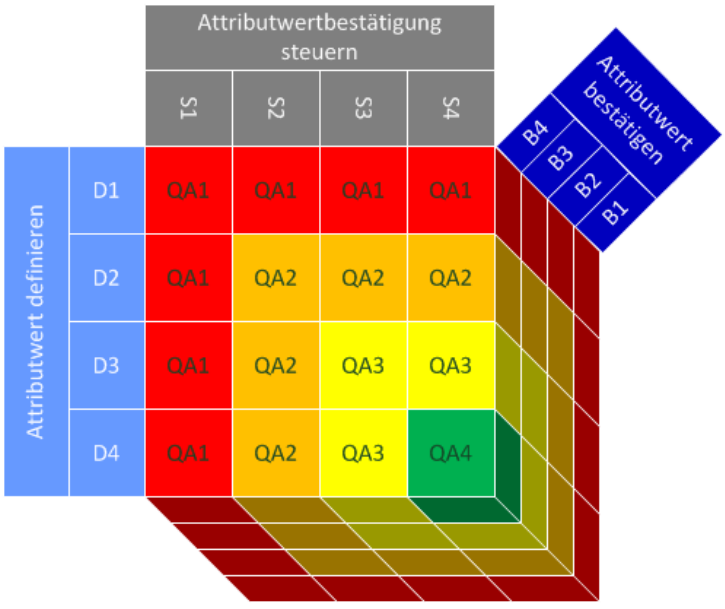

Abbildung 10: Bestimmung Qualität Attributwertbestätigung

Nur wenn jede Prozessbewertung die Stufe 4 erhält, ist die vierte Qualitätsstufe für Attributwertbestätigungen möglich.

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

[eCH-0048]	eCH-0048 PKI-Zertifikatsklassen, V1.10, 10.04.2012, http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0048&documentVersion=1.10
[eCH-0107]	eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM), V2.00, 10.09.2013, http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0107&documentVersion=2.0
[eCH-0170]	eCH-0170 Qualitätsmodell für elektronische Identitäten, V1.00, 04.09.2013, http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0170&documentVersion=1.0
[ISO29115]	ISO 29115 Information technology — Security techniques — Entity authentication assurance framework, First Edition, 01.04.2013
[NIST 800-63-2]	NIST 800-63-2 Electronic Authentication Guideline, 01.08.2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf
[STORK D3.2]	D3.2 – QAA Status Report, 07.2013, https://www.eid-stork2.eu/index.php?option=com_jdownloads&Itemid=107&view=viewdownload&catid=4&cid=31

Anhang B – Mitarbeit & Überprüfung

Martin Topfel	Berner Fachhochschule
Andreas Spichiger	Berner Fachhochschule
Thomas Jarchow	Berner Fachhochschule
Ronny Bernold	Berner Fachhochschule
Hans Häni	Berner Fachhochschule
Raffael Buff	Abraxas Informatik AG
Erich Lambelet	Bedag Informatik AG