Juli 2020

Vertrauens- und Qualitätsmanagement

Nützliche Informationen und Hinweise zur Gründung einer IDV-Domäne

Zweck dieses Dokuments

Gespräche mit potentiellen Interessenten an IDV Schweiz haben gezeigt, dass bezüglich Sicherheit, Qualitätsnormen und Vertrauensbeziehungen einige Missverständnisse vorherrschen. Das vorliegende Dokument erklärt den Zusammenhang zwischen Vertrauen und Qualität im Identitätsverbund und zeigt auf, wie IDV-Domänen eigene Regeln definieren können. Soviel sei schon vorweg verraten: Es trifft nicht zu, dass

- die Webdienste dem IDV Broker blind vertrauen müssen,
- die Webdienste jeden beliebigen Identity Provider, der bei IDV Schweiz angeschlossen ist, für die Anmeldung akzeptieren müssen,
- IDV Schweiz die Identity Provider zu einer Qualitätszertifizierung zwingt.

Definitionen

Identity Provider (IdP): Elektronischer Dienst, der digitale Identitäten von Usern verwaltet und die Identität der User überprüft (der User wird *authentifiziert*), z.B. mittels Passwort oder Smartcard oder anderweitig.

Authentisierung, *Authentisieren*: Vorgang, bei dem sich ein User von einem IdP seine Identität bestätigen lässt, auf Webseiten oft "Anmeldung" genannt. (Der gleiche Vorgang aus Sicht des IdP heisst *Authentifizierung*. Ein User authentisiert sich beim IdP, ein IdP authentifiziert den User.)

User: Natürliche Person, die sich bei einem IdP authentisiert.

Security-Ticket: Ein vom IdP herausgegebenes Datenpaket, das die erfolgreiche Authentisierung des Users bestätigt. Das Security-Ticket enthält mindestens eine Identifikationsnummer des Users und kann weitere Personendaten enthalten.

Attribute: Personendaten des Users, die der IdP im Security-Ticket mitgibt.

Relying Party (RP): Eine Dienstleistung oder Ressource, die einen authentifizierten User erfordert. Die RP überlässt die Authentifizierung einem IdP und verlässt sich auf die Angaben im Security-Ticket.

IDV-Domäne: Eine Gemeinschaft von IdPs und RPs, die sich zu einem eigenständigen Identitätsverbund zusammenschliessen. Sie legen eigene Regeln fest, definieren Qualitätsstufen und Prinzipien für gegenseitiges Vertrauen.

Ausgangslage

Der IDV Broker (kurz "Broker") vermittelt digitale Identitäten von potentiell vielen IdPs an potentiell viele RPs, im Einzelfall aber immer von genau einem IdP zu einer RP. Vermitteln bedeutet, dass die Authentisierungsanfrage der RP an den vom User bezeichneten IdP weitergeleitet wird, als würde der Broker selber die Authentisierung anfordern. Aus dem Security-Tickets des IdP erstellt der Broker ein eigenes und übergibt dieses an die RP. Bei diesem Vorgang sind sowohl die RPs als auch die IdPs auf echte und unverfälschte Informationen angewiesen. Der Broker spielt eine zentrale Rolle in der Gewährleistung von Qualität und Sicherheit; er ist der Vertrauensanker für IdPs und RPs zugleich.

Wer sich als RP oder IdP dem IDV anschliesst, wird Fragen zur Qualität und Sicherheit haben. Bevor einige davon im einzelnen beantwortet werden, sei zuvor das Prinzip der IDV-Domänen erklärt.

IDV-Domänen

Einen Identitätsverbund aufzubauen heisst, technische und organisatorische Vorgaben für die angeschlossenen Teilnehmer zu erstellen. Die Anforderungen an die IdPs hängen vom Einsatzgebiet ab, sie lauten im E-Government für Private anders als im Gesundheitswesen, im Justizumfeld oder in einem Hochschulnetzwerk. Es gibt nicht den einen Identitätsverbund, der alle Bedürfnisse abdecken kann, vielmehr benötigen die unterschiedlichen Einsatzgebiete ihren eigenen Broker. Hier kommen IDV-Domänen ins Spiel. IDV-Domänen werden von IdPs und RPs aufgebaut, die sich einem eigenen, von den Mitgliedern definierten Regelwerk unterstellen und die eigene Qualitätsstufen und Vertrauensgrundlagen festlegen.

IDV-Domänen haben die eine Gemeinsamkeit, dass sie die gleiche technische Infrastruktur nutzen, nämlich IDV Schweiz. Ansonsten sind IDV-Domänen in sich abgeschlossene Benutzerkreise, die voneinander isoliert sind. Die Mitglieder einer Domäne sehen nur ihre eigenen Mitspieler, aber keine aus anderen Domänen. Beispielsweise wird der Broker nie eine RP aus einer Domäne des Gesundheitsbereichs an einen IdP aus einer Domäne des Justizbereichs vermitteln.

Qualität, Vertrauen und das IDV Trust Framework

Qualität

Für die Qualität von Identitätsmanagementsystemen existieren nationale und internationale Standards, z.B. eCH-0170, eIDAS-Verordnung 910/2014, ISO/IEC 29115, NIST SP 800-63-3 und mehr. Alle haben ihre Stärken und Schwächen. Beim Aufbau des IDV Trust Frameworks (vgl. weiter unten) hat man sich am Qualitätsmodell von eCH-0170 orientiert, welches vier Vertrauensstufen definiert, die sich ihrerseits aus vier Qualitätsdimensionen ergeben:

- Die Qualität der Authentifizierung ergibt sich aus der Stärke und möglichen Zertifizierungen eines Authentifizierungsmittels.
- Die Qualität der Identifikation und Registrierung einer natürlichen Person bestimmt sich durch die Stärke der Identifikation und der Übergabe des Authentifizierungsmittels.
- Die Qualität der Steuerung (Governance) betrifft die Aufsicht, Haftung und Maturität.
- Die Qualität der Föderierung wird von der Authentizität, dem Vertraulichkeitsschutz, der Übermittlungsform und dem Nachweis des Besitzes der Authentifizierungsbestätigung bestimmt.

Aus den Qualitätsdimensionen ergibt sich ein Gesamtbild über die Güte der Identifikation und Authentisierung, wobei die Dimension, die am schwächsten abschneidet, das Schlussergebnis mehr oder weniger festlegt. Anders gesagt: ist eine Dimension schwach, so ist es die Gesamtqualität auch. Das macht durchaus Sinn, denn eine hohe Güte setzt eben hohe Qualität in allen Bereichen voraus. Was nützt eine technisch bestens geschützte Übertragung einer digitalen Identität (Föderierung), wenn die Identifizierung der Person lediglich über Email-Kontakt zustande kam und man im Grunde nicht weiss, mit wem man es zu tun hat?

IDV Schweiz ist nicht auf ein bestimmtes Qualitätsmodell festgelegt und überlässt die Definition der Qualitätskriterien jeder einzelnen IDV-Domäne, denn nur sie weiss, was sie braucht. Aus technischen Gründen gibt IDV Schweiz ein paar wenige Grenzen für das Qualitätsmodell vor, z.B. können in einer Domäne nicht mehr als vier Qualitätsstufen unterschieden werden. Was jede Stufe bedeutet und welche Kriterien sich dahinter verbergen, braucht der Broker nicht zu wissen. Eine Domäne kann die Stufen 1 bis 4 definieren, eine andere nur drei, A bis C, noch eine andere nennt sie Silber, Gold und Platin. Das alles ist für IDV Schweiz unbedeutend, solange die höchste vorkommende Qualität diejenige des Brokers nicht überschreitet. Was heisst das? Aus den vier Qualitätsdimensionen betrifft nur eine den Broker direkt, nämlich die Föderierung. Der Broker unterstützt die Vertrauensstufe 3 nach eCH-0170, was einer Qualität entspricht, die nur selten gefordert wird. Eine IDV-Domäne, deren Ansprüche bis auf Stufe 4 gehen, würde IDV Schweiz nicht unterstützen können. Diese Limitierung dürfte jedoch für die anvisierten Anwendungsfälle von IDV Schweiz kaum jemals ein Problem darstellen. Zum Vergleich: SuisseID wäre auf Stufe 2 einzuordnen.

Vertrauen

Es stellt sich die folgende Frage: Aus welchen Gründen soll man sich auf eine Fremdleistung verlassen, die die eigene Sicherheit betrifft und im schlimmsten Fall gefährden könnte? Im Kontext von IDV Schweiz besteht diese Fremdleistung aus zwei Komponenten, erstens das Security-Ticket eines unbekannten IdP und zweitens, die Vermittlung des Security-Tickets durch den Broker. Die Gefährdung

besteht darin, dass entweder der IdP oder der Broker oder beide ihre jeweilige Aufgabe nicht gewissenhaft oder kompetent genug ausführen und die RP in der Folge den User auf Basis eines qualitativ unzureichenden Security-Tickets autorisiert, ohne sich dessen im klaren zu sein.

Die primäre Vertrauensbeziehung ist die zwischen der RP und dem Broker. Die RP verlässt sich darauf, dass der Broker nur Security-Tickets von angeschlossenen IdPs genügend hoher Qualität vermittelt und der User im Zuge einer Anmeldung zur RP nur geeignete IdPs zur Auswahl erhält. Der Broker muss bei der Vermittlung den Qualitätsanspruch der RP mit der Authentisierungsstärke des IdP verknüpfen, was ein Qualitätsmodell voraussetzt, das von allen angeschlossenen IdPs und RPs auf gleiche Weise interpretiert und akzeptiert wird.

Grundlagen der Vertrauensbildung im IDV

Im nachfolgenden Beispiel hat die Domäne ein Qualitätsmodell mit drei Stufen festgelegt, die sie mit Level of Assurance (LOA) bezeichnet. Ein gemeinsames Verständnis über die Qualität innerhalb der Domäne bildet die Grundlage für die Vermittlungstätigkeit des Brokers.

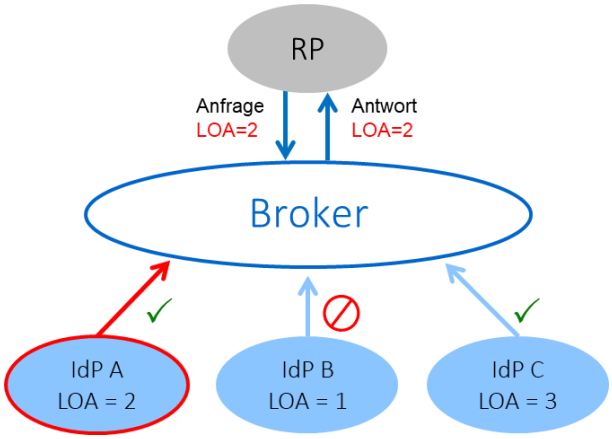

Illustration: Übereinstimmung von Qualitätsstufen bei der Vermittlung

Die RP verlangt in der Anfrage die Qualität LOA=2, was IdP B von der Vermittlung im vornherein ausschliesst. Dem User werden die IdPs A und C zur Auswahl angeboten und der User benutzt A. Die Antwort des Brokers an die RP enthält die tatsächliche Qualitätsstufe LOA=2. Hätte der User den IdP C verwendet, würde statt dessen LOA=3 in der Antwort stehen.

Damit das Vertrauen in diese Vorgänge gerechtfertigt ist, müssen zwei Voraussetzungen geschaffen werden: Erstens muss die RP über Informationen verfügen, um entscheiden zu können, ob der Broker korrekt, sicher und unter Wahrung aller Datenschutzkriterien arbeitet. Zweitens muss eine RP sich jederzeit und unabhängig vergewissern können, dass die Qualität eines IdP tatsächlich dem entspricht, was als LOA-Wert angeliefert wird. Damit ist nicht gemeint, dass bei jeder Authentisierung automatisch Kontrollen und Recherchen durchgeführt werden sollen, sondern es bedeutet, dass ein Offline-Weg vorhanden sein muss, damit RPs bei Bedarf die Qualität eines IdP überprüfen können.

Die erste Voraussetzung betrifft das Vertrauensverhältnis zwischen IDV Schweiz und der RP. Der Betrieb, die Wartung und die Weiterentwicklung des Brokers werden in Zukunft durch eine Organisation des öffentlichen Rechts geführt, in deren Steuerungsgremien u.a. Vertreter von IDV-Domänen sitzen. Das Vertrauen in IDV Schweiz ist das Vertrauen in eine funktionierende öffentliche Administration und die Qualität ihrer Dienstleistung. Will eine Domäne den Broker vertrauenstechnisch bestmöglich aus dem Spiel nehmen, so kann sie die Domäne so konfigurieren, dass der Broker das Security-Ticket des IdP seinem eigenen beilegt, was eine Überprüfung des originalen Security-Tickets ermöglicht.

Die zweite Voraussetzung betrifft das Vertrauensverhältnis zwischen IdP und RP. Der Broker selber vermittelt lediglich die aus seiner Sicht nicht verifizierbaren Angaben des IdP an die RP. Der Betreiber des Brokers kann und wird keine Garantie für diese Informationen übernehmen, seine Aufgabe ist die sichere, vertrauliche und integre Übertragung des Security-Tickets von einem Ende ans andere. Den Inhalt hat nicht er zu verantworten, das ist Sache des ausstellenden IdP. Aber genau hier liegt der Kern des Vertrauens, den die RP aufbringen müssen. Wie das Problem gelöst werden kann, hat das Projekt IDV Schweiz demonstriert. Im Rahmen des Aufbaus der Broker-Plattform wurde ein Trust Framework als Hilfestellung für künftige Domänen entwickelt. Damit ist es einer Domäne möglich, die Vertrauensbildung zwischen IdPs und RPs zu gestalten und sicherzustellen.

Trust Framework für E-Government Anwendungen

Das Trust Framework ist eine organisatorische Massnahme, damit die Mitglieder einer IDV-Domäne das nötige Vertrauen aufbauen können. Bei der Entwicklung von IDV Schweiz haben einige kantonalen Stellen aktiv mitgearbeitet und es bestand eine Bereitschaft, IDV Schweiz für die gegenseitige kantonsübergreifende Identifizierung und Authentisierung einzusetzen. Sie taten dies unter der Voraussetzung, dass ein geeignetes Instrumentarium für die gegenseitige Anerkennung der Qualitätsstufen von kantonalen IdPs existiert, auf das sich alle berufen können.

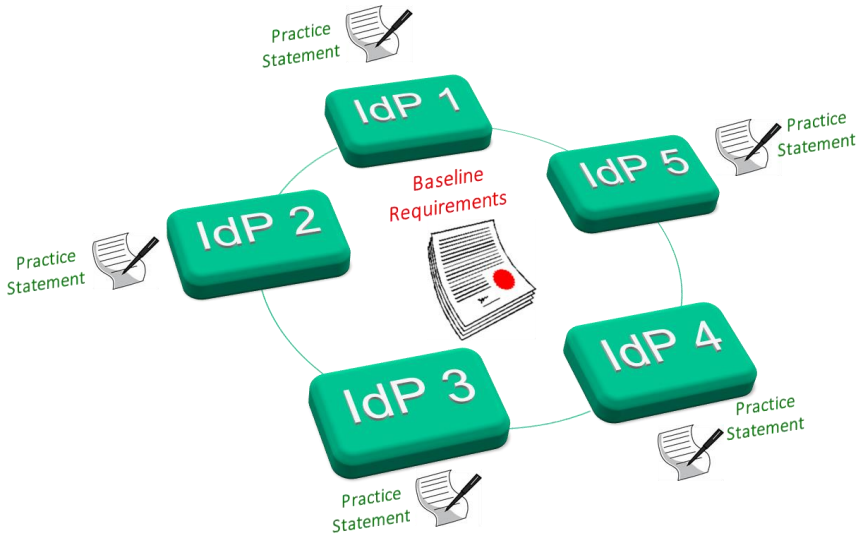

Illustration: Trust Framework

Das Trust Framework umfasst zwei Hauptartefakte: Baseline Requirements und Practice Statement. Es handelt sich um Dokumente, die sich primär an die IdPs in einer Domäne richten.

Baseline Requirements beschreiben die Qualitätsstufen und enthalten eine detaillierte Spezifikation der technischen und organisatorischen Massnahmen, die IdPs bei der Identifizierung von Personen und der Ausstellung von Security-Tickets einhalten müssen. Mithilfe dieses Dokuments lernen die RPs, welches Qualitätsmodell zur Anwendung kommt, wie sie ihre Qualitätsanforderung dem Broker mitteilen und welche Anforderungen ein IdP einhalten muss, wenn er angibt, eine bestimmte Qualitätsstufe zu erfüllen.

Practice Statements sind Selbstdeklarationen der IdPs über ihre eigene Qualität. Darin dokumentiert jeder IdP, wie die Anforderungen aus den Baseline Requirements im Einzelnen umgesetzt werden. Practice Statements sind allen Teilnehmern der Domäne zugänglich zu machen. IdPs können diese Informationen als Grundlage für ein Benchmarking verwenden, RPs werden daraus ihre Bereitschaft begründen, Security-Tickets von bis dahin unbekannten IdPs anzuerkennen, oder einfacher gesagt, den IdPs zu vertrauen.

IDV Schweiz führt selber keine Audits der IdPs durch und ist auch nicht als Schlichtungsstelle geeignet. Ein Trust Framework zu implementieren ist einzig Sache der Domäne. Sie kann die Baseline Requirements beliebig ausgestalten und z.B. das Recht auf gegenseitige Inspektion, eine Pflicht zu regelmässigen externen oder internen Audits vorsehen, eine Zertifizierung verlangen und Sanktionen vorsehen.

Was IDV Schweiz leistet, und wofür der Broker gebaut wurde, ist die garantierte, sichere Vermittlung von IdPs einer bestimmten Qualität an RPs. Der Broker verlässt sich auf die Angaben in den Authentisierungsanfragen resp. den hinterlegten Metadaten der teilnehmenden IdPs und RPs. Was der Broker macht, ist eine rein technische Vermittlung von Sicherheitsdaten.

Um teilnehmenden Kantonen eine Basis für die Errichtung einer Domäne geben zu können, wurden musterhafte Baseline Requirements erstellt. Darin wird auf 25 Seiten detailliert beschrieben, welche Massnahmen, Prozesse und technischen Funktionen ein IdP implementieren muss, wenn er die LOA-Stufe 2 gemäss eCH-0170 erreichen will. Das Dokument *Baseline Requirements for the E-Gov Domain of the Identity Network Switzerland (INS)* steht unter www.idv-fsi.ch zum Herunterladen bereit. Künftige Domänen sind eingeladen, diese Baseline Requirements als Mustervorlage für eine eigene Domäne zu verwenden.

Fragen einer Relying Party

Welche technischen Sicherheitsmassnahmen setzt IDV Schweiz um? Die Sicherheit des Brokers ist nach dem Stand der Technik entwickelt worden. Die Datenkommunikation ist verschlüsselt und durch digitale Signaturen vor unerlaubter Manipulation geschützt. Der Broker implementiert mehrere SAML-Bindings, insb. Web SSO over HTTP und Artifact Binding. Der Broker erreicht damit die Stufe LOA 3 gemäss dem Standard eCH-0170, *Qualitätsmodell zur Authentifizierung von Subjekten*.

Welche Authentisierungsstärke bieten die IdPs? Jeder IdP authentisiert den User mit den ihm zur Verfügung stehenden Mitteln. IDV Schweiz macht keine Vorgaben und die Qualität ist von IdP zu IdP unterschiedlich. Es ist der Domäne überlassen, in den Baseline Requirements eine Qualitätsskala zu definieren und die IdPs den Kriterien entsprechend zu klassifizieren. Erst dann können RPs entscheiden, welche Qualität sie vom Broker, und somit von den IdPs der Domäne, einfordern wollen.

Wie kann die Qualität eines IdP beurteilt werden? Jede Domäne definiert ihre eigene Qualitätsskala, die sie in den Baseline Requirements zugänglich macht. Darin steht, welche Massnahmen in welcher Qualitätsstufe von jedem IdP gefordert werden. Wer wissen will, wie ein bestimmter IdP diese Anforderungen im Einzelnen erfüllt, informiert sich im Practice Statement des IdP.

Kann eine Mindestqualität angefordert werden? Ja. Abhängig von der Betriebsart des Brokers wird die Mindestqualität, die eine RP für die Anmeldung benötigt, in den Metadaten hinterlegt oder dynamisch an den Broker übermittelt. In beiden Fällen wird der Broker nur IdPs für die Vermittlung berücksichtigen, welche die Qualitätsanforderung erfüllen.

Muss jeder IdP akzeptiert werden? Nein. Durch die Qualitätskriterien werden die potentiellen IdPs automatisch eingeschränkt und es werden nur solche vermittelt, die den Ansprüchen der RP genügen.

Kann man einen bestimmten IdP von der Vermittlung ausschliessen? Einen bestimmten IdP auszugrenzen gehört nicht zu den Grundfunktionen des Brokers, es werden grundsätzlich alle qualitativ geeigneten IdPs zur Vermittlung angeboten. Eine Umgehungsmöglichkeit gibt es dennoch: Falls die Domäne so konfiguriert ist, dass der Broker nebst dem eigenen, vom Broker signierten Security-Ticket noch dasjenige des IdP mitliefert, kann eine RP den für sie ungeeigneten IdP herausfiltern.

Welche Qualität gilt für die Attribute? Eine Domäne kann die Qualität von Attributen in den Baseline Requirements festlegen. Eine anderweitige Qualitätsbestimmung, z.B. in Form einer separaten Güteskala für Attribute, existiert nicht. Eine Domäne ist frei, ihre Qualitätsskala auf Basis beliebiger Kriterien zu definieren und kann die Qualität von Attributen in die Klassifizierung der IdPs mit einbeziehen.

Hängt die Menge der Attribute von der Authentisierungsqualität ab? Es obliegt der Domäne, festzulegen, ob und wie die Authentisierungsstärke mit der Menge der gelieferten Attribute korrelieren soll. Die Domäne definiert eine solche Regelung in den Baseline Requirements.

Haftet IDV Schweiz für eine falsche Authentisierung? Die Frage kann erst beantwortet werden, wenn die Betreiberorganisation feststeht. Das gilt wohlgemerkt für die Kernaufgabe des Brokers, d.h. die Vermittlung von Security-Tickets. Die Domänen sind frei, ein Haftungsregime zu etablieren, um das Vertrauen in die IdPs weiter zu stärken und im Fehlerfall Sanktionen auszusprechen.

Fragen eines Identity Providers

Welche Authentisierungsstärke ist für die Teilnahme am IDV erforderlich? Grundsätzlich steht IDV Schweiz jedem IdP offen, IDV Schweiz gibt die Qualität nicht vor. Eine Domäne wird für sich festlegen, welche Kriterien ein IdP zur Teilnahme erfüllen muss.

Wird eine Zertifizierung benötigt? IDV Schweiz gibt nichts dergleichen vor. Jede Domäne definiert für sich, welche Qualitätskriterien sie den IdPs auferlegt, eine Zertifizierung kann Teil davon sein.

Woher kommen die Qualitätskriterien? Eine Domäne setzt sich aus Teilnehmern zusammen, die sich einem gemeinsamen, von allen getragenen Regelwerk unterstellen. Die Definition der Qualitätsstufen und die Kriterien zu ihrer Einhaltung werden in den Baseline Requirements definiert.

Wo steht der eigene IdP im Vergleich mit anderen? Gemäss dem IDV Trust Framework zeigt ein IdP in seinem Practice Statement detailliert auf, welche technischen und organisatorischen Massnahmen er zur Einhaltung der Qualitätsanforderung ergreift. IdPs können ihre eigenen Massnahmen mit denen anderer vergleichen.

□