Februar 2020

Technische Anbindung des IDV Brokers

Rahmenbedingungen aus der Perspektive der Relying Party

Zweck dieses Dokuments

Der IDV Broker setzt Identity Federation technisch um. Das vorliegende Dokumente erläutert die verschiedenen Betriebsoptionen des IDV Brokers und nennt die Rahmenbedingungen, die eine Relying Party bei der Einbindung des IDV Brokers berücksichtigen muss.

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.

Ausgangslage

Moderne RPs sind so aufgebaut, dass sie die Authentifizierung nicht selber vornehmen, sondern dafür einen (externen) IdP einbinden, dem sie genügend vertrauen. Zudem will man es dem User einfach machen und ihm eine Auswahl von IdPs anbieten, aus denen er auswählen und die Anmeldung durchführen kann. Idealerweise soll ein User keine separate Registrierung bei der RP durchführen müssen und sich statt dessen bei einen der zur Verfügung stehenden IdPs anmelden können.

Dieses Prinzip setzt voraus, dass die RP für jeden IdP, den sie den Usern als "Anmelde-Option" anbietet, eine Vertrauensstellung aufbaut und dessen Security-Ticket interpretieren und validieren kann. Security Tickets von verschiedenen IdPs sind in der Regel unterschiedlich aufgebaut, was für RPs hohe technische und organisatorische Mehraufwände mit sich bringt, weil jeder IdP einzeln integriert werden muss.

Die Lösung: Ein zwischengeschalteter Dienst übernimmt die technische und organisatorische Anbindung von IdPs und präsentiert sich gegenüber der RP als IdP, den diese technisch einbinden muss. Aus Sicht der RP gibt es nur einen einzigen IdP, der für theoretisch beliebig viele andere IdPs stellvertretend agiert. Dieser eine zentrale IdP wird *Identity Broker* genannt, das beschriebene Verfahren nennt sich *Identity Federation*.

Konzeptionelle Grundlagen

Generische Anwendungsfälle für Identity Federation

Ein Identity Broker ist aus Sicht einer RP ein IdP und deckt die gleichen generischen Hauptanwendungsfälle ab:

(1) *Authentisierung* (Authentication Brokering). Der Identity Broker vermittelt einen geeigneten IdP für die Authentisierung bei einer RP.

(2) *Identifizierung* (Identity Brokering). Der Anwendungsfall ist weniger häufig als die reine Authentisierung und wird beispielsweise für eine User-Registrierung eingesetzt. Der Identity Broker vermittelt einen IdP, der nebst einer Authentisierungsbestätigung Attribute des Users, d.h. Personendaten, mitgeben kann.

(3) *Zustandsabfrage* (Attribute Brokering). Der Identity Broker vermittelt einen geeigneten IdP für die (wiederkehrende) Abfrage von sich zeitlich verändernden Attributen. Solche Attribute können sein: "ist älter als 18 Jahre" (isOver18) oder "ist Mitglied von" (isMemberOf).

User Identifikator (nameID)

Zur eindeutigen Unterscheidung erhält jeder User eines IdP eine Nummer, den *User Identifikator*, technisch: *nameID*. nameID wird im Security-Ticket an die RP mitgegeben. Es werden zwei Arten unterschieden:

- *Persistent* (dauerhaft zugewiesen): nameID lautet in jedem Security-Ticket, das der IdP über die Zeit für einen bestimmten User ausgibt, stets gleich.
- *Transient* (zwischenzeitlich zugewiesen): nameID wechselt mit jedem Security-Ticket, das der IdP für einen bestimmten User ausgibt.

Persistent ist die gängige Art der Identifikation und ermöglicht es einer RP, den User in wiederholten Anmeldungen wiederzuerkennen und eine Historie von Aktionen des Users aufrechtzuerhalten, z.B. in Form eines Benutzerkontos.

Transient ist eine geeignete Technik, um User-Anonymität zu implementieren. Wiederholte Anmeldungen können von den RPs dem User nicht zugeordnet werden und es kann weder ein Profil noch eine Historie über die Aktionen des Users erstellt werden.

Aggregation und Identity-Linking

Dem Identity Broker sind im Normalfall unterschiedliche IdPs angeschlossen, wovon einige ausschliesslich den Anwendungsfall Authentisierung unterstützen, andere zusätzlich den Anwendungsfall Identifikation, d.h. sie verfügen über Personendaten des Users.

Aggregation

Aggregation bezeichnet die Zusammenführung von Attributen aus unterschiedlichen IdPs. Beispiel: IdP A enthält Personalien, wie Name, Vorname und mehr. IdP B ist an ein Personenregister angebunden, das u.a. Heimatorte von Personen enthält. Eine RP, welche eine Authentisierungsbestätigung mit Name, Vorname und Heimatort des Users benötigt, hat zwei Möglichkeiten, Daten zu aggregieren:

a) *Durch die RP gesteuert*: Die RP fordert in einer ersten Anfrage an den Identity Broker Name und Vorname des Users sowie eine Authentisierungsbestätigung. In einer zweiten Anfrage wird der Heimatort abgefragt. Es handelt sich somit um zwei aufeinanderfolgende Abfragen an den Identity Broker, die einzelnen Ergebnisse werden danach von der RP zusammengeführt.

b) *Durch den Broker gesteuert*: Die RP fordert mit einer einzigen Anfrage Name, Vorname und Heimatort beim Identity Broker an. Dieser orchestriert zwei separate interne Anfragen, eine an den IdP A und eine an den IdP B. Danach führt er die einzelnen Ergebnisse zusammen und übergibt sie an die RP.

Identity Linking

Um Attribute aus unterschiedlichen IdPs zusammenzuführen, muss der Identity Broker von jedem User wissen, ob dieser bei einem angeschlossenen IdP registriert ist und falls ja, unter welcher nameID. Nur so ist es ihm möglich, bei einer Attributabfrage die zum User passenden Attribute bei allen IdPs anzufordern. Das Prinzip, wonach der Identity Broker die unterschiedlichen nameID eines Users bei den IdPs kennt, heisst *Identity-Linking*.

Ohne Identity-Linking ist es der RP überlassen, die unterschiedlichen nameID eines Users zusammenzuführen und entsprechende Einzel-Abfragen beim Identity Broker durchführen zu lassen. Das erfordert entweder eine Kooperation und Datenaustausch zwischen der RP und allen IdPs, was in den meisten Fällen Datenschutzprobleme mit sich bringt, oder aber die aktive Mitwirkung des Users, damit dieser seine verschiedenen nameID in einem speziellen Abgleich-Prozess dem Identity Broker bekannt gibt. Letzteres ist ein komplexer Vorgang, aber auch eine Herausforderung in Sachen Usability und einem normalen User nur schwer vermittelbar.

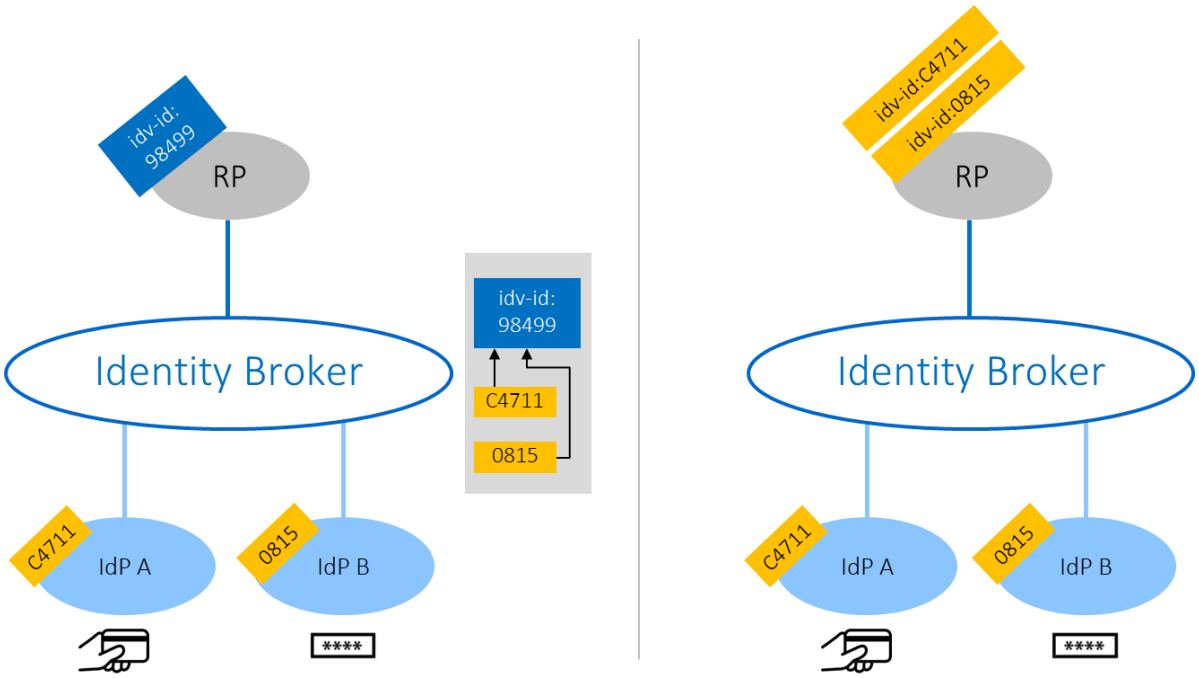

Illustration: Identity Linking (links: mit, rechts: ohne)

Attribut-Linking und Attribut-Harmonisierung

Im Allgemeinen verwendet jeder IdP eigene Bezeichnungen für Attribute. Beispielsweise kann das Attribut für den Vornamen bei IdP A *name* heissen und bei IdP B *firstName*. Wenn eine RP das Attribut Vorname anfordert und er hätte dafür den IdP B ausgewählt, so würde der Identity Broker das Attribut *firstName* beim IdP abfragen. Der Identity Broker muss also für jeden IdP wissen, wie dieser ein bestimmtes Attribut nennt und die von der RP angefragten Attribute entsprechend dieser Nomenklatur transformieren. Diese Eigenschaft des Identity Brokers wird *Attribute-Linking* genannt.

Attribut-Harmonisierung bedeutet, dass alle IdPs ein bestimmtes Attribut gleich bezeichnen, was ein Attribut-Linking obsolet macht. Beispielsweise könnte das Attribut für den Vornamen von allen *name* genannt werden. Attribut-Harmonisierung setzt eine organisatorische Vereinheitlichung voraus, was für Gruppen von IdPs einer bestimmten Anwenderdomäne oder Branche eine Option sein kann.

Aggregationsverfahren

Es existieren mehrere Verfahren, wie ein Identity Broker Attribute aus den IdPs aggregieren kann.

(1) Abfrage an einen IdP: Der Identity Broker agiert als Discovery Service (welcher IdP führt welche Attribute?). Eine Aggregation erübrigt sich, da die Attribute aus nur einem IdP stammen.

(2) Abfrage an mehrere IdPs mit harmonisierter nameID: Das Verfahren eignet sich für Gruppen von IdPs und Anwenderdomänen, die einem gemeinsamen Regelwerk unterstellt sind und für die User einheitlich den gleichen nameID einsetzen, z.B. die Sozialversicherungsnummer AHVN13 oder die SuisseID Nummer.

(3) Abfrage an mehreren IdPs ohne harmonisierte nameID: Das komplexeste Verfahren überhaupt, da es sowohl Identity-Linking als auch Attribut-Linking voraussetzt.

Proxying

Relaying gem. eCH 0168 bedeutet, dass der Identity Broker das originale Security-Ticket des IdP ohne weitere Transformation von Attributnamen und nameID an die RP weiterreicht.

Proxying gem. eCH 0168 bedeutet, dass ein Identity Broker das Security-Ticket des IdP als Basis für das eigene Security-Ticket verwendet und dieses der RP übergibt.

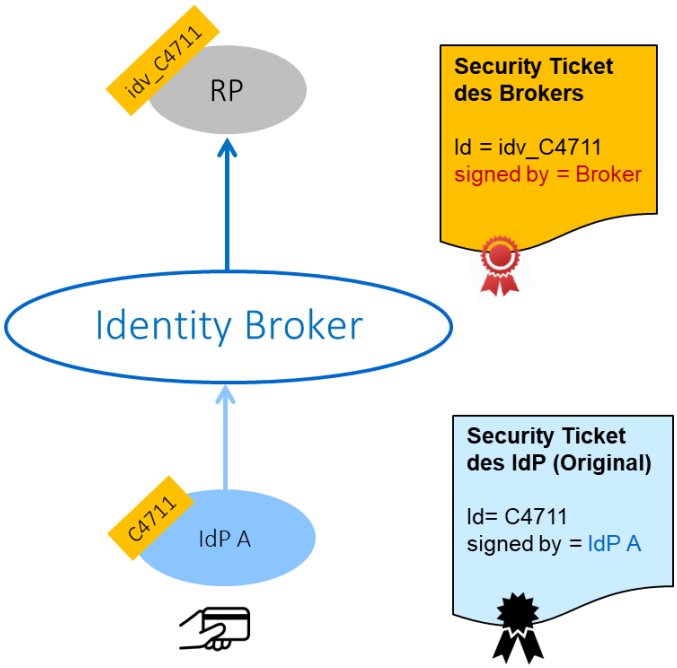

Illustration: Proxying

IDV Broker

Der IDV Broker ist ein Identity Broker und implementiert das Identity Federation Prinzip. Dem IDV Broker angeschlossen sind verschiedene IdPs und RPs. Diese verwenden eine standardisierte Schnittstelle für die Kommunikation von und zum IDV Broker.

Der IDV Broker führt selber keine Authentisierung durch, sondern delegiert diese Aufgabe an einen der IdPs (A oder B in der Illustration). Sobald sich der User bei der RP anmelden will, schaltet sich der IDV Broker dazwischen und bietet ihm die angeschlossenen IdPs zur Auswahl an. Der User wählt einen IdP, z.B. A, und führt die Authentisierung bei diesem durch.

Das beschriebene Vorgehen setzt voraus, dass der User bei mindestens einem der angeschlossenen IdPs registriert ist und dort die Authentisierung durchführen kann. Falls diese Voraussetzung nicht erfüllt ist, muss sich der User bei der RP auf herkömmliche Art und Weise registrieren und authentisieren.

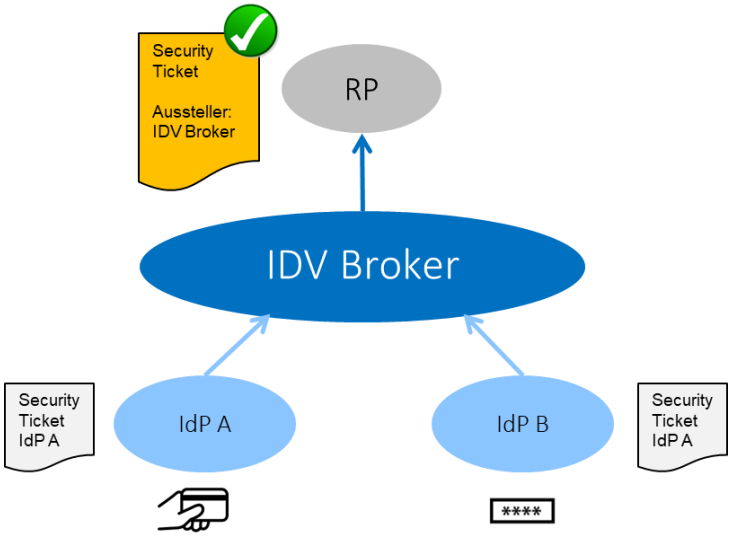

Illustration: Identity Federation mit IDV Broker

IDV Broker Betriebsmodus

IDV Broker unterstützt den Betriebsmodus *Proxying* gem. eCH 0168 mit Erweiterungen, konkret:

- Der IDV Broker ermöglicht die Authentisierung resp. den Bezug von Attributen aus einem der angeschlossenen IdPs (vgl. Aggregationsverfahren 1 auf Seite 3).
- Der IDV Broker verwendet das Security Ticket des IdP, bei dem der User sich authentisiert hat, und erstellt ein neues Security Ticket in eigenem Namen und durch den IDV Broker signiert.
- Der IDV Broker kann so konfiguriert werden, dass nameID wahlweise persistent oder transient ist. Persistent hilft der RP, den User bei wiederholten Anmeldungen als den gleichen Kunden wiederzuerkennen, wohingegen transient den Kunden wirksam anonymisiert.
- Es kann nicht ausgeschlossen werden, dass zwei unterschiedliche Personen bei verschiedenen IdPs einen gleichlautenden nameID besitzen. Der IDV Broker stellt die Eindeutigkeit von nameID über alle IdPs sicher, d.h. er erstellt eine eigene nameID und übergibt diese im Security Ticket an die RP.
- Der IDV Broker setzt Attribut-Harmonisierung um, indem er Attribute nach vorgegebenen Regeln transformiert. Die Attributbezeichnung, die der IdP intern verwendet, wird ausgeblendet und ist irrelevant. Beispielsweise erhält die RP vom IDV Broker stets das Attribut *firstName* für Vornamen, auch wenn der IdP das Attribut bei sich unter einer anderen Bezeichnung führt.
- Die RP vertraut dem IDV Broker und kann auf eine separate Überprüfung des originalen Security Tickets des IdP verzichten.

Hinzu kommt eine zusätzliche Anforderung:

- Der IDV Broker kann so konfiguriert werden, dass das originale Security-Ticket des IdP demjenigen des Brokers beigefügt wird. Damit erhält die RP die Möglichkeit, die Herkunft und Echtheit der vom IdP bestätigten Daten zu überprüfen.

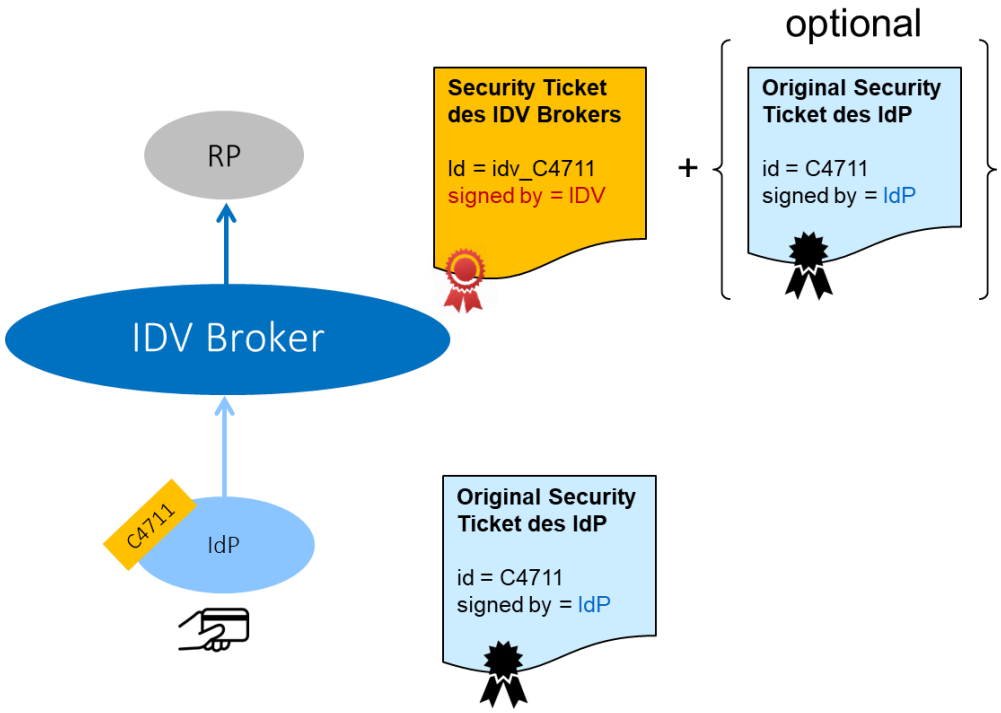

Illustration: Proxying mit originalem Security-Ticket

Mit dem Proxying-Modus erhält der IDV Broker Informationen über die Verbindung von User-zu-RP und User-zu-IdP und er verarbeitet die durch ihn vermittelten Attribute im Klartext. Darum müssen die RPs dem IDV Broker volles Vertrauen entgegenbringen, insbesondere können sie nicht überprüfen, welcher IdP das originale Security Ticket ausgestellt hat. Proxying ist die "normale Werkseinstellung" des IDV Brokers und die RPs stützen ihr Identity-Management weitgehend darauf ab.

Mit der Option, das originale Security-Ticket beizufügen, ist die RP nicht darauf angewiesen, dem IDV Broker allein zu vertrauen. Die RP erhält zusätzliche Informationen über die Verbindung zwischen User und IdP, was datenschutztechnisch nachteilig sein kann.

Anmeldung bei wechselnden IdPs

Szenario: Der User meldet sich bei der RP unter abwechselnder Verwendung von unterschiedlichen IdPs an, z.B. einmal über IdP A und ein anderes Mal über IdP B. Im ersten Fall wird nameID *C4711* gemeldet, im zweiten Fall *0815*.

Damit die RP eine Person bei Verwendung unterschiedlicher IdPs als den gleichen User erkennen kann, müsste der IDV Broker Identity-Linking anbieten und ein Verfahren implementieren, um die verschiedenen nameID des Users im Broker logisch zu verknüpfen. Ohne Identity-Linking kann die RP nicht unterscheiden, ob die nameID zweier unterschiedlicher IdPs zum gleichen User gehören oder nicht.

Identity-Linking ist beim IDV Broker aus Gründen der Usability und des Datenschutzes nicht umgesetzt worden. Das ist einer der Gründe, wieso der IDV Broker keine User-Konten benötigt. User müssen keine Einstellungen oder Daten verwalten, der IDV Broker ist für sie lediglich als Suchfunktion zur Ermittlung geeigneter IdPs wahrnehmbar und bleibt ansonsten im Hintergrund.

Eine RP ist frei, dem User ihr eigenes Identity-Linking anzubieten. Sie muss dazu den User in einen Abstimmungsprozess einbinden, was eine Herausforderung betr. Usability, Sicherheit und Datenschutz darstellen kann.

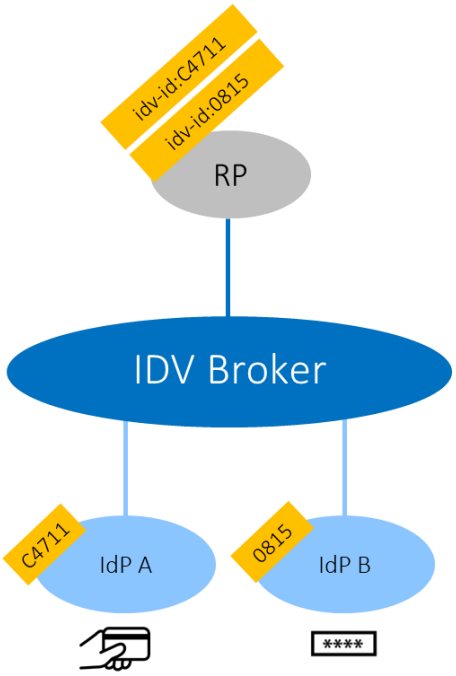

Illustration: Anmeldung des Users bei wechselnden IdPs

Anonymisierung des IdP

In manchen Fällen ist es erwünscht, die Herkunft eines Security Tickets zu verschleiern, man spricht von *Anonymisierung des IdP*. Meistens geht es darum, dass die RP nicht erkennen soll, bei welchem IdP sich der User angemeldet hat, weil daraus Rückschlüsse auf den User selbst möglich sind. Beispiel: Ein User, der den IdP der Polizei verwendet, soll durch die RP nicht als Mitarbeiter der Polizei identifiziert werden können. Aus diesem Grund wird der IdP im Security Token nicht aufgeführt.

Der IDV Broker kann so konfiguriert werden, dass er den IdP, bei dem sich der User angemeldet hatte, nicht preisgibt. RPs müssen darauf vorbereitet sein, dass sie weder das originale Security Tikket verifizieren noch dessen Ursprung ermitteln können. Anonymisierung des IdP setzt volles Vertrauen in den IDV Broker voraus.

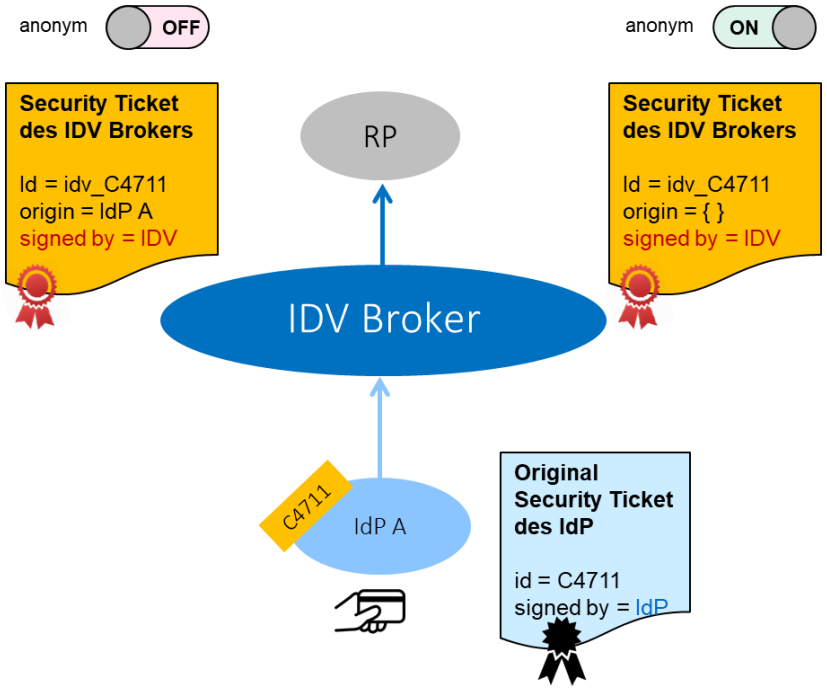

Illustration: Anonymisierung des IdP ist konfigurierbar

Fazit: Technische Integration des IDV Brokers für RPs

RPs, die den IDV Broker in einsetzen, müssen die folgenden Rahmenbedingungen berücksichtigen.

1. Der IDV Broker vermittelt digitale Identitäten von Usern aus angeschlossenen IdPs und teilt der RP im Security Ticket eine eindeutige nameID des Users mit, die nicht mit der nameID des verwendeten IdP übereinstimmt. Es ist die nameID des IDV Brokers.
2. Der IDV Broker ist so konzipiert, dass die IdPs und RPs ihm grundsätzlich vertrauen. Ein Security Ticket validieren heisst sicherstellen, dass der IDV Broker der Herausgeber ist. So müssen RPs nur eine einzige IdP-Schnittstelle integrieren, jene des IDV Brokers, um Zugang zu den angeschlossenen IdPs zu erhalten.
3. Der IDV Broker kann wahlweise persistente oder transiente nameID unterstützen. Persistente nameID sind nur dann möglich, wenn die angeschlossenen IdP ihre eigenen nameID ebenfalls persistent liefern. Transiente nameID können vom IDV Broker immer unterstützt werden.
4. Sofern ein IdP persistente nameID verwendet, so bleibt die nameID, die der IDV Broker in seinem Security Ticket mitgibt, für diesen IdP ebenfalls persistent.
5. Der IDV Broker unterstützt kein Identity-Linking. Die vom IDV Broker mitgegebene nameID lautet für den gleichen User je nach IdP anders.
6. Der IDV Broker kann das originale Security Ticket des IdP mit seinem eigenen mitliefern. So kann die RP die Herkunft und Echtheit bei Bedarf separat überprüfen, d.h. die RP muss dem IDV Broker nicht uneingeschränkt vertrauen.
7. Der IDV Broker kann den verwendeten IdP maskieren, damit die RP diesen nicht identifizieren kann und nicht weiss, wo sich ein User authentisiert hat (Anonymisierung des IdP).
8. Der IDV Broker unterstützt die Attribut-Aggregation aus verschiedenen IdPs nicht. Werden Attribute aus mehreren IdPs benötigt, so ist die RP für die serielle Abfrage bei den IdPs und die Zusammenführung der Attribute selber verantwortlich.