Kurzfassung des WPV-Rulebooks

Der WPV soll eine Kooperationsbasis für verschiedene Diensteanbieter im Internet bieten, um durch organisationsübergreifende Nutzung von Benutzeridentitäten elektronische Geschäftsprozesse sicherer und effizienter abwickeln zu können. Somit muss nicht für jede Beziehung zwischen einem Benutzer und einem Service ein eigener Benutzer-Account angelegt werden. Stattdessen übermittelt ein Identity Provider (IdP) auf Betreiben des Benutzers dessen Identität und/oder bestimmte Attribute an einen Service Provider (SP). Die dafür erforderliche rechtliche, organisatorische und technische Abstimmung leistet das Rulebook als zentrale, für alle Teilnehmer verbindliche rechtliche Grundlage der operativen Tätigkeit des WPV.

Architektur des WPV

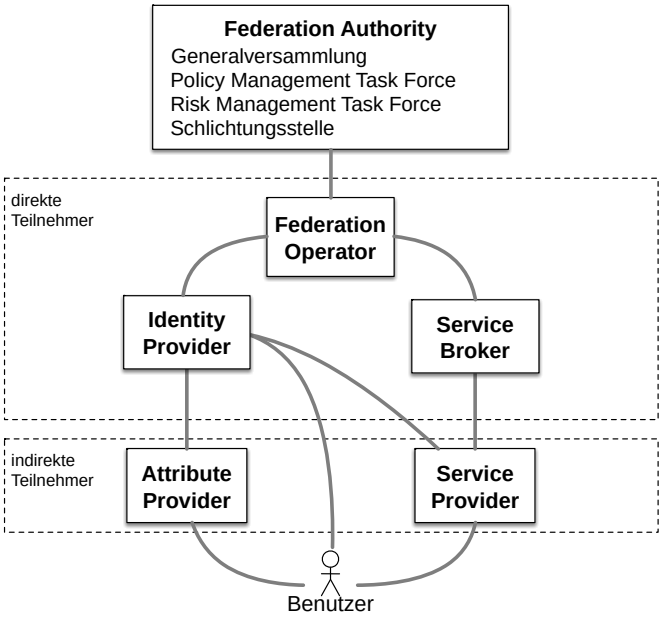
Der Verein „Wirtschaftsportalverbund – Verein zur Entwicklung und Organisation föderierter Identitätsmanagementsysteme“ ist die zentrale Trägerorganisation (Federation Authority, FA) für die Governance des WPV. Unter dieser Governance können mehrere unabhängige Federations existieren, die von je einem Federation Operator (FO) betrieben werden. Somit ergeben sich zwei Verwaltungsebenen: Die globale Ebene (WPV) sowie die Ebene der einzelnen Federations. Angelegenheiten, die nicht im Rulebook geregelt sind, können vom FO auf Ebene einer einzelnen Federation geregelt werden.

Zu den Kernfunktionen der FA gehören:

- Pflege des Rulebooks unter Mitbestimmung der Teilnehmer
- Abschluss von FO-Verträgen mit FO zur Errichtung von Federations
- Sicherstellung der Einhaltung des Rulebooks
- Bearbeitung von Konflikten und von Meldungen über Vorfälle

Zu den Kernfunktionen der FO gehören:

- Pflege und Publikation der Federation-spezifischen Policy-Dokumente
- Abschluss und Verwaltung von Verträgen mit IdP und SB sowie Akkreditierung von SP
- Betrieb eines Verzeichnisdienstes für SB und IdP sowie technische Metadaten
- Bearbeitung von Konflikten und von Meldungen über Vorfälle auf Federation-Ebene



Eine zentrale Rolle in jeder Federation spielen die **Service Broker (SB)**. Sie erfüllen zwei wesentliche Funktionen:

- Sämtliche Transaktionen zwischen IdP und SP müssen über einen SB laufen, sodass der IdP nicht unmittelbar feststellen kann, mit welchen SP der Benutzer interagiert (Beschränkung der Beobachtbarkeit, siehe Kasten nächste Seite)
- SB sind die einzigen Vertragspartner der SP und die technischen Ansprechpartner bei der Integration der SP in eine Federation.

Teilnahme am WPV, Akkreditierung und Audits

Teilnehmer (FO, IdP, AP, SB und SP) können natürliche Personen, Personengemeinschaften oder juristische Personen sein. Diese werden zu Teilnehmern, indem sie in der Absicht, eine bestimmte Rolle einzunehmen, einen bilateralen Vertrag mit einem bestehenden direkten Teilnehmer schließen, der dieser Rolle in der Hierarchie direkt übergeordnet ist, und sich in diesem Vertrag zur Einhaltung des Rulebooks verpflichten. Ein solcher Vertrag ist Voraussetzung für eine Akkreditierung.

Bevor sie ihren Betrieb aufnehmen können, müssen Federations, IdP, SB und SP akkreditiert werden. Die Akkreditierung von Federations, IdP oder SB wird von der FA durchgeführt. Die Akkreditierung von SP wird vom FO durchgeführt. Attribute Provider (AP) sind nur mittelbar Teil einer Federation: Ein IdP kann auf seine eigene Verantwortung Attribute, die ein AP von einem Benutzer kennt, in einer Federation bereitstellen. Der AP tritt dabei in der Federation nicht in Erscheinung.

Die Einhaltung des Rulebooks durch die einzelnen Teilnehmer wird durch externe Auditoren überprüft.

Unvereinbarkeiten

Teilnehmer dürfen keine Aktivitäten betreiben, die geeignet sind, das Vertrauen in ihre Leistungen oder in das Gesamtsystem zu beeinträchtigen. Das Rulebook definiert deswegen auch Unvereinbarkeiten, insbesondere zwischen den Rollen FO, IdP und SB. Im Einvernehmen mit der FA können auf Basis einer Risikoanalyse auch Ausnahmen davon festgelegt werden.

Rechte und Pflichten der Teilnehmer

Alle Teilnehmer sind verpflichtet, das Rulebook einzuhalten sowie die ihnen aufgrund ihrer Rolle zukommenden Aufgaben nach dem Stand der Technik mit der Sorgfalt eines ordentlichen Unternehmers zu erfüllen und insbesondere angemessene Datensicherheitsmaßnahmen zu ergreifen. Darüber hinaus sind im Rulebook für Teilnehmer folgende Pflichten näher geregelt:

- Geheimhaltung
- Datenminimierung
- Einhaltung aller anwendbaren Datenschutzbestimmungen
- Meldung von Vorfällen, Konflikten und eigenen oder fremden Verstößen gegen Gesetze oder das Rulebook
- Logging, dreijährige Aufbewahrungspflicht für Transaktionsdaten sowie Datenherausgabe in bestimmten Fällen
- Keine Weiterverwendung von Benutzerdaten für systematisches Identity Management ohne WPV

Das Rulebook enthält darüber hinaus verpflichtende spezifische Regeln für FO, IdP, SB und SP insbesondere zu Fragen der Aufnahme des Betriebs, des laufenden Betriebs und der Einstellung des Betriebes bzw. der Teilnahme

Spezielle Datenschutzprinzipien des WPV:

Beschränkung der Verknüpfbarkeit
Die personenbezogenen Daten eines Benutzers dürfen bei der Übermittlung an unterschiedliche Teilnehmer oder an denselben Teilnehmer für unterschiedliche Zwecke nicht mit demselben Identifikationsschlüssel versehen werden, sodass die Übermittlungsempfänger nicht in der Lage sind, die personenbezogenen Daten eines Benutzers, die sie jeweils innehaben, mittels deren Identifikationsschlüssel zu verknüpfen. Unabhängig davon darf ein Teilnehmer auch nicht auf andere Weise personenbezogene Daten über Benutzer des WPV mit einem anderen Teilnehmer austauschen oder abgleichen oder an diesen übermitteln.

Beschränkung der Beobachtbarkeit
Ein IdP darf weder einsehen können noch Daten darüber speichern können, welche SP ein Benutzer verwendet und insbesondere an welche SP Attributsdaten eines Benutzers übertragen werden. Dies gilt nicht nur als Verpflichtung des IdP, sondern ist durch die technische Implementierung des Gesamtsystems auszuschließen. Ein SB darf Attributsdaten von Benutzern nicht verarbeiten können. Zu diesem Zweck ist deren Speicherung sowie unberechtigte Nutzung und Weitergabe durch SB-interne oder externe Angreifer mittels organisatorischer und technischer Maßnahmen des Gesamtsystems auszuschließen. Dabei sind Maßnahmen, bei denen die Attribute dem SB nicht im Klartext zugänglich sind, anderen Maßnahmen vorzuziehen.

Haftung und Entzug der Akkreditierung

Jeder Teilnehmer ist verpflichtet, einen anderen Teilnehmer sowie die FA zur Gänze schad- und klaglos zu halten, wenn aufgrund seines Verstoßes gegen das Rulebook oder seines sonstigen rechtswidrigen Verhaltens der andere Teilnehmer oder die FA einen Schaden erleidet oder von einem Dritten in Anspruch genommen wird.

Beseitigt der Teilnehmer den gegen dieses Rulebook bzw. gegen einschlägige gesetzliche oder vertragliche Bestimmungen verstoßenden Zustand nicht oder sind Art oder Folgen des Verstoßes so gravierend, dass dem Teilnehmer kein Vertrauen mehr entgegengebracht werden kann, kann ihm die Akkreditierung entzogen werden.

Datensicherheitsvorgaben

Technische Spezifikationen werden initial nicht vorgegeben, können aber als Recommendations (d.h. nicht verpflichtend) ins Rulebook aufgenommen werden. Auf Federation-Ebene müssen verpflichtende technische Spezifikationen vorgegeben werden.

Ausnahmen vom Rulebook

Die FA kann in begründeten Ausnahmefällen betreffend einzelne Federations schriftliche Abweichungen von den verpflichtenden Bestimmungen dieses Rulebooks beschließen. Das kann notwendig sein, um das Regelwerk z.B. an bestehende Infrastruktur oder spezifische Anforderungen der Teilnehmer anzupassen.

Schlichtungsstelle

Bevor ein Teilnehmer gegen einen anderen Teilnehmer in einer Angelegenheit, die mit dem WPV direkt oder indirekt in Zusammenhang steht, gerichtlich vorgeht, hat er die Schlichtungsstelle mit dieser Angelegenheit zu befassen, sofern dies gesetzlich im Einzelfall zulässig ist. Über Sachverhalte, für die dieses Rulebook keine Regeln trifft, hat die Schlichtungsstelle im Sinne der Grundprinzipien des WPV unter Beachtung der allgemeinen Rechtslage nach Billigkeit zu entscheiden.

Die vorliegende Kurzfassung des WPV-Rulebooks wurde erstellt, um Interessenten und Entscheidungsträgern einen möglichst knappen und verständlichen Überblick über dessen Inhalt zu geben. Verbindliche und vollständige Informationen über den Inhalt des Rulebooks können ausschließlich dem Rulebook selbst entnommen werden.