Wirtschaftsportalverbund Rulebook

Version 1.17, approbiert 1.6.2017

Policy Management Taskforce

Siegfried Gruber, Walter Hötzendorfer, Rainer Hörbe, Thomas Rössler

Inhalt

Vorbemerkungen zum Projektabschnitt „Grobkonzept WPV":

Definitionen der in diesem Dokument verwendeten Begriffe siehe unten in Kapitel 1 des Rulebooks „Begriffe und Rollen".

Ergebnisdokumente des Projektabschnitts Grobkonzept:

1. *Entwurf Rulebook („WPV Rulebook")*
2. *Architekturmodell („WPV Modell")*
3. *Wirtschaftliches Konzept („WPV FA Businessplan")*
4. *FA Governance-Anforderungen („WPV Anforderungen Governance")*
5. Recherche zu den Rechtsgrundlagen des WPV („WPV Rechtsgrundlagen")

Dieses Dokument basiert auf Ergebnisdokument 1 (Rulebook), wobei – soweit sinnvoll – Inhalte der anderen Ergebnisdokumente in das Rulebook eingearbeitet wurden, insbesondere das Glossar aus dem Architekturmodell.

Vorbemerkungen zum Projektabschnitt „Feinkonzept WPV":

Im Projektabschnitt Feinkonzept wurde das Rulebook überarbeitet und ergänzt. Das Ergebnis davon ist dieses Dokument.

Diese Version enthält alle Bestimmungen, die aus gegenwärtiger Perspektive bereits formuliert werden konnten. Weitere Bestimmungen dieses Rulebooks sind aus der Praxis, d.h. im Zuge des Aufbaus der ersten Federations zu formulieren (dies ist nicht zu verwechseln mit den Federation-spezifischen Rulebook-Erweiterungen, die zusätzlich bei Aufbau jeder Federation zu formulieren sind).

Im Zuge des Aufbaus der ersten Federations kann sich Bedarf zur Formulierung weiterer Bestimmungen ergeben, der gegenwärtig noch nicht abzusehen ist, und auch in weiterer Folge sieht der WPV einen Mechanismus für weitere Anpassungen des Rulebooks vor, wenn dafür Bedarf besteht.

Vorbemerkungen zur Rulebook-Version 1.17:

Seit dem Jahr 2016 wurde bzw. wird die Gründung einer ersten Federation vorangetrieben und im Zuge dessen das Rulebook weiterentwickelt. Unter Anderem wurden

- das Konzept der Meldungen dahingehend umgestellt, dass der FO eine zentrale Rolle spielt,
- (Tipp-)Fehler und Inkonsistenzen korrigiert,
- Formale Verbesserungen vorgenommen.

Legende für dieses Dokument:

- *Kursiver Text: Erläuternde und zusätzliche Informationen sowie Aufzählungen weiterer Inhalte, die noch formuliert werden müssen.*
- Nicht kursiver Text: Ausformulierte Bestimmungen des Rulebooks (vorläufig)
- *Begründungen und Anmerkungen: Zu einzelnen Punkten wurden kursive, eingerückte Begründungen oder Anmerkungen eingefügt. Diese sind dazu gedacht, den Erstellungsprozess zu begleiten sowie zu verhindern, dass wichtige Überlegungen verloren gehen. Diese Begründungen und Anmerkungen werden am Ende aus der finalen Version entfernt.*

Liste der rechtlichen Artefakte, die zur Umsetzung des WPV benötigt werden

1. *Governance-Regeln FA (Statuten Verein „Wirtschaftsportalverbund – Verein zur Entwicklung und Organisation föderierter Identitätsmanagementsysteme")*
2. *Rulebook (das gegenständliche Dokument)*
3. *Federation-spezifische Rulebook-Erweiterungen*
4. *FO-Vertrag (Vertrag zwischen FA und FO)*
5. *IdP-Vertrag (Vertrag zwischen FO und IdP)*
6. *SB-Vertrag (Vertrag zwischen FO und SB)*
7. *SP-Vertrag (Vertrag zwischen SB und SP)*
8. *AP-Vertrag (Vertrag zwischen IdP und AP)*
9. *Audit-Verträge (Verträge zwischen Auditor und Auditiertem): Werden für jeden Audit oder für eine bestimmte Zeit nach Bedarf abgeschlossen*

Anmerkungen zu den rechtlichen Artefakten:

- *Die Akkreditierung selbst ist kein Vertrag, sondern die Nennung auf einer offiziellen Liste der FA (für IdP und SB) bzw. der FO (für SP)*
- *Nicht alle rechtlichen Artefakte werden zentral vorgegeben*

- *Audit-Agreements werden vom Auditor gestaltet*

Weitere Verträge/Vereinbarungen im Kontext des WPV (Inhalt frei):

- *Vertrag zwischen Benutzer und SP*
- *Vertrag zwischen Benutzer und IdP*
- *Vertrag zwischen Benutzerorganisation und IdP*

[Nachfolgend beginnt das eigentliche Rulebook]

Präambel

Dieses Dokument enthält das Rulebook, das als rechtliche Grundlage des Wirtschaftsportalverbunds (WPV) dienen wird. Das verbindliche Rulebook beginnt unten mit dem Abschnitt 1 „Begriffe und Rollen“. Diese Präambel dient als rechtlich unverbindliche Einführung, die den WPV und seine Prinzipien vorstellt.

Der WPV soll eine Kooperationsbasis für verschiedene Diensteanbieter der Wirtschaft im Internet darstellen, um elektronische Geschäftsprozesse sicherer und effizienter als bisher abwickeln zu können. Als zentrale Voraussetzung hierfür sollen gesicherte elektronische (Unternehmens-)Identitäten zur Verfügung gestellt und von den Partnern des WPV gemeinsam („föderiert“) verwaltet werden.

Der WPV setzt somit das Prinzip der „Identity Federation“ um. Dies bedeutet im Wesentlichen, dass Identitäten über Organisationsgrenzen hinweg mehrfach verwendet werden und nicht für jede Beziehung zwischen einem Benutzer und einem Service ein eigener Benutzer-Account angelegt werden muss. Als Analogie sei die Idee der Kreditkarte genannt: Kreditkarten ermöglichen Zahlungen, unabhängig davon, mit welchen Banken ein Kunde und ein Verkäufer eine Geschäftsbeziehung haben.

Um dies möglich zu machen, ist die rechtliche, organisatorische und technische Abstimmung zwischen den Teilnehmern erforderlich, sodass diese in einem gemeinsamen „Identity-Ökosystem“ arbeiten können. Diesem Zweck dient das nachfolgende Rulebook.

Leistungsbeschreibung des WPV:

Leistung	Details
Authentifizierung durch Dritte	Wenn nicht authentifizierte Benutzer (oder allgemeiner: Principals) auf Ressourcen eines SP zugreifen wollen, delegiert der SP die Authentifizierung an die Federation. Im Zuge der Authentifizierung können auch Attribute der Benutzer übermittelt werden.
Identity Life Cycle Management	Der Lebenszyklus von Identitäten umfasst Erstanmeldung, Attributverwaltung und Terminierung. Der Prozess der Erstanmeldung von Benutzern und Geräten besteht aus folgenden Teilaktivitäten: • Antrag einbringen (und/oder pseudonym registrieren) • Identitätsfeststellung, optional Erhebung weiterer Attribute • Registrierung

Leistung	Details
	Die Attributverwaltung umfasst die Aktualisierung von Attributen sowie die Prüfung, ob einmal erhobene Attribute noch aktuell sind.
Clearing - Info sharing	Clearing: Abrechnung von transaktionsbezogenen Leistungen zwischen verschiedenen SP, z.B. für ein Kundenbindungsprogramm. Damit verbunden ist Info sharing, bei dem mehrere SP Daten austauschen.
Intra-Federation Messaging	Messaging ermöglicht die Zustellung von personenbezogenen Nachrichten zwischen direkten und indirekten Teilnehmern der Federation sowie Benutzern außerhalb einer Transaktion des Benutzers. Personenbezogen heißt, dass in der Adresse oder im Inhalt der Nachricht ein Benutzer eindeutig identifiziert wird, dabei werden die Anforderungen von Nicht-Verknüpfbarkeit und Nicht-Beobachtbarkeit gewahrt. Die Qualität des Messaging (reliable, best effort, fire&forget) ist vom Federation Operator festzulegen. Anwendungsbeispiele: A) Vermeidung von E-Mail-Adressen als Attribute SP können mit dem Benutzer kommunizieren ohne eine global eindeutige Kommunikationsadresse zu haben. Das kann z.B. erreicht werden, indem folgender Ablauf eingerichtet wird: • Der SP schickt die Nachricht an den SB. Dabei wird der SP-spezifische Identifier zur Adressierung der Nachricht verwendet. • Der SB schickt die Nachricht an den IdP, und ersetzt dafür den SP-spezifischen Identifier durch den IdP-spezifischen. • Der IdP leitet die Nachricht an die beim IdP registrierte Mail-Adresse. B) Meldung von Missbrauchsfällen Wenn ein SP feststellt, dass eine Benutzerkennung unzulässig verwendet wird, kann mittels Messaging der IdP benachrichtigt werden, um dort geeignete Maßnahmen zu

Leistung	Details
	treffen, etwa um den Account zu sperren. Die Realisierung erfolgt idR durch Hintergrundprüfungen; z.B. wenn in einem Spitalsverbund jemand auf Daten eines Patienten ohne Behandlungsverhältnis zugreift; oder jemand einen Finanztransaktion mit ungewöhnlichen Parametern (Ort, Betrag, Zeit) durchführt. C) Clearing Service Nachrichten zu einem Benutzer können zwischen SPs ausgetauscht werden, z.B. Transaktionsdaten für Bonuspunkte zwischen einem eShop und einem Loyalty Clearing Service.

Der WPV und somit das Rulebook sind entsprechend den nachfolgenden Prinzipien und Zielen gestaltet.

Die Grundprinzipien des WPV:

Grundprinzip	Details
Anpassungsfähigkeit	Die Organisation des WPV ermöglicht die Anpassung an geänderte rechtliche, wirtschaftliche und technische Voraussetzungen. Änderungen am Rulebook gelten für alle Teilnehmer und sind innerhalb einer gegebenen Frist umzusetzen, wobei signifikante Änderungen einen Kündigungsgrund darstellen.
Branchenneutralität	Der WPV ist so allgemein aufgestellt, dass seine Dienste in unterschiedlichen Sektoren genutzt und angeboten werden können.
Durchsetzbarkeit von Ansprüchen	Die rechtlichen Beziehungen ermöglichen die direkte Durchsetzbarkeit von Ansprüchen zwischen Teilnehmern. Zudem ist ein Streitschlichtungsverfahren innerhalb des WPV zu installieren, das zur Streitbeilegung führen soll, bevor der ordentliche Rechtsweg beschritten wird.

Grundprinzip	Details
Freie Wahl technischer Mittel	Die Teilnehmer sind in der Wahl der eingesetzten Mittel frei, soweit diesbezüglich keine Festlegungen im Rulebook getroffen werden.
Interessenausgleich	Das Regelwerk hat für den Interessenausgleich der Teilnehmer zu sorgen.
Interoperabilität	Die zwischen den direkten Teilnehmern zu verwendenden technischen Protokolle sind in den Federation-spezifischen Rulebook-Erweiterungen auf Federation-Ebene festgelegt. (In ihrer Beziehung mit Dritten können Teilnehmer beliebige Standards und Protokolle verwenden.)
Kooperation und Wettbewerb	Teilnehmer des WPV können im Wettbewerb zueinander stehen, verpflichten sich jedoch zur Kooperation auf der Ebene der organisationsübergreifenden Infrastruktur für IT-Sicherheit und Identitätsmanagement sowie zur Schaffung und Erhalt von Anwendervertrauen.
Meldeverpflichtung	Teilnehmer haben für die Bewertung des Risikos in der Federation die notwendigen Key Performance Indikatoren dem FO und der Governance Task Force bereitzustellen.
Offenlegungspflicht	Die Teilnehmer haben die Pflicht, ihren Betriebszweck und dessen organisatorische Implementierung offenzulegen. Diese Informationen müssen öffentlich zugänglich sein.
Schutz der Geschäftsinteressen	Mitglieder der Federation müssen ihre eigenen Geschäftsinteressen wahren können.
Selbstorganisation und Mitbestimmung	Rechtliche Regeln der Federation werden nach demokratischen Regeln mit paritätischer Mitbestimmung selbst organisiert. Die Mitbestimmung betrifft die Änderung und Weiterentwicklung der WPV-Prinzipien, der WPV-Governance und des Rulebooks.
Stabilität	Die Teilnehmer des WPV haben den Betrieb, die Organisation und die Veränderung des Systems so zu gestalten, dass die wirtschaftliche, organisatorische und technische Stabilität des Systems gewährleistet bleibt.

Grundprinzip	Details
Standardisierung	Es sollen sowohl nationale als auch internationale Standards berücksichtigt und Abweichungen davon begründet werden. Die Regeln des WPV sollen nicht ausschließen, dass branchenspezifische Regeln oder Normen von den Teilnehmern eingehalten werden, etwa eGovernment (z.B. STORK), Zahlungsverkehr (z.B. Stuzza, ebInterface) und Energie (z.B. Smart Meter). Der WPV soll versuchen, Inkompatibilitäten und damit technische Eintrittsbarrieren und Ausschlusskriterien zu vermeiden. Sollte eine tatsächliche Inkompatibilität auftreten, so sollten organisatorische oder strukturelle Möglichkeiten geschaffen werden, dass die Teilnehmer dadurch nicht in ihrem Angebot beschränkt, oder an der Teilnahme am WPV gehindert werden.

Die Sicherheitsziele des WPV:

Sicherheitsziel	Details
Vertraulichkeit	Definition laut ISO/IEC 27000:2016: Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.
Integrität	Definition laut ISO/IEC 27000:2016: Eigenschaft des Schutzes von Richtigkeit und Vollständigkeit von Vermögenswerten.
Verfügbarkeit	Definition laut ISO/IEC 27000:2016: Eigenschaft, einer berechtigten Einheit auf Verlangen zugänglich und nutzbar zu sein.
Nachvollziehbarkeit	Die Anforderung, dass die Aktionen einer Entität eindeutig zu ihr rückverfolgbar sind.

Die Datenschutzprinzipien des WPV:

Der Schutz personenbezogener Daten spielt in der Gestaltung des WPV eine wesentliche Rolle. Diesem Grundsatz entsprechen die nachfolgenden Einzelprinzipien. Die datenschutzorientierte Gestaltung umfasst die Einhaltung aller gesetzlichen Datenschutzbestimmungen sowie zahlreiche darüber hinausgehende Maßnahmen.

Datenschutzprinzip	**Herkunft**
Informierte und freiwillige Einwilligung	ISO/IEC 29100 (5.2)
Erhebung nur für den angegebenen Zweck	ISO/IEC 29100 (5.4)
Begrenzung auf rechtmäßigen Zweck	ISO/IEC 29100 (5.3)
Datenminimierung	ISO/IEC 29100 (5.5)
Beschränkte Verwendung, Aufbewahrung und Weitergabe	ISO/IEC 29100 (5.6)
Qualität und Richtigkeit	ISO/IEC 29100 (5.7)
Offenheit, Transparenz und Information	ISO/IEC 29100 (5.8)
Individuelle Teilnahme und Zugriff	ISO/IEC 29100 (5.9)
Nachvollziehbarkeit	ISO/IEC 29100 (5.10)
Maßnahmen zur Informationssicherheit	ISO/IEC 29100 (5.11)
Ordnungsgemäße Durchführung	ISO/IEC 29100 (5.12)

1 Begriffe und Rollen

In diesem Rulebook sowie generell im Zusammenhang mit dem WPV gelten die folgenden Begriffsdefinitionen:

	Term	Definition
1.1.	Assertion	Eine Assertion ist die Bestätigung der Identität und/oder von Attributen eines Principals durch einen Verifier. Ein Verifier ist der technische Agent eines IdP.
1.2	Attribut	Attribute sind Angaben über einen Benutzer, die diesem eindeutig zugeordnet werden können. Diese „Angaben“ müssen nicht zwingend die abstrakte Eigenschaft beschreiben.
1.3	Attribute Provider	Ein Attribute Provider (AP) führt Attribute über einen Benutzer oder Principal und stellt diese über einen IdP für eine Authentifizierung bei einem SP bereit. Eine direkte Übermittlung von Attributen an SB oder SP ist im WPV nicht vorgesehen. Der AP ist für die anderen Teilnehmer der Federation nicht sichtbar, sondern ein Teil der Funktionalität des IdP, der den AP auf der vertraglichen Ebene vermittelt. Der AP kann jedoch Attribute für einen SP verschlüsseln. Dafür bestätigt der FO, dass es sich um einen gültigen SP der Federation handelt.
1.4	Auditor	Ein Auditor ist eine Person, die durch Befragen, Beobachten, Zuhören überprüft ob Vereinbarungen eingehalten werden.
1.5	Benutzer	Benutzer oder ihre Geräte benötigen Zugriff auf ein Service und sind dafür bei einem IdP registriert. Der Begriff wird hier synonym für Principal verwendet, und umfasst sinngemäß auch Entitäten, die keine Personen sind.
1.6	Betroffener	Natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden. Auf Englisch im Datenschutz oft als data subject bezeichnet.
1.7	Cross-Federation	Die Teilnahme von Teilnehmern an mehreren Federations, wenn diese gemeinsam für mehrere Teilnehmer über den FO etabliert wird.
1.8	Direkte Teilnehmer	Direkte Teilnehmer ist der Überbegriff für FO, IdP und SB.
1.9	Externer IdP	Ein externer IdP hat keine direkte Beziehung mit der Federation, sondern wird von einem teilnehmenden IdP vertraglich vertreten und auch technisch vermittelt. Die Pflichten des teilnehmenden IdP sind von diesem an den externen IdP zu überbinden.

	Term	Definition
1.10	Federation	Eine Federation ist eine Gemeinschaft von Entitäten, die ein gemeinsames Interesse an der Organisation von vertrauenswürdiger elektronischer Kommunikation haben und sich zu diesem Zweck zusammengeschlossen haben. Diese Gemeinschaften können auf einen gemeinsamen Markt bezogen sein, und ihre Mitgliedschaft in diesem Sinn beschränken. Es kann aber auch andere Gründe für ein gemeinsames Interesse geben, etwa die geographische Region oder andere Geschäftsbeziehungen. (Zum Begriff „Identity Federation“ als theoretisches Konzept siehe dort.)
1.11	Federation Authority	Die Federation Authority ist als Trägerorganisation für die Governance des WPV zuständig. Zu den Kernfunktionen gehören (unverbindlicher Auszug): • Die Pflege des Rulebooks unter Mitbestimmung der Teilnehmer • Der Abschluss von FO-Verträgen mit FO zur Errichtung von Federations nach diesem Rulebook • Die Sicherstellung der Einhaltung des Rulebooks • Die Bearbeitung von Konflikten und von Meldungen über Vorfälle
1.12	Federation Operator	Der Federation Operator betreibt die zentralen Dienste der Federation. Diese Dienste umfassen (unverbindlicher Auszug): • Der Abschluss und Verwaltung von Verträgen mit IdP und SB • Die Akkreditierung der SP • Der Betrieb eines Verzeichnisdienstes für direkte Teilnehmer und deren Dienste sowie technische Metadaten • Der Betrieb eines IdP Discovery Service und Account Selectors (optional) • Die Operative Umsetzung von Cross-Federations • Die Pflege und Publikation der Federation-spezifischen Policy-Dokumente • Die Bearbeitung von Konflikten und von Meldungen über Vorfälle
1.13	Federation-CA	Ein Zertifizierungsdienst (Certificate Authority), dessen Zertifikate die Vertrauensstellungen zwischen den Teilnehmern einer Federation herstellen. Die Federation-CA kann vom FO betrieben werden.
1.14	FO-Auditor	Ein FO-Auditor ist ein Auditor, der von der FA zur Prüfung eines FO akkreditiert ist.

	Term	Definition
1.15	Identity Federation	Identity Federation ist das Konzept der organisationsübergreifenden Nutzung elektronischer Identitäten. (Zum Begriff Federation als organisatorische Einheit siehe dort.)
1.16	Identity Provider	Der Identity Provider (IdP) gewährleistet die eindeutige und überprüfbare Identität einer Entität (natürliche Person, Organisation, Device) und vermittelt zugehörige Attribute. Die dafür notwendigen Teilfunktionen für Registrierung, Bereitstellung von Credentials und Attributen sind vom IdP intern zu verwalten.
1.17	IdP-Discovery-Service	Der IdP-Discovery-Service bietet die Auswahl des IdP im Zuge der Authentifizierung
1.18	Indirekte Teilnehmer	Indirekte Teilnehmer ist der Überbegriff für AP, SP und Clearing Provider.
1.19	Policy Management Task Force	Die PMTF ist eine Gruppe von Experten, die dazu bestimmt und in der Lage ist, die inhaltliche Arbeit an der Weiterentwicklung des Rulebooks durchzuführen.
1.20	Principal	Principals repräsentieren Betroffene oder deren Geräte oder Services, wenn sie bei einem Identity Provider (z.B. für die Durchführung von Transaktionen, Zugriff auf Datenanwendungen und Kommunikation) registriert und berechtigt sind.
1.21	Risk Management Task Force	Die RMTF ist eine Gruppe von Experten, die Vorschläge zur Verminderung des Risikos im WPV erarbeitet.
1.22	Schlichtungsstelle	Die Schlichtungsstelle ist das Schiedsgericht des WPV nach § 17 der Statuten. Sie dient der außergerichtlichen Beilegung von Konflikten innerhalb des WPV.
1.23	Service Broker	Ein Service Broker (SB) vermittelt die Beziehung zwischen SP und Federation (IdP, FO). Der SB hat dabei folgende Funktionen (unverbindlicher Auszug): • Vertragspartner der Federation, stellvertretend für die SP in allen Belangen. Es gibt daher keine direkten vertraglichen Beziehungen und Durchgriffsrechte der jeweiligen Partner. Davon ausgenommen ist die Akkreditierung des SP. • (SAML-)IdP-Proxy. Er beschränkt damit die Möglichkeit, dass der IdP das Ziel der Transaktion feststellen kann. Der SB ist kein Proxy für die Anwendung selbst, sondern nur für Authentifizierung und Messaging. • Der SB kann auch als Protokolladapter dienen, um von den technischen Protokollen der Federation abweichende Interfaces zu bedienen. • Verrechnungsstelle für IdP-Leistungen an SP

	Term	Definition
		• Service Discovery • Consent Service • Integrator. Der SB ist technischer Ansprechpartner bei Integration des SP in die Federation und damit verbundenen betrieblichen Aufgaben.
1.24	Service Provider	Service Provider bezeichnet eine Entität, die eine Ressource betreibt, auf die dieser entsprechend einer Zugriffspolicy einem Principal Zugriff gewährt. Anmerkung: Zur Vereinfachung wird in diesem Kontext der Begriff SP synonym mit Relying Party und dem Betreiber einer Anwendung oder Ressource verwendet.
1.25	Sicherheitsklasse	Eine Sicherheitsklasse (Level of Assurance) ist eine Bezeichnung für eine Sicherheitsrichtlinie, mit der ein Benutzer (Principal) identifiziert wird. Sicherheitsklassen sind hierarchisch konzipiert, d.h. dass etwa die Anforderungen einer niederwertigen Sicherheitsklasse (zum Beispiel Sicherheitsklasse 2) vollständig in den Anforderungen höherwertigerer Sicherheitsklassen (zum Beispiel Sicherheitsklasse 3) enthalten und damit abgedeckt sind.
1.26	Stakeholder	Stakeholder sind Entitäten (Organisationen oder Personengruppen), die ein berechtigtes Interesse an Entstehung, Betrieb oder Wirkung des WPV haben.
1.27	Teilnehmer	Die Teilnehmer sind die Gesamtheit der direkten und indirekten Teilnehmer. Die Teilnehmer sind eine Teilmenge der Stakeholder. *Begründung: Eine umschreibende Definition hätte keinen Mehrwert und wäre potenziell missverständlich.*
1.28	Transaktion	Übertragung von Identitäts- und oder Attributsdaten eines Nutzers von einem Teilnehmer zu einem anderen.

In diesem Rulebook sowie generell im Zusammenhang mit dem WPV gelten die folgenden Abkürzungen:

Abkürzung	**Term**
AP	Attribute Provider
FA	Federation Authority
FO	Federation Operator
IdP	Identity Provider
PMTF	Policy Management Task Force
RMTF	Risk Management Task Force
SAML	Security Assertion Markup Language
SB	Service Broker
SP	Service Provider
WPV	Wirtschaftsportalverbund

2 Architektur des WPV

2.1 Der WPV besteht aus einer FA und weiteren Teilnehmern, die für die Erfüllung verschiedener globaler Funktionen und für die Aufrechterhaltung des Betriebs erforderlich sind, sowie aus mehreren Federations, die von je einem FO betrieben und verwaltet werden.

2.2 Angelegenheiten, die nicht gemäß diesem Rulebook auf Ebene der FA geregelt sind, können vom FO auf Ebene einer einzelnen Federation geregelt werden. Somit ergeben sich zwei Verwaltungsebenen: Die globale Ebene (WPV) sowie die Ebene der einzelnen Federations.

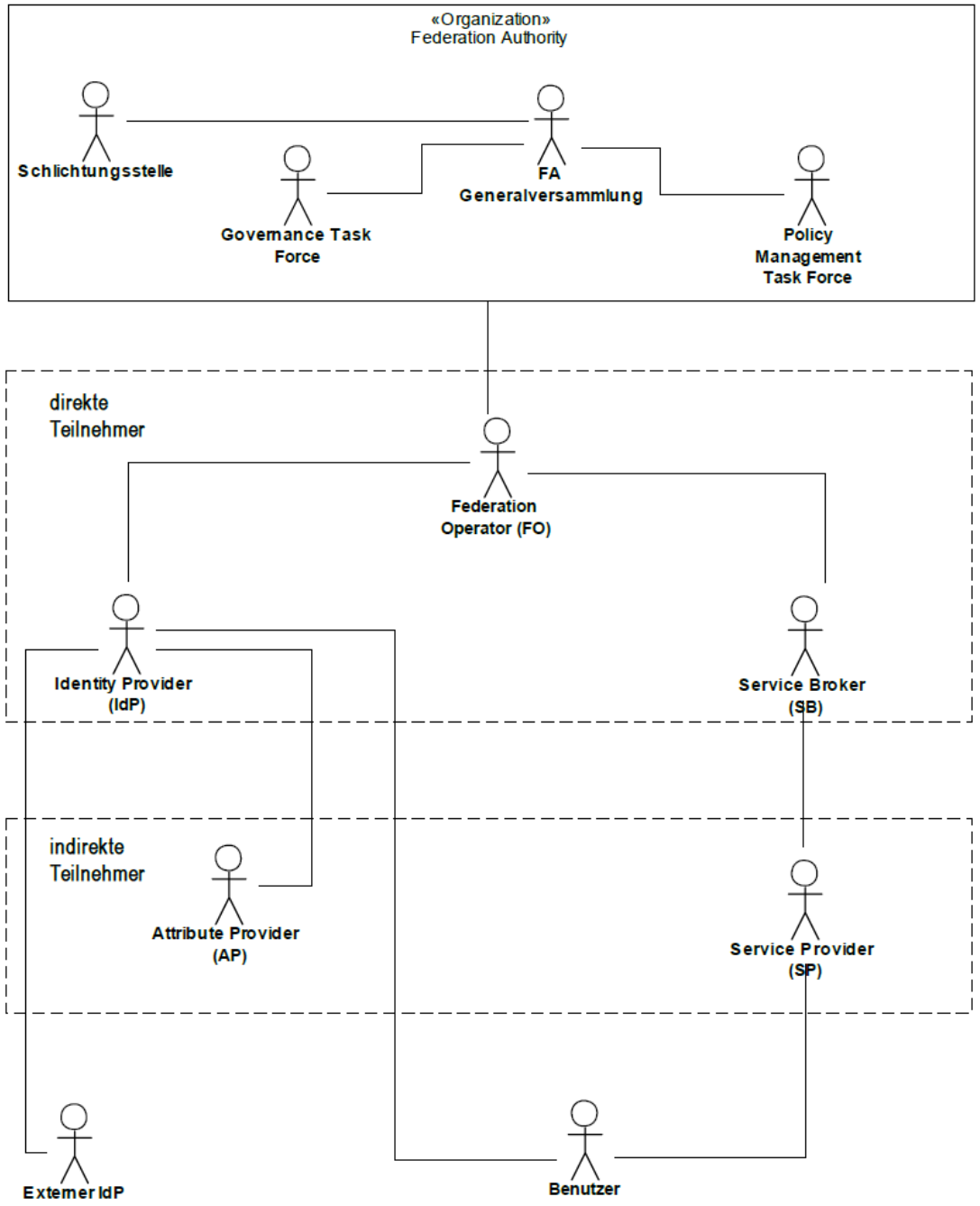

Abbildung 1: Grafische Darstellung der Architektur des WPV

2.3 Die Teilnehmerstruktur des WPV ist hierarchisch aufgebaut:

- Die erste und oberste Hierarchieebene bildet die FA.
- Die zweite Hierarchieebene bilden die FO.
- Die dritte Hierarchieebene bilden die IdP und SB, die jeweils einem oder mehreren FO zugeordnet sind.
- Die vierte und unterste Hierarchieebene bilden die AP und SP, wobei ein AP einem oder mehreren IdP und ein SP einem oder mehreren SB zugeordnet ist.

2.4 Federations sind funktional nach einer dreistufigen Architektur aufgebaut. Dies bedeutet, dass sämtliche Transaktionen zwischen IdP und SP über einen SB laufen müssen.

3 Teilnahme am WPV

3.1 Teilnehmer 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.

3.2 Ein solcher Vertrag ist Voraussetzung für eine Akkreditierung.

4 Akkreditierung von Teilnehmern

4.1 Bevor sie ihren Betrieb aufnehmen können, müssen Federations, IdP, SB und SP akkreditiert werden.

4.2 Die Akkreditierung von Federations, IdP oder SB wird von der FA durchgeführt.

4.3 Eine Federation, ein IdP oder ein SB ist akkreditiert, wenn sie/er in der von der FA geführten Akkreditierungsliste eingetragen ist. Ein FO gilt als akkreditiert, wenn mindestens eine von ihm betriebene Federation akkreditiert ist. Der Akkreditierung von FO kommt jedoch keine eigenständige Bedeutung zu.

4.4 Die Akkreditierung eines SP wird vom FO durchgeführt.

4.5 Ein SP ist für eine Federation akkreditiert, wenn er in der vom FO geführte Akkreditierungsliste der Federation eingetragen ist.

4.6 Die Voraussetzungen für die jeweilige Akkreditierung sind bei den Rechten und Pflichten der jeweiligen Teilnehmer geregelt.

5 Audit

5.1 Durch Audits wird die Einhaltung des Rulebooks, sowie allfällig vertraglicher Vereinbarungen durch externe Auditoren überprüft.

5.2 Externe Auditoren sind unabhängig von der Organisation, die auditiert wird, frei von Voreingenommenheit und Interessenskonflikten und erstellen Ihren jeweiligen Bericht unter angemessener Sorgfalt auf Basis von Nachweisen. Die Beurteilung der fachlichen Eignung eines Auditors obliegt der jeweils akkreditierende Stelle, die eine Liste der akkreditierten Auditoren zu führen und den zu auditierenden Teilnehmern zur Verfügung zu stellen hat.

5.3 FOs und von ihnen betriebene Federations sind spätestens 6 Monate nach Inbetriebnahme und danach alle 24 Monate durch einen von der FA akkreditierten Auditor zu auditieren.

5.4 IdP und SB sind spätestens 6 Monate nach Inbetriebnahme und danach alle 24 Monate von einem Auditor zu auditieren, der durch jenen FO akkreditiert wurde, der die Federation betreibt, welcher der IdP bzw. SB angehört.

5.5 Der SP unterliegt nach diesem Rulebook keinen Auflagen betreffend allfälliger Auditierungen.

5.6 Die Kosten der Auditierung trägt der jeweils auditierte Teilnehmer.

6 Federation Authority (FA)

Die Rolle der FA im Rahmen des WPV wird durch den Verein „Wirtschaftsportalverbund – Verein zur Entwicklung und Organisation föderierter Identitätsmanagementsysteme“) wahrgenommen.

Aufbau und Funktionen der FA sind in den Statuten des WPV geregelt. Diese Statuten regeln auch den Modus zur Änderung des Rulebooks.

6.1 Haftung

6.1.1 Eine Haftung der FA und ihrer Organe für allfällige Schäden, die durch Mängel des Rulebooks und darauf basierender Systeme und Implementierungen ist - soweit die FA und ihre Organe kein Verschulden aufgrund von grober Fahrlässigkeit oder Vorsatz trifft - ausgeschlossen

6.1.2 Eine Haftung der FA und ihrer Organe für allfällige Schäden im Zusammenhang mit der Auswahl von Personen die sie für die Erfüllung verschiedener Aufgaben einsetzt, noch für deren Handlungen und Unterlassungen ist - soweit die FA und ihre Organe kein Verschulden aufgrund von grober Fahrlässigkeit oder Vorsatz trifft - ausgeschlossen.

6.1.3 Die FA und ihre Organe übernehmen keinerlei Haftung für von ihr akkreditierte Teilnehmer.

6.2 Geheimhaltung

Die FA, ihre Organe und die für die FA tätigen Personen sind zur Geheimhaltung von personenbezogenen Daten und sowie von Betriebs- und Geschäftsgeheimnissen der Teilnehmer verpflichtet, von denen sie im Zuge ihrer Tätigkeit Kenntnis erlangen. Die Pflicht zur Geheimhaltung gilt unbeschränkt über die Dauer der Funktion der FA, ihrer Organe oder die Dauer der Tätigkeit für die FA hinaus.

6.3 Archivierung

Die FA betreibt ein Archiv, in dem sie nach den Bestimmungen dieses Rulebooks Daten speichert und ggf. bereitstellt, die sie nach den Bestimmungen dieses Rulebooks von Teilnehmern übernimmt, die ihren Betrieb oder ihre Teilnahme einstellen.

Die FA legt in diesem Zusammenhang den Inhalt und das Format der zu archivierenden Daten fest.

6.4 Bearbeitung von Meldungen

6.4.1 Die FA hat nach Punkt 8.2.3 von FO an sie gemeldete Statistiken und nach Punkt 8.2.4 von FO an sie gemeldete Vorfälle zu dokumentieren und in eine für alle Teilnehmer zugängliche aussagekräftige Statistik aufzunehmen.

6.4.2 Die FA hat alle in Punkt 6.4.1 genannten Informationen dahingehend zu analysieren, ob sich daraus Bedarf zur Änderung der geltenden Bestimmungen des WPV ergibt, insbesondere um solche Vorfälle in Hinkunft zu vermeiden.

6.5 Bearbeitung von Konflikten

Wird der FA ein Konflikt zwischen Teilnehmern gemäß Punkt 7.5.1 gemeldet oder auf sonstige Weise bekannt, hat sie den FO der betreffenden Federation, sofern dieser nicht ohnehin Konfliktpartei ist, über diesen Konflikt zu informieren, auf die Beilegung dieses Konflikts hinzuwirken und schließlich, wenn ansonsten in angemessener Zeit keine Beilegung zu erwarten ist, die Schlichtungsstelle mit dem Konflikt zu befassen.

7 Rechte und Pflichten aller Teilnehmer

7.1 Allgemeine Sorgfaltspflicht

7.1.1 Jeder Teilnehmer hat unabhängig von den in diesem Rulebook festgelegten Pflichten die ihm aufgrund seiner Rolle zukommenden Aufgaben nach dem Stand der Technik mit der

Sorgfalt eines ordentlichen Unternehmers zu erfüllen (§ 347 UGB) und insbesondere angemessene Datensicherheitsmaßnahmen zu ergreifen.

7.1.2 Jeder Teilnehmer hat Personal und gegebenenfalls Unterauftragnehmer zu beschäftigen, das bzw. die über das erforderliche Fachwissen, die erforderliche Zuverlässigkeit, die erforderliche Erfahrung und die erforderlichen Qualifikationen verfügt bzw. verfügen.

7.2 Pflicht zur Umsetzung von Änderungen des Rulebooks

Die Teilnehmer am WPV verpflichten sich im Zuge Ihres Antrages zur Akkreditierung zur Einhaltung der für sie einschlägigen Bestimmungen des Rulebooks. Soweit das Rulebook im Laufe der aufrechten Teilnahme Änderungen erfährt, sind die Teilnehmer zur Übernahme der sie betreffenden Änderungen in den durch die FA festgelegten Fristen verpflichtet. Sollte ein Teilnehmer diese Änderungen aus welchen Gründen auch immer nicht umsetzen können oder wollen, so hat er dies unverzüglich der FA mitzuteilen.

Die FA entscheidet binnen 6 Wochen ab Einlangen der Mitteilung, ob im Rahmen von individuellen Erweiterungen des Rulebooks eine Lösung für den Teilnehmer möglich ist und unterbreitet die diesbezüglichen Vorschläge dem Teilnehmer. Sollte keine individuelle Lösung möglich sein, so ist die Tätigkeit des Teilnehmers im WPV mit dem Ablauf der für die Umsetzung der Änderungen definierten Frist nach den Bestimmungen des Rulebook in der geltenden Fassung zu beenden.

7.3 Datenschutz und Datensicherheit

7.3.1 Allgemeines

7.3.1.1 Sofern nicht im Einzelnen anders definiert gelten in diesem Rulebook die Begriffe des DSG 2000 in der zum Zeitpunkt des in Kraft Tretens dieses Rulebooks geltenden Fassung so wie sie dort definiert sind.

7.3.1.2 Jeder Teilnehmer ist kraft dieser Bestimmung verpflichtet, personenbezogene Daten nur im Rahmen des nach den geltenden gesetzlichen Bestimmungen Zulässigen zu verwenden und insbesondere die datenschutzrechtlich gebotenen Sicherheitsmaßnahmen zu treffen.

7.3.2 Geheimhaltung

7.3.2.1 Teilnehmer dürfen die von ihnen verarbeiteten personenbezogenen und transaktionsbezogenen Daten nicht an andere Teilnehmer oder an Dritte weitergeben, es sei denn, dies ist im Zuge der Durchführung einer Transaktion nach den Regeln dieses Rulebooks erforderlich oder es liegt eine gesetzliche Verpflichtung nach den Bestimmungen der Europäischen Union oder eines ihrer Mitgliedstaaten oder einer der unter 7.6.1 genannten Fälle vor.

7.3.2.2 Jeder Teilnehmer hat seine Mitarbeiter nachweislich über die gesetzlich und/oder nach diesem Rulebook bestehenden Geheimhaltungs-, Datenschutz- und Datensicherheitspflichten zu belehren.

7.3.3 Datenminimierung

Jeder Teilnehmer darf nur jene personenbezogenen Daten einsehen und verwenden können, die er benötigt, um eine bestimmte Transaktion durchzuführen bzw. seine Aufgaben im WPV zu erfüllen.

7.3.4 Beschränkung der Verknüpfbarkeit

7.3.4.1 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. Die Übermittlung von Attributen, die eine eindeutige Identifizierung des Benutzers zulassen, soweit diese datenschutzrechtlich zulässig ist, ist dadurch nicht beschränkt.

7.3.4.2 Darüber hinaus sollen auch andere personenbezogene Attribute nur im erforderlichen Umfang übermittelt werden und für eindeutige Kontaktadressen wie E-Mail möglichst eine pseudonymisierte Version verwendet werden.

> *Begründung: Nicht-Verknüpfbarkeit kann nicht als Vorschrift umgesetzt werden. Name und Geburtsdatum machen die Daten meist eindeutig verknüpfbar. Man kann nur Maßnahmen vorschreiben, die das Verknüpfen faktisch erschweren (privacy by design) sowie das Verknüpfen verbieten.*

7.3.4.3 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. Davon ausgenommen sind Fälle, in denen eine Zustimmung des Betroffenen oder eine Herausgabepflicht laut 7.6.1 vorliegt.

7.3.5 Beschränkung der Beobachtbarkeit

7.3.5.1 Ein IdP darf weder einsehen können noch Daten darüber speichern können, welche Service Provider ein Benutzer verwendet und insbesondere an welche Service Provider Attributsdaten eines Benutzers übertragen werden. Dies gilt nicht nur als Verpflichtung des IdP, sondern ist durch die technische Implementierung des Gesamtsystems auszuschließen. Die Grundlage dafür ist die dreistufige funktionale Architektur von Federations (siehe unter Architektur).

7.3.5.2 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, z.B. der kurzen Speicherung von Logdateien oder Aufteilung der SB auf mehrere unabhängige Entitäten, vorzuziehen.

7.3.6 Meldeverpflichtungen

Ungeachtet der Pflicht zur Meldung von Verstößen gemäß Punkt 7.4.2 dieses Rulebooks und ungeachtet allfälliger gesetzlicher Meldepflichten hat jeder direkte Teilnehmer Vorfälle der Kompromittierung von Sicherheitsmaßnahem, unbefugte Zugriffe, unbefugte Manipulationen und Fehlfunktionen betreffend Systeme, die er zur Erbringung seiner diesem Rulebook unterliegenden Dienste betreibt, an die FO aller betroffenen Federations zu melden, unabhängig davon, ob durch das zu meldende Ereignis ein Schaden entstanden ist.

> *Begründung: Diese Meldepflicht bezieht sich insbesondere auf Hacker-Angriffe aber auch auf unbefugte Handlungen die von Mitarbeitern der Teilnehmer oder mit deren Wissen durchgeführt werden. Ein FO muss über die Informationssicherheitslage in seiner Federation informiert sein und auch aggregierte Informationen über die Meldungen an die FA weiterleiten (siehe unten), denn auch die FA muss über die Informationssicherheitslage im WPV im Bilde sein, um wenn nötig geeignete Maßnahmen, wie insbesondere Anpassung des Regelwerks treffen zu können.*

7.3.7 Logging und Aufbewahrung von Daten

7.3.7.1 Alle Teilnehmer, insbesondere SB und IdP, müssen über Vorgänge der Übermittlung von Identitätsdaten an andere Teilnehmer detaillierte Protokolle führen, aus denen hervorgeht, welche Art von Daten betreffend welchen Benutzer zu welchem Zeitpunkt an welchen anderen Teilnehmer übermittelt wurden.

7.3.7.2 Die Protokolle sind drei Jahre lang aufzubewahren und danach zu löschen. Daten, die Gegenstand eines Rechtsstreits sind, sind erst nach dessen Ende zu löschen.

7.4 Folgen rechtswidriger Handlungen der Teilnehmer

7.4.1 Haftung für rechtswidrige Handlungen

7.4.1.1 Jeder Teilnehmer ist verpflichtet, die FA zur Gänze schad- und klaglos zu halten, wenn diese aufgrund seines Verstoßes gegen dieses Rulebook oder seines sonstigen rechtswidrigen Verhaltens einen Schaden erleidet oder von einem Dritten in Anspruch genommen wird. Im Fall der Inanspruchnahme durch einen Dritten hat die FA dem Teilnehmer, der rechtswidrig bzw. entgegen einer Bestimmung dieses Rulebooks gehandelt hat, den Streit zu verkünden.

7.4.1.2 Jeder Teilnehmer ist verpflichtet, einen anderen Teilnehmer zur Gänze schad- und klaglos zu halten, wenn aufgrund seines Verstoßes gegen dieses Rulebook oder seines sonstigen rechtswidrigen Verhaltens der andere Teilnehmer einen Schaden erleidet oder von einem Dritten in Anspruch genommen wird. Im Fall der Inanspruchnahme durch einen Dritten hat der in Anspruch genommene Teilnehmer dem Teilnehmer, der rechtswidrig bzw. entgegen eine Bestimmung dieses Rulebooks gehandelt hat, den Streit zu verkünden oder, sollte der Teilnehmer, der ein Fehlverhalten zeigt, nicht bekannt oder ausfindig gemacht werden können, den Streit an die FA zu melden.

7.4.2 Meldung und Behandlung von rechtswidrigen Handlungen

7.4.2.1 Erkennt oder vermutet ein Teilnehmer einen Verstoß gegen dieses Rulebook oder gegen eine einschlägige gesetzliche oder vertragliche Bestimmung bei sich oder einem anderen Teilnehmer, so hat er dies an die FO aller betroffenen Federations zu melden, sofern dieser Verstoß oder die dem Verstoß zugrundeliegende Ursache oder die Auswirkungen des Verstoßes über den Zeitpunkt der Erkennung hinauswirken.

7.4.2.2 Geht eine solche Meldung eines Verstoßes bei einem FO ein, hat der FO eine Untersuchung durchzuführen, wobei der betroffene Teilnehmer zur Kooperation verpflichtet ist, soweit ihm dies zugemutet werden kann. Bestätigt sich dabei, dass ein Verstoß gegen dieses Rulebook oder gegen einschlägige gesetzliche oder vertragliche Bestimmungen vorliegt, ist der betroffene Teilnehmer vom FO zur Beseitigung des gegen dieses Rulebook bzw. gegen einschlägige gesetzliche oder vertragliche Bestimmungen verstoßenden Zustands aufzufordern, wobei eine angemessene Frist zu setzen ist. Im Falle von Gefahr in Verzug kann dem betroffenen Teilnehmer bis zur Beseitigung der Gefahr der Zugriff auf die betroffene Federation verwehrt und/oder die Akkreditierung mit sofortiger Wirkung entzogen werden. 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 für eine weitere Kooperation kein Vertrauen mehr entgegengebracht werden kann, kann ihm, wenn es sich um einen SP handelt, der FO oder, wenn es sich um einen FO, IdP oder SB handelt, die FA die Akkreditierung entziehen.

7.5 Konflikte zwischen Teilnehmern

7.5.1 Jeder Teilnehmer hat jeden Konflikt mit einem anderen Teilnehmer, der sich auf seine Tätigkeit im Rahmen des WPV bezieht oder sich auf diese auswirkt und nicht unverzüglich ausgeräumt wird, an die FO aller betroffenen Federations zu melden, bzw. an die FA, wenn es sich bei einem der in Konflikt befindlichen Teilnehmer um einen FO handelt.

7.5.2 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.

7.6 Weitere Pflichten aller Teilnehmer

7.6.1 Protokollierung und Datenherausgabe

7.6.1.1 Um einzelne Transaktionen bei Bedarf nachvollziehen zu können, haben Teilnehmer alle Daten, die sie im Zuge von Transaktionen innehaben und einsehen können, in Bezug auf alle Transaktionen, an denen sie beteiligt sind, zu speichern und für einen Zeitraum von drei Jahren aufzubewahren.

7.6.1.2 Diese protokollierten Daten in Bezug auf eine bestimmte Transaktion müssen in folgenden Fällen an die FA im durch die FA gem 6.3 definierten Format herausgegeben werden, wobei die FA jeweils zu prüfen hat, ob das Datenschutzrecht eine Herausgabe zulässt:

a) Die Daten einer Transaktion werden benötigt, um einen mutmaßlichen Verstoß gegen dieses Rulebook aufzuklären, der ohne diese Daten nicht aufgeklärt werden kann.

b) Die Daten einer Transaktion werden von der Schlichtungsstelle benötigt, um einen Konflikt zwischen Teilnehmern oder zwischen einem Benutzer und einem Teilnehmer beizulegen.

c) Die Daten einer Transaktion werden von einer Behörde in Ausübung ihrer Befugnisse verlangt.

7.6.1.3 Allfällige gesetzliche Herausgabepflichten, die sich aus Bestimmungen der Europäischen Union oder eines ihrer Mitgliedstaaten ergeben, bleiben davon unberührt.

7.6.2 Weiterverwendung von Benutzerdaten

Teilnehmer dürfen Benutzerdaten, die aus der Federation stammen, nicht dazu verwenden, unabhängig von der Federation systematisch Identity Management für Dritte zu betreiben, auch dann nicht, wenn der Benutzer dem zugestimmt hat.

7.6.3 Auslagerung von Aufgaben

7.6.3.1 Wenn nicht im Einzelnen anders angegeben, kann sich jeder Teilnehmer zur Erfüllung der in diesem Rulebook für ihn festgelegten Aufgaben und Pflichten Dritter bedienen. Diesen hat er dabei seine mit den überbundenen Aufgaben und Pflichten zusammenhängenden Pflichten so zu überbinden, wie sie für ihn nach diesem Rulebook gelten. Jeder Teilnehmer haftet für die Erfüllung der in diesem Rulebook für ihn festgelegten Aufgaben und Pflichten, unabhängig davon, ober er diese Dritten überbunden hat oder nicht.

7.6.3.2 Bedient sich ein Teilnehmer zur Erfüllung der in diesem Rulebook für ihn festgelegten Aufgaben und Pflichten Dritter, hat er dies bei einem Audit unaufgefordert offenzulegen sowie auf Anfrage auch gegenüber der FA und der Schlichtungsstelle.

7.6.4 Andere Federations

7.6.4.1 Der FO einer Federation, die mit einer anderen Federation Cross-Federation betreiben möchte, kann dies selbst beschließen, muss dies aber der FA melden. Die Etablierung einer Cross-Federation muss jedoch mit den einzelnen Bestimmungen dieses Rulebooks vereinbar sein.

7.6.4.2 Teilnehmer haben das Recht, auch an Federations teilzunehmen, die unabhängig vom WPV und von diesem Rulebook agieren, sofern diese Teilnahme mit den einzelnen Bestimmungen dieses Rulebooks vereinbar ist. Ein Teilnehmer, der von diesem Recht Gebrauch macht, hat dies an die FO, an deren Federations er teilnimmt, und an die FA zu melden.

8 Regeln für FO

8.1 Aufnahme des Betriebs einer Federation

8.1.1 Voraussetzung für den Betrieb einer Federation nach diesem Rulebook ist der Abschluss eines Vertrags über den Betrieb einer Federation (FO-Vertrag) zwischen FO und FA und die Akkreditierung der Federation durch die FA. Ein FO kann mehrere Federations betreiben, die dazu jeweils einer eigenen Akkreditierung durch die FA bedürfen.

8.1.2 Der Akkreditierung muss eine Anmeldung der Federation bei der FA vorausgehen. Diese hat zu enthalten:

a) Name, Rechtsform, Sitz und Anschrift des FO

b) Bezeichnung der Federation

c) Zweck und Beschreibung der Federation inklusive allfällige Einschränkungen auf Branchen, Arten von Transaktionen oder Ähnliches

d) Erklärung zur wirtschaftlichen Kontinuität des FO, auf Basis von wirtschaftlicher Leistungsfähigkeit oder gesetzlicher Grundlage etc., abhängig von der Rechtsform

e) Offenlegung der zur Beurteilung des Bestehens von Unvereinbarkeiten nach Punkt 12 notwendigen Informationen

f) Erklärung der FO, die ihn betreffenden Bestimmungen des Rulebooks zu akzeptieren;

g) Die gemäß 8.1.5 verpflichtend auszuarbeitenden Federation-spezifischen Rulebook-Erweiterungen.

8.1.3 Die FA hat binnen 4 Wochen nach Einlangen einer Anmeldung über die Akkreditierung zu entscheiden. Sie entscheidet nach freiem Ermessen und muss ihre Entscheidung nicht begründen.

8.1.4 Fällt diese Entscheidung positiv aus, hat die FA die Federation unverzüglich in die Akkreditierungsliste für Federations einzutragen und dabei die in 8.1.2 genannten Informationen mit Ausnahme der Erklärung zur wirtschaftlichen Kontinuität und der zur Beurteilung des Bestehens von Unvereinbarkeiten nach Punkt 12 notwendigen Informationen anzuführen.

8.1.5 Jeder FO hat für eine Federation zumindest folgende Rulebook-Erweiterungen zu definieren, zu beschreiben und die Beschreibung an die FA zu übermitteln:

a) Detaillierte technische Umsetzung der Vorgaben dieses Rulebooks, um Interoperabilität innerhalb der Federation herzustellen

b) Detaillierung der Sicherheitsklassen

c) Konzept und Schlüssel zur Aufteilung der Wertschöpfungskette innerhalb der Federation

d) Höhe der zwingend vorzusehenden Pönale für Verstöße gegen die Bestimmung von Punkt 7.6.2

e) Vorgaben an Teilnehmer der Federation betreffend Verfügbarkeit ausreichender Finanzmittel und/oder Abschluss einer angemessenen Haftpflichtversicherung in Bezug auf das Haftungsrisiko, das sie aufgrund ihrer Teilnahme an der Federation trifft

f) Gemäß 7.6.1 verwendeten Daten.

8.2 Pflichten für den Betrieb einer Federation

8.2.1 Jeder FO hat folgende Aufgaben für den Betrieb einer Federation zu erfüllen:

a) Abschluss und Verwaltung von Verträgen mit IdP und SB;

b) Akkreditierung von SP nach den unten dafür vorgesehenen Bestimmungen und Führen einer Akkreditierungsliste für SP;

c) Abschluss von Cross-Federation-Verträgen mit anderen FOs;

d) Betrieb eines Verzeichnisdienstes für direkte Teilnehmer und deren Dienste sowie technische Metadaten;

e) Pflege und Publikation der Federation-spezifischen Rulebook-Erweiterungen und allfälliger sonstiger Policy-Dokumente.

8.2.2 Wird dem FO ein Konflikt zwischen Teilnehmern gemäß Punkt 7.5.1 gemeldet oder auf sonstige Weise bekannt, hat er auf die Beilegung dieses Konflikts hinzuwirken und schließlich, wenn ansonsten in angemessener Zeit keine Beilegung zu erwarten ist, die FA über den Konflikt zu informieren und die Schlichtungsstelle mit dem Konflikt zu befassen.

8.2.3 Der FO hat alle nach den Punkten 7.3.6 und 7.4.2 dieses Rulebooks an ihn gemeldeten oder ihm auf sonstige Weise bekannt gewordenen derartigen Vorfälle zu dokumentieren und eine für alle Teilnehmer zugängliche aussagekräftige und stets aktuelle Statistik über diese zu führen sowie monatlich der FA zu übermitteln.

8.2.4 Der FO hat alle von einem in 8.2.3 genannten Vorfall – nicht bloß unwesentlich – betroffenen Teilnehmer und auch die FA über den Vorfall unverzüglich in geeigneter Form zu informieren, und, wenn dies zur Abwehr von Schäden geboten ist, auch die Öffentlichkeit über den Vorfall unverzüglich in geeigneter Form zu informieren

8.2.5 Die FO hat jeden in Punkt 8.2.3 genannten Vorfall dahingehend zu analysieren, ob sich daraus Bedarf zur Änderung der geltenden Bestimmungen der Federation oder des WPV ergibt, insbesondere um solche Vorfälle in Hinkunft zu vermeiden. Ggf. hat er dies der FA mitzuteilen.

8.3 Einstellung des Betriebs einer Federation

8.3.1 Möchte ein FO den Betrieb einer Federation einstellen, hat er darüber die FA sowie alle Teilnehmer dieser Federation ehestmöglich, spätestens jedoch ein Jahr vor der beabsichtigten Einstellung zu informieren und einen diesbezüglichen Beendigungsplan vorzulegen. Die Teilnehmer der Federation, die FA und der FO können im Einzelfall einvernehmlich auch eine kürzere als die oben genannte Einjahresfrist vereinbaren.

8.3.2 Haben Teilnehmer dieser Federation ein Interesse an der Fortführung von deren Betrieb und kann ein FO gefunden werden, der den Betrieb fortführt, so ist der Betrieb nach den Bestimmungen des Abschnitts 9.4 an diesen zu übergeben.

8.3.3 Bei Einstellung des Betriebs der Federation sind folgende Fälle zu unterscheiden:

a) Wird der FO weiterexistieren, hat dieser weiterhin für Aufbewahrung und ggf. Bereitstellung der Daten der Federation zu sorgen, zu deren Aufbewahrung und ggf. Bereitstellung er nach Gesetz oder nach diesem Rulebook verpflichtet ist.

b) Wird der FO nicht weiterexistieren, sind die Daten der Federation, die nach Gesetz oder nach diesem Rulebook einer Pflicht zur Aufbewahrung und ggf. zur

Bereitstellung unterliegen, rechtzeitig an die FA zu übermitteln und von dieser in ihrem Archiv aufzubewahren und ggf. bereitzustellen.

8.3.4 Ist der Grund für die Einstellung des Betriebs einer Federation die Insolvenz des FO, ist die FA unverzüglich darüber zu informieren und im Übrigen ebenfalls sinngemäß so weit als möglich nach den Bestimmungen dieses Abschnitts vorzugehen.

8.3.5 Über strittige Fragen im Zusammenhang mit der Einstellung des Betriebs einer Federation hat die Schlichtungsstelle nach Billigkeit zu entscheiden.

8.4 Übergabe des Betriebs einer Federation an einen anderen FO

8.4.1 Möchte ein FO den Betrieb einer Federation an einen anderen FO übergeben, hat er darüber die FA sowie alle Teilnehmer dieser Federation ehestmöglich, spätestens jedoch ein Jahr vor der beabsichtigten Übergabe zu informieren und einen diesbezüglichen Übergabeplan vorzulegen. Die Teilnehmer der Federation, die FA und die beteiligten FO können im Einzelfall einvernehmlich auch eine kürzere als die oben genannte Einjahresfrist vereinbaren.

8.4.2 Der übernehmende FO muss alle nach diesem Rulebook bestehenden Voraussetzungen für den Betrieb einer Federation erfüllen.

8.4.3 Der übergebende FO hat alle für den Weiterbetrieb nötigen Unterlagen und Daten, einschließlich jene, die einer Aufbewahrungspflicht nach Gesetz oder nach diesem Rulebook unterliegen, an den übernehmenden FO zu übergeben.

9 Regeln für IdP

9.1 Aufnahme des Betriebs eines IdP

9.1.1 Voraussetzung für den Betrieb eines IdP in einer Federation nach diesem Rulebook ist der Abschluss eines Vertrags über den Betrieb eines IdP (IdP-Vertrag) zwischen IdP und FO und die Akkreditierung des IdP durch die FA.

9.1.2 Der Akkreditierung muss eine Anmeldung des IdP bei der FA vorausgehen. Diese hat zu enthalten:

a) Name, Rechtsform und Sitz des IdP

b) Betriebsmodell

c) Offenlegung der zur Beurteilung des Bestehens von Unvereinbarkeiten nach Punkt 12 notwendigen Informationen

d) Unterstützte Sicherheitsklassen

e) Erklärung des IdP, die ihn betreffenden Bestimmungen des Rulebooks zu akzeptieren;

9.1.3 Die FA hat binnen 4 Wochen nach Einlangen einer Anmeldung über die Akkreditierung zu entscheiden. Sie entscheidet nach freiem Ermessen und muss ihre Entscheidung nicht begründen.

9.1.4 Fällt diese Entscheidung positiv aus, hat die FA den IdP unverzüglich in die Akkreditierungsliste für IdP einzutragen und dabei die in 9.1.2 genannten Informationen mit Ausnahme der zur Beurteilung des Bestehens von Unvereinbarkeiten nach Punkt 12 notwendigen Informationen anzuführen.

9.1.5 Ein IdP kann Teilnehmer in mehreren Federations sein, sofern er die Federation-spezifischen Rulebook-Erweiterungen aller Federations erfüllt, an denen er teilnimmt.

9.2 Betrieb eines IdP

Ein IdP darf weder direkt noch indirekt Daten darüber erheben oder speichern, welche Services ein Benutzer verwendet und insbesondere an welche Services Attributsdaten eines Benutzers übertragen werden.

> *Begründung: Neben der Festlegung der „Beschränkung der Beobachtbarkeit“ oben soll hier auch ein Verbot definiert sein, das den IdP daran hindert, die zur Realisierung der Nicht-Beobachtbarkeit getroffenen Maßnahmen zu umgehen.*

9.3 Protokollierung

9.3.1 Ein IdP muss Protokoll über jeden Vorgang der Authentifizierung (Login und Logout) und der Übertragung von Identitätsdaten an einen SB führen.

> *Begründung: Es wird bewusst der Begriff „Übertragung“ und nicht „Übermittlung“ verwendet, um die Auslegung auszuschließen, dass nur Übermittlungen im Sinne des Datenschutzgesetzes erfasst sind (auch wenn derzeit nur dies denkbar erscheint).*

9.3.2 Jeder solche Protokolleintrag muss enthalten, welche Attribute – nicht jedoch Attributswerte – betreffend welchen Benutzer zu welchem Zeitpunkt an welchen SB übermittelt wurden.

9.3.3 Jeder solche Protokolleintrag ist mit einer eindeutigen Nummer zu versehen, die auch dem SB, der Empfänger der Datenübertragung ist, zu übermitteln ist.

> *Begründung: Der SB muss diese Nummer in seinen Protokolleeintrag über diese Datenübertragung speichern. Dies dient der Nachvollziehbarkeit der Transaktionen.*

9.3.4 Die Protokolle sind drei Jahre lang aufzubewahren und danach zu löschen. Daten, die Gegenstand eines Rechtsstreits sind, sind erst nach dessen Ende zu löschen.

9.4 Beendigung der Teilnahme eines IdP

9.4.1 Möchte ein IdP die Teilnahme an einer Federation beenden, hat er darüber den FO ehestmöglich, spätestens jedoch ein Jahr vor der beabsichtigten Einstellung zu informieren und einen diesbezüglichen Beendigungsplan vorzulegen. Der FO hat darüber alle davon betroffenen Teilnehmer zu informieren. Diese und der FO können im Einzelfall einvernehmlich auch eine kürzere als die oben genannte Einjahresfrist vereinbaren.

9.4.2 Der IdP muss jedem seiner Benutzer anbieten, ihr jeweiliges Benutzerkonto auf einen anderen IdP derselben Federation, der dazu bereit ist, übergehen zu lassen. Dies muss nicht für alle betroffenen Benutzer derselbe IdP sein. Dabei ist nach Punkt 9.5.2 vorzugehen. Zur Übertragung ist die Zustimmung des Benutzers nachweislich einzuholen.

9.4.3 Für die Daten all jener Benutzerkonten, die nach Ablauf einer vom FO festzulegenden Frist nicht gemäß Punkt 9.4.2 auf einen anderen IdP übergegangen sind, hat der FO (pauschal) nach Konsultation der FA zu entscheiden, ob der IdP

a) nach Einstellung seiner Teilnahme weiterhin für deren Aufbewahrung und ggf. Bereitstellung zu sorgen hat, insoweit er zu deren Aufbewahrung und ggf. Bereitstellung er nach Gesetz oder nach diesem Rulebook verpflichtet ist, oder

b) diese, insoweit sie nach Gesetz oder nach diesem Rulebook einer Pflicht zur Aufbewahrung und ggf. zur Bereitstellung unterliegen, an die FA zu übermitteln hat, welche diese in ihrem Archiv aufzubewahren und ggf. bereitzustellen hat.

9.5 Einstellung des Betriebs eines IdP

9.5.1 Möchte ein IdP den Betrieb einstellen, hat er darüber den FO ehestmöglich, spätestens jedoch ein Jahr vor der beabsichtigten Einstellung zu informieren und einen diesbezüglichen Beendigungsplan vorzulegen. Der FO hat darüber alle davon betroffenen Teilnehmer zu informieren. Diese und der FO können im Einzelfall einvernehmlich auch eine kürzere als die oben genannte Einjahresfrist vereinbaren.

9.5.2 Der IdP muss jedem seiner Benutzer anbieten, ihr jeweiliges Benutzerkonto auf einen anderen IdP derselben Federation, der dazu bereit ist, übergehen zu lassen. Dies muss nicht für alle betroffenen Benutzer derselbe IdP sein. Den Benutzern ist möglichst eine Wahl zwischen mehreren IdP zu ermöglichen. Erteilt ein Benutzer für den Übergang seines Benutzerkontos auf einen anderen IdP seine Zustimmung, hat der einzustellende IdP dem übernehmenden IdP alle Daten des jeweiligen Benutzerkontos sowie alle damit in Zusammenhang stehenden Daten, die nach Gesetz oder nach diesem Rulebook einer Pflicht zur Aufbewahrung und ggf. zur Bereitstellung unterliegen, unverzüglich zu übermitteln.

9.5.3 Die Daten all jener Benutzerkonten, die nach Ablauf einer vom FO festzulegenden Frist nicht an nach Punkt 9.5.2 auf einen anderen IdP übergegangen sind hat der IdP, insoweit sie

nach Gesetz oder nach diesem Rulebook einer Pflicht zur Aufbewahrung und ggf. zur Bereitstellung unterliegen, an die FA zu übermitteln hat, welche diese in ihrem Archiv aufzubewahren und ggf. bereitzustellen hat.

9.5.4 Ist der Grund für die Einstellung des Betriebs einer Federation die Insolvenz des IdP, ist der FO unverzüglich darüber zu informieren und im Übrigen ebenfalls sinngemäß so weit als möglich nach den Bestimmungen dieses Abschnitts vorzugehen.

9.5.5 Über strittige Fragen im Zusammenhang mit der Einstellung des Betriebs eines IdP hat die Schlichtungsstelle nach Billigkeit zu entscheiden.

10 Regeln für SB

10.1 Aufnahme des Betriebs eines SB

10.1.1 Voraussetzung für den Betrieb eines SB in einer Federation nach diesem Rulebook ist der Abschluss eines Vertrags über den Betrieb eines SB (SB-Vertrag) zwischen SB und FO und die Akkreditierung des SB durch die FA.

10.1.2 Der Akkreditierung muss eine Anmeldung des SB bei der FA vorausgehen. Diese hat zu enthalten:

a) Name, Rechtsform und Sitz des SB;

b) Betriebsmodell;

c) Offenlegung der zur Beurteilung des Bestehens von Unvereinbarkeiten nach Punkt 12 notwendigen Informationen gemäß Offenlegungspflichten dieses Rulebooks;

d) Erklärung zur wirtschaftlichen Kontinuität des SB, auf Basis von wirtschaftlicher Leistungsfähigkeit oder gesetzlicher Grundlage etc., abhängig von der Rechtsform;

e) Erklärung des SB, die ihn betreffenden Bestimmungen des Rulebooks zu akzeptieren.

10.1.3 Die FA hat binnen 4 Wochen nach Einlangen einer Anmeldung über die Akkreditierung zu entscheiden. Sie entscheidet nach freiem Ermessen und muss ihre Entscheidung nicht begründen.

10.1.4 Fällt diese Entscheidung positiv aus, hat die FA den SB unverzüglich in die Akkreditierungsliste für SB einzutragen und dabei die in 10.1.2 genannten Informationen mit Ausnahme der Erklärung zur wirtschaftlichen Kontinuität und der zur Beurteilung des Bestehens von Unvereinbarkeiten nach Punkt 12 notwendigen Informationen anzuführen.

10.1.5 Ein SB kann Teilnehmer in mehreren Federations sein, sofern er die Federation-spezifischen Rulebook-Erweiterungen aller Federations erfüllt, an denen er teilnimmt.

10.2 Betrieb eines SB

10.2.1 Die primäre Aufgabe eines SB ist es, Identitätsdaten sowie diesbezügliche Anfragen zwischen IdP und SP zu vermitteln, ohne dass der IdP feststellen kann, um welchen SP es sich handelt.

10.2.2 Darüber hinaus hat jeder SB folgende Aufgaben zu erfüllen:

a) Abschluss und Verwaltung von Verträgen mit SP;

b) Unterstützung der ihm nachgeordneten SP in allen Belangen von deren Teilnahme an der Federation;

c) Betrieb eines Verzeichnisdienstes aller ihm nachgeordneten SP und deren Dienste sowie technische Metadaten;

d) Einholen und Verwaltung von Zustimmungen der Benutzer;

e) Speicherung der Protokolldaten gemäß 7.5.1.

10.2.3 Ein SB darf die Identität der Benutzer, deren Daten er verarbeitet, nicht kennen und nicht bestimmen. Sollte das technisch und wirtschaftlich nicht möglich sein, ist das Ziel der beschränkten Beobachtbarkeit mit anderen Maßnahmen umzusetzen.

10.3 Protokollierung

10.3.1 Ein SB muss Protokoll über jeden Vorgang des Erhalts von Identitätsdaten von einem IdP und deren Weiterleitung an einen SP führen.

10.3.2 Jeder solche Protokolleintrag muss enthalten, um welchen IdP und um welchen SP es sich dabei handelt, sowie die eindeutige Nummer, die der SB vom IdP gemäß Punkt 9.3.3 erhalten hat.

10.3.3 Über diese Transaktionsdaten hinaus darf der SB jedoch keine Daten speichern, insbesondere keine Inhaltsdaten.

10.4 Beendigung der Teilnahme eines SB

10.4.1 Möchte ein SB die Teilnahme an einer Federation beenden, hat er darüber den FO ehestmöglich, spätestens jedoch ein Jahr vor der beabsichtigten Einstellung zu informieren und einen diesbezüglichen Beendigungsplan vorzulegen. Der FO hat darüber alle davon betroffenen Teilnehmer zu informieren. Diese und der FO können im Einzelfall einvernehmlich auch eine kürzere als die oben genannte Einjahresfrist vereinbaren.

10.4.2 Der FO hat, möglichst im Einvernehmen mit dem SB zu entscheiden, ob der SB entweder

a) nach Einstellung seiner Teilnahme weiterhin für Aufbewahrung und ggf. Bereitstellung der Daten zu sorgen hat, zu deren Aufbewahrung und ggf. Bereitstellung er nach Gesetz oder nach diesem Rulebook verpflichtet ist, oder

b) ein anderer SB derselben Federation die Aufgaben des SB übernimmt, wobei nach Punkt 10.5.2 vorzugehen ist.

10.5 Einstellung des Betriebs eines SB

10.5.1 Möchte ein SB den Betrieb einstellen, hat er darüber den FO ehestmöglich, spätestens jedoch ein Jahr vor der beabsichtigten Einstellung zu informieren und einen diesbezüglichen Beendigungsplan vorzulegen. Der FO hat darüber alle davon betroffenen Teilnehmer zu informieren. Diese und der FO können im Einzelfall einvernehmlich auch eine kürzere als die oben genannte Einjahresfrist vereinbaren.

10.5.2 Der FO kann einem anderen SB derselben Federation anbieten die Aufgaben des einzustellenden SB und die Daten, die dafür notwendig sind sowie die nach Gesetz oder nach diesem Rulebook einer Pflicht zur Aufbewahrung und ggf. zur Bereitstellung unterliegen, zu übernehmen. Dabei hat der FO das Einvernehmen mit beiden SB herzustellen, wobei die Interessen des übernehmenden SB schwerer wiegen als die Interessen des übergebenden SB.

10.5.3 Der einzustellende SB hat dem übernehmenden SB rechtzeitig die genannten Daten zu übermitteln.

10.5.4 Ist keinem anderen SB in derselben Federation die Übernahme der Aufgaben des einzustellenden SB zuzumuten, hat der einzustellende SB die Daten, die nach Gesetz oder nach diesem Rulebook einer Pflicht zur Aufbewahrung und ggf. zur Bereitstellung unterliegen, rechtzeitig an die FA zu übermitteln. Diese sind von der FA in ihrem Archiv aufzubewahren und ggf. bereitzustellen.

10.5.5 Ist der Grund für die Einstellung des Betriebs einer Federation die Insolvenz des SB, ist der FO unverzüglich darüber zu informieren und im Übrigen ebenfalls sinngemäß so weit als möglich nach den Bestimmungen dieses Abschnitts vorzugehen.

10.5.6 Über strittige Fragen im Zusammenhang mit der Einstellung des Betriebs eines SB hat die Schlichtungsstelle nach Billigkeit zu entscheiden.

11 Regeln für SP

11.1 Beginn der Teilnahme eines SP

11.1.1 Voraussetzung für die Teilnahme eines SP an einer Federation nach diesem Rulebook ist der Abschluss eines Vertrags über das Verbinden eines Service mit einer Federation (SP-Vertrag) zwischen SP und SB und die Akkreditierung des SP durch den FO. Im Fall der Cross-Federation reichen für die Teilnahme an beiden Federations ein SP-Vertrag in einer der beiden Federations und eine Akkreditierung durch den FO dieser Federation aus.

11.1.2 Der Akkreditierung muss eine Anmeldung des SP beim FO vorausgehen. Diese hat zu enthalten:

a) Name, Rechtsform und Sitz des SP

b) Name und Beschreibung des Service/der Services

c) Vollständige Liste der Attribute, die jeden Service potenziell aus der Federation beziehen möchte

d) Offenlegung der zur Beurteilung des Bestehens von Unvereinbarkeiten nach Punkt 12 notwendigen Informationen

e) Erklärung des SP, die ihn betreffenden Bestimmungen des Rulebooks zu akzeptieren.

11.1.3 Der FO hat binnen 4 Wochen nach Einlangen einer Anmeldung über die Akkreditierung zu entscheiden. Er entscheidet nach freiem Ermessen und muss ihre Entscheidung nicht begründen.

11.1.4 Fällt diese Entscheidung positiv aus, hat die FO den SP unverzüglich in die Akkreditierungsliste für SP einzutragen und dabei die in 11.1.2 genannten Informationen mit Ausnahme der zur Beurteilung des Bestehens von Unvereinbarkeiten nach Punkt 12 notwendigen Informationen anzuführen.

11.1.5 Ein SP kann Teilnehmer in mehreren Federations sein, sofern er die Rulebook-Erweiterungen aller Federations erfüllt, an denen er teilnimmt.

11.2 Teilnahme eines SP

11.2.1 Ein SP darf für jeden Service nur jene Attribute von Benutzern aus einer Federation beziehen, die er bei der Anmeldung des Service angegeben hat.

11.2.2 Ein SP darf nur via SB Attribute von Benutzern aus einer Federation beziehen.

11.2.3 Ein SP ist für die Wahl der Sicherheitsklasse für eine bestimmte Transaktion selbst verantwortlich, insbesondere dafür, dass die Vertrauenswürdigkeit der für einen bestimmten

Zweck übermittelten Identitäts- und Attributsdaten jenen Vorgaben entspricht, die sein internes Risikomanagement für diesen Zweck vorsieht.

11.3 Beendigung der Teilnahme eines SP

Möchte ein SP die Teilnahme an einer Federation beenden, hat er darüber den SB, mit dem er einen Vertrag gemäß Punkt 12.1 geschlossen hat, 8 Wochen vor der beabsichtigten Einstellung zu informieren.

11.4 Einstellung des Betriebs eines SP

Bei der Einstellung des Betriebs eines SP ist wie bei der Beendigung der Teilnahme eines SP nach Punkt 11.3 vorzugehen.

12 Unvereinbarkeiten

12.1 Teilnehmer dürfen keine Aktivitäten betreiben, die geeignet sind, das Vertrauen in ihre Leistungen oder in das Gesamtsystem zu beeinträchtigen.

12.2 Insbesondere gelten folgende Unvereinbarkeiten:

a) Ein FO muss rechtlich, organisatorisch und wirtschaftlich von allen IdP und SB unabhängig sein.

b) Ein SB muss darüber hinaus rechtlich, organisatorisch und wirtschaftlich von allen IdP, SP und Federation-CAs unabhängig sein.

c) Ein IdP muss darüber hinaus rechtlich, organisatorisch und wirtschaftlich von allen Federation-CAs unabhängig sein.

d) Ein Auditor muss rechtlich, organisatorisch und wirtschaftlich von den durch ihn auditierten Teilnehmern des WPV unabhängig sein.

Begründung: Einsicht in die für den Betrieb der Federation verwendeten Zertifikate könnte dem IdP ermöglichen, Teilnehmer von Transaktionen nachzuvollziehen, was dem Prinzip der Nicht-Beobachtbarkeit zuwiderlaufen würde.

12.3 Als organisatorische Abhängigkeit zweier Teilnehmer gilt insbesondere, wenn eine Person in beiden Teilnehmern eine Organfunktion bekleidet, wobei es sich nicht um die gleiche Organfunktion handeln muss.

12.4 Die wirtschaftliche Abhängigkeit zweier Teilnehmer gilt insbesondere dann als gegeben, wenn diese im Sinne der Empfehlung 2003/361/EG[1] der EU-Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen als verbunden gelten.

12.5 Der FO kann insbesondere für die Phase des Aufbaus einer Federation oder für Federations, an denen Gebietskörperschaften oder Selbstverwaltungskörper beteiligt sind, im Einvernehmen mit der FA auf Basis einer Risikoanalyse von den Bestimmungen dieses Abschnitts abweichende Regelungen treffen.

13 Gebühren

13.1 Für Mitglieder des Vereines WPV

Durch Zahlung der Mitgliedsbeiträge durch den jeweiligen Teilnehmer sind die Kosten für die Tätigkeiten der FA, eine allenfalls erforderliche Akkreditierung durch die FA, sowie für die Archivierung von Protokolldaten im Falle der Beendigung der Rolle des Teilnehmers abgedeckt.

Die Festsetzung der Höhe der Mitgliedsbeiträge sowie allfällige Folgen der Nichtzahlung sind im Vereinsstatut geregelt.

Die Vorschreibung der Mitgliedsbeiträge erfolgt jährlich durch den Verein unter Angabe der Fälligkeit und allfälligen näheren Angaben zur Zahlungsweise.

13.2 Für Nicht-Mitglieder des Vereines WPV

Soweit einzelne Teilnehmer keine Mitglieder im Verein WPV sind, werden diesen für die unter 13.1. Absatz 1 genannten Leistungen jährliche Kostenbeiträge in Höhe der jeweils festgelegten Mitgliedsbeiträge für ordentliche Mitglieder durch die FA in Rechnung gestellt.

14 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.

Die Datensicherheitsvorgaben sind so zu organisieren, dass sie zwischen verschieden Federations möglichst gut vergleichbar sind. Dazu ist im Dokument „WPV SP-Risikomgmt“

[1] http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=DE und http://ec.europa.eu/DocsRoom/documents/15582/attachments/1/translations/de/renditions/native.

eine Struktur vorgegeben. Aus diesem Dokument werden die Datensicherheitsvorgaben für FO, SB und IDP abgeleitet.

15 Ausnahmen von diesem 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.

16 Anwendbares Recht, Gerichtsstand, Schlichtungsstelle

16.1 Auf den WPV, dieses Rulebook und die auf dessen Basis entstandenen Rechtsbeziehungen, Verträge, Organisationen und Federations ist österreichisches Recht anzuwenden, mit Ausnahme des UN-Kaufrechts.

16.2 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.

16.3 Für gerichtliche Streitigkeiten aus diesem Rulebook ist das jeweils sachlich zuständige Gericht im Sprengel des Handelsgerichts Wien zuständig, wobei Bestimmungen dieses Rulebooks zu beachten sind, die die Anrufung der Schlichtungsstelle vor Anrufung der ordentlichen Gerichte vorsehen.