Wirtschaftsportalverbund Risikokonzept

Version 10.9.2014

Walter Hötzendorfer

Inhalt

1 Vorbemerkungen zum Thema Risiken[1]

Eine Risikoanalyse wird häufig in die Phasen Risikoidentifizierung, Risikoquantifizierung und Risikomanagement eingeteilt. Demgegenüber geht das vorliegende Risikokonzept etwas anders vor. Der Wirtschaftsportalverbund ist ein komplexes System, bestehend aus verschiedenen Akteuren in verschiedenen Rollen, das primär dem Identitätsmanagement für nachgeordnete Zwecke (ganz allgemein: der Erbringung bestimmter Services) dient. Weil diese nachgeordneten Zwecke sehr unterschiedlich und daher nicht generalisierbar und auch nicht abschließend bekannt sind, ist eine Quantifizierung der identifizierten Risiken nicht sinnvoll möglich, wie unten noch näher erläutert wird. Zugleich spielt aufgrund der Natur des WPV als System aus zahlreichen unabhängigen Akteuren die Frage der Zuordnung der Risiken zu den verschiedenen Rollen der Akteure eine besondere Rolle.
Das vorliegende Risikokonzept kann daher in die Schritte Risikoidentifikation, Risikobeschreibung, Risikotypisierung und Risikozuordnung gegliedert werden.

1.1 Risikoidentifikation

Wie jedes komplexe technische System ist der WPV Gefährdungen ausgesetzt. Diese können durch höhere Gewalt, organisatorische Mängel, technische Fehler, menschliche Fehler oder vorsätzliche Handlungen bedingt sein.
Besonders relevant sind im vorliegenden Zusammenhang Risiken, die sich durch äußere Angreifer ergeben, Risiken, die sich aus technischen oder menschlichen Fehlern ergeben, und Risiken, die sich aufgrund organisatorischer Mängel aus divergierenden Interessen der Beteiligten ergeben. Die verschiedenen Akteure haben zum Teil gemeinsame, zum Teil jedoch unterschiedliche oder sogar divergierende Ziele, wie z.B. den Schutz der eigenen Privatsphäre, die Aufrechterhaltung ihres Betriebs, die Verbesserung der eigenen Marktposition, die Gewinnung von Kunden, das Niedrighalten der eigenen Kosten, das Niedrighalten des administrativen Aufwands, das Steigern der eigenen Reputation etc.

Erster und wichtigster Zweck des vorliegenden Risikokonzepts ist daher die Risikoidentifikation: Es muss abgeschätzt werden, was im System WPV „passieren kann“. Die möglichst umfassende Auflistung und Beschreibung der möglichen Risiken ist eine wichtige Grundlage für die Ausarbeitung der Sicherheitsklassen und der dabei festgelegten Maßnahmen sowie für die Beantwortung der Frage, wer welches Risiko tragen soll.

1.2 Risikoquantifizierung

Allgemein hängt die Höhe eines sich aus einer Gefährdung ergebenden Risikos von folgenden Faktoren ab:

- Potenzieller Schaden durch die Gefährdung und sonstige Folgen, Funktionseinschränkungen etc.
- Eintrittswahrscheinlichkeit der Gefährdung

Das Risiko einer Gefährdung kann wie folgt quantifiziert werden:

[1] Die hier vorgestellten Grundlagen sind zum Teil angelehnt an *Freiling/Grimm/Großpietsch/Keller/Mottok et al.*, Technische Sicherheit und Informationssicherheit, Informatik-Spektrum 2013, 14.

Risiko = Schadeneintrittswahrscheinlichkeit x Schadenshöhe

Nach anfänglichen Versuchen, die potenzielle Schadenshöhe und die Eintrittswahrscheinlichkeit der im WPV identifizierten Risiken abzuschätzen, wurde deutlich, dass diese fast ausschließlich vom Anwendungsfall abhängen. Die potenzielle Schadenshöhe entspricht dem größten anzunehmenden Schaden, der im jeweiligen Kontext bei Eintritt der Gefährdung entstehen kann, und dieser kann sehr unterschiedlich sein. Wenn z.B. aufgrund falscher oder missbräuchlich verwendeter Identitätsdaten unbefugt Banküberweisungen getätigt werden können, ist der Schaden ungleich höher, als wenn „nur" ein zehnprozentiger Stammkunden- oder Studentenrabatt unbefugt in Anspruch genommen wird.

1.3 Umgang mit Risiken

Die mit der Nutzung technischer Systeme notwendigerweise verbundenen Risiken müssen möglichst umfassend identifiziert und kontrolliert werden, nicht alle können jedoch vollständig ausgeschlossen werden und müssen daher in Kauf genommen werden, sofern der angestrebte Nutzen höher ist als das jeweilige Risiko. Für den Umgang mit Risiken bestehen folgende Möglichkeiten, die auch kombiniert werden können:

- Vermeidung des Risikos: Treffen von Maßnahmen, die dazu führen, dass das Eintreten einer bestimmten Gefährdung ausgeschlossen werden kann.
- Reduktion des Risikos: Treffen von Maßnahmen, die die Eintrittswahrscheinlichkeit oder die potenzielle Schadenshöhe einer Gefährdung reduzieren.
- Transfer des Risikos: Abwälzen des Risikos auf einen Dritten, z.B. durch Abschluss einer Versicherung oder Outsourcing.
- Akzeptanz des Risikos: Das Risiko wird nach Abwägung mit dem zu erzielenden Nutzen in Kauf genommen, insbesondere dann, wenn die zuvor genannten Möglichkeiten ausgeschöpft sind.

Im Zuge der Ausarbeitung der Risikoklassen werden Maßnahmen festgelegt, die der Vermeidung von Risiken, der Reduktion von Risiken sowie dem Transfer von Risiken dienen.

2 Haftung

2.1 Allgemeines zum Schadenersatzrecht (Haftpflichtrecht)

Das Thema Haftung kommt immer dann auf, wenn ein Schaden eintritt, sei dieser monetärer oder nichtmonetärer Natur. Die Grundregel ist, dass jene Partei, die den Schaden hat, diesen selbst zu tragen hat (§ 1311 ABGB Satz 1). Rechtliche Bestimmungen können die Gefahrtragung jedoch unter bestimmten Voraussetzungen einer anderen Partei auferlegen. Dies können entweder gesetzliche oder vertragliche Bestimmungen sein.
Im Allgemeinen gilt die Verschuldenshaftung, sodass eine Partei grundsätzlich nur dann für einen Schaden haftet, wenn sie ein Verschulden für diesen Schaden trifft. Im Einzelfall können Ausnahmen von der Verschuldenshaftung bestehen, etwa im Fall der Gefährdungshaftung oder bei entsprechender vertraglicher Vereinbarung. Letzteres ist z.B. im Kreditkartenwesen der Fall: Das Kreditkartenunternehmen haftet i.d.R. stets für jede unautorisierte Vermögensverschiebung, unabhängig von deren Ursache.

Wenn aus wirtschaftlichen oder anderen Gründen die gesetzliche Haftung für ein bestimmtes Risiko nicht angemessen erscheint, ist zu untersuchen, ob und inwieweit diese Haftung vertraglich anders geregelt werden kann.
Zur Verschuldenshaftung kann es kommen, wenn jemand schuldhaft einen Schaden dadurch verursacht, dass er rechtswidrig handelt, indem er entweder allgemein bestehenden Pflichten zuwiderhandelt (deliktische Haftung) oder einen Vertrag verletzt (vertragliche Haftung) (§ 1295 ABGB).
Wie einleitend beschrieben soll hier zunächst die gesetzliche Haftungssituation bei Nichtbestehen einer entsprechenden vertraglichen Regelung untersucht werden, sodass auf die deliktische Haftung näher einzugehen ist. Die Rechtswidrigkeit kann sich im Zivilrecht nicht nur aus einem strafbaren Verhalten ergeben, sondern generell aus dem Eingriff in ein absolutes Recht (vor allem Leben, Gesundheit, Freiheit, Eigentum), aus einer Schutzgesetzverletzung, oder wenn – unabhängig vom betroffenen Rechtsgut – in einer gegen die guten Sitten verstoßenden Weise absichtlich Schaden zugefügt wird (§ 1295 Abs 2 ABGB).

2.2 Sachverständigenhaftung

Die §§ 1299 f ABGB treffen besondere Haftungsregeln für „Sachverständige“, wobei dies ein sehr weiter Begriff ist. § 1299 stellt für Sachverständige einen strengeren Verschuldensmaßstab auf: Sachverständige müssen die durchschnittlichen Fähigkeiten ihres Berufsstandes haben. § 1300 ABGB regelt die Haftung für Auskünfte durch Sachverständige. Diese wird etwa auch auf Bonitätsauskünfte von Banken angewendet. Diesbezüglich hat sich in Rechtsprechung und Literatur folgende Auslegung der §§ 1299 f etabliert:
„Für unrichtige Bonitätsauskünfte haftet eine Bank gem §§ 1299, 1300 Satz 1 dann, wenn die Auskunft nicht aus bloßer Gefälligkeit, sondern im Rahmen eines Verpflichtungsverhältnisses erteilt wurde und die Bank zumindest fahrlässig gehandelt hat. Die Haftung nach § 1300 Satz 1 ist jedenfalls zu bejahen, wenn ein Auskunftsvertrag vorliegt, was dann der Fall ist, wenn für die Auskunfterteilung ein Entgelt vereinbart wird. Darüber hinaus haftet die Bank auch dann, wenn die Auskunfterteilung als Nebenleistung einem Gesamtauftrag zugeordnet werden kann, oder wenn eine ständige Geschäftsbeziehung zwischen Bank und Auskunftsempfänger besteht. Auch in diesem letzteren Fall liegt nämlich ein Vertrags- und Vertrauensverhältnis vor, das die Annahme ausschließt, dass die Auskunft aus bloßer Gefälligkeit erteilt wird.
Darüber hinaus bejahen Rsp und Lehre eine Haftung nach § 1300 Satz 1 auch bei einmaliger Auskunfterteilung außerhalb eines Gesamtverhältnisses und außerhalb einer ständigen Geschäftsbeziehung, wenn Auskunft nicht völlig selbstlos gegeben wurde. Str ist diesbezüglich nur der Haftungsgrund. Die Rsp nimmt teilweise einen schlüssig abgeschlossenen Auskunftsvertrag an; die Lehre hingegen – abl gegenüber der Konstruktion eines eigenständigen Auskunftsvertrages – stützt die Haftung auf objektiv-rechtliche Schutzpflichten, die aus dem Vertrauensverhältnis resultieren, das auch schon bei erstmaliger Kontaktaufnahme außerhalb eines laufenden Geschäftskontaktes entstehen kann. […]
Soll eine Bank eine Bonitätsauskunft über jemanden, der nicht ihr Kunde ist, geben, so muss sie diese Information bei einem anderen Kreditinstitut einholen. Für diese Auskunft haftet sie nur dann nach § 1300 Satz 1, wenn sie die Information nicht erkennbar als eine fremde (von einer anderen Bank eingeholte) Information, sondern als eigenes Wissen weitergibt. Teilt die Bank hingegen erkennbar nur mit, was sie selbst bei einer anderen Bank erfahren

hat, dann haftet sie nur, wenn die Unrichtigkeit der Auskunft für die Bank erkennbar gewesen wäre. Eine Dritthaftung jener Bank, die an die Bank des Auskunft Ersuchenden die Informationen weitergegeben hat, ist typischerweise zu verneinen, weil diese Bank dem Auskunftsersuchenden gegenüber regelmäßig nicht in Erscheinung tritt. Der Haftungskreis wäre unüberschaubar; auch hat die Bank bei Auskunfterteilung gegenüber einer anderen Bank regelmäßig keinen Nutzen."[2]

Wenn eine Bank für Bonitätsauskünfte, die sie gibt, nach den Regeln der Sachverständigenhaftung haftet, muss dies auch für Identity Provider und Attribute Provider zutreffen, wenn sie gegen Entgelt Identitätsdaten an Relying Partys weitergeben. Bei Identity Providern ist dies geradezu ihr Kerngeschäft; bei Attribute Providern kann die Weitergabe von Identitätsdaten entweder auch das Kerngeschäft sein, oder es ist zwar nicht ihr Kerngeschäft, aber – vergleichbar mit Bonitätsauskünften bei Banken – ein im Rahmen ihrer Tätigkeit üblicher Vorgang. Dies lässt sich bereits aus dem Umstand der Teilnahme an einer Federation in der Rolle eines Attribute Providers ableiten

Legt man nun die dargestellte Rechtslage betreffend Bonitätsauskünfte durch Banken auf Identity Provider und Attribute Provider um, würde dies bedeuten, IdP und AP haften für weitergegebene Identitätsdaten, wenn dies im Rahmen eines diesbezüglichen entgeltlichen Vertrages oder einer ständigen Geschäftsbeziehung erfolgt. Das Verhältnis zweier Teilnehmer einer Federation, zwischen denen es zum Austausch von Identitätsdaten kommt, ist wohl jedenfalls mit einer ständigen Geschäftsbeziehung gleichzusetzen.

2.3 Haftungsfreizeichnung und Haftungsbeschränkung

Wie soeben dargelegt, ist die gesetzliche Grundregel somit das Bestehen einer Haftung für die Richtigkeit der Identitätsdaten, die vonseiten der IdP und AP in einer Federation weitergegeben werden. IdP und AP sind somit ersatzpflichtig für den Schaden, der bei der Relying Party durch – allgemein formuliert – unrichtige Identitätsdaten entsteht. Dies ist nach der Konzeption des WPV jedoch nicht immer oder nicht uneingeschränkt erwünscht. Wie im Konzept für die WPV-Sicherheitsklassen beschrieben, sind zwei Arten von Qualitäts- und Sicherheitsanforderungen vorgesehen, einerseits „risikoorientierte Anforderungen", die eine betragsmäßige Haftungsobergrenze vorsehen (z.B. für die Richtigkeit der Benutzeridentifikation wird bis max. 100 Euro pro Login gehaftet), und andererseits „maßnahmenorientierte Anforderungen" (z.B. „Die Feststellung der Identität des Betroffenen muss gemäß § 40 Abs 1 Bankwesengesetz erfolgen").

Bei maßnahmenorientierten Anforderungen wird die Haftung entsprechend der gesetzlichen Grundregel erwünscht sein, z.B. die Haftung für die Richtigkeit der Angabe, dass die Identität des Betroffenen gemäß § 40 Abs 1 Bankwesengesetz festgestellt wurde. Ist jedoch für bestimmte Angaben eine betragsmäßige Haftungsobergrenze erwünscht, was der Regelfall sein wird, stellt sich die Frage, ob die betragsmäßige Beschränkung der Haftung, also ein vertragliches Abweichen von der gesetzlichen Grundregel, rechtlich zulässig ist.

Gemäß § 6 Abs 1 Z 9 KSchG ist eine Haftungsfreizeichnung oder Haftungsbeschränkung für grobe Fahrlässigkeit (und Vorsatz) gegenüber Verbrauchern unwirksam. Strittig ist die Wirksamkeit der Haftungsfreizeichnung oder Haftungsbeschränkung für grobe Fahrlässigkeit unter Unternehmern bei entgeltlichen Auskünften.[3] Der OGH trifft in diesem Zusammenhang eine – unübliche – Unterscheidung zwischen grober Fahrlässigkeit und

[2] *Schacherreiter* in *Kletečka/Schauer*, ABGB-ON[1.01] § 1299 Rz 55 ff.

[3] Siehe dazu *Jabornegg*, Formularmäßige Haftungsfreizeichnung für grob fahrlässige Auskunft, JBl 1986, 144.

„krasser“ grober Fahrlässigkeit und hält bei Bonitätsauskünften von Banken eine Haftungsbeschränkung bei grober Fahrlässigkeit für zulässig,[4] bei krasser grober Fahrlässigkeit jedoch für unzulässig.[5] Die Zulässigkeit der Haftungsbeschränkung bei schlichter grober Fahrlässigkeit bejaht der OGH mit dem Argument, dass Unternehmen das Risiko der Zahlungsunfähigkeit ihrer Kunden nicht ohne weiteres auf Banken überwälzen können sollen; die Übertragbarkeit dieser Wertung auf andere Bereiche ist daher fraglich.[6]
Die betragsmäßige Haftungsbeschränkung ist für leichte Fahrlässigkeit somit zulässig, für grobe Fahrlässigkeit ist die Zulässigkeit fraglich. Zu klären ist daher, ob im WPV auch betragsmäßige Haftungsbeschränkungen für grobe Fahrlässigkeit erwünscht sind. In diesem Fall wären noch weitere Recherchen und Überlegungen zu dieser Frage nötig.

3 Risiken

Im Folgenden sind die im Zusammenhang mit dem WPV identifizierten Risiken systematisch aufgelistet. Diese Auflistung wurde nach bestem Wissen und Gewissen erstellt, erhebt aber nicht den Anspruch auf Vollständigkeit. Das gilt insbesondere auch für die Auflistung der möglichen Folgen des Eintritts eines Risikos. Bei der Erstellung wurde versucht, durch Einbindung anderer Experten sowie der Stakeholder, wie insbesondere zukünftiger Teilnehmer des WPV, unterschiedliche Perspektiven einzunehmen, um ein möglichst breites Bild dessen zu erhalten, „was im WPV passieren kann“. Es ist aber auch nach der Fertigstellung dieser ersten Version der Risikoanalyse noch nicht zu spät, weitere Risiken in die Liste aufzunehmen, die noch nicht enthalten sind und auch nicht einen Unterfall eines der enthaltenen Risiken darstellen. Diesbezügliche Anregungen durch Leser dieses Dokuments sind ausdrücklich erwünscht.
Die identifizierten Risiken sind hierarchisch in Kategorien eingeteilt, beginnend mit der Unterscheidung zwischen operativen Risiken, die im täglichen Betrieb einer Federation auftreten, und den nichtoperativen Risiken, die z.B. mit der Teilnahme am WPV oder mit dem WPV als Ganzes in Zusammenhang stehen.
Unabhängig von der hierarchischen Gliederung, die primär der Übersicht und Strukturierung dient, wurden die Risiken einem (oder in Ausnahmefällen mehreren) der folgenden sechs grundlegenden **Risikotypen** zugeordnet:

AV	Verfügbarkeits-Risiken („Availability“) inkl. Business Continuity
DP	Datenschutz-Risiken („Data Protection“)
ID	Identifikations-Risiken
Aufsicht	Aufsichts-Risiken
Recht	Rechtliche Risiken
SC	Skalierbarkeits-Risiken („Scalability“)

Tabelle 1 - Risikotypen

Die Risikotypen sind so gewählt, dass die jeweils einem Typ zugeordneten Risiken Gemeinsamkeiten hinsichtlich ihrer Wirkrichtung und/oder des Umgangs mit ihnen im WPV aufweisen.

[4] OGH 22. 11. 1984, 7 Ob 666/84 und OGH 9. 5. 1985, 6 Ob 836/83.
[5] OGH 22. 11. 1984, 7 Ob 666/84, vgl. *Reischauer* in *Rummel*[3], § 1300 Rz 10 mwN.
[6] Vgl. *Reischauer* in *Rummel*[3], § 1300 Rz 10 mwN.

Über die Wirkrichtung kann aus der Außenperspektive, also der Perspektive der WPV-„Kunden“, das sind die Service Provider und die Nutzer, Folgendes festgestellt werden:

- Verfügbarkeits-Risiken (AV) treffen i.d.R. sowohl Nutzer als auch Service Provider unmittelbar.
- Datenschutz-Risiken (DP) treffen unmittelbar die Nutzer.
- Identifikations-Risiken (ID), Aufsichts-Risiken, rechtliche Risiken und Skalierbarkeits-Risiken treffen unmittelbar die Service Provider.

Die einzelnen Risiken werden in folgender Form beschrieben:

[Risikobezeichnung]			**[Typ]**
Verantwortlich:	[Welche Akteure sind primär für den Eintritt des Risikos verantwortlich?]	**Primär geschädigt:**	[Welche Akteure sind primär vom Eintritt des Risikos betroffen?]
[Risikobeschreibung]			
Mögliche Folgen:	[Welche Folgen kann der Eintritt des Risikos haben?]		

Tabelle 2 – Legende zur Risikobeschreibung

Die identifizierten Risiken liegen auch in Form einer Excel-Tabelle als Anhang zu diesem Dokument vor.

3.1 Operative Risiken

3.1.1 Registrierungs-Risiken

Erfundene Identität			**ID**
Verantwortlich:	IdP, Nutzer	**Primär geschädigt:**	SP, IdP
Ein Nutzer tritt unter einer erfundenen Identität auf, weil er bei der initialen Registrierung falsche Angaben gemacht hat und/oder diese nicht ordnungsgemäß funktioniert hat. Die wahre Identität des Nutzers ist somit im gesamten System unbekannt.			
Mögliche Folgen:	- Ein SP erbringt eine Leistung für einen unbekannten Empfänger. - Unberechtigte Vermögensverschiebung. - Unberechtigter Datentransfer.		

Fremde Identität ("Identitätsdiebstahl")			**ID**
Verantwortlich:	IdP, Nutzer	**Primär geschädigt:**	Nutzer, SP, IdP
Ein Nutzer tritt unter einer fremden Identität auf, weil er bei der initialen Registrierung falsche Angaben gemacht hat und/oder diese nicht ordnungsgemäß funktioniert hat. Die wahre Identität des Nutzers ist somit unbekannt.			
Mögliche Folgen:	- Ein SP erbringt eine Leistung für einen unbekannten Empfänger. - Der Nutzer erhält Zugriff auf fremde Daten. - Unberechtigte Vermögensverschiebung. - Unberechtigter Datentransfer.		

Abstreiten der Identität			**ID**
Verantwortlich:	IdP, Nutzer	**Primär geschädigt:**	SP, (IdP)
Ein Nutzer behauptet fälschlicherweise, sich niemals registriert zu haben und daher nichts mit einer bestimmten Identität zu tun zu haben. (*Ist vermeidbar, wenn das Enrolment richtig gemacht wurde und bewiesen werden kann.*)			
Mögliche Folgen:	- Handlungen können keinem Nutzer zugerechnet werden.		

Verlust der Identität			**AV**
Verantwortlich:	IdP, (Nutzer)	**Primär geschädigt:**	Nutzer, SP
Eine registrierte elektronische Identität kann nicht mehr verwendet werden.			
Mögliche Folgen:	- Der Zugriff auf Services und Daten ist nicht mehr möglich.		

3.1.2 Authentifizierungs-Risiken

False Positive			**DP, ID**
Verantwortlich:	IdP, (Nutzer)	**Primär geschädigt:**	Nutzer, SP, IdP
Ein Nutzer tritt unter einer fremden Identität auf, da es ihm gelungen ist, sich mit fremden Zugangsdaten zu authentisieren, oder die Authentifizierung nicht ordnungsgemäß funktioniert hat.			
Mögliche Folgen:	- Ein SP erbringt eine Leistung für einen unbekannten Empfänger. - Der Benutzer erhält Zugriff auf fremde Daten. - Unberechtigte Vermögensverschiebung. - Unberechtigter Datentransfer.		

False Negative			**AV**
Verantwortlich:	IdP	**Primär geschädigt:**	Nutzer, SP
Ein ordnungsgemäß registrierter, berechtigter Nutzer schafft es nicht, sich ordnungsgemäß zu authentisieren.			
Mögliche Folgen:	- Durchführung einer Transaktion nicht möglich. - Wenn dauerhaft -> **Verlust der Identität**		

Abstreiten der Authentifizierung			**ID**
Verantwortlich:	IdP, Nutzer	**Primär geschädigt:**	SP, (IdP)
Ein Nutzer behauptet fälschlicherweise, eine bestimmte Transaktion nicht durchgeführt zu haben, d.h. sich in einem bestimmten Kontext nicht authentisiert zu haben. (*Ist ab einem bestimmten Assurance Level vermeidbar.*)			
Mögliche Folgen:	- Konflikt über die Konsequenzen der Transaktion, Tragung der Kosten etc.		

3.1.3 Attributs-Risiken

Falsche Attributsangabe			**ID**
Verantwortlich:	AP, Nutzer	**Primär geschädigt:**	SP
Ein AP leitet an eine Relying Party ein falsches (d.h. nicht den Tatsachen entsprechendes) Attribut weiter, weil es dem Nutzer gelungen ist, dem AP bewusst ein falsches Attribut bekanntzugeben.			
Mögliche Folgen:	- Ein SP erbringt eine Leistung auf der Basis falscher Angaben. - Unberechtigte Vermögensverschiebung. - Unberechtigter Datentransfer.		

Falsche Attributsweiterleitung			**ID, (AV)**
Verantwortlich:	AP	**Primär geschädigt:**	Nutzer, SP
Ein AP leitet an eine Relying Party ein falsches (d.h. nicht den Tatsachen entsprechendes) Attribut weiter, ohne dass der Nutzer falsche Angaben gemacht hat.			
Mögliche Folgen:	- Ein SP erbringt eine Leistung auf der Basis falscher Angaben. - Unberechtigte Vermögensverschiebung. - Unberechtigter Datentransfer. - ODER: Eine eigentlich zulässige Transaktion wird aufgrund des falschen Attributs nicht zugelassen.		

Attributsmissbrauch			**DP**
Verantwortlich:	Der jeweilige Teilnehmer (SP, IdP, AP)	**Primär geschädigt:**	Nutzer
Ein Attribut wird von einem Teilnehmer entgegen den Willen des Betroffenen, entgegen eine gesetzliche Bestimmung oder entgegen eine vertragliche Vereinbarung gebraucht.			
Mögliche Folgen:	- Eingriff in die Privatsphäre. - Ansprüche des Betroffenen. - Reputationsschaden beim AP.		

3.1.4 Performance-Risiken (3rd-Party-Risk)

Nichterfüllungs-Risiko			**AV**
Verantwortlich:	Der jeweilige Teilnehmer	**Primär geschädigt:**	Potenziell alle
Ein anderer Teilnehmer erfüllt seine Funktion bzw. seine Verpflichtungen nicht.			
Mögliche Folgen:	- Durchführung einer Transaktion nicht möglich.		

Schlechterfüllungs-Risiko			*****
Verantwortlich:	Der jeweilige Teilnehmer	**Primär geschädigt:**	Potenziell alle
Ein anderer Teilnehmer erfüllt seine Funktion bzw. seine Verpflichtungen nicht ordnungsgemäß.			
Mögliche Folgen:	- Abhängig von der Rolle des Teilnehmers können sich alle anderen Risiken verwirklichen.		

* Das Schlechterfüllungs-Risiko kann potenziell zur Verwirklichung der anderen, spezifischeren Risiken führen. Es nimmt daher eine Sonderstellung ein und kann nicht sinnvoll einzelnen Kategorien zugeordnet werden.

Ausscheidens-Risiko			**AV**
Verantwortlich:	Der jeweilige Teilnehmer	**Primär geschädigt:**	Potenziell alle
Ein Teilnehmer stellt seinen Betrieb ein.			
Mögliche Folgen:	- Der vom Teilnehmer betriebene Dienst ist nicht mehr verfügbar. - Der Übergang des Betriebs auf andere Teilnehmer muss durchgeführt werden. - Daten müssen archiviert werden.		

3.1.5 Informationssicherheits-Risiken

Vertraulichkeits-Risiko			**DP, ID**
Verantwortlich:	Der jeweilige Teilnehmer	**Primär geschädigt:**	Potenziell alle
Unautorisierter Zugriff auf Daten.			
Mögliche Folgen:	- Schaden beim Betroffenen. - Andere Risiken können sich verwirklichen: Datenschutz-Risiken, Compliance-Risiken etc.		

Integritäts-Risiko			**ID**
Verantwortlich:	Der jeweilige Teilnehmer	**Primär geschädigt:**	Potenziell alle
Unautorisierte Modifikation von Daten.			
Mögliche Folgen:	- Andere Risiken können sich verwirklichen: Registrierungs-Risiken, Authentifizierungs-Risiken, Attributs-Risiken etc.		

Anmerkung: Die Verfügbarkeit, als weiteres Schutzziel der Informationssicherheit, ist nicht durch ein einzelnes Risiko, sondern durch den Risikotyp „AV“ abgedeckt und somit durch mehrere, spezifischere Risiken, die diesem Typ zugeordnet sind.

3.1.6 Privatsphäre-Risiken

Datenmissbrauchs-Risiko			**DP, ID**
Verantwortlich:	Der jeweilige Teilnehmer	**Primär geschädigt:**	Nutzer
Verwendung von personenbezogenen Daten entgegen der diesbezüglichen Regeln. (Dies geht über die Erfüllung der datenschutzrechtlichen Anforderungen hinaus und ist auch nicht deckungsgleich mit dem Vertraulichkeits-Risiko.)			
Mögliche Folgen:	- Eingriff in die Privatsphäre. - Ansprüche des Betroffenen aus Vertrag oder aus dem Datenschutzgesetz.		

Datenherausgabe-Risiko			**DP**
Verantwortlich:	SP	**Primär geschädigt:**	Nutzer
Der Nutzer wird von einem SP dazu gebracht, seine zivile Identität und/oder bestimmte Attribute herauszugeben, weil dies mittels FIM so bequem möglich ist, ohne dass diese Informationen für eine Transaktion tatsächlich nötig wären.			
Mögliche Folgen:	- Eingriff in die Privatsphäre. - (Ansprüche des Betroffenen aus Vertrag oder aus dem Datenschutzgesetz.)		

3.1.7 Technische Risiken

Technische Risiken, wie insbesondere Ausfall oder Fehlfunktion einer technischen Komponente, nehmen unter den operativen Risiken eine Sonderstellung ein. Sie sind zwar eine wesentliche Risikokategorie, stehen aber, ähnlich wie das Schlechterfüllungs-Risiko oben, orthogonal zu den anderen, spezifischeren operativen Risiken. Das bedeutet, technische Risiken können zur Verwirklichung der meisten anderen Risiken führen. Sie sind also meist Ursache für andere Risiken. Bedeutender als die Ursache ist jedoch aus der Perspektive der Geschädigten die Wirkung, also das spezifische verwirklichte Risiko, das im Rahmen dieser Auflistung jeweils separat behandelt wird.

3.2 Nichtoperative Risiken

3.2.1 Compliance-Risiken

Regulatorisches Risiko			**Recht**
Verantwortlich:	Der jeweilige Teilnehmer	**Primär geschädigt:**	Potenziell alle
Ein Prozess eines Teilnehmers oder eine bestimmte Transaktion widerspricht einer Regel des Rulebooks.			
Mögliche Folgen:	- Die vom Rulebook vorgesehene Sanktion tritt ein. - Der Geschädigte erhebt Ansprüche.		

Rechtswidrigkeits-Risiko			**Recht**
Verantwortlich:	Der jeweilige Teilnehmer, WPV	**Primär geschädigt:**	Potenziell alle
Ein Aspekt der Gestaltung des WPV, ein Prozess eines Teilnehmers oder eine bestimmte Transaktion widerspricht einer Rechtsnorm.			
Mögliche Folgen:	- Die von der Rechtsnorm vorgesehene Sanktion tritt ein. - Der Geschädigte erhebt Ansprüche.		

3.2.2 Rechtsdurchsetzungs-Risiko

Rechtsdurchsetzungs-Risiko			**Recht**
Verantwortlich:	WPV	**Primär geschädigt:**	Potenziell alle
Bestehende Ansprüche können nicht durchgesetzt werden.			
Mögliche Folgen:	- Bestehende Ansprüche können nicht durchgesetzt werden.		

3.2.3 Wirtschaftliche Risiken

Zahlungsausfall-Risiko			**AV**
Verantwortlich:	Der jeweilige Teilnehmer	**Primär geschädigt:**	Potenziell alle
Ein Teilnehmer kommt einer Zahlungspflicht nicht nach.			
Mögliche Folgen:	- Zahlungsausstand - Eintreibungsaufwand - Andere Teilnehmer stellen den Geschäftsverkehr mit dem jeweiligen Teilnehmer ein.		

Insolvenz-Risiko			**AV**
Verantwortlich:	Der jeweilige Teilnehmer	**Primär geschädigt:**	Potenziell alle
Ein Teilnehmer wird insolvent.			
Mögliche Folgen:	- Der Teilnehmer stellt seinen Betrieb ein. - Bestehende Ansprüche können nicht durchgesetzt werden.		

3.2.4 Akkreditierungs-Risiken

Akkreditierungsfehler-Risiko			**Aufsicht**
Verantwortlich:	Akkreditierender (FA oder FO)	**Primär geschädigt:**	Potenziell alle
Eine Akkreditierung fällt zu Unrecht positiv aus, weil der Akkreditierende einen Fehler begeht.			
Mögliche Folgen:	- Ungeeigneter Teilnehmer im WPV. - Zahlreiche andere Risiken können sich verwirklichen.		

Akkreditierungsbetrugs-Risiko			**Aufsicht**
Verantwortlich:	Akkreditierender (FA oder FO)	**Primär geschädigt:**	Potenziell alle
Eine Akkreditierung wird zu Unrecht durchgeführt, weil der zu Akkreditierende falsche Angaben macht oder sich auf sonstige Weise die Akkreditierung erschleicht.			

Mögliche Folgen:	- Ungeeigneter Teilnehmer im WPV. - Zahlreiche andere Risiken können sich verwirklichen.

Akkreditierung negativ			**Aufsicht**
Verantwortlich:	Akkreditierender (FA oder FO)	**Primär geschädigt:**	Potenzielle Teilnehmer
Eine Akkreditierung wird zu Unrecht abgelehnt.			
Mögliche Folgen:	- Ein geeigneter Teilnehmer kann nicht teilnehmen.		

3.2.5 Audit-Risiken

Auditfehler-Risiko			**Aufsicht**
Verantwortlich:	Auditor, auditierter Teilnehmer	**Primär geschädigt:**	Potenziell alle
Ein Audit fällt zu Unrecht positiv aus, weil der Auditor selbst einen Fehler begeht.			
Mögliche Folgen:	- Ungeeigneter Teilnehmer im WPV. - Zahlreiche andere Risiken können sich verwirklichen.		

Auditbetrugs-Risiko			**Aufsicht**
Verantwortlich:	Auditor	**Primär geschädigt:**	Potenziell alle
Ein Audit fällt zu Unrecht positiv aus, weil der Auditierte falsche Angaben macht oder sich auf sonstige Weise eine positive Bestätigung erschleicht.			
Mögliche Folgen:	- Ungeeigneter Teilnehmer im WPV. - Zahlreiche andere Risiken können sich verwirklichen.		

Audit negativ			**Aufsicht**
Verantwortlich:	Auditor	**Primär geschädigt:**	Potenziell IdP, SB, FO
Ein Audit fällt zu Unrecht negativ aus.			
Mögliche Folgen:	- Ein geeigneter Teilnehmer kann nicht weiter teilnehmen.		

3.2.6 Skalierbarkeits-Risiko

Skalierbarkeits-Risiko				**SC**
Verantwortlich:	WPV	**Primär geschädigt:**	Potenziell alle	
Ein Aspekt der Gestaltung des WPV verhindert das angestrebte Wachstum des WPV				
Mögliche Folgen:	- Die Skalierbarkeit des WPV ist behindert.			

Anmerkung: Image-Verlust kann eine Folge des Eintretens jedes einzelnen Risikos sein. Der Image-Verlust wurde daher nicht als einzelnes Risiko angeführt.

4 Umgang mit den identifizierten Risiken

In diesem Kapitel wird – gleichsam als „Überleitung“ zum Dokument „Sicherheitsklassen“ – das erarbeitete Konzept zum Umgang mit den identifizierten Risiken erläutert.

Alle identifizierten Risiken müssen bei der Gestaltung des WPV, insbesondere des Rulebooks berücksichtigt werden. Die Auflistung im vorigen Kapitel bzw. die Risikotabelle kann als Checkliste dienen, um zu klären, ob für jedes identifizierte Risiko in der Gestaltung des WPV Vorkehrungen getroffen wurden oder die bewusste Entscheidung der Akzeptanz des Risikos getroffen wurde.

Eine wesentliche Maßnahme, um den identifizierten Risiken Rechnung zu tragen, ist die Ausarbeitung der Sicherheitsklassen und der zugehörigen Maßnahmen. Dabei spielen hauptsächlich die operativen Risiken eine Rolle. Die Maßnahmen sind in die vier Kategorien „Organisation und Infrastruktur“, „Identity Management“, „Datenschutzkriterien“ und „Interoperabilität“ gegliedert. Nachfolgend ist dargestellt, durch welche Maßnahmenkategorien welchen Risikotypen Rechnung getragen wird:

Maßnahmenkategorie		**Risikotyp**			
		AV	**DP**	**ID**	**SC**
CO	Organisation und Infrastruktur	X	X	X	
IDM	Identity Management			X	
DP	Datenschutzkriterien		X		
IOP	Interoperabilität				X

Tabelle 3 – Zuordnung der Maßnahmenkategorien zu Risikokategorien

Daraus ergibt sich für die Identifikations-Risiken ein flexibles Konzept, das an die Anforderungen des jeweiligen Anwendungsfalls – auch unter den damit verbundenen wirtschaftlichen Gesichtspunkten – angepasst werden kann. Für die Datenschutz-Risiken wurde bewusst ein striktes Konzept gewählt.

In den Diskussionen im Zuge der Ausarbeitung des Risikokonzepts und der Sicherheitsklassen hat sich darüber hinaus ergeben, dass es wohl nicht sinnvoll ist, den Verfügbarkeits-Risiken durch Service Level Agreements, die mit einer Haftung unterlegt sind, zu begegnen, sondern dass ein Best-Effort-Konzept realistischer erscheint. Die Verfügbarkeits-Risiken gehören zwar aus wirtschaftlicher Sicht zu den bedeutendsten, weil in vielen Anwendungsfällen der größte wirtschaftliche Schaden durch den Ausfall des Identitätsmanagements entstünde, der einem Ausfall der davon abhängigen Services gleichkäme; dem steht aber auch ohne Haftung ein wirtschaftlicher Druck der WPV-Teilnehmer entgegen, solche Ausfälle möglichst zu vermeiden.
Die Aufsichts-Risiken und rechtlichen Risiken sind besonders in der Gesamtkonzeption des WPV zu berücksichtigen, bis hin zur Governance in der Federation Authority.

Es empfiehlt sich, alle operativen Risiken in vertraglichen Regelungen zu berücksichtigen, also etwa auch festzuschreiben, dass – wie soeben beschrieben – für Verfügbarkeit nicht gehaftet wird. Auch solche vertraglichen Regelungen, die mit den gesetzlichen Haftungsregeln übereinstimmen, sind sinnvoll, da sie die jeweilige Frage für jeden leicht erkennbar außer Zweifel stellen.
Wer die einzelnen Risiken letztlich zu tragen hat, kann im Rahmen dieses Risikokonzepts nicht abschließend festgelegt werden. Dies ist nicht zuletzt eine Frage mit starken wirtschaftlichen Auswirkungen, die im Diskurs der Stakeholder zu entscheiden ist.