# Wirtschaftsportalverbund Sicherheitsklassen

Version 30.8.2014

Rainer Hörbe

# Inhalt



# *Begriffe*

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

# 1 Einführung

Wenn sich mehrere Organisationen abstimmen um gemeinsame Ziele zu verfolgen, liegen gegenseitig abhängig Regeln, Spezifikationen und Verträge zu Grunde. Diese Vereinbarungen haben rechtliche, geschäftliche und technische Aspekte. Sie werden als Rulebook (WPV), Trust framework (Kantara, FICAM), Common Operating Rules (TSCP), Operating Regulations (Visa) usw. bezeichnet. Das Ziel dieser Art von Kooperationen ist es Prozesse zu vereinfachen, die Erfüllung von Qualitäts- und Sicherheitszielen zur Behandlung von Risiken durchzusetzen und die Vertrauenswürdigkeit der Kooperationsplattform zu fördern. Für elektronischen Identitäten sind das die Ziele für Informationssicherheit und Datenschutz. Um diese Ziele zu erreichen werden die Qualitäts- und Sicherheitsanforderungen normiert. Da es für unterschiedliche Benutzergruppen und Dienste innerhalb einer Kooperationsplattform verschiedene Ziele gibt, kann keine einheitliche Richtlinie für alle Teilnehmer gelten.
Die Anforderungen werden hier in folgende Gruppen unterteilt:

1. Risikoorientierte Anforderungen (z.B. für die Richtigkeit der Benutzeridentifikation wird bis max. 100€ pro Login gehaftet.)
2. Maßnahmenorientierte Anforderungen (z.B. „Die Feststellung der Identität des Betroffenen muss gemäß § 40 Abs 1 Bankwesengesetz erfolgen“)

Dieses Dokument beschreibt den zweiten Punkt, die maßnahmenorientierten Sicherheitsanforderungen. Die Philosophie ist, dass für die Skalierbarkeit und Interoperabilität nur die unbedingt erforderlichen Maßnahmen vereinbart werden, und das restliche Risiko über die Haftung ausgelagert wird.
Damit gegenüber dem Status Quo eine signifikatne Vereinfachung möglich wird, werden die Regeln in Klassen zusammengefasst. Beispiele dafür sind:

- Level of Assurance 1-4 (ISO 29115 „Entity Authentication Assurance Framework“)
- Gewöhnliche, fortgeschrittene und qualifizierte Signatur (Signaturgesetz);
- Sicherheitsklassen 0-3 (Portalverbundvereinbarung der österr. Verwaltung)

Im Folgenden wird im Kontext des WPV Rulebooks der Begriff Sicherheitsklasse verwendet. Sicherheitsklassen basieren auf dem Ansatz, dass in Abhängigkeit von den Sicherheitsanforderungen Risikoklassen und Maßnahmen in Sicherheitsklassen

zusammengefasst werden können, meistens in einer Hierarchie, bei der die Regeln einer höherwertigen Klasse die der darunterliegenden einschließen. Diese ursprünglich aus dem Militärwesen stammende Klassifikation für Dokumente konnte sich jedoch für IT-Systeme nicht einheitlich durchsetzen, da unterschiedliche rechtliche, organisatorische und technische Anforderungen bestehen, erschwert durch unterschiedliche Vokabulare. Die bekannten Frameworks wurden top-down entwickelt und resultierten in monolithischen Regelwerken, die nicht leicht an neue Anforderungen angepasst werden können.

Die Struktur des WPV ist föderal in dem Sinn, dass verschiedene Federations ihre Regeln primär nach den Anforderungen ihres Sektors und Geschäftsmodells bestimmen. Dabei sollen aber die Teilnehmer nicht mit einer Federation ein neues - wenn auch größeres - Identitätssilos bilden, sondern die Vernetzung und Interoperabilität zwischen verschiedenen Federations soll möglich sein und gefördert werden.
Das soll durch die Standardisierung der Bewertungskriterien erreicht werden. Aus ihnen sollen die Sicherheitsklassen modular zusammengestellt werden können, wie im Maschinenbau des 19. Jahrhundert genormte Schrauben und Teile Konstruktion die Produktion revolutioniert hatten. Die Liste der Einstufungskriterien würde etwa 200-300 einzelne Maßnahmen enthalten, aus der die Muss-Kriterien für eine Sicherheitsklasse ausgewählt werden. Im WPV-Rulebook werden Referenzsicherheitsklassen definiert, mit denen übliche Anwendungsbereiche erfasst werden. Die Definition von Sicherheitsklassen für eine konkrete Federation ermöglicht es, von diesen Referenzklassen abzuweichen, allerdings ist schriftlich zu begründen, warum die Vorgabe zu Nachteilen für die Teilnehmer der Federation führen würde.
Eine Zerlegung von Regelwerken in einheitliche Bausteine erzeugt zwar noch keine vollständige Interoperabilität, hat aber folgende Vorteile:

- Unterschiede verschiedener Regelwerke, die auf Grund schwammiger Terminologie, fehlender Ausarbeitung oder Mangel an vorgegebenen Normen entstehen können, werden a priori ausgeräumt.
- Der Normierungsprozess erzeugt ein gemeinsames Interesse, den Bausteinkatalog zu pflegen und die Interessen und Anforderungen dabei abzustimmen.
- Identitäts- und Serviceprovider können wesentlich einfacher ihre Dienste in verschiedenen Federations anbieten, weil die Übersetzungsarbeit entfällt.

# 2 Geltungsbereich der Sicherheitsklassen

Das Rulebook ist die Grundlage für das Vertrauen in die elektronische Kommunikation zwischen den Teilnehmern einer Federation. Die Sicherheitsklassen beziehen sich nur auf den Teilbereich der Zusicherung von Identitäten an den Service Provider. Für andere Risikokategorien (z.B. Datenschutz) haben die Sicherheitsklassen keine Geltung.

Eine Sicherheitsklasse im WPV umfasst folgende Aspekte:

- Sicherung der Kommunikation auf der technischen Ebene
- Erfüllung der Schutzziele Vertraulichkeit, Integrität und Nachvollziehbarkeit
- Regelung der Vertrauensstellung SP → SB (was zum Großteil 1:1 auf den IdP überbunden wird)

- Geschäftsprozesse Identitätsfeststellung- und verwaltung, Authentifizierung, Sicherung einer Online-Session.

# 3 Risikoübermittlung und Sicherheitsklassen

Das Prinzip der automatisierten Aushandlung von Vertrauensstellungen gewährt dem SP, dass der Zugriff von Nutzern nur unter den vorgegebenen Haftungsbedingungen und Maßnahmen der geforderten Sicherheitsklasse erfolgt. Dafür ist es notwendig, dass die Transaktion mit einem Risikowert assoziiert werden, mit dem IdP und SP ihre Erwartungshaltungen abstimmen. Diese Einstufung wird grundsätzlich pro Attribut angeboten, wobei Mappings zur Vereinfachung für den SP erlaubt sind. Wird vom SP die Übermittlung von Haftungsrahmen und Sicherheitsklasse angefordert, dann sind diese voneinander unabhängig und werden parallel übertragen.

# 4 Die Referenzsicherheitsklassen

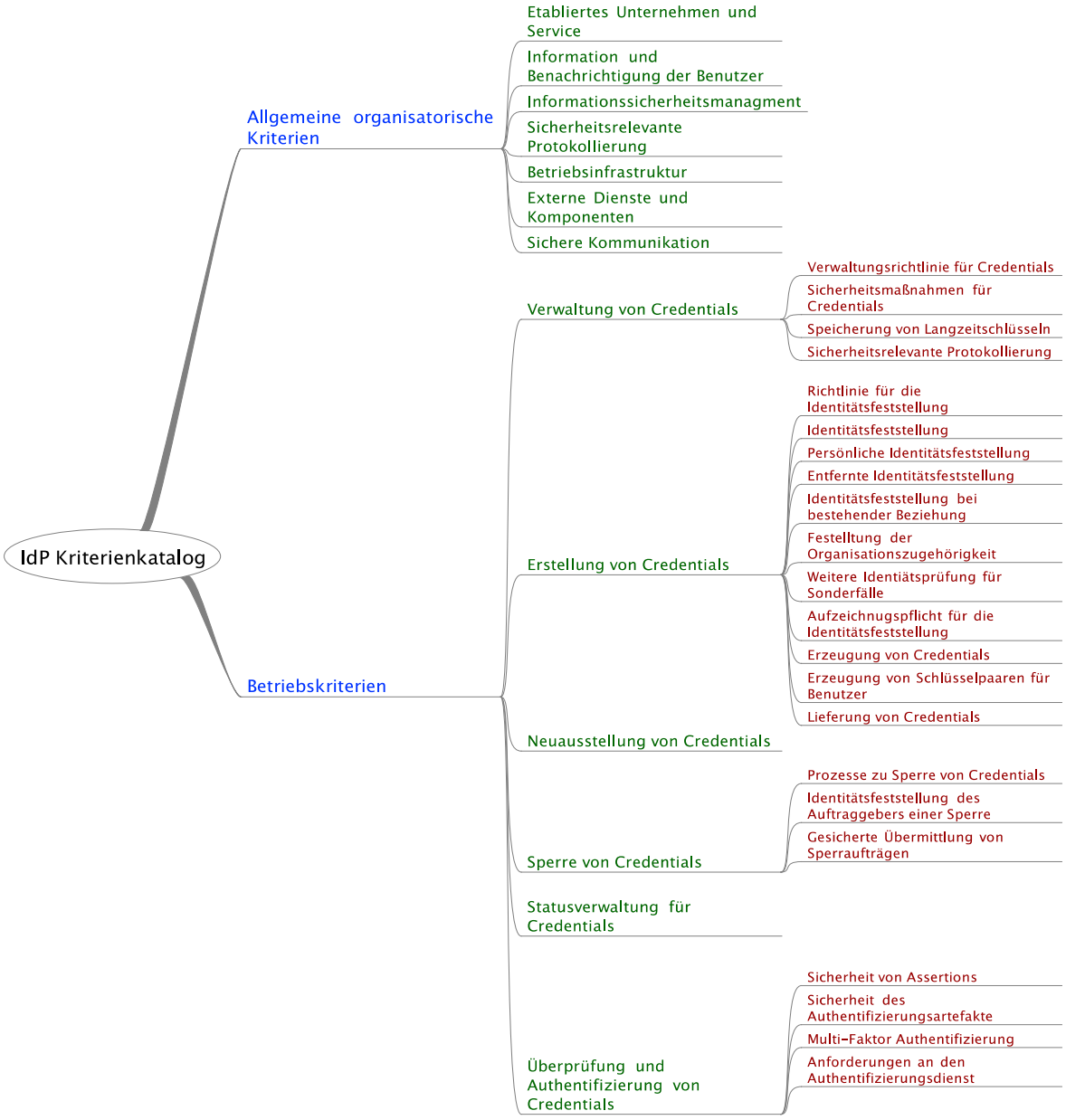
Als Grundeinteilung werden 3 Sicherheitsklassen vorgegeben, die wie grob wie folgt ausgerichtet sind.

| | 1 | 2 | 3 |
|---|---|---|---|
| Identitätsfeststellung | selbstbehauptet | Kontext, einfache Prüfung | Wie bei qualifizierter Signatur |
| Credentialqualität | 1 Faktor mit Authentifizierung | 1-Faktor mit Mindestqualität | 2-Faktor Authentifizierung |
| Providersicherheit | gewöhnlich | gut | Hoch |
| Provider-Revision | minimal | einfach | Strikt |

Jede dieser Sicherheitsklassen ist durch die konkrete Auswahl der Einstufungskriterien festgelegt. Die Kriterien müssen aus dem vom Rulebook definierten Kriterienkatalog ausgewählt werden. Änderungen und Erweiterungen haben den statutengemäßen Abstimmungsprozess im WPV zu durchlaufen.

# 5 Der Kriterienkatalog für IdP

Die Kriterien werden wie folgt klassifiziert.




Die Kriterienkataloge sind im Anhang enthalten.