WPV Feinkonzept: Risikokonzept & Sicherheitsklassen

AUSTRIAN IDENTITY
FEDERATION AUTHORITY

Rainer Hörbe,
Walter Hötzendorfer
18.9.2014

Wirtschaftsportalverbund – Einleitung (1)

Der WPV organisiert die Verwendung von eIDs von Personen und Unternehmen

Was bedeutet “elektronische Identität (eID)”?

- Nachweis: Benutzer *ist wer er vorgibt zu sein*
- Dadurch Zugriff auf Daten und Dienste
- Verschiedene eIDs eines Benutzers pro Kontext

Welche Funktion (en) haben eiD in einer weitgehend digitalen Wirtschaft?

- Kosten: Benutzersupport und –verwaltung; Ausstellung von eIDs
- Kooperation: gemeinsame Infrastruktur (wie Zahlungsverkehr und Internet)

eIDs in praktischen Beispielen: national, europäisch, international

- E-Government (Bürgerkarte, Portalverbund)
- Forschung & Lehre (AAI, CERN)
- Wirtschaft (BEPAC, FI/Versicherung, Pharma, Aerospace)

Wirtschaftsportalverbund – Einleitung (2)

- **Volkswirtschaftliche Bedeutung der eID**
  - bedeutende Infrastruktur für die digitalisierte Wirtschaft
  - wichtiger Standortfaktor für unsere Unternehmen

- **Herausforderungen/Fragen dazu**
  - wer ist mein „Gegenüber“ in einer elektronischen Transaktion (Identität)?
  - was darf er/sie (Rolle)?
  - wie sicher ist die Übermittlung (identitätsbezogener Daten, inhaltliche Daten)?
  - wie kann Betrug/Identitätsdiebstahl bestmöglich verhindert werden?
  - was tun im Betrugsfall? wie kann der Schaden begrenzt werden? wer haftet?

- **Identitäten gemeinsam und sicher verwalten > Federation**
  - mehrere Akteure betreiben federiertes Identitätsmanagement (Federation)
  - mehrere/viele Federationen arbeiten effizient und sicher zusammen (“Wirtschaftsportalverbund”)
  - es gibt definierte, für alle gültigen Regeln (Rulebook)

Wirtschaftsportalverbund – Einleitung (3)

Standards für Identitätsmanagement

- wichtig für die österreichische Wirtschaft
- Engagement der Wirtschaftskammer Österreich
- gleiche Regeln für alle, Kommunikation an alle Branchen

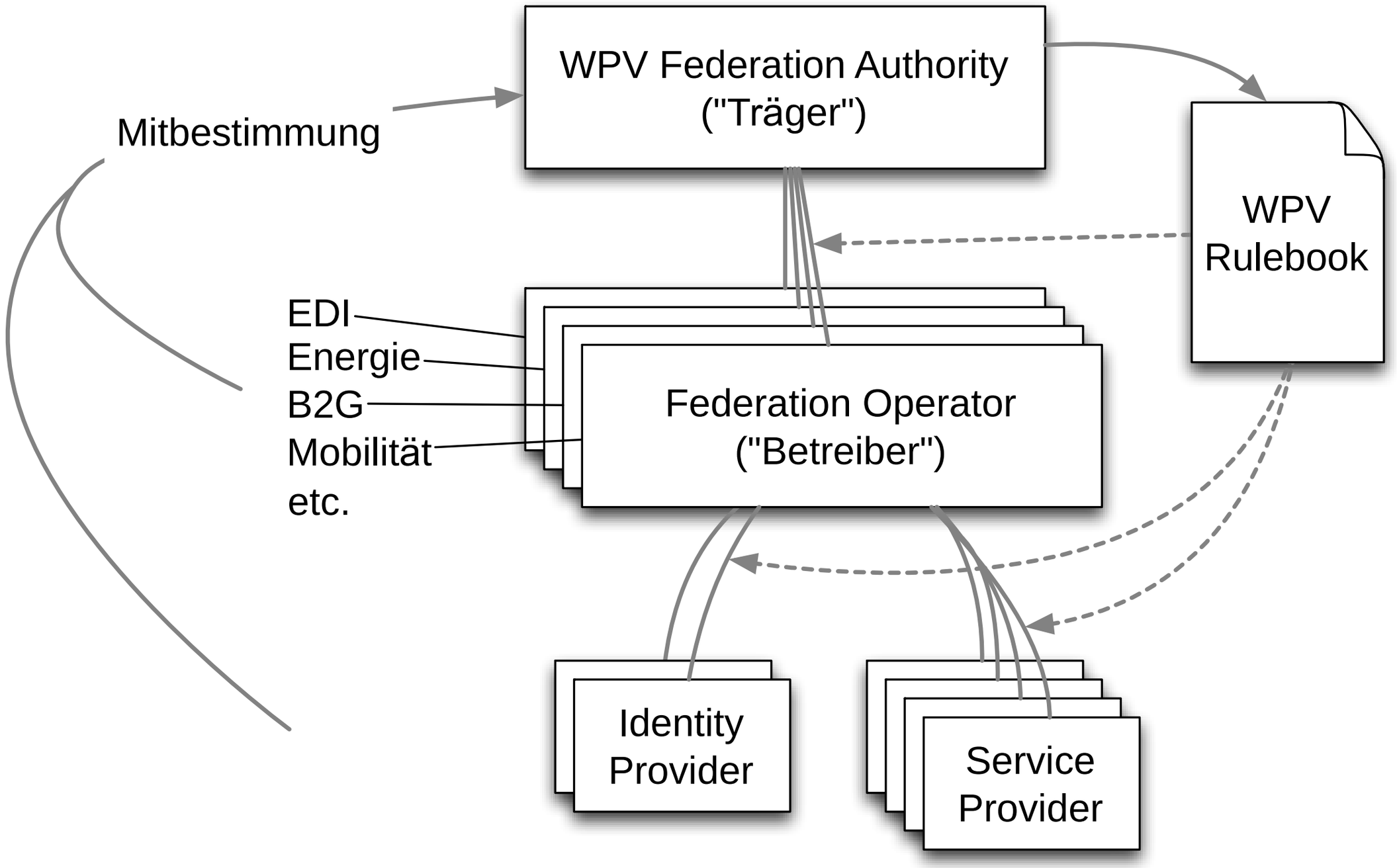
Engagement der AUSTRIAPRO als Standardisierungsplattform der WKÖ

- Standardisierung, Demonstratoren, Umsetzungen

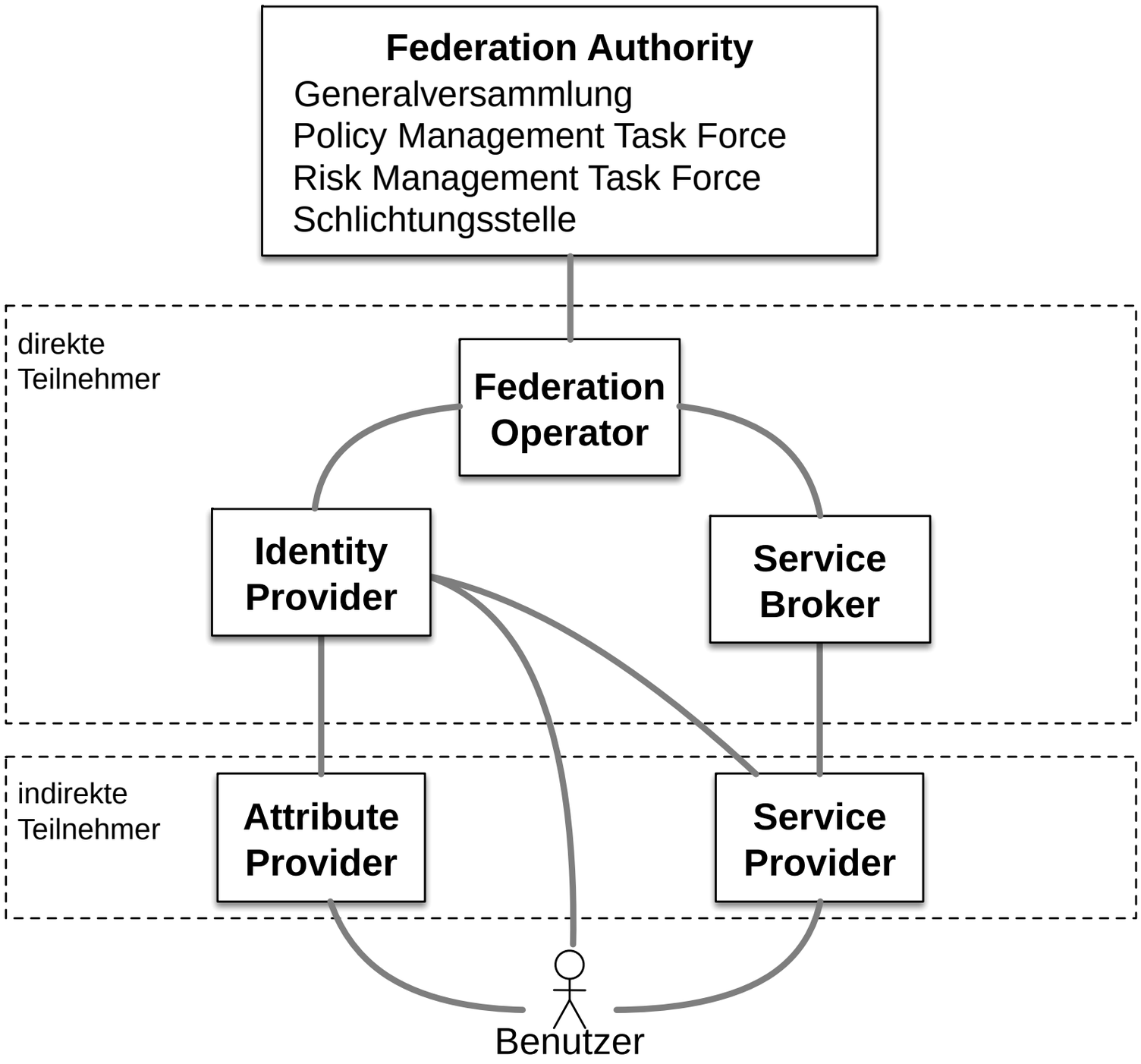
das Pilotprojekt Wirtschaftsportalverbund WPV von WKÖ und AUSTRIAPRO

- Geschichte, Intention, Status Quo
- geplante Umsetzung, Zeithorizont
- wie kann ich mitwirken? (Arbeitskreis, Verein)

WPV-Struktur - Übersicht



WPV-Akteure


Federation Authority
Generalversammlung
Policy Management Task Force
Risk Management Task Force
Schlichtungsstelle
direkte Teilnehmer
Federation Operator
Identity Provider
Service Broker
indirekte Teilnehmer
Attribute Provider
Service Provider
Benutzer

Das Grobkonzept umfasst:

- Architekturmodell
  - Anforderungen
  - Domain Model
  - Use Cases
- Governance-Anforderungen für FA
  - Basierend darauf wurden Vereinsstatuten erstellt und die Federation Authority Ende 2013 als Verein gegründet.
- Entwurf Rulebook, dieses regelt:
  - Begriffs- und Rollendefinitionen (Glossar)
  - Regeln zu Teilnahme und Akkreditierung
  - Rechte und Pflichten der Teilnehmer
  - etc.
- Wirtschaftliches Konzept

Neu hinzu kam jetzt:

- Die Risiken im WPV wurden identifiziert, beschrieben und typisiert, als Grundlage für
  - die Basisrichtlinie mit Maßnahmenkatalog und
  - die weitere (vertragliche) Gestaltung des WPV.
- Rechtliche Grundlagen zur Haftung und Haftungsbeschränkungen wurden ausgearbeitet.
- Einer Basisrichtlinie mit einem Katalog von Maßnahmen wurde erstellt.
  - Federations können die Richtlinie um weitere Maßnahmen erweitern.
  - Richtlinie ist Basis für Audit und Zertifizierung.

Anforderungen

- Sicherheitsanforderungen verschiedener Geschäftsfälle unter einen Hut bringen
- Flexibilität einzelner Federations gegen Interoperabilität des Gesamtsystems abwägen
- Aufwand für Audit optimieren

WPV Risikokonzept

- Betrachtung aus der Perspektive der WPV-„Kunden“: Nutzer und Service Provider
- Klassischer Ansatz der Quantifizierung
  Risiko = Eintrittswahrscheinlichkeit * Schadenshöhe
  ist in einer Federation schwer zu schätzen und auch kontextbezogen.
- Risikotransfer wird der Risikominderung vorgezogen: lieber Haftung in € als Controls
- Controls müssen jedenfalls eingehalten werden wenn sie (gesetzlich) vorgeschrieben sind

Risiken: Beispiele

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 Angabe 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.		

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.		

WPV Risikokategorien

		Risikotyp	Nutzer	SP	LoA	SLA
operativ	AV	Verfügbarkeit	X	X		X
	DP	Datenschutz	X			
	ID	Identifikation		X	1-3	
n/o	*	Skalierbarkeit, Aufbau, Teilnahme, Schadensregulierung				

WPV Maßnahmenkategorien

Maßnahmen werden für operative Risiken definiert

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

AV=Verfügbarkeit, DP=Datenschutz,
ID=Identifikation, SC=Skalierbarkeit

WPV Maßnahmenkatalog

- Insgesamt ca. 200 Controls
- Struktur großteils nach Kantara IAF (→Zertifizierung)
- Controls sind im Rulebook Empfehlungen, ausgenommen die „Minimalen Maßnahmen“
- Neue und geänderte Controls in Federations sind zu begründen und erfordern eine Aufnahme ins Rulebook

WPV Minimale Maßnahmen

	Maßnahme	FO	IDP	SB	SP
CO	IT-Haftpflicht		X		X
DP	Datenschutz		X	X	X
ID	Identifikation LoA 3		qual. Sig.		
IOP	Interoperabilität		X	X	X