TeleTrusT
Pioneers in IT security.

Ergebnisse der TeleTrusT-AG "SOA"

SOA Security in der Praxis – Entwurfsmuster für eine sichere Umsetzung

TeleTrusT-AG "SOA"

TeleTrusT
Pioneers in IT security.

Arbeitsergebnisse des SOA Security AKs

- Anfang 2009 - Themenfindung für das Dokument
- Mitte 2009 Vorgehenskonzept erarbeitet
- Mitte 2009 – Mitte 2010 – Dokument erstellen
- Juni 2010 Fertigstellung des Dokumentes

TeleTrusT
Pioneers in IT security.

Motivation

- Hohe Komplexität von SOA Security – durch viele …
  - Ansätze
  - Technologien
  - Standards
- Ziel des Dokumentes
  - Empfehlung für die Nutzung von SOA Security
  - Vorgabe von Sicherheitsanforderung
  - Bewertung verfügbarer Sicherheitsmechanismen

Das Ergebnis….

- ***SOA Security in der Praxis – Entwurfsmuster für eine Umsetzung***
  - Einleitung
  - Beschreibung der Vorgehensweise Model
  - Architekturen für Service-orientierte Architekturen
  - Anwendungsfälle für Service-orientierte Architekturen
  - Entwurfsmuster
    - Authentizität, Integrität, Vertraulichkeit, Nichtabstritbarkeit, Autorisierung, …)
  - Beispiele Vorgehensweise
  - ***….***

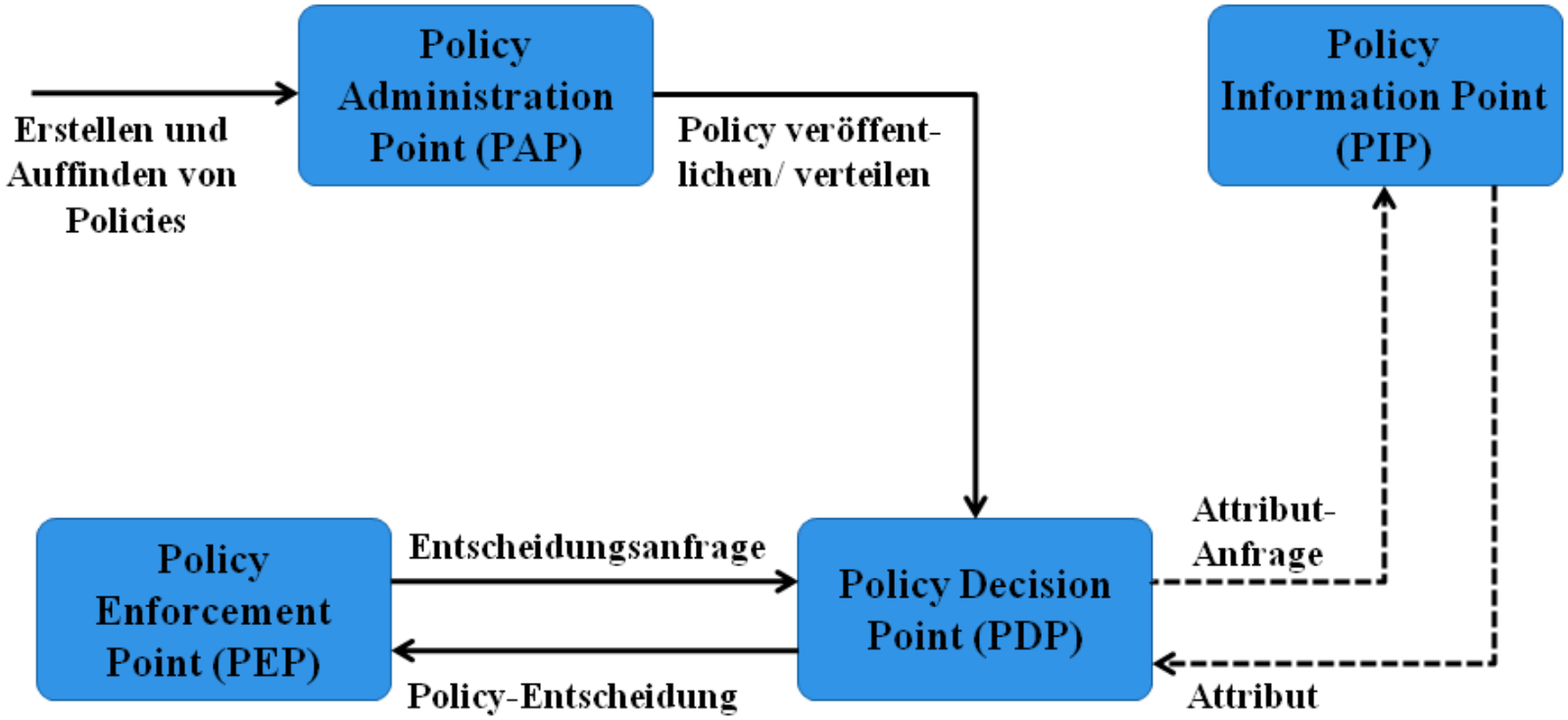
TeleTrusT
Pioneers in IT security.

Sicherheitsanforderungen

- Authentisierung
- Autorisierung
- Integrität
- Vertraqulichkeit und Datenschutz
- Nichtabstreitbarkeit
- Weitere Sicherheitsanforderungen

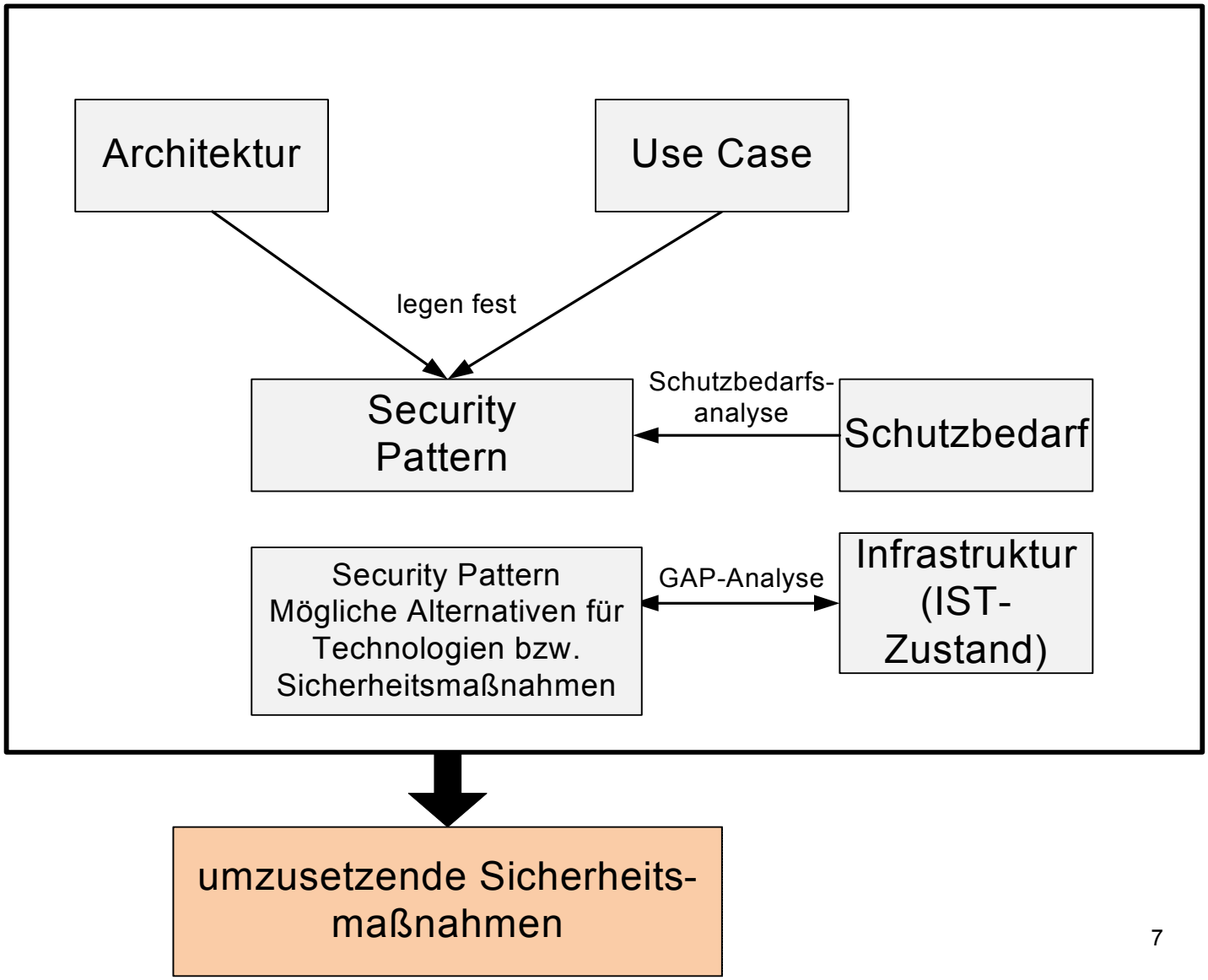
TeleTrusT
Pioneers in IT security.

Umsetzung von Sicherheitsanforderungen

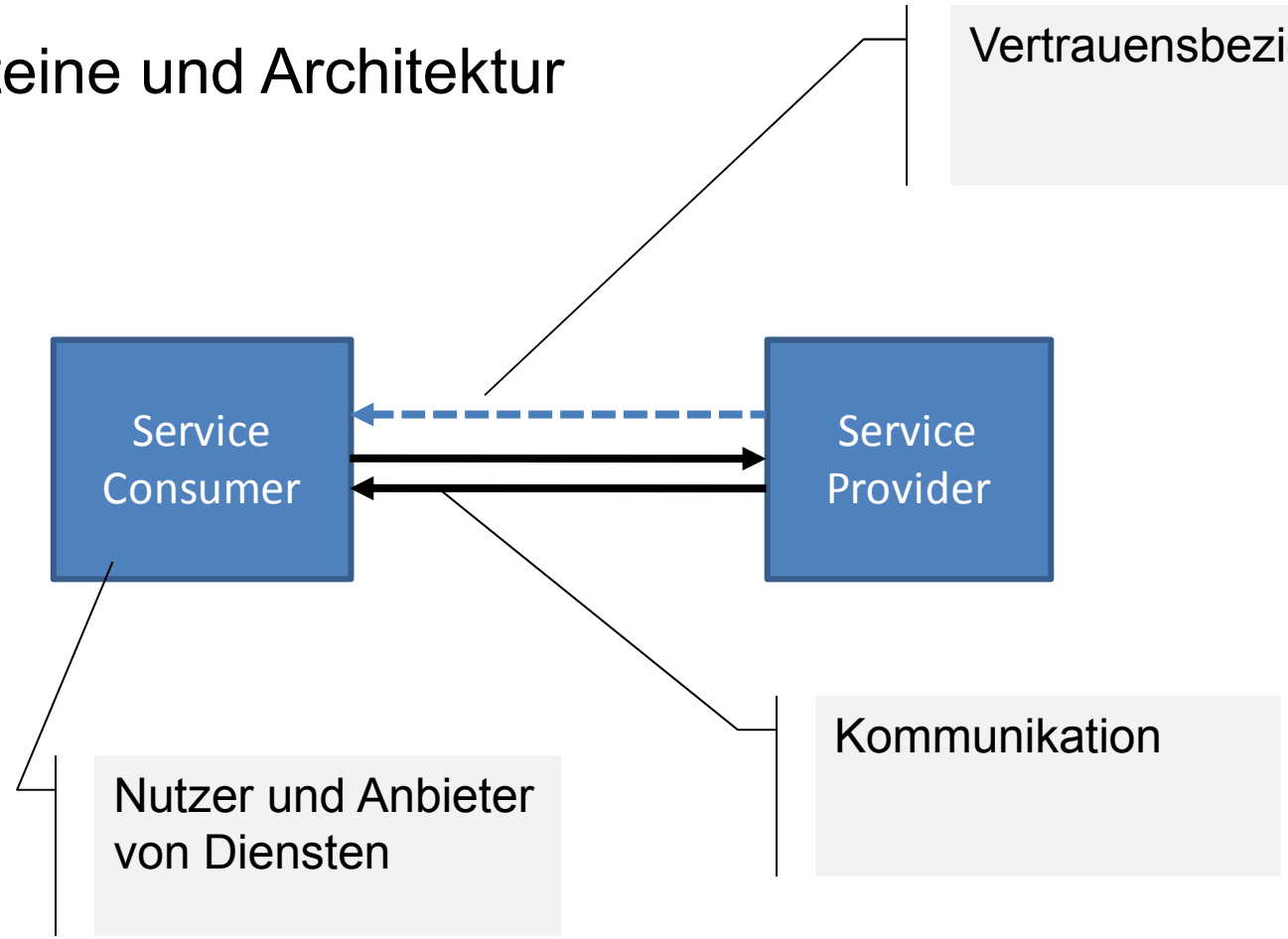


TeleTrusT
Pioneers in IT security.

Vorgehensmodell



Beispiel für Architekturbausteine und Architektur

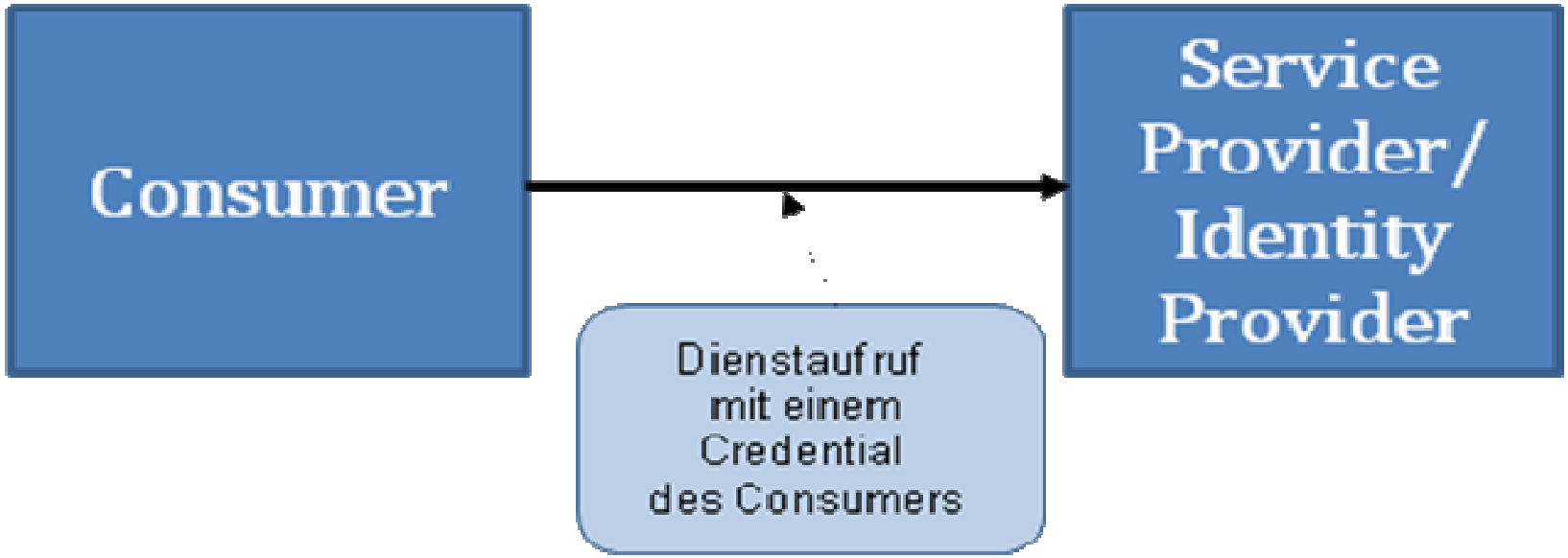


Anwendungsfälle hinsichtlich der Authentifizierung

TeleTrusT
Pioneers in IT security.

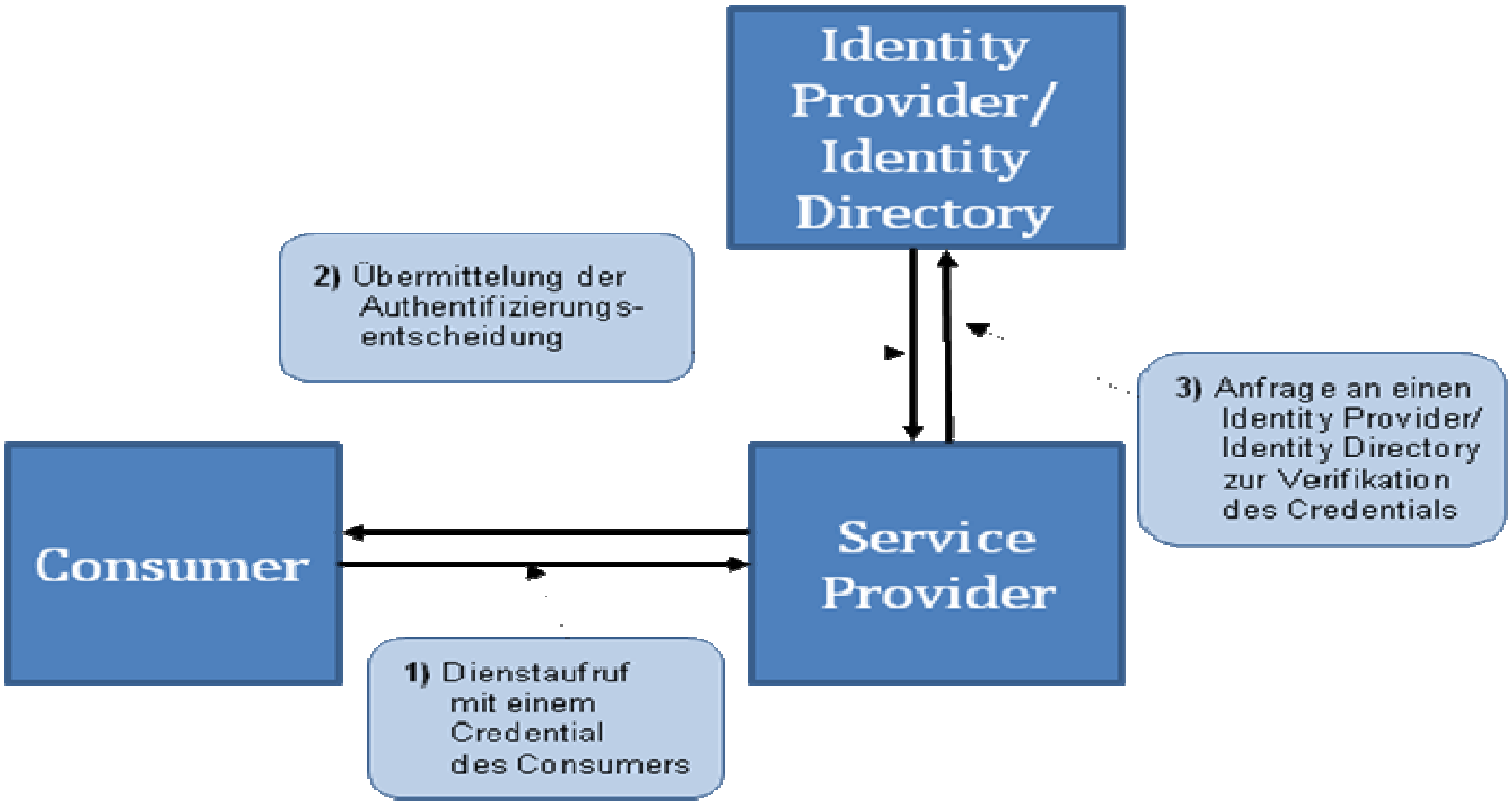
Authentication - Wie sind die Benutzer einem Dienst bekannt? / Wer soll einen Dienst benutzen dürfen?	
Registrieren eines Consumer bei einem Provider (Beispiele: Bürger/Unternehmen registriert sich bei einer Behörde)	**Auth_U1**
Anmelden eines Consumers bei einem Provider (Authentifizierung bei einem Web Service)	**Auth_U2**
Anmelden eines Consumers bei einer Domain (man möchte verschiedene Dienste in der gleichen Domain mit einer Anmeldung benutzen)	**Auth_U3**
Anmelden eines Consumers bei einem Provider mit SSO bei anderen Providern	**Auth_U4**

Muster: Direkte Authentifizierung



Der Service Consumer verwendet ein Credential mit einer Aussage über sich selbst (z.B. ich bin Benutzer X) und einer Authentifizierungsinformation. Der Service Provider überprüft verifiziert das Credential selbst, um den Benutzer zu authentisieren

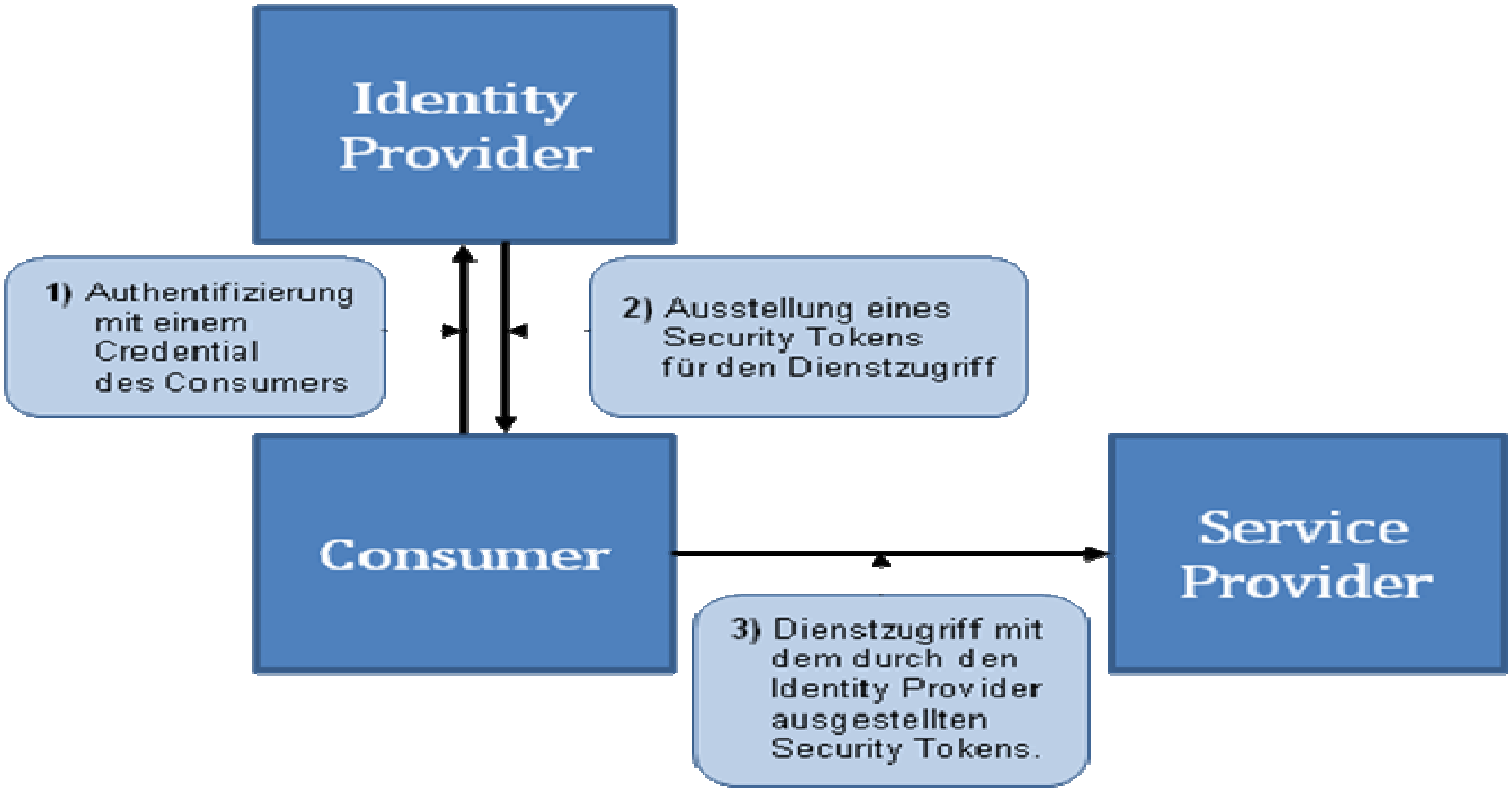
Muster: Delegierte Provider-zentrische Authentifizierung



Service Consumer verwendet ein Credential mit einer Aussage über sich selbst (z.B. ich bin Benutzer X) und einer Authentifizierungsinformation. Der Service Provider kontaktiert einen Identity Provider/ Identity Directory, um das Credential verifizieren zu lassen.

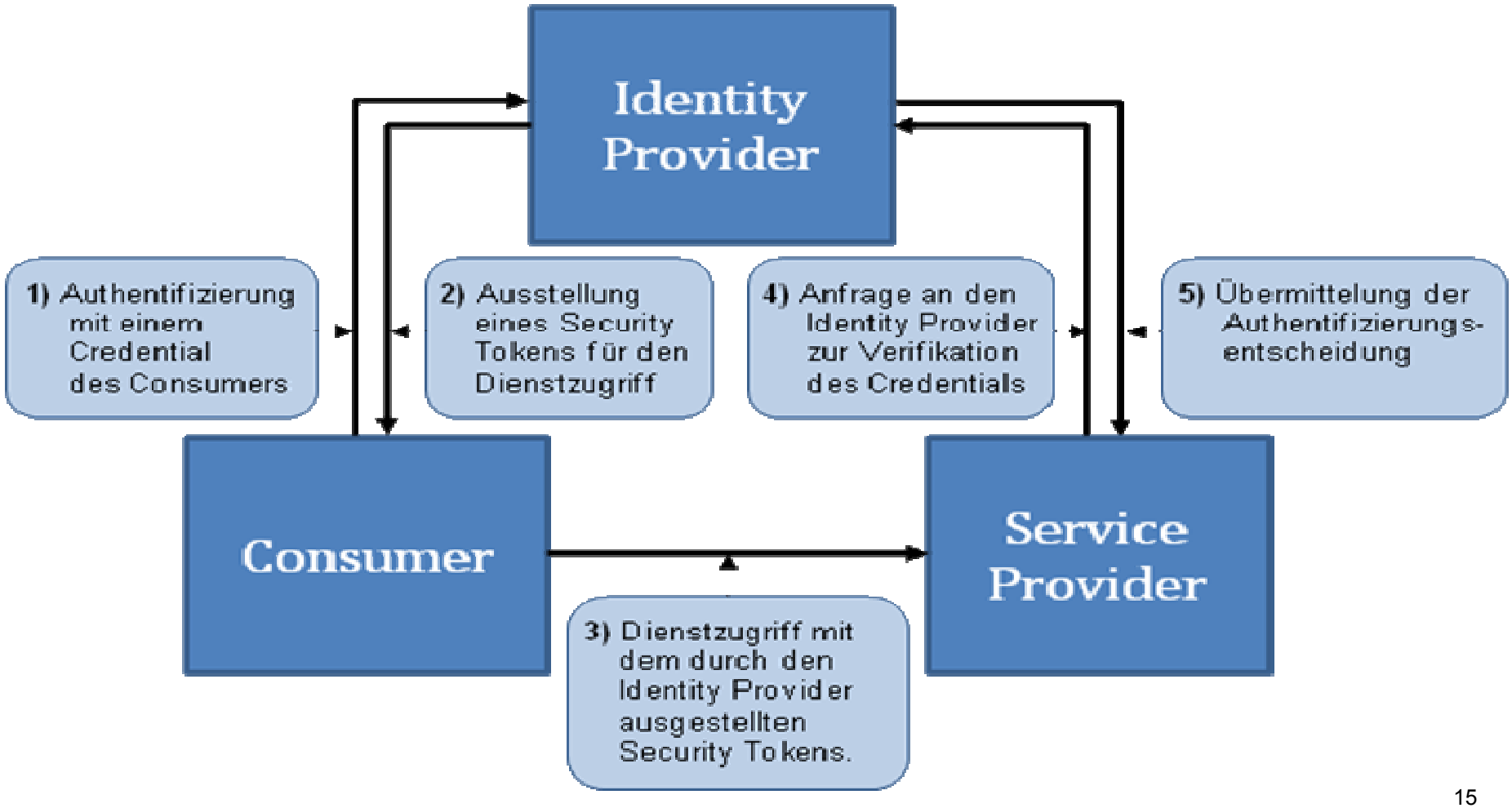
Beispielszenarien	Authentifizierung eines Nutzers mittels eines unternehmensinternen LDAP.
Beispiele für Technologien	
Aspekt	**Mögliche Technologien/ Standards**
Authentifizierung des Benutzers:	Benutzername/Passwort,…
Umsetzung des Identity Providers/Identity Directory	LDAP, WS-Trust,…

Muster: Delegierte Consumer-zentrische Authentifizierung



Beispielszenarien	• Zentrale Benutzerverwaltung im Unternehmen, • Bereitstellung zentraler Daten, wie unternehmensweites Adressbuch, etc. • Unternehmensweites SSO für Unternehmensanwendungen • SSO für offene Umgebungen wie das Internet mit mehreren potenziellen Identitätsprovidern (Beispiel InformationCard)
Beipiele für Technologien	
Aspekt	**Mögliche Technologien/ Standards**
Authentifizierung des Benutzers:	Benutzername/Passwort,…
Bereitstellung der Authentifizierungsentscheidung:	SAML, Kerberos, …
Abrufen der Authentifizierungstokens:	WS-Trust, SAML, Kerberos

Muster: Delegierte Consumer-zentrische Authentifizierung mit Rückkopplung



Beispielszenarien	Zentrale Benutzerverwaltung im Unternehmen (Beispiel RSA Token) als auch offene Umgebungen wie das Internet mit mehreren potenziellen Identitätsprovidern (Beispiel OpenID)
Beispiele für die Technologien	
Aspekt	**Mögliche Technologien/ Standards**
Authentifizierung des Benutzers:	Benutzername/Passwort,…
Bereitstellung der Authentifizierungsentscheidung:	OpenID, RSAToken, …
Abrufen der Authentifizierungstokens:	OpenId, RSAToken, ..

Auswahl der Technologien und Methoden

Für den Aspekt Authentifizierung des Nutzers gelten die in folgender Tabelle möglichen Technologien und Methoden:

Schutzbedarf	Technologien und Methoden	Erläuterungen
normal	Username- Password, PIN Challenge-Response-Verfahren (z.B. Captcha) Location-based (IP-Range, Geographie) SAML-Token (mit Aussagen über den Nutzer)	
hoch	2-Faktor-Authentisierung	Challenge-Response-Verfahren (RSA Token …) Zertifikatsbasierte Authentifizierung (softwarebasiert)
Sehr hoch	2-Faktor-Authentisierung nach gesetzlichen Anforderungen	Zertifikatsbasierte Authentifizierung (Hardware (SmartCard)) neuer Personalausweis: eID Karte Smartcard der Behörde

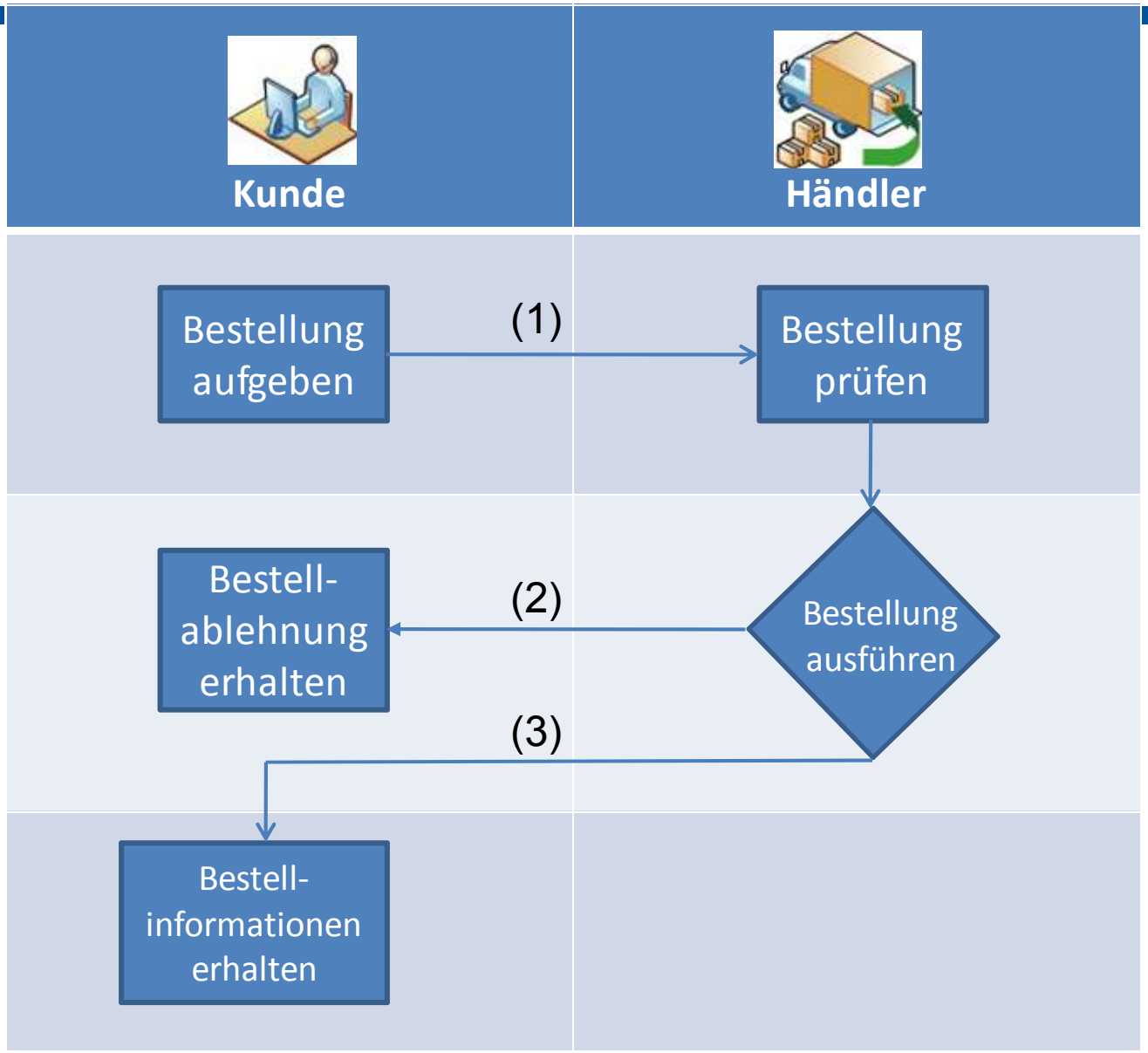
TeleTrusT
Pioneers in IT security.

Beispiel zur Vorgehensweise

1. Identifizierung der zutreffenden Architektur
2. Identifizierung der zugehörigen Anwendungsfälle
3. Auswahl der Entwurfsmusters gemäß den Ergebnissen aus den Arbeitsschritten 1 und 2
4. Bestimmung des Schutzbedarfs der verarbeiteten Daten und Informationen
5. Auswahl der möglichen Technologien und Methoden, um für die identifizierten Architekturen und Anwendungsfälle den geforderten Schutzbedarf für die verschiedenen Schutzziele zu erfüllen.
6. Auswahl der umzusetzenden Technologien und Methoden (Sicherheitsmaßnahmen) auf der Grundlage von bereits existierender Infrastruktur, die genutzt werden kann

TeleTrusT
Pioneers in IT security.

Bestellvorgang, aus SOA-Security-Kompendium



Kommunikation	Archi-tektur	Anwen-dungs-fall	Schutz-bedarf	Entwurfs-muster
Nr.1: Bestellung aufgeben; Nr.2: Bestellablehnung erhalten	A4, A5	DS_U1	Nr.1: hoch, Nr.2: normal	Integrität: P1 Vertraulichkeit: P1
Nr.1: Bestellung aufgeben; Nr.3: Bestellinformationen erhalten	A4, A5		Nr.1: hoch, Nr.2: normal	Integrität: P1 Vertraulichkeit: P1

Ergebnis

- Dokument mit ca 65 Seiten
- Teletrust Druck
- PDF Download über Webseite

- Offen – Übersetzung für Schwesterverbände ?

TeleTrusT
Pioneers in IT security.

Mitwirkende Editoren

- I. Thomas, M. Menzel — HPI
- T. Störtkuhl — Secaron
- E. Saar — T-Systems
- B. Quint — CORISECIO

- Alle Mitglieder der Arbeitsgruppe SOA Security