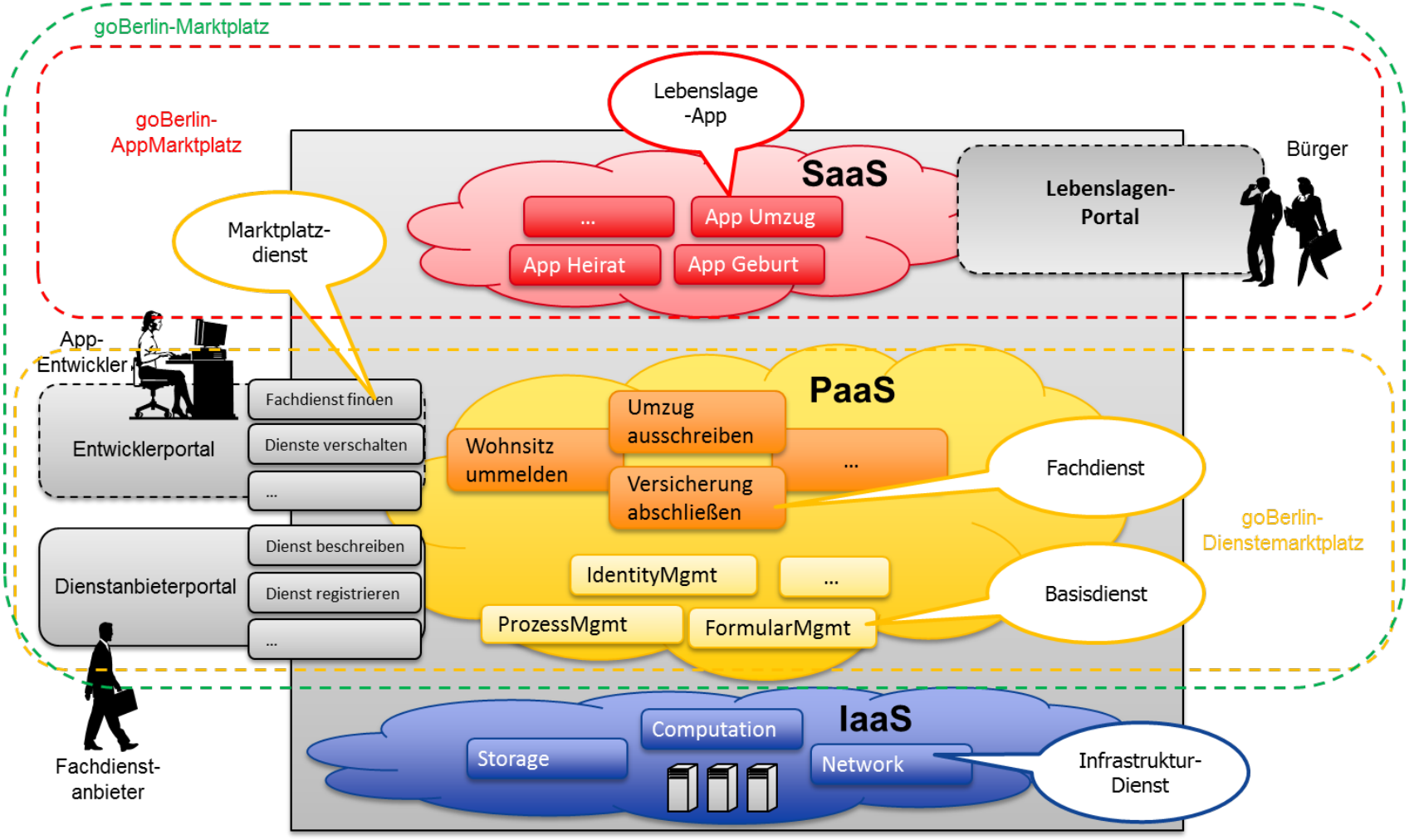
Vertrauenswürdige Identitäten für die Cloud

Anforderungen und Lösungsansätze für das Identitätsmanagement in private Clouds am Beispiel des goBerlin-Projektes

Florian Thiemer

9. September 2013

goBerlin


goBerlin-Marktplatz
goBerlin-
AppMarktplatz
Lebenslage
-App
SaaS
...
App Umzug
App Heirat
App Geburt
Lebenslagen-
Portal
Bürger
Marktplatz-
dienst
App-
Entwickler
Entwicklerportal
Fachdienst finden
Dienste verschalten
...
PaaS
Umzug
ausschreiben
Wohnsitz
ummelden
...
Versicherung
abschließen
Fachdienst
goBerlin-
Dienstemarktplatz
Dienstanbieterportal
Dienst beschreiben
Dienst registrieren
...
IdentityMgmt
...
Basisdienst
ProzessMgmt
FormularMgmt
IaaS
Computation
Storage
Network
Infrastruktur-
Dienst
Fachdienst-
anbieter

goBerlin - Das Projekt - Akteur: Bürger

Über den goBerlin Marktplatz sollen Bürger an Lebenslagen ausgerichtete Anwendungen (Apps) finden, die sowohl die notwendigen Verwaltungsprozesse der Ämter als auch darüber hinausgehende Angebote von privatwirtschaftlichen Anbietern enthalten.

goBerlin - Das Projekt - Akteur: Fachdienstanbieter

Fachdienste in Form von Verwaltungsdiensten und privatwirtschaftlichen Diensten sollen durch Fachdienstanbieter auf dem Marktplatz eingestellt werden können und damit das Spektrum an Dienstleistungen erweitern.

goBerlin - Das Projekt - Akteur: App-Anbieter

Darüber hinaus sollen Unternehmen angesprochen werden, die auf Grundlage der auf dem Marktplatz zur Verfügung stehenden privatwirtschaftlichen und verwaltungsorientierten Dienste neue Apps schaffen die auf bestimmte Lebenslagen zugeschnitten sind.

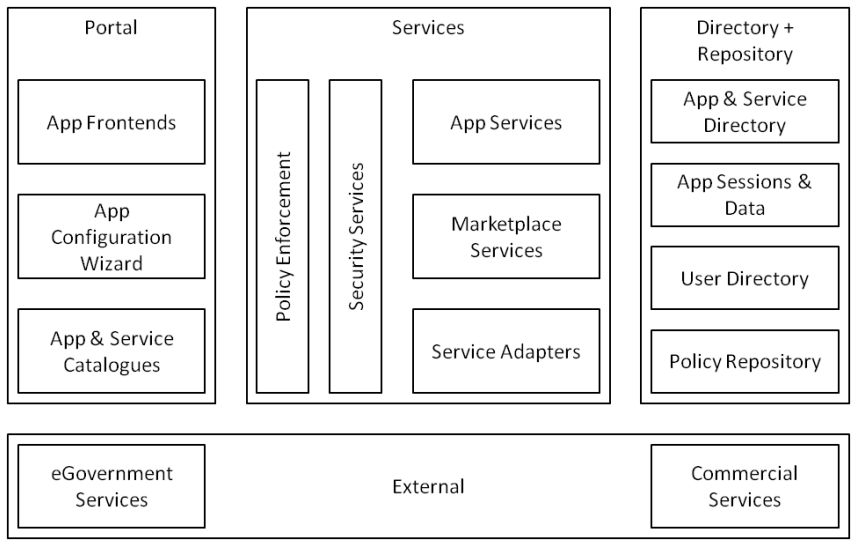
goBerlin - Die zentrale Herausforderung

Wie stellt man sicher, dass eine App auch nur das tut, was ihr erlaubt wird?

- Programmierfehler des App-Entwicklers
- Unerlaubte Nutzung von Marktplatzdiensten (z.B. Auslesen von Profil-Attributen)
- Unerlaubtes Weiterleiten von persönliche Daten
- Bösartiger Code, um den Nutzer, Fachdienstanbieter oder Marktplatz anzugreifen (XSS, DoS, Softwarelücken, ...)

goBerlin - Die Architektur

- Trennung der Anwendungs- und Sicherheitsarchitektur.
- SoA Ansatz kapselt Marktplatzfunktionen über Marktplatzdienste.
- Sicherheitsarchitektur besteht aus Diensten zum
  - Authentifizieren über einen Identity Provider (IdP)
  - Access Control über einen Policy Enforcement Point (PEP)



goBerlin - Identity Management

Das IdM muss folgende Entitäten authentifizieren können:

- Nutzer des Marktplatzes
- Komponenten des Marktplatzes (z.B. Portal, Marktplatzdienste, ...)
- Apps und Fachdienste

goBerlin - IdM

Durch eine PKI wird die Authentifizierung von Komponenten zu Komponenten umgesetzt.

- statische Struktur der Marktplatzkommunikation kann dadurch direkt abgebildet werden.
- Truststores definieren welche Komponenten untereinander kommunizieren dürfen.
  - Grundlegende Kommunikationsmuster aus der Anforderungsanalyse können so implizit erlaubt werden.
  - Kommunikationsbeziehungen die nicht vorgesehen sind werden von vornherein ausgeschlossen.
- Kommunikation zwischen den zu trennenden Zonen der Entwicklungs-, Test- und Produktivumgebung wird direkt unterbunden.

Verschlüsselt und signiert wird über SOAP und XML-ENC nachrichtenbasiert. Per WS-Policy werden diese Sicherheitsrichtlinien an jede WSDL der Marktplatzkomponenten angegeben.

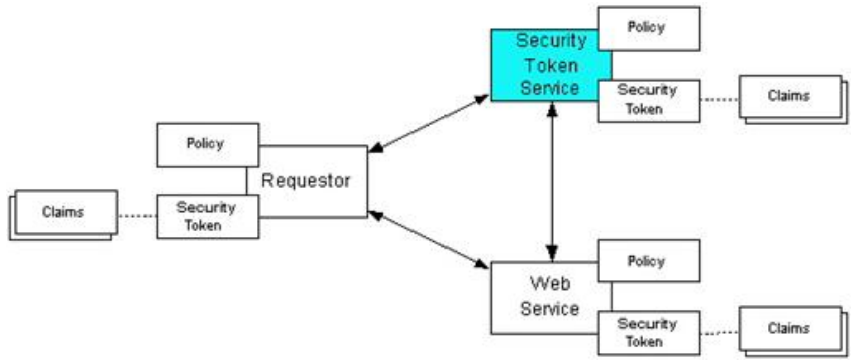
goBerlin - IdM - der Identity Provider

Authentifikation von Nutzern unterliegt ganz anderen Anforderungen.

- Mehrere Anmeldemöglichkeiten (Passwort, nPA, Zertifikat)
- Nutzer stehen im vornhinein nicht fest.
- Auswahl von Nutzer-Attributen.

Lösung durch Identity Provider:

- Zentralisiertes IdM zur Nutzerauthentifikation
- Anwendung des WS-Trust Patterns
- IdP stellt Identitätsnachweise in Form



goBerlin - IdM - Authentifikation einer App

Das Starten einer App wird immer durch einen Nutzer angestoßen. Daraufhin wird diese App-Instanz innerhalb eines Nutzerkontextes ausgeführt. Dieser Nutzerkontext muss transportiert werden können, um folgende Marktplatzfunktionalitäten umsetzen zu können:

- Eine App darf berechtigt sein Teile - oder sogar das vollständige Profil - dieses Nutzers auszulesen.
- Die App darf dann bestimmte Fachdienste aufrufen, wenn der Nutzer dies erlaubt hat.

Eine App-Instanz wird gemäß dem Cloud-Paradigma aus einem App-Template zur Laufzeit initialisiert.

goBerlin - IdM - Authentifikation einer App

Zwei Möglichkeiten mit unterschiedlichen Stärken und Schwächen:

- Zertifikatsbasiert
  - Nutzung des X.509 Zertifikats + Private Key aus dem App-Template.
  - Identity Assertion des Nutzers wird bei jeder Interaktion mit der App versendet.
  - Vorteil:
    - Homogene Nutzung der WS-Policies.

    Nachteile:
    - Identity Assertion ist ein Bearer Token.
- Token basiert
  - App wird über eine SAML-Assertion authentifiziert. Ausstellung der Assertion wird beim Starten der App angestoßen.
  - App-ID und Nutzer-ID in der SAML-Assertion kodiert.
  - Vorteile:
    - Nachweisbarkeit der Ownership der SAML-Assertion.
  - Nachteile:
    - Liste der Aufrufbaren Diensten muss bekannt sein.
    - Zusätzlicher Implementierungsoverhead.

goBerlin - Access Control

Die Zugriffskontrolle wird über Policy Enforcement Points (PEP) angestoßen. Dazu wird an jeder abzusichernden Komponente per Interceptor Pattern ein PEP eingebunden.
Die Zugriffsregeln werden als XACML Policies definiert.

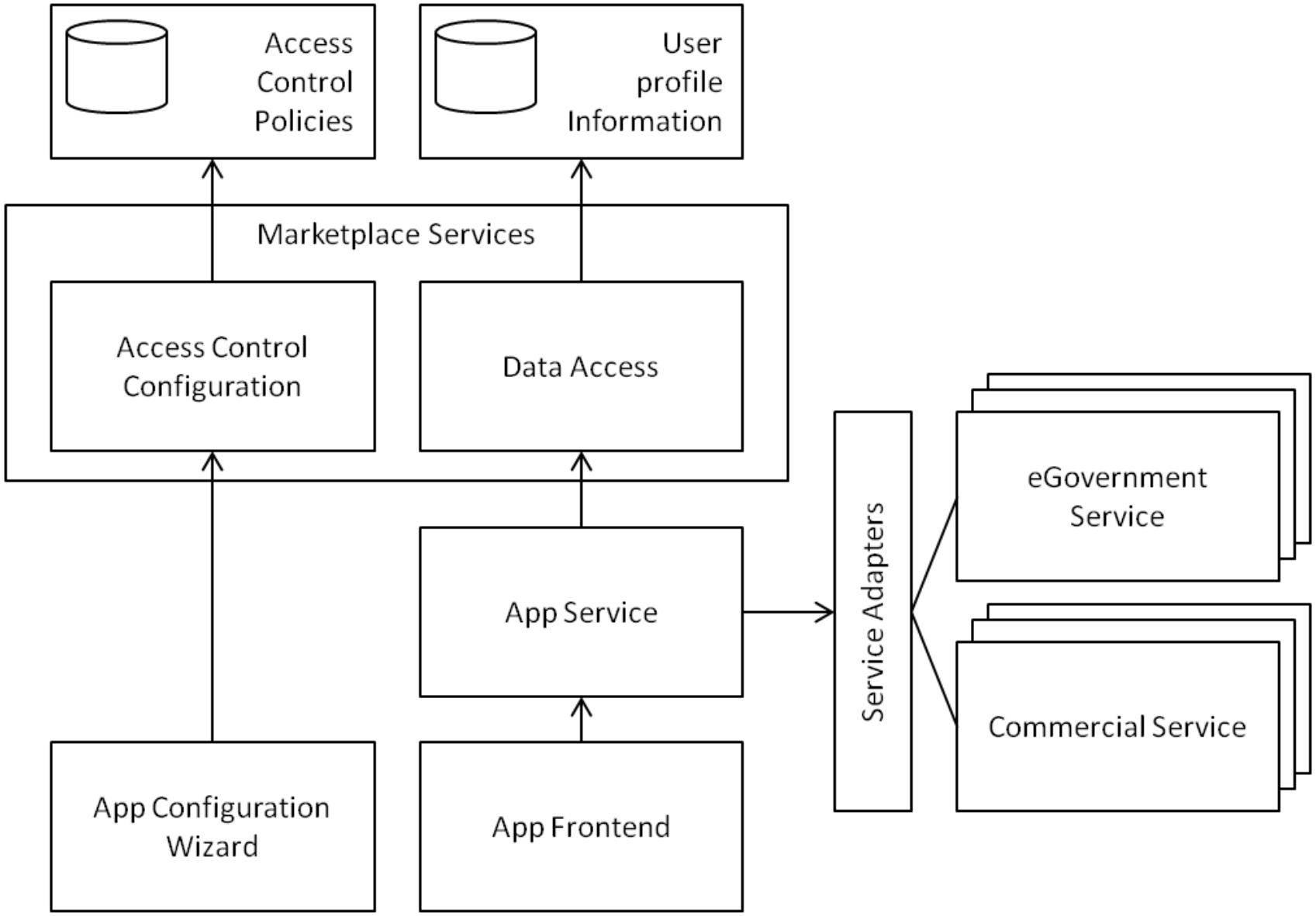
- Ein Nutzer darf nur sein eigenes Profil einsehen und editieren.
- Apps dürfen nur vom Nutzer erlaubte Fachdienste aufrufen und Profilattribute auslesen.

Die Zugriffsberechtigungen werden als Attribute einer Entität abgebildet.

- ID eines Nutzers um Zugriffe auf ein Profil zu regeln.
- Liste von erlaubten Fachdiensten auf die eine App-Instanz zugreifen kann.

Zugriffsregeln und Attribute werden durch die PAP und PIP Komponenten des AC-Systems abrufbar gemacht.

goBerlin - Zusammenführung



goBerlin - Dienstassistent

Über den Dienstassistent konfiguriert ein Nutzer die Sicherheitseinstellungen einer App sowie dessen Konfiguration.

- Abrufberechtigung für Teile des Nutzer-Profils.
- Aufrufberechtigungen von Fachdiensten.
- Synchronisation von App-Konfiguration und Zugriffsberechtigung.

Enforcement und Erstellung von Zugriffsberechtigung ist nicht Aufgabe der App sonden wird durch den Dienstassistenten und den PEP's durch den Marktplatzbetreiber forciert und somit entkoppelt von der App.

Vielen Dank