Sicher FHIR: OAuth2 und OpenID Connect

Ingo Wolf, IT-Architekt, Innovation
gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH | Friedrichstraße 136 | 10117 Berlin

Motivation

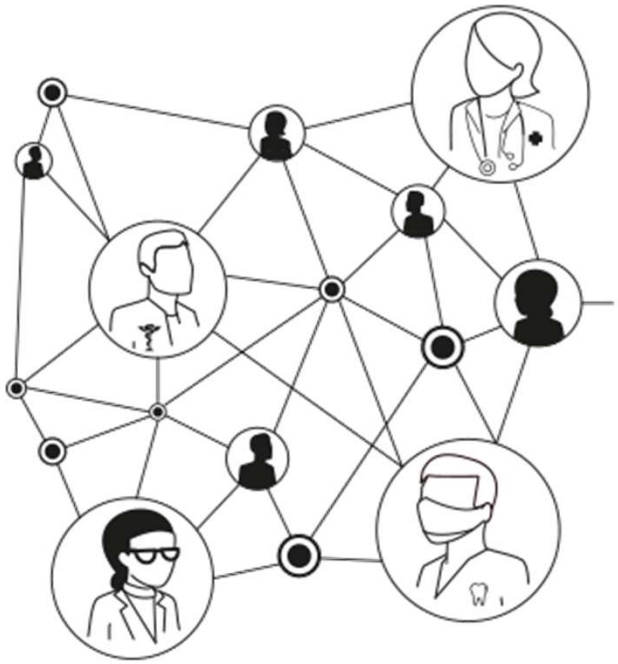
Ziele aus dem E-Health-Gesetz:

- „Öffnung der TI für weitere Anwendungen im Gesundheitswesen“
- „mobile Szenarien“

Die Abteilung Innovation der gematik beschäftigt sich mit Technologien, die zukünftig in der Telematikinfrastruktur relevant werden können.

Idee → Unterstützung weiterer Anwendungen im Gesundheitswesen durch nachnutzbare Sicherheitsdienste zum Identitäts- und Berechtigungsmanagement der (Karten-)Nutzer für mobile Szenarien

Identitäts- und Berechtigungsmanagement



Zielsetzung

- Unterstützung von etablierten Web-Plattformen und IAM-Lösungen (Identity and Access Management) als Plattform für eine effiziente Vernetzung aller Beteiligten
- Unterstützung von Web-Applikationen und nativen mobile Clients
- Fokus → aktuelle, anerkannte und aufstrebende Standards für eine einfache Integration bestehender Lösungen und Erstellung neuer Anwendungen:
  - Web-API: RESTful Web-Services
  - Signatur und Encryption/Decryption: JSON Signature und Encryption (JOSE, JWS, JWE, JWA, JWK, …)
  - Identity Management und Authentifizierung: OpenID (JWT, OAuth2 und OpenID Connect) http://openid.net/connect

FHIR – Sicherheitsmechanismen

„FHIR ist kein Sicherheitsprotokoll und definiert auch keine sicherheitsrelevanten Funktionen. FHIR definiert jedoch Austauschprotokolle und Content-Modelle, die mit verschiedenen Sicherheitsprotokollen verwendet werden müssen, welche an anderer Stelle definiert sind.“

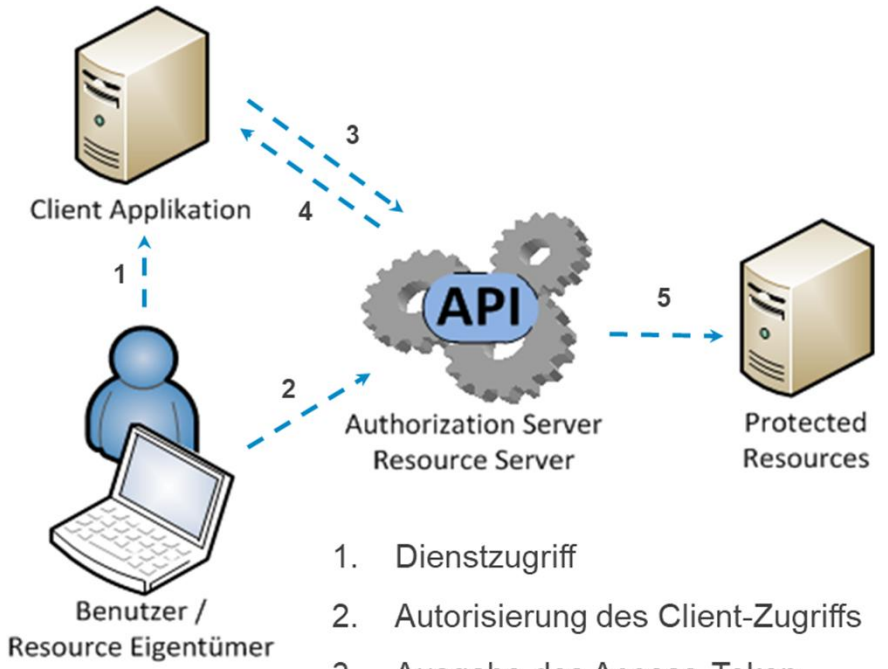
Quelle: https://www.hl7.org/fhir/security.html

Generische Funktionen eines Sicherheitssystems	Empfehlung
Authentifizierung: identifiziert und authentifiziert den Benutzer	**OpenID Connect**
Zugriffskontrollsystem: entscheidet, ob FHIR-Operationen erlaubt sind (RBAC, ABAC)	**OAuth** **Smart-On-FHIR**
Audit-Protokoll: zeichnet Aktionen auf, um spätere Überprüfung und Erkennung von Eindringlingen oder unangemessener Nutzung zu ermöglichen	**UMA, weitere …**

OAuth2 – was bringt es?

- OAuth 2.0 ist ein Autorisierungs-Framework und kein Authentifizierungsprotokoll.
  https://oauth.net/articles/authentication/
- Trennung zwischen Token-Ausstellung und -Verwendung ermöglicht geschützte Schnittstelle (oder API) für Zugriffe von unterschiedlichen Clients mit verschiedenen Geschäftsmodellen
- Bekannt als Architektur-Fundament für verschiedene, darauf aufbauende Standards

Sicherheitsmechanismen

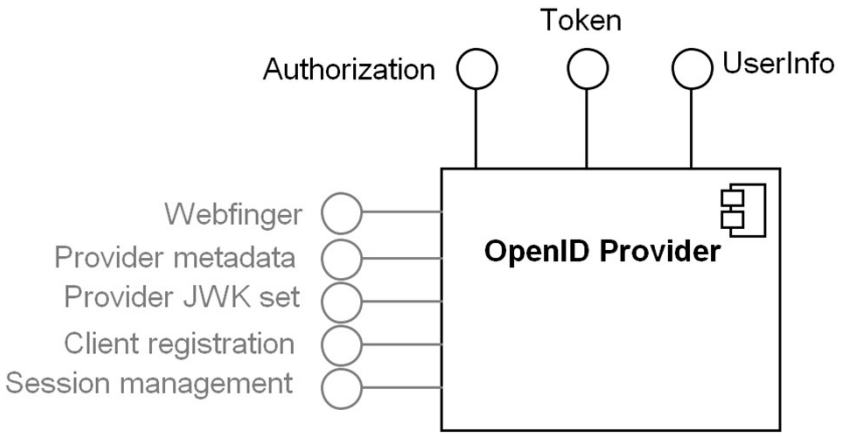


1. Dienstzugriff
2. Autorisierung des Client-Zugriffs
3. Ausgabe des Access-Token
4. Zugriff auf geschützte Resource
5. Autorisierter Zugriff auf geschützte Resource

OpenID Connect – was bringt es?

- Identity Protocol basierend auf OAuth 2.0 mit der Zielsetzung einfacher Implementierbarkeit auf allen Plattformen und beantwortet die Fragen:
  - Wer ist der Nutzer, der authentifiziert wurde?
  - Wo, wann und wie (stark) wurde der Nutzer authentifiziert? (ISO/IEC 29115 Entity Authentication Assurance, LoA 1-4)
  - Welche Attribute können in der elektronischen Identität bestätigt werden?
  - Warum sind bestimmte Attribute enthalten?

Sicherheitsmechanismen



- Wichtiger Baustein für attribut-basierte Zugriffskontroll-Systeme (ABAC) in einer resource-orientierten Architektur (REST friendly), Single-Sign-On (SSO) in verteilten Systemen

OpenID Connect – was bringt es?

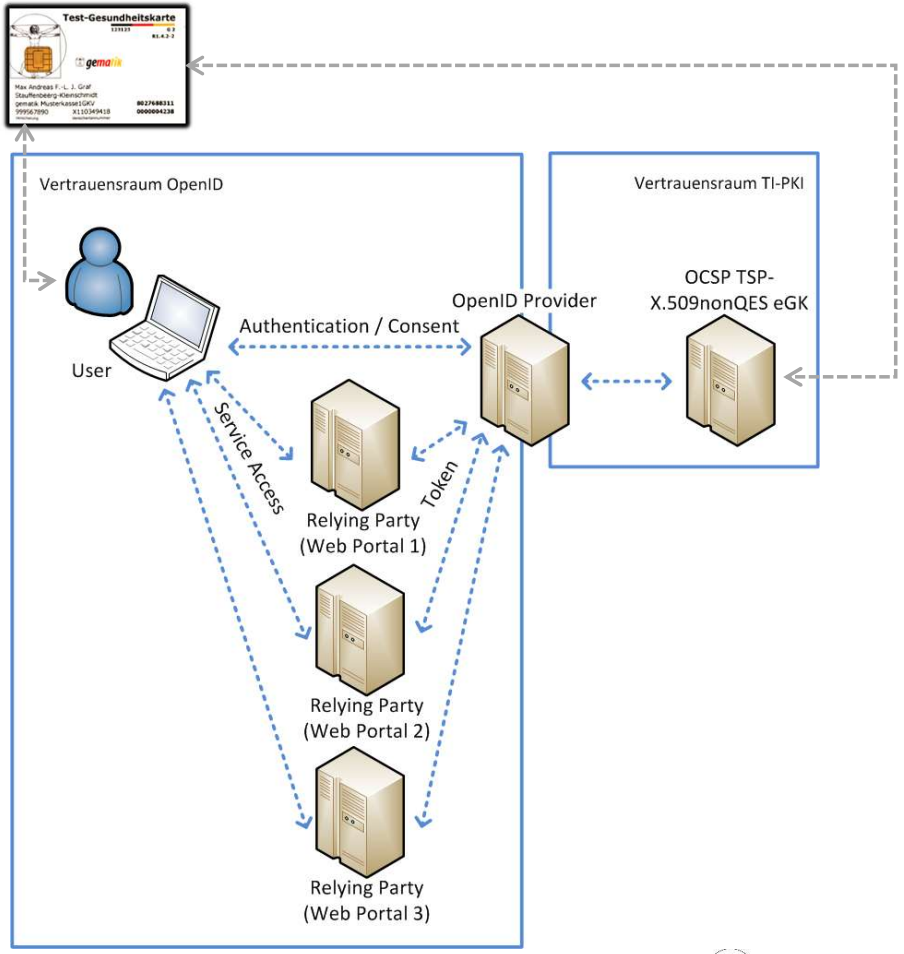
- Übernimmt die bewährten Ansätze historischer Entwicklungen (Kerberos, SAML/WS-Trust) bezogen auf die Trennung von Fach- und Sicherheitslogik
  →
  Nutzerverwaltung und -authentifizierung werden an Identity-Provider delegiert.

- Vorteile gegenüber SAML/WS-Trust/WS-*:
  - Schnelle und einfache Implementierung
  - JSON statt XML (weniger Overhead an Metadaten)
  - „der Standard“ auf mobilen Plattformen und Eignung im Desktop-Umfeld
  - Token-Austausch via „back-channel“, nicht über User-Agent („front-channel“)
  - Flexibles Authentisierungsverfahren (Username/Password, 2-Faktor, Smartcard/PKI etc.)

Beispiel: Versichertenportale (OpenID Connect)

- OpenID-Provider realisiert den Übergang vom Vertrauensraum der TI in den Vertrauensraum OpenID
- Authentisierung erfolgt unter Nutzung der TI-PKI (AUTH-Zertifikate auf der eGK)
- OpenID-Provider sichert die User-Identität den Web- Portalen zu. Web-Portale vertrauen dem OpenID-Provider
- OpenID-Standard ermöglicht:
  - Single Sign-on
  - Subject Sessions
  - Authorization Management

Sicherheitsmechanismen



Fazit

Sicherheit in FHIR-Systemen ist mit gängigen, offenen Standards interoperabel umsetzbar:

- OAuth2.0 Core:
  - OAuth 2.0 Framework – RFC 6749
  - Bearer Token Usage – RFC 6750
  - Threat Model and Security Considerations – RFC 6819
- OAuth2.0 Extensions:
  - OAuth 2.0 Token Introspection – RFC 7662
  - PKCE – Proof Key for Code Exchange
  - JSON Web Token – RFC 7519
- OpenId Connect:
  - http://openid.net/specs/openid-connect-core-1_0.html
  - http://openid.net/specs/openid-connect-registration-1_0.html
- User-Managed Access (UMA) 2.0: https://docs.kantarainitiative.org/uma/ed/uma-core-2.0-01.html

Vielen Dank für Ihre Aufmerksamkeit!

Wir sind offen für Anregungen und an fachlichem Austausch interessiert.

Kommen Sie auf uns zu!