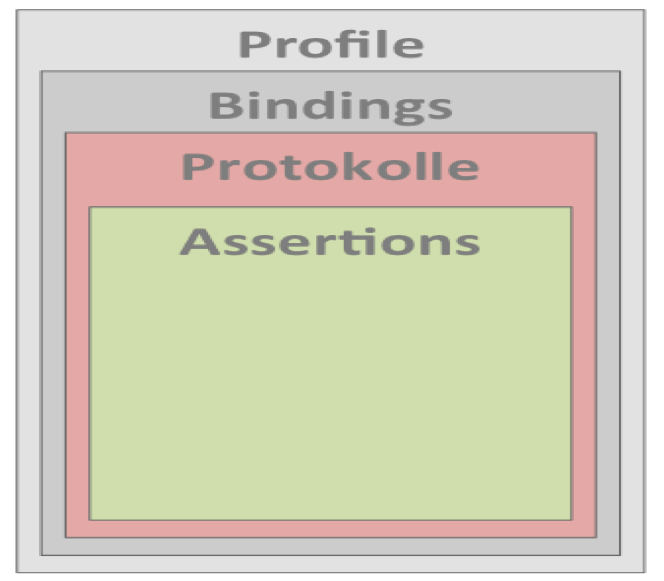
## Recherche über SAML (Security Assertion Markup Language)

* XML basiertes Framework (alle Anfragen und Antworten werden mit XML-Dokumenten umgesetzt -> plattformunabhängig)
* Applikation (Service Provider) identifiziert Nutzer und leitet die Informationen weiter zum ID Provider als XML Dokument
* ID Provider erstellt ebenfalls XML Dokument mit Nutzername oder Passwort, signiert es mit einem X.059 Zertifikat und sendet dieses zurück zum Service Provider
* SAML besteht aus vier Komponenten:

Assertion: XML-Struktur, die Eigenschaften des Benutzers enthält (werden vom ID Provider erstellt)

Protokoll: Frage-Antwort Muster

Bindings: Übertragungsweg (SOAP oder http)

Profile: bündeln die anderen Komponenten für bestimmte Anwendungsfälle

## Fazit und Vor- / Nachteile

* OpenID Connect macht das Gleiche wie SAML
* OAuth ist KEIN Authentifizierungsprotokoll, nur Autorisierung!
  + id\_token ist vergleichbar mit einer SAML Assertion
* SAML: nur Webseiten, OpenID Connect: auch mobile Anwendungen -> der neue Weg
* SAML ist dann eine Wahl, wenn die Infrastruktur bereits steht, für neue Projekte eher OpenID Connect

Für das Projekt „ID Management in E-Health“ ist OpenID Connect eine gute Wahl.

## Quellen

<https://www.nds.rub.de/media/attachments/files/2012/03/Weiss_2010_SAML-basierte_Single_Sign_On_Frameworks.pdf>

https://www.gluu.org/blog/oauth-vs-saml-vs-openid-connect/

https://jaxenter.de/anwendungssicherheit-saml-eine-einfuehrung-18066