

# IT Sicherheit

02 AAA / Radius

Authentication Authorization Accounting

# AAA – Triple A

- **A**uthentication
  - **A**uthorization
  - **A**ccounting
- 
- Framework zur Steuerung Protokollierung von Zugriffen in Netzwerken

# AAA - Authentication

- Nachweis einer Identität (z.B. Benutzername & Passwort)
- Wichtig:
  - Übertragung der Authentifizierungsdaten nur verschlüsselt
  - Wenn verschlüsselte Übertragung nicht möglich, kann ein CR-Verfahren angewendet werden
  - Wenn möglich/sinnvoll: TFA/MFA

# AAA - Authentication

- CR-Verfahren anhand eines Beispiels: Alice möchte sich bei Bob authentifizieren
  - Bob schickt ein Nonce und die zu verwendende Hash-Funktion an Alice
    - Nonce: 2389d92n9, Hash-Funktion: SHA256
  - Alice bildet die Hash-Funktion von ihrem Passwort und dem Nonce
    - $\text{SHA256}(\langle \text{PASSWORT} \rangle \langle \text{NONCE} \rangle)$
  - Alice schickt das Ergebnis der Hash-Funktion an Bob. Bob berechnet die selbe Hash-Funktion und vergleicht es mit der Antwort von Alice

# AAA - Authentication

- Probleme mit CR-Verfahren:
  - Replay-Attacken
    - Mögliche Lösung: Zusätzlich wird zum Nonce der aktuelle Zeitpunkt an das Passwort angefügt und davon die Hash-Funktion gebildet.
    - Der verwendete Zeitpunkt muss auch an Bob übertragen werden. Bob akzeptiert die Antwort nur, wenn der verwendete Zeitpunkt in einem kleinen Zeitfenster ist (z.B. 60 Sekunden)
  - Wörterbuch-Attacken
    - Da das Nonce unverschlüsselt übertragen wird, kann ein Angreifer das Passwort von Alice erraten und die Hash-Funktion bilden und sich damit authentifizieren
  - Passwort bei Bob als (Salted-)Hash gespeichert
    - Entweder Bob speichert das Passwort in Plain-Text (No No No), oder Alice muss den selben (salted) Passwort-Hash, wie Bob berechnen, um die Response berechnen zu können

# AAA - Authorization

- Erteilen einer Berechtigung
  - Richtlinien legen fest welche Identitäten welche Art von Zugriff auf eine Ressource haben
    - Z.B. Benutzer in der Gruppe “Schüler” haben lesenden Zugriff auf den Ordner “Unterlagen”, aber schreibenden Zugriff auf den Ordner “Notizen”
- “Principle of least privilege”
  - Einer Identität sollte immer nur jener Zugriff gewährt werden, welcher zur Erfüllung einer Aufgabe notwendig ist
    - Z.B. Nur MitarbeiterInnen der Personalabteilung haben Zugriff auf die Stammdaten der MitarbeiterInnen

# AAA - Accounting

- Protokollierung von Änderungen – Audit Log
- Beispiele:
  - Alice hat sich in das WLAN verbunden (Zeitpunkt, SSID, MAC von Alice, ID des Accesspoint, zugewiesenes VLAN, ...)
  - Alice ist (noch immer) in das WLAN verbundene
  - Alice hat sich von dem WLAN getrennt
  - Alice' SIM-Karte hat sich von einem Sender zu einem anderen verbunden
- Notwendig, um
  - im Nachhinein Prozesse nachvollziehen zu können
  - eine Verrechnung der verwendeten Dienste machen zu können

# AAA - Protokolle

- TACACS+ / Terminal Access Controller Access-Control System Plus
  - Cisco Protokoll
  - Verbindungsorientiert (TCP)
  - Gesamte Kommunikation verschlüsselt
- RADIUS
  - Am meisten verbreitetes AAA Protokoll
  - Verbindungslos (UDP) - typischerweise
  - Nur Passwörter werden gehasht übertragen, Rest in plain text - typischerweise
- DIAMETER
  - Weiterentwicklung von RADIUS
  - Verbindungsorientiert (TCP)
  - Transport-Verschlüsselung über IPSEC oder TLS



# RADIUS

- Remote Authentication Dial-In User Service
- AAA Protokoll zur zentralen Verwaltung von Benutzern mit Zugriff auf Netzwerk Dienste
- Einfaches Client/Server Protokoll
  - Client: NAS – Network Access Server (z.B. Accesspoint, Switch, ...)
  - Server: RADIUS Server Instanz
- Zwei Arten:
  - AA – Authentication and Authorization
  - A - Accounting

# RADIUS – Authentication and Authorization

- Benutzer möchte Zugriff auf einen Netzwerk-Dienst erhalten
- Benutzer übermittelt Zugangsdaten (Benutzername/Passwort/Zertifikat) an NAS (= RADIUS Client)
- NAS sendet eine “Access Request” Nachricht an den RADIUS Server
  - Inhalt der Nachricht sind neben den Zugangsdaten noch weitere Attribute die dem NAS bekannt sind (z.B. MAC, ...)
  - Server antwortet mit einer von drei Antworten:
    - Access Reject: Zugriff verweigert (z.B. Passwort falsch, deaktivierter Benutzer, ...)
    - Access Challenge: Weiterer Faktor notwendig
    - Access Accept: Zugriff erlaubt und Berechtigung erteilt
      - Weiterer Antwort-Parameter: VLAN-ID, IP-Adresse, QoS-Parameter, Session Lifetime, ...

# RADIUS – Accounting

- Accounting kann an den RADIUS Server oder einen weiteren Server gesendet werden
- Accounting ist optional und dient hauptsächlich der korrekten Verrechnung bzw. der Erstellung von Statistiken
- Nach AA, sendet der NAS eine “Accounting Start” Nachricht
- In regelmäßigen Intervallen sendet der NAS “Interim Update” Nachrichten, so lange der Benutzer den Netzwerk-Dienst verwendet
- Nach der Trennung des Benutzers vom Netzwerk-Dienst, wird eine “Accounting Stop” Nachricht gesendet

# RADIUS – Roaming

- Benutzer können sich auf Netzwerk-Diensten von verbundenen Institutionen anmelden
- eduroam
  - Weltweit vernetzte Institutionen aus dem Forschungsbereich erlauben den Zugriff auf z.B. das lokale WLAN mit den Zugangsdaten der eigenen Institution
  - Zuordnung auf Basis von REALMs – dadurch werden die Nachrichten an den “Heimat-RADIUS-Server” gesendet

# SSO – Single Sign-On



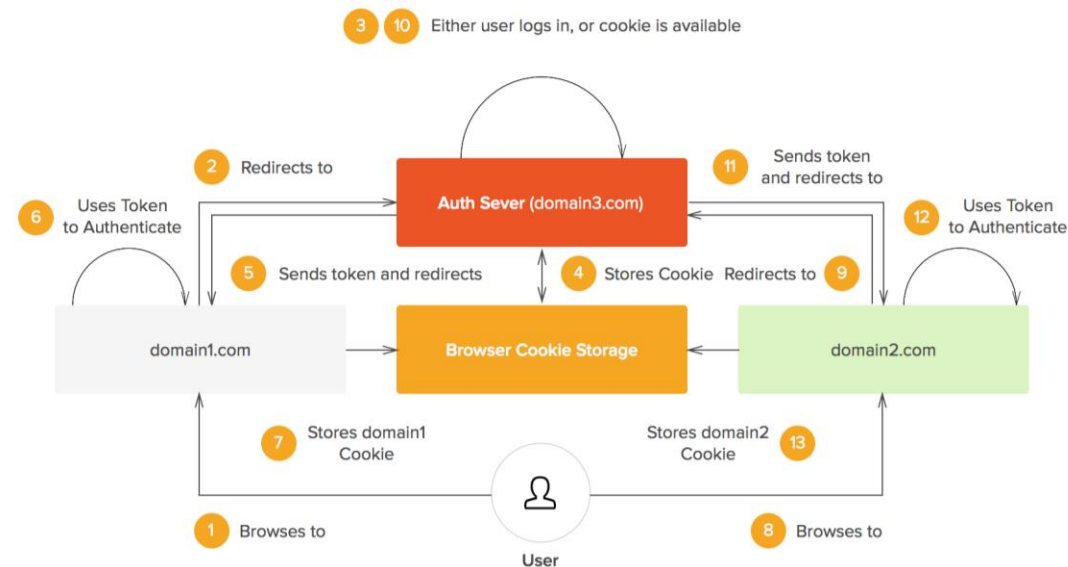
## • Szenario

- Benutzer müssen mehrere Services verwenden
- Services erfordern, dass sich ein Benutzer authentifiziert

## • Probleme:

- Benutzer verwenden bei allen/vielen Services das gleiche (einfache) Passwort
- Benutzer müssen sich regelmäßig bei allen Services anmelden (kostet in Summe viel Zeit und ist für Benutzer mühsam)

# SSO – Single Sign-On



- Lösung: Single Sign-On
- Benutzer melden sich **nur** bei einem Authentifizierungsservice an
- Die Anmeldung bei den einzelnen Services wird über den Authentifizierungsservice geleitet
- Der Authentifizierungsservice führt auch die Autorisierung durch und führt den Sign-On nur auf berechtigte Services durch

# SSO – Single Sign-On

- Vorteile:
  - Authentifizierung muss nur einmal durchgeführt werden
  - MFA kann an einem zentralen Platz eingerichtet und verwaltet werden
  - Autorisierung kann an einem zentralen Platz durchgeführt werden
- Nachteile:
  - Zugriff auf eine Session am Authentifizierungsserver ermöglicht Zugriff auf alle berechtigten Services
  - Single Sign-Off üblicherweise nicht implementiert -> Timeout meldet Benutzer bei einzelnen Services ab

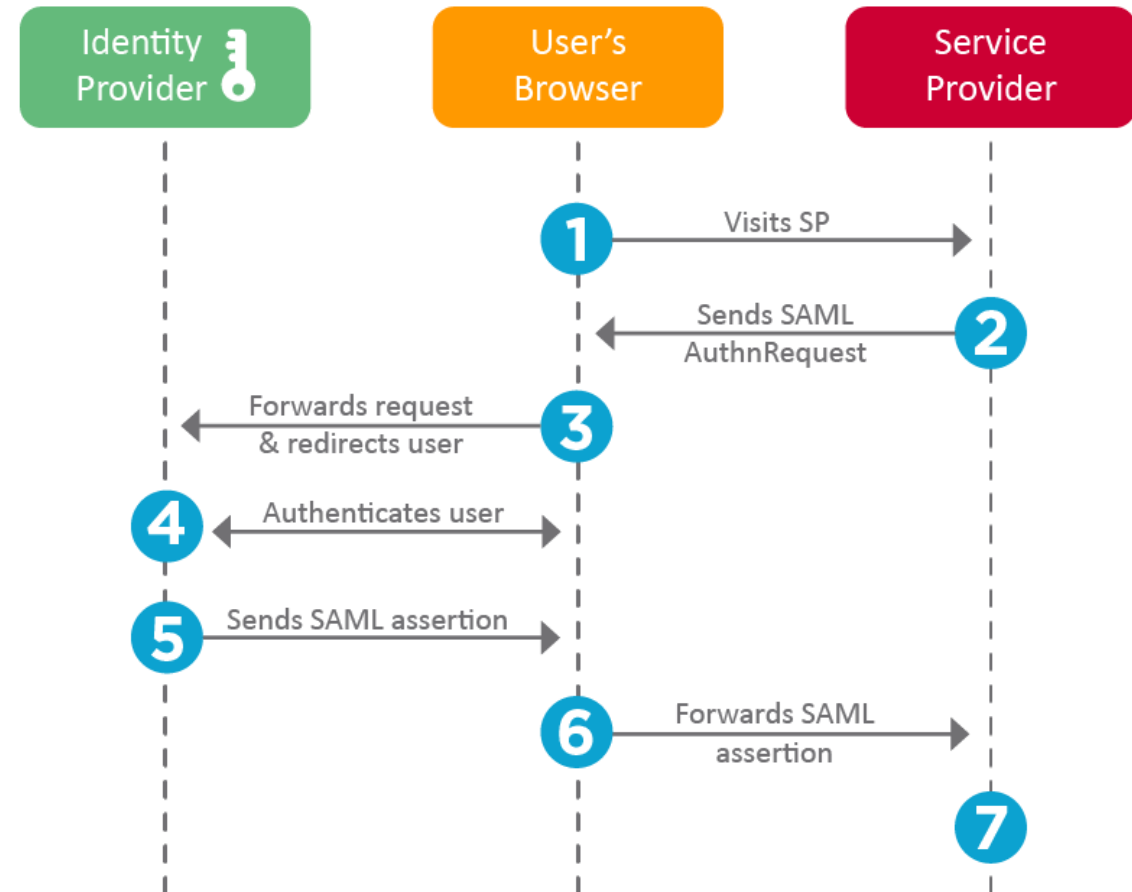
# SSO - SAML

- SAML = Security Assertion Markup Language
- XML basiertes Framework zum Austausch von “Assertions”
- Involvierte Rollen:
  - Principal (Benutzer)
  - Identity Provider (Idp) -> Authentifizierungsservice
  - Service Provider (SP) -> Service



# SSO - SAML

- Typischer SAML Sign-On
  - 1-7: SP-initiated SSO
  - 3-7: IdP-initiated SSO

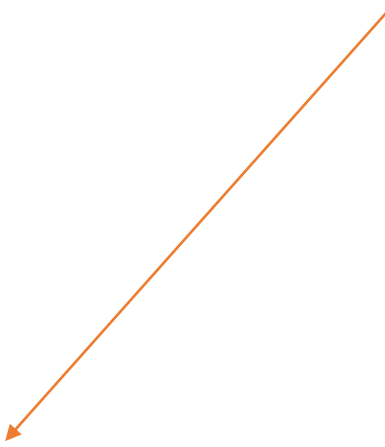


# SSO - SAML

- SAML AuthnRequest Beispiel

Ziel für SAML Assertion

```
<samlp:AuthnRequest
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="ONELOGIN_809707f0030a5d00620c9d9df97f627afe9dcc24"
  Version="2.0"
  ProviderName="SP test"
  IssueInstant="2014-07-16T23:52:45Z"
  Destination="https://idp.example.com/SSOService.php"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  AssertionConsumerServiceURL="https://sp.example.com/demol/index.php?acs">
  <saml:Issuer>https://sp.example.com/demol/metadata.php</saml:Issuer>
  <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" AllowCreate="true" />
  <samlp:RequestedAuthnContext Comparison="exact">
    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```



# SSO - SAML

- SAML Response Beispiel

Signatur zur  
Verifikation, dass  
Response von IdP

Attribute, die von SP  
zum Login des  
Benutzers  
verwendet werden

```
<saml:Response
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="8e8dc5f69a98cc4c1ff3427e5ce34606fd672f91e6"
  Version="2.0"
  IssueInstant="2014-07-17T01:01:48Z"
  Destination="https://sp.example.com/demo1/index.php?acs"
  InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
  <saml:Issuer>https://idp.example.com/metadata.php</saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:Assertion
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="pfxecb67158-2883-a785-ff4a-1711fe6b9901" Version="2.0">
    <saml:Issuer>https://idp.example.com/metadata.php</saml:Issuer>
    <ds:Signature
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:SignatureValue>k/nuHw0sPn/15q1J/PvJvMZQhJDovW5X7Ifu9JmZQwexpDamfYSjN5FoP+LC6PHHA+Lt/d60xtlb1
        <ds:KeyInfo>
          <ds:X509Data>
            <ds:X509Certificate>MIICajCCAdOgAwIBAgIBADANBgkqhkiG9w0BAQ0FADBSMQswCQYDVQQGEWJ1czETMBEC
            </ds:X509Data>
          </ds:KeyInfo>
        </ds:Signature>
      </ds:Signature>
    <saml:Subject>
      <saml:NameID SPNameQualifier="https://sp.example.com/demo1/metadata.php" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:emailAddress">test@example.com</saml:NameID>
      <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData NotOnOrAfter="2024-01-18T06:21:48Z" Recipient="https://sp.example.com/demo1/index.php?acs"></saml:SubjectConfirmationData>
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions NotBefore="2014-07-17T01:01:18Z" NotOnOrAfter="2024-01-18T06:21:48Z">
      <saml:AudienceRestriction>
        <saml:Audience>https://sp.example.com/demo1/metadata.php</saml:Audience>
      </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement AuthnInstant="2014-07-17T01:01:48Z" SessionNotOnOrAfter="2024-07-17T09:01:48Z">
      <saml:AuthnContext>
        <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
      </saml:AuthnContext>
    </saml:AuthnStatement>
    <saml:AttributeStatement>
      <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">test</saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
```

# SSO - SAML

- SAML AuthnRequest:
  - Wird Base64 enkodiert im **GET-Parameter SAMLRequest** übertragen
  - [https://idp.example.org/SAML2/SSO/Redirect?SAMLRequest=PH ..... Vz dD4=](https://idp.example.org/SAML2/SSO/Redirect?SAMLRequest=PH.....VzdD4=)
- SAML Response:
  - Wird Base64 enkodiert im **POST-Parameter SAMLResponse** an den SP übertragen

# SSO - OIDC

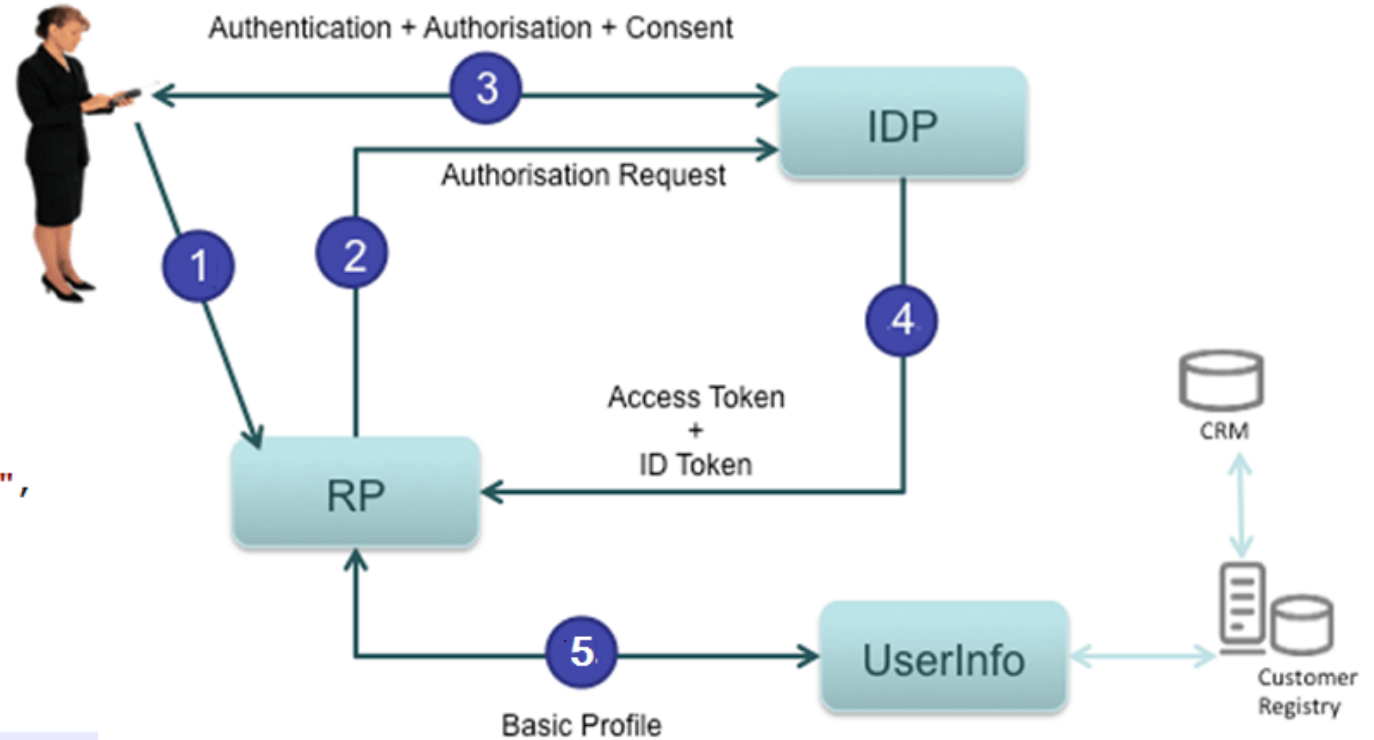
- OIDC = OpenID Connect
- Involvierte Rollen:
  - User
  - Identity Provider (IdP) -> Authentifizierungsservice
  - Replying Party -> Service

# SSO - OIDC

- Typischer OIDC Sign-On

## ID Token

```
{
  "iss": "https://openid.service.com/oidc",
  "sub": "RP-UID",
  "aud": "RP-CLIENT-ID",
  "exp": 1445349320,
  "iat": 1445345720,
  "auth_time": 1445345455,
  "acr": 0
}
```



# SSO - OIDC

- Claims
  - Können von der RP angegeben werden
  - Z.B. name, given\_name, email ...
  - Müssen vom Benutzer freigegeben werden (Consent)
  - Können mit dem Access Token vom Userinfo Endpoint abgefragt werden