Das Gemüse: Token

Stephan Verbücheln

Cnlab Herbsttagung
KOSMOS, Zürich, 7. September 2022

cnlab

OTP Hardware?

- RSA SecureID
- Vasco
- ...

Die sind nicht gemeint!

Blockchains?

- Token in der Blockchain
- Token Economy
- Non-Fungible Tokens (NFT)
- ...

Die sind auch nicht gemeint!

Authentication/Authorization Token

Klassifizierung

- Self-contained Token («Assertion»)
  - Security Assertion Markup Language (SAML)
    - SAML Request
    - SAML Response
  - JSON Web Token (JWT)
    - ID Token
    - Access Token

- Opaque Token
  - Auth Code
  - Refresh Token

- Verwendung
  - Bearer Token
  - Sender-constrained Token (Proof Token)

SAML: Security Assertion Markup Language

- Standardisiert seit 2001 von OASIS (Organization for the Advancement of Structured Information Standards)
- Basiert auf XML
- Verwendet bekannte XML-Standards, z.B. für Signaturen und Verschlüsselung
- Mächtige Syntax
- Anfälligkeit für XML-typische Schwachstellen

JWT: JSON Web Tokens

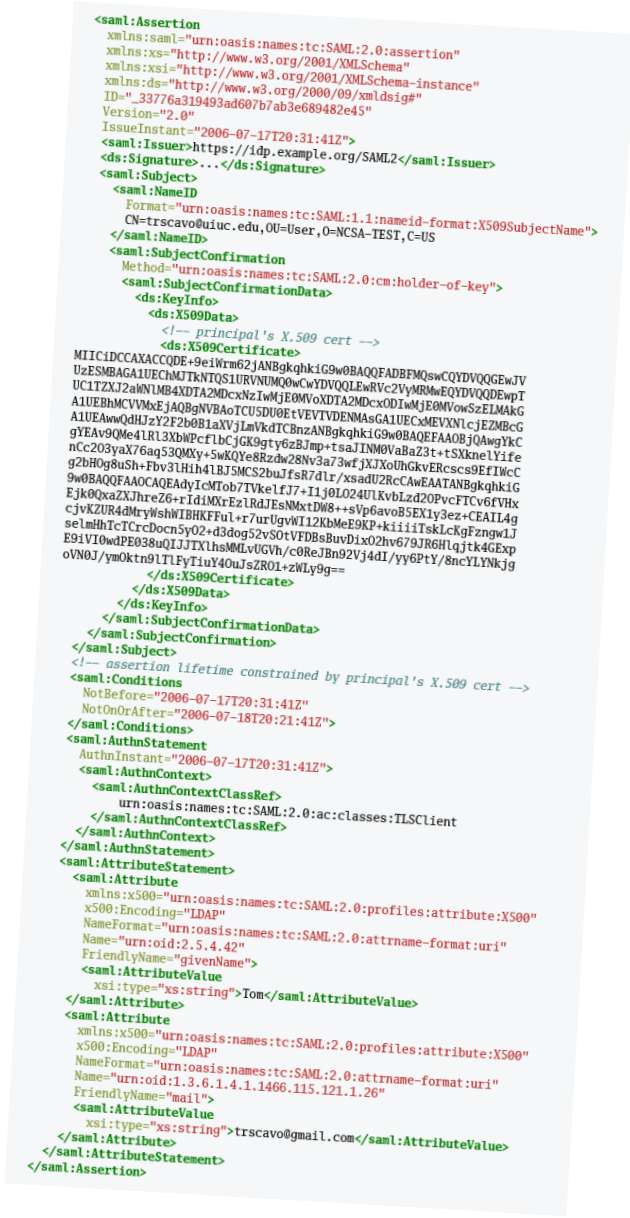
- Standardisiert seit 2015 in RFC7519 (und andere)
- Basiert auf JSON
- Verwendet entsprechende Standards für Verschlüsselung und Signatur
- Einfache Syntax
- Weniger Angriffsfläche

SAML Request und Response

- Bei SAML gibt es zwei Token: Request und Response

Request

- Enthält Informationen für die Ausstellung des Tokens
- Sollte signiert werden
  - So weiss der IDP, wofür später das Token ausgestellt wird



SAML Response

- Das Token zur Authentisierung
- Es enthält eine Referenz zum Request

Weitere Daten:

- Eindeutiger Name (Subject)
- Gültigkeitsdatum (von/bis)
- Signatur

```
<samlp:Response
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="identifier_2"
  InResponseTo="identifier_1"
  Version="2.0"
  IssueInstant="2004-12-05T09:22:05Z"
  Destination="https://sp.example.com/SAML2/SSO/POST">
  <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode
      Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <saml:Assertion
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="identifier_3"
    Version="2.0"
    IssueInstant="2004-12-05T09:22:05Z">
    <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer>
    <!-- a POSTed assertion MUST be signed -->
    <ds:Signature
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
    <saml:Subject>
      <saml:NameID
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
        3f7b3dcf-1674-4ecd-92c8-1544f346baf8
      </saml:NameID>
      <saml:SubjectConfirmation
        Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml:SubjectConfirmationData
          InResponseTo="identifier_1"
          Recipient="https://sp.example.com/SAML2/SSO/POST"
          NotOnOrAfter="2004-12-05T09:27:05Z"/>
      </saml:SubjectConfirmation>
    </saml:Subject>
    <saml:Conditions
      NotBefore="2004-12-05T09:17:05Z"
      NotOnOrAfter="2004-12-05T09:27:05Z">
      <saml:AudienceRestriction>
        <saml:Audience>https://sp.example.com/SAML2</saml:Audience>
      </saml:AudienceRestriction>
    </saml:Conditions>
    <saml:AuthnStatement
      AuthnInstant="2004-12-05T09:22:00Z"
      SessionIndex="identifier_3">
      <saml:AuthnContext>
        <saml:AuthnContextClassRef>
          urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
        </saml:AuthnContextClassRef>
      </saml:AuthnContext>
    </saml:AuthnStatement>
  </saml:Assertion>
</samlp:Response>
```

JWT: ID Token

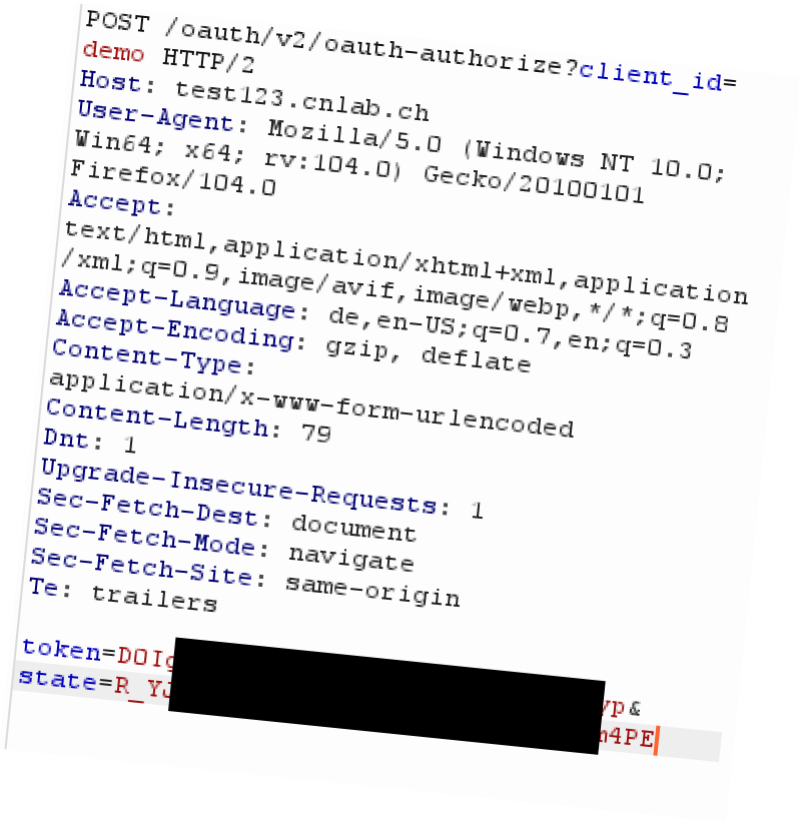
- Enthält Informationen zur Identität
- Universell gültig bis zum Ablaufdatum
- Erforderliche Felder (Payload):
  - Eindeutiger Name (Subject)
  - Gültigkeitsdatum (von/bis)
  - Aussteller (Issuer)
  - Audience
- Weitere Felder (Payload): :
  - Authentisierungsmethode
  - Nonce

JWT: Access Token

- Enthält neben der Identität weitere Einschränkungen
- Entsprechend eingeschränkt gültig bis zum Ablaufdatum
- Erforderliche Felder:
  - Eindeutiger Name (Subject)
  - Gültigkeitsdatum (von/bis)
  - Aussteller (Issuer)
  - Scope des Tokens
- Mögliche weitere Felder:
  - Rollen
  - Berechtigungen

Opaque Token

- Keine JSON-Datenstruktur
- Zufälliger String
- Die zugehörigen Daten sind in einer internen Datenbank gespeichert
- Daten werden nur im Hintergrund ausgetauscht



Beispiel: Refresh Token

- Berechtigt zum Holen von neuen Token

Unterschied zu Zertifikaten

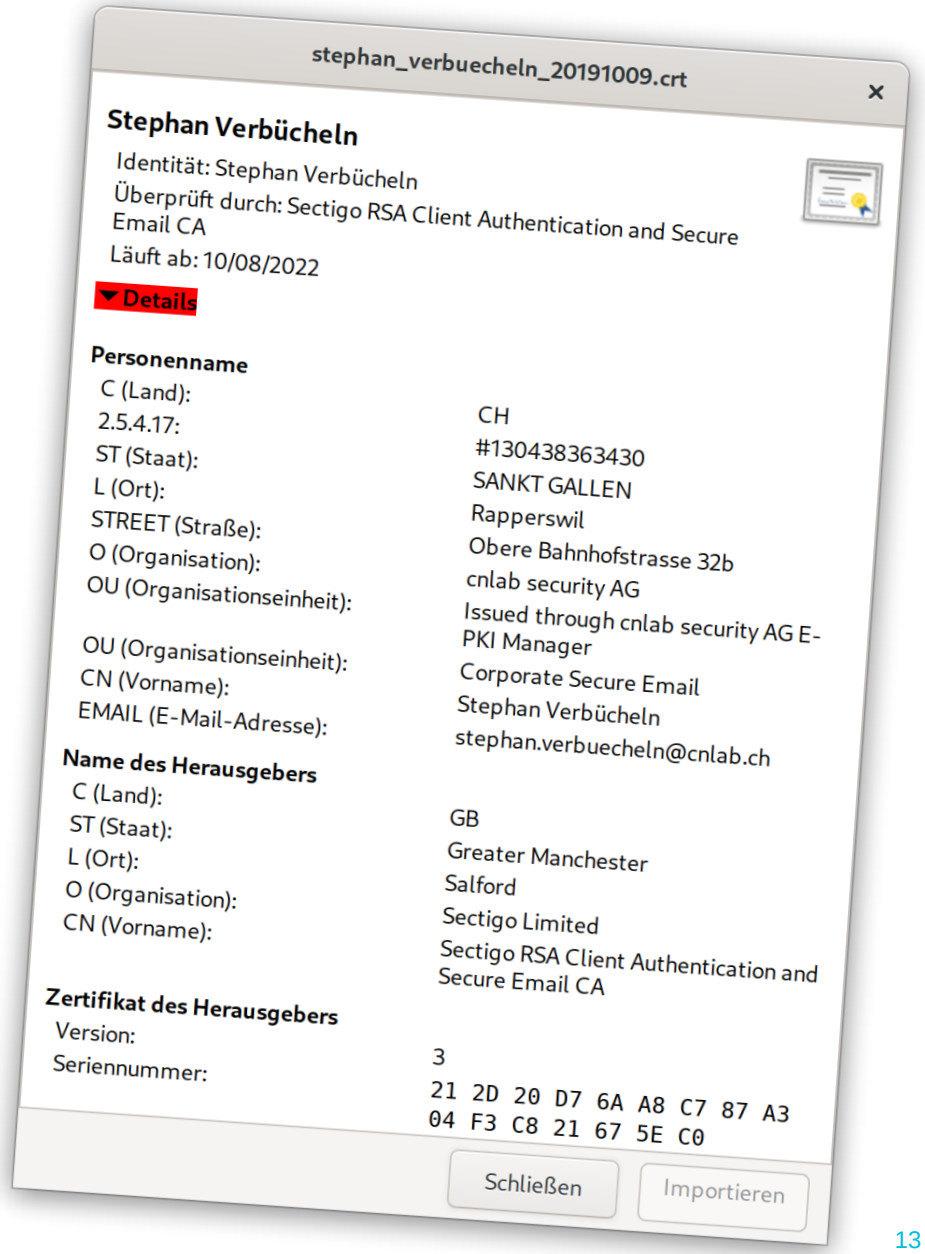
- X.509
- OpenPGP

Ähnlichkeiten

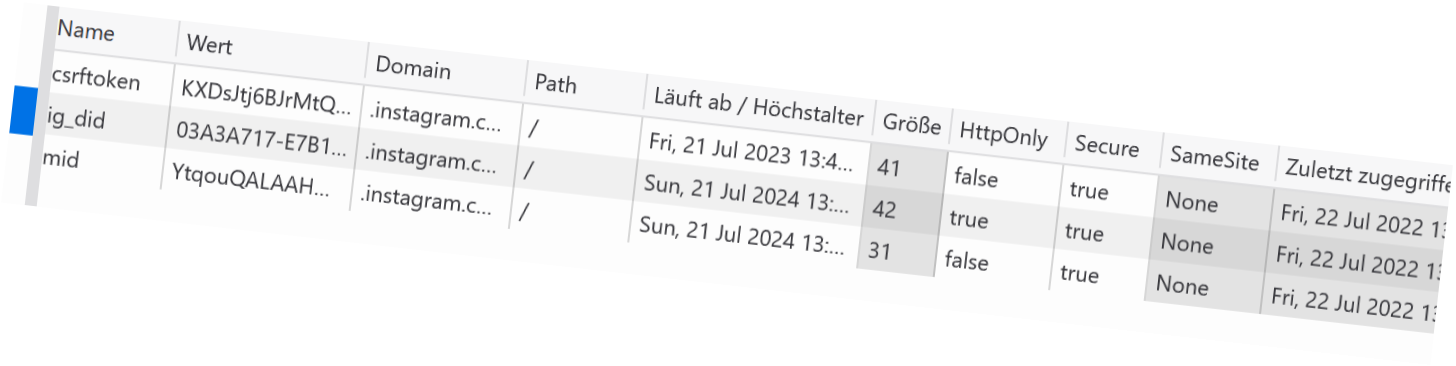
- enthält Namen
- ist von einem Aussteller signiert
- hat ein Ablaufdatum

Unterschiede

- Zertifikate haben privaten Key zur Authentisierung
- ein Token muss nur vorgezeigt werden



Session IDs



Name	Wert	Domain	Path	Läuft ab / Höchstalter	Größe	HttpOnly	Secure	SameSite	Zuletzt zugegriffe
csrftoken	KXDsJtj6BJrMtQ...	.instagram.c...	/	Fri, 21 Jul 2023 13:4...	41	false	true	None	Fri, 22 Jul 2022 1
ig_did	03A3A717-E7B1...	.instagram.c...	/	Sun, 21 Jul 2024 13:...	42	true	true	None	Fri, 22 Jul 2022 1
mid	YtqouQALAAH...	.instagram.c...	/	Sun, 21 Jul 2024 13:...	31	false	true	None	Fri, 22 Jul 2022 1

Tokens vs. HTTP Cookies

Ähnlichkeiten

- muss nur vorgezeigt werden

Unterschiede

- Inhalt für den Client undurchsichtig
- JWT-/SAML-Token haben bekannte Struktur
- JWT-/SAML-Token haben bekannte Felder (Scope, Ablaufdatum)

Kerberos Tickets

- Verbreitete Methode für SSO in Firmennetzen
- Beispiel: Windows besorgt Kerberos Ticket für den Benutzer, um ihn ohne Passwort an einer internen Website anzumelden

- Entspricht der Definition eines self-contained Token (anderes Format als JWT und SAML)
- In der Regel nicht gemeint, wenn im Web-Umfeld von «Token» gesprochen wird

Weitere Begriffe

- Bearer Token
  - Ein Token, das jeder durch Vorzeigen verwenden kann
  - Typischerweise via HTTP-Header mitgegeben
    - «Authorization: Bearer»

- SAML Assertion
  - weiteres Wort für SAML Token

Zusammenfassung

- Formate
  - SAML
  - JWT
  - Opaque

- Self-contained Token
  - SAML Request
  - SAML Response
  - ID Token (JWT)
  - Access Token (JWT)

- Opaque Token
  - Auth Code
  - Refresh Token

Vielen Dank für Ihre Aufmerksamkeit_

Stephan Verbücheln

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland

cnlab