Maximilian Schmidt
FB Informatik

Freie Universität Berlin

Vertrauenswürdige Identitäten mit dem neuen Personalausweis

Maximilian Schmidt

Inhalt

1. **Einführung**
   - Arbeitstitel
   - Motivation
2. **Evaluation**
   - Kandidaten
   - AC Systeme
   - Hürden
3. **Entwurf & Umsetzung**
   - Protokolle
   - Komponenten / Software
4. **Fazit**
   - Rückblick
   - Ausblick

Einführung: Arbeitstitel

Freie Universität Berlin

Vertrauenswürdige

Identitäten mit dem

neuen Personalausweis

„Einfaches, effizientes und vertrauenswürdiges Identitätsmanagement auf Basis von Software-Token“

Einführung: Motivation

Nutzerclient

ST Aussteller

Zertifikat ausstellen/sperren

Attribute auslesen

eID Auslesevorgang

Anforderungen:

- ✓ Software-basierte Token
- ✓ Authentizität der Identität
- ✓ Selektive Datenabfrage
- ✓ Einfache Integration
- ✓ Nutzerzentrische Datenhaltung

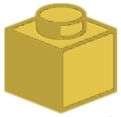
Diensteanbieter

eID-Server

Inhalt

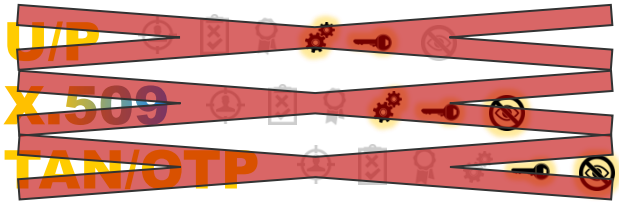
1. **Einführung**
   - Arbeitstitel
   - Motivation
2. **Evaluation**
   - Kandidaten
   - AC Systeme
   - Hürden
3. **Entwurf & Umsetzung**
   - Protokolle
   - Komponenten / Software
4. **Fazit**
   - Rückblick
   - Ausblick

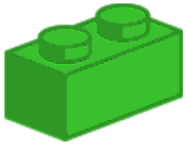
Evaluation: Kandidaten



Token

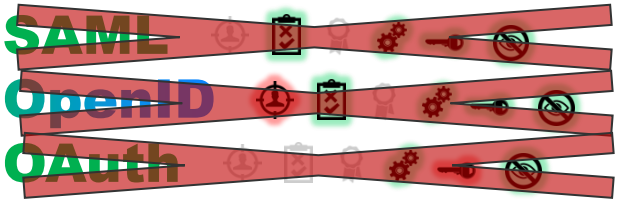
- U/P
- X.509
- TAN/OTP



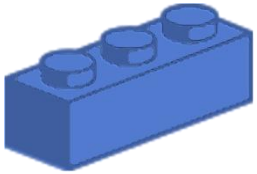


Protokolle

- SAML
- OpenID
- OAuth



- Nutzerzentrisch
- Selektive Datenextraktion
- Sperren & Verifikation
- Integration
- Authentifizierung
- Autorisierung



Identitätsmgmt-Systeme (IdMS)

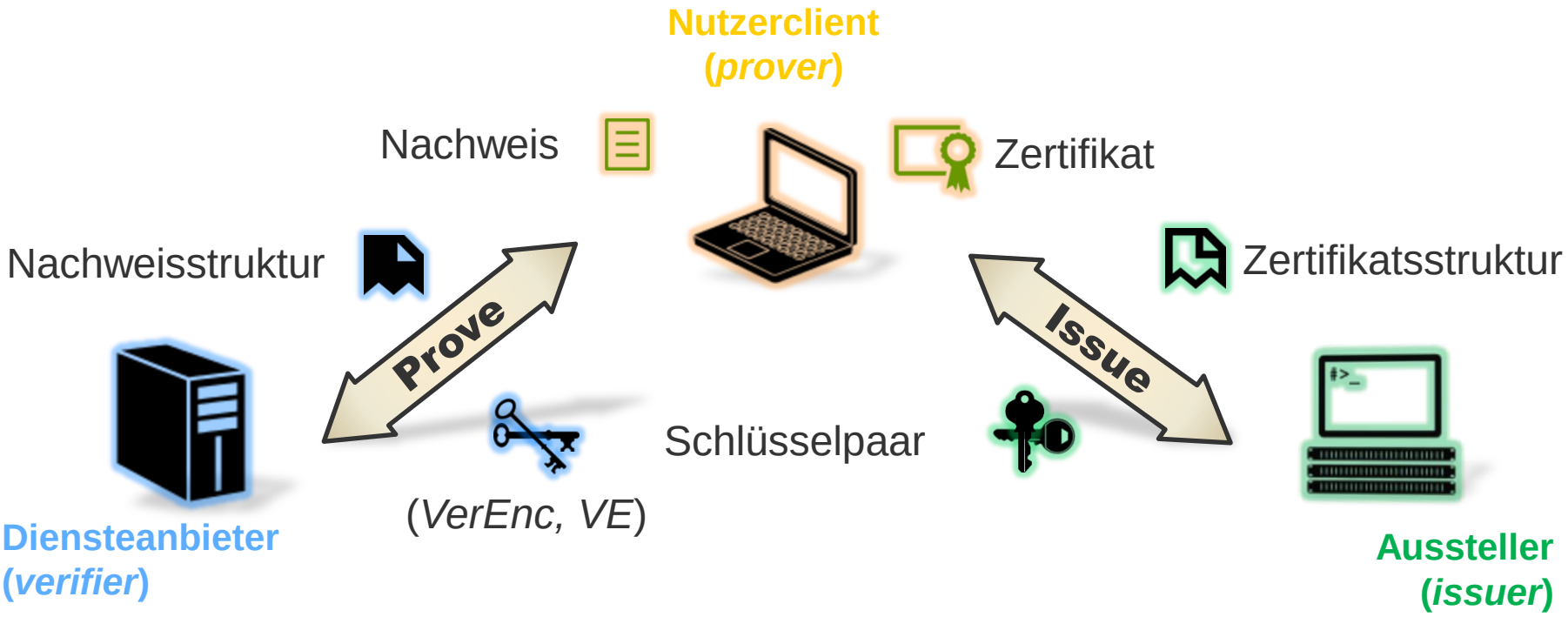
- U-Prove
- Identity Mixer
- nPA

AC Systeme: Artefakte/Protokolle

Freie Universität Berlin

Kandidaten U-Prove / Identity-Mixer:

- Anonymous Credential Systeme
  (Basis: Zero-Knowledge-Proof/Blind-Signatures)
- **Vorhanden**: Selektive Datenabfrage, Nutzerzentrisch, Anonym/Pseudonym
- **Benötigt**: Authentizität durch nPA-Integration, Sperren/Verifikation



Evaluation: Hürden

Freie Universität Berlin

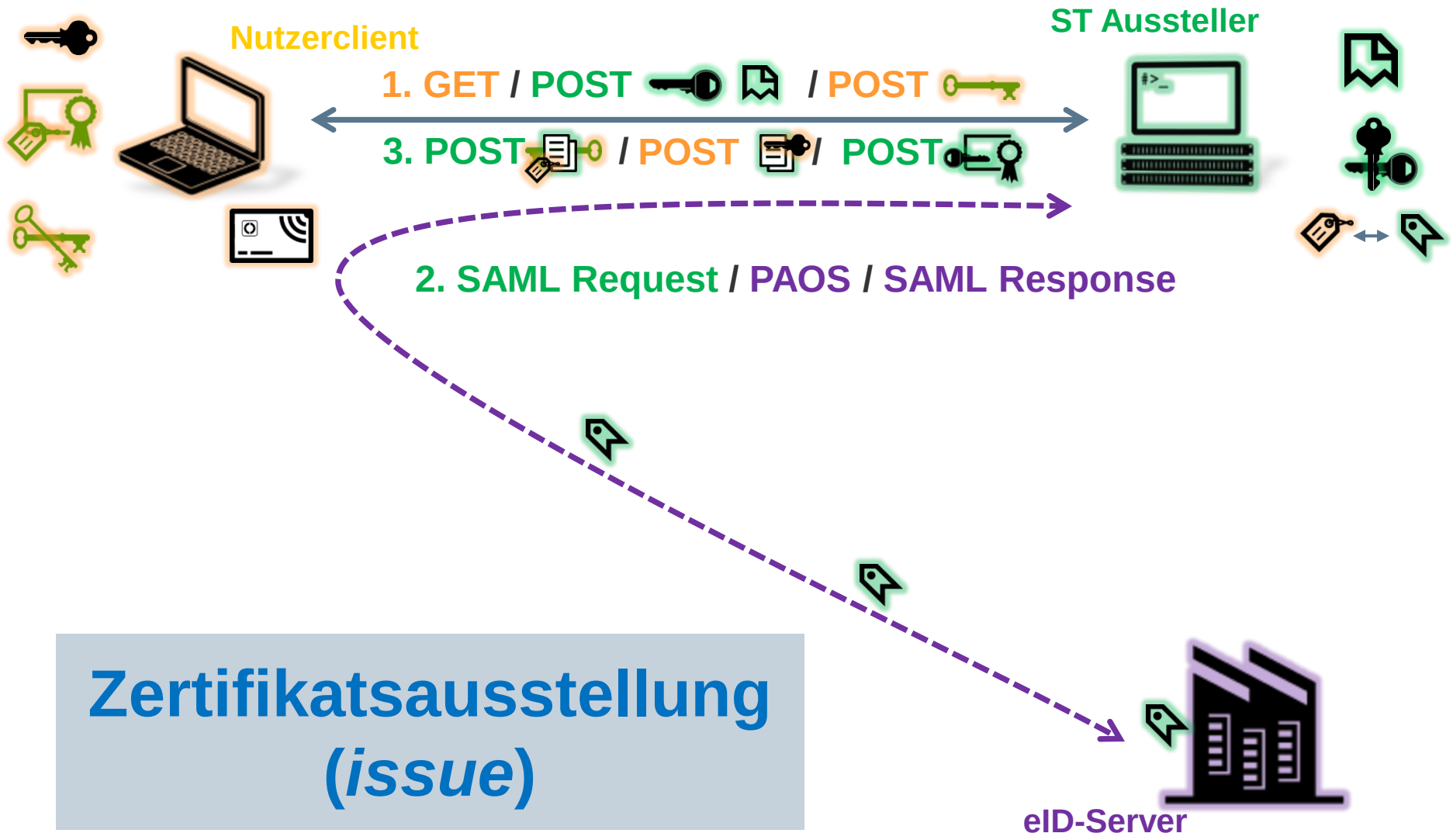
- Transportkanal undefiniert → HTTP(S)
- Zertifikatsattribute (eID-Daten) müssen vom Client vorbereitet werden (zusätzl. Protokollverschlüsselung)
- Sperren/Verifikation beim Aussteller muss möglich sein → Zertifikats-ID (verschlüsselt)
- Unvollständige Nachweise können vom Client nicht erzeugt werden → Protokollfehler ausdefinieren
- Integration kompatibel → eID-Integration optional

Inhalt

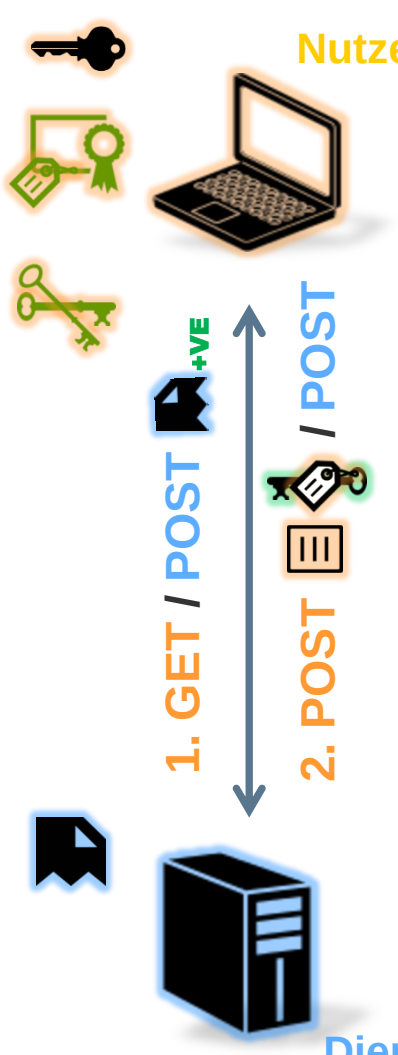
Freie Universität Berlin

1. **Einführung**
   - Arbeitstitel
   - Motivation
2. **Evaluation**
   - Kandidaten
   - AC Systeme
   - Hürden
3. **Entwurf & Umsetzung**
   - Protokolle
   - Komponenten / Software
4. **Fazit**
   - Rückblick
   - Ausblick

Entwurf: Protokollerweiterungen

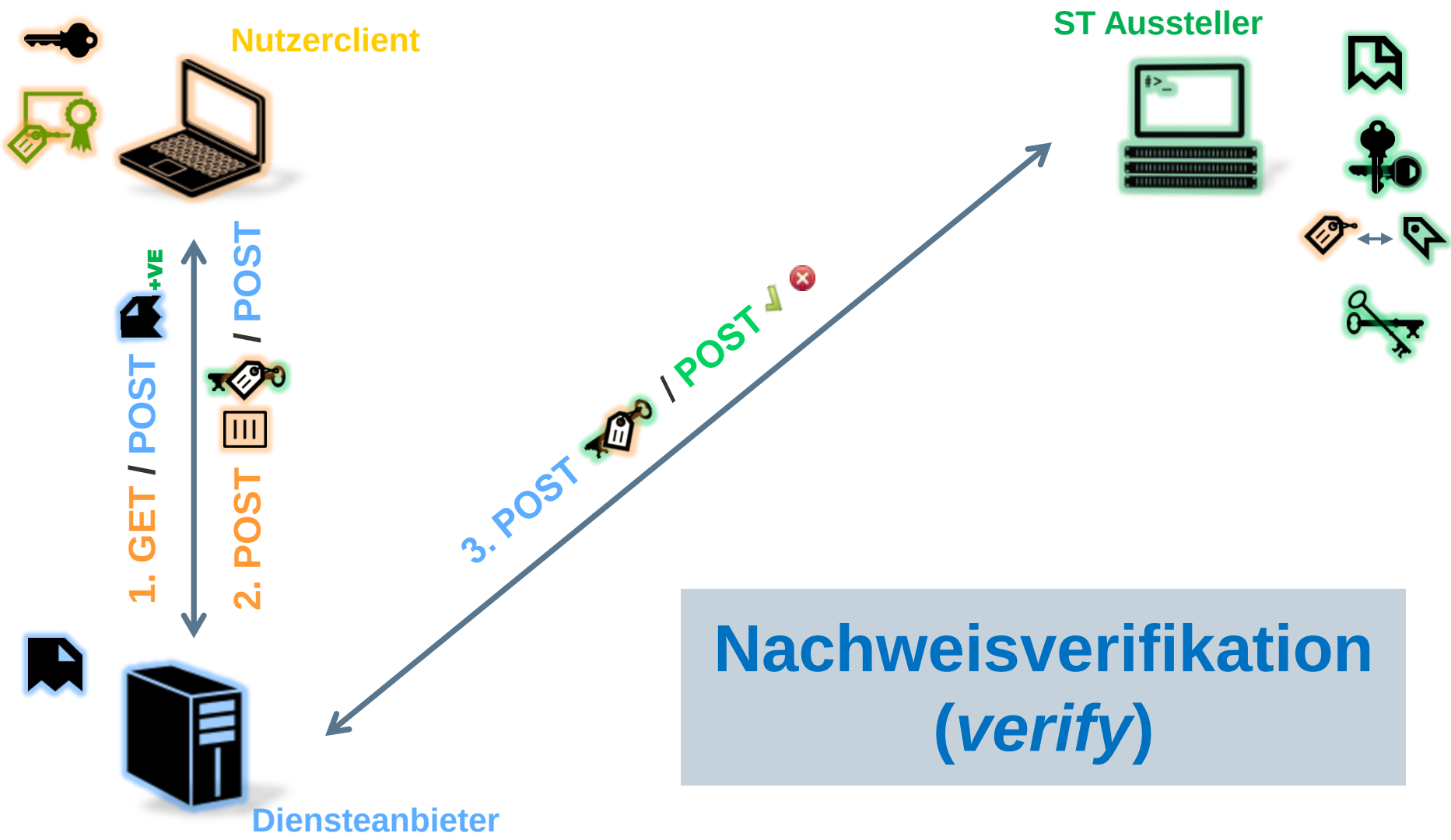


Entwurf: Protokollerweiterungen



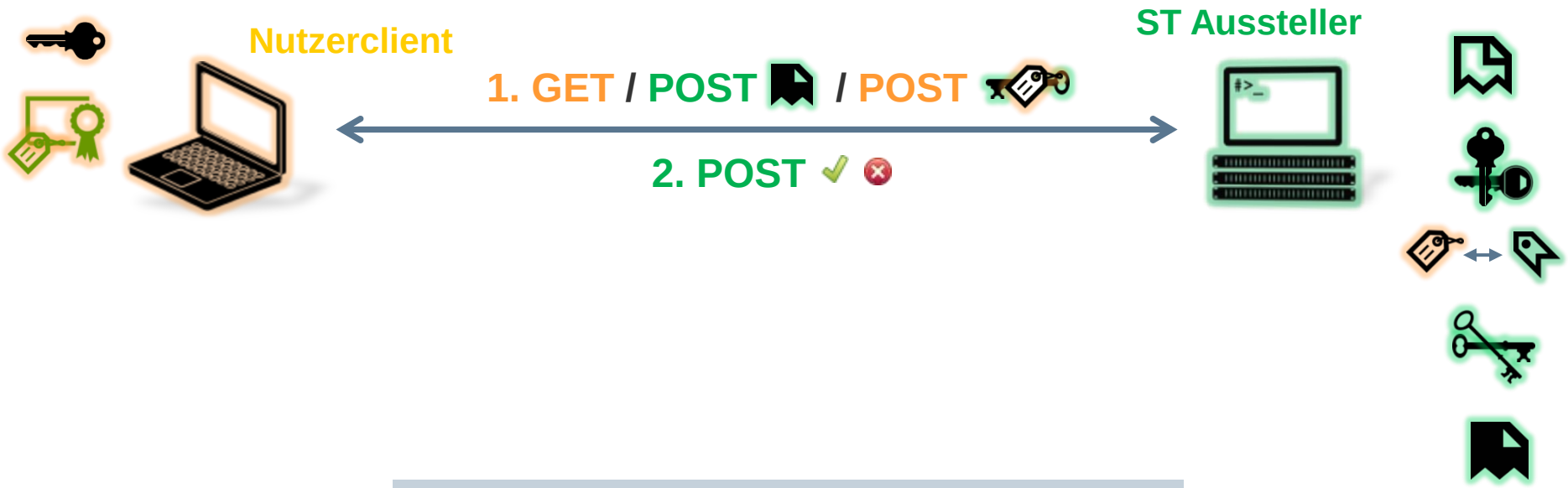
Nachweiserzeugung (*prove*)

Entwurf: Protokollerweiterungen



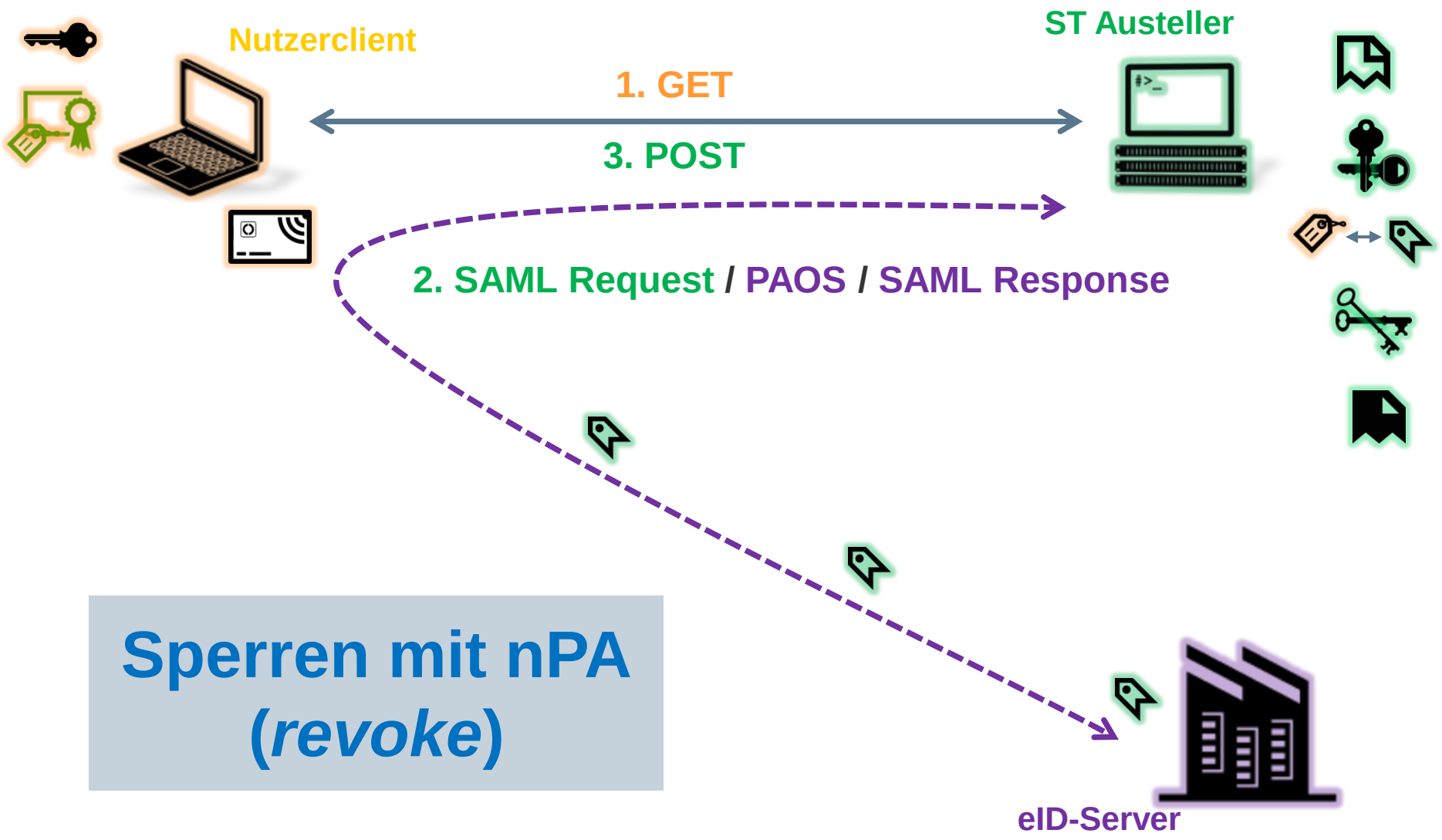
Nachweisverifikation (*verify*)

Entwurf: Protokollerweiterungen



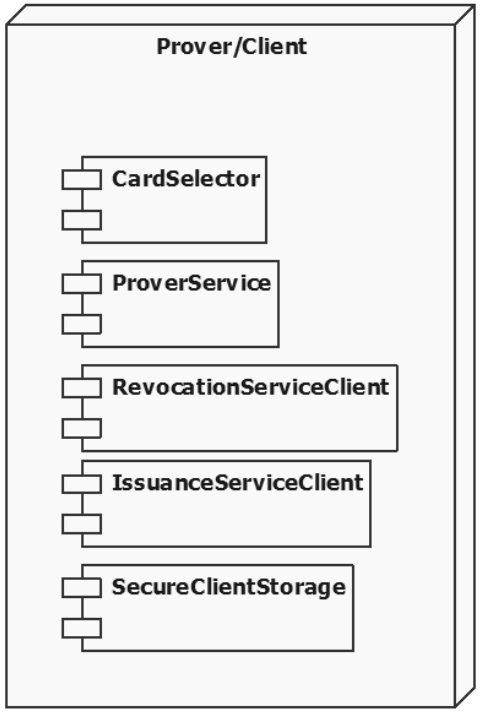
Sperren mit Zertifikat (*revoke*)

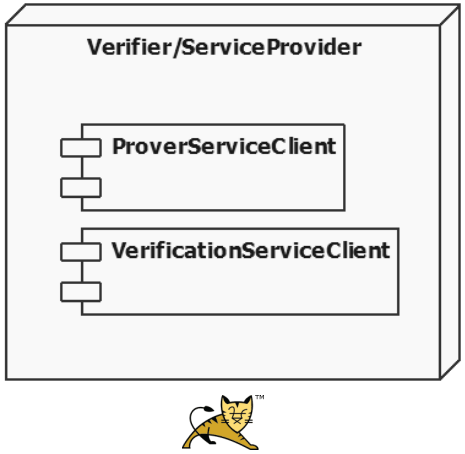
Entwurf: Protokollerweiterungen

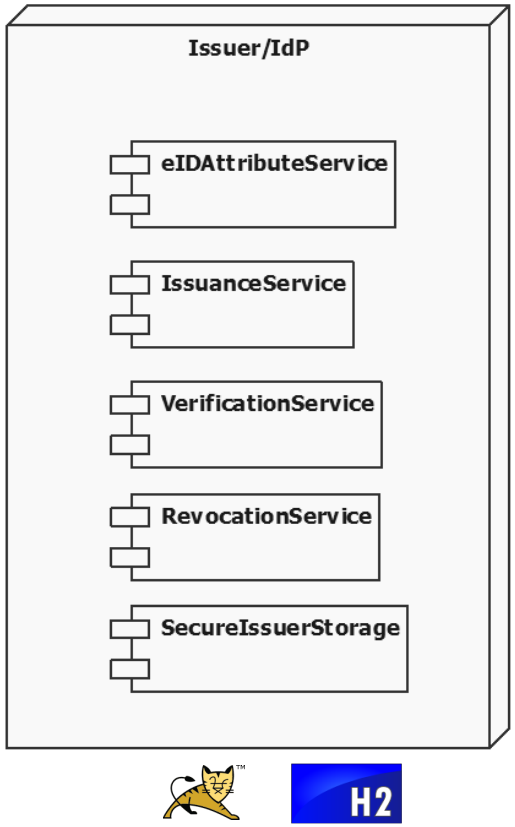


Sperren mit nPA (*revoke*)

Umsetzung: Komponenten / SW







- Testing mit JUnit
- Buildsystem maven
- Continuous Integration Jenkins
- Codemanagement SUBVERSION
- Codeanalyse PMD
- Basissprache Java
- Cryptobibliothek idemix

Inhalt

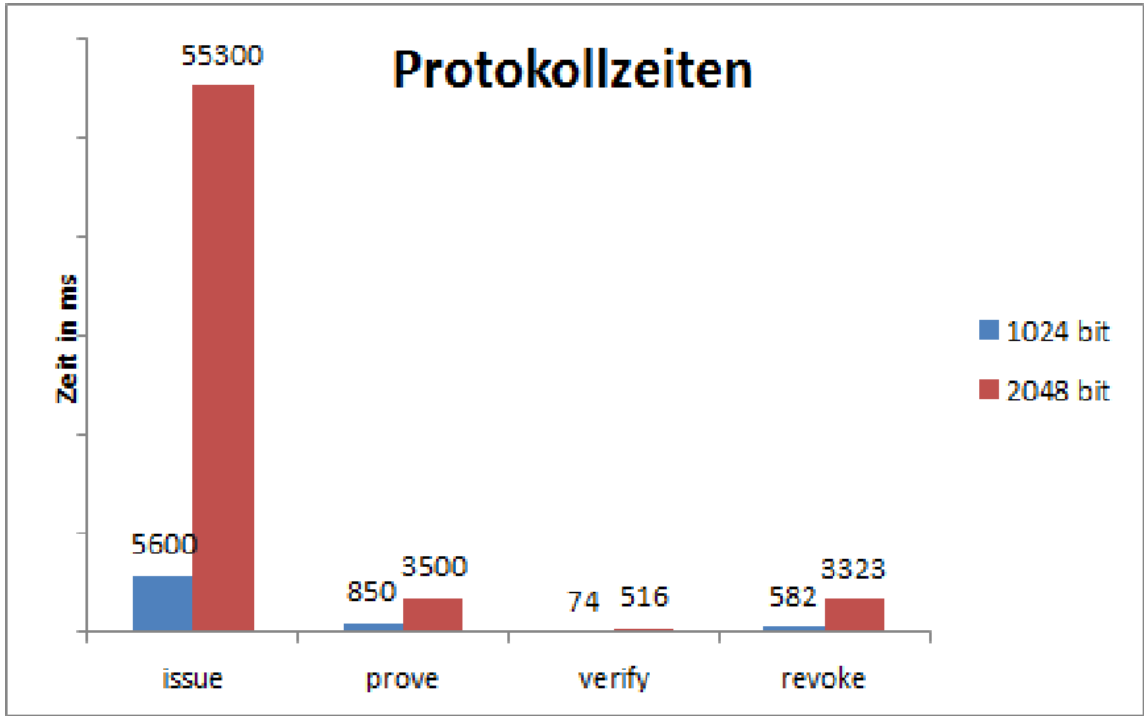
Freie Universität Berlin

1. **Einführung**
   - Arbeitstitel
   - Motivation
2. **Evaluation**
   - Kandidaten
   - AC Systeme
   - Hürden
3. **Entwurf & Umsetzung**
   - Protokolle
   - Komponenten / Software
4. **Fazit**
   - Rückblick
   - Ausblick

Rückblick: Messungen

Messungen

- Generieren von Ausstellerschlüsseln
- Generieren von VE-Schlüsseln
- Ver-/Entschlüsselung mittels VE
- Erzeugen von Nachweisen
- Protokolllaufzeiten



Rückblick: Herausforderungen

Freie Universität Berlin

- **Idemix – Mängel / erweiterte Funktionalität**
- **Unverschlüsselte Übertragung bei Protokollerweiterungen**
- **Zeitverhalten bei *issue*-Erweiterung**
- **Betrachtung von Mandantenmanagement (Aussteller)**
- **Sperren von Zertifikaten wenn Zertifikat/nPA nicht verfügar**
- **SSL-Zertifikat (Client), selbstsigniert und unsicher abgelegt**

Zusammenfassung/Ausblick

Freie Universität Berlin

Zusammfassung

„Einfaches, effizientes und vertrauenswürdiges Identitätsmanagement auf Basis von Software-Token“

- ✓ Software-basierte Token
- ✓ Authentizität der Identität
- ✓ Selektive Datenabfrage
- ✓ Einfache Integration
- ✓ Nutzerzentrische Datenhaltung

Idemix

- Weiterentwicklung im Kontext von https://abc4trust.eu/
- Kooperation u.a. von Microsoft und IBM zur Integration von U-Prove und Identity Mixer

Projektresultate

- Temporär verfügbar unter http://userpage.fu-berlin.de/kazcor/thesis
- Optimierung und Dokumentation vor Veröffentlichung (BSD-Lizenz)

Ende

Freie Universität Berlin

DANKE!