TeleTrusT/VOI-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 23.09.2021

SSI mit Blockchain - the chain of trust

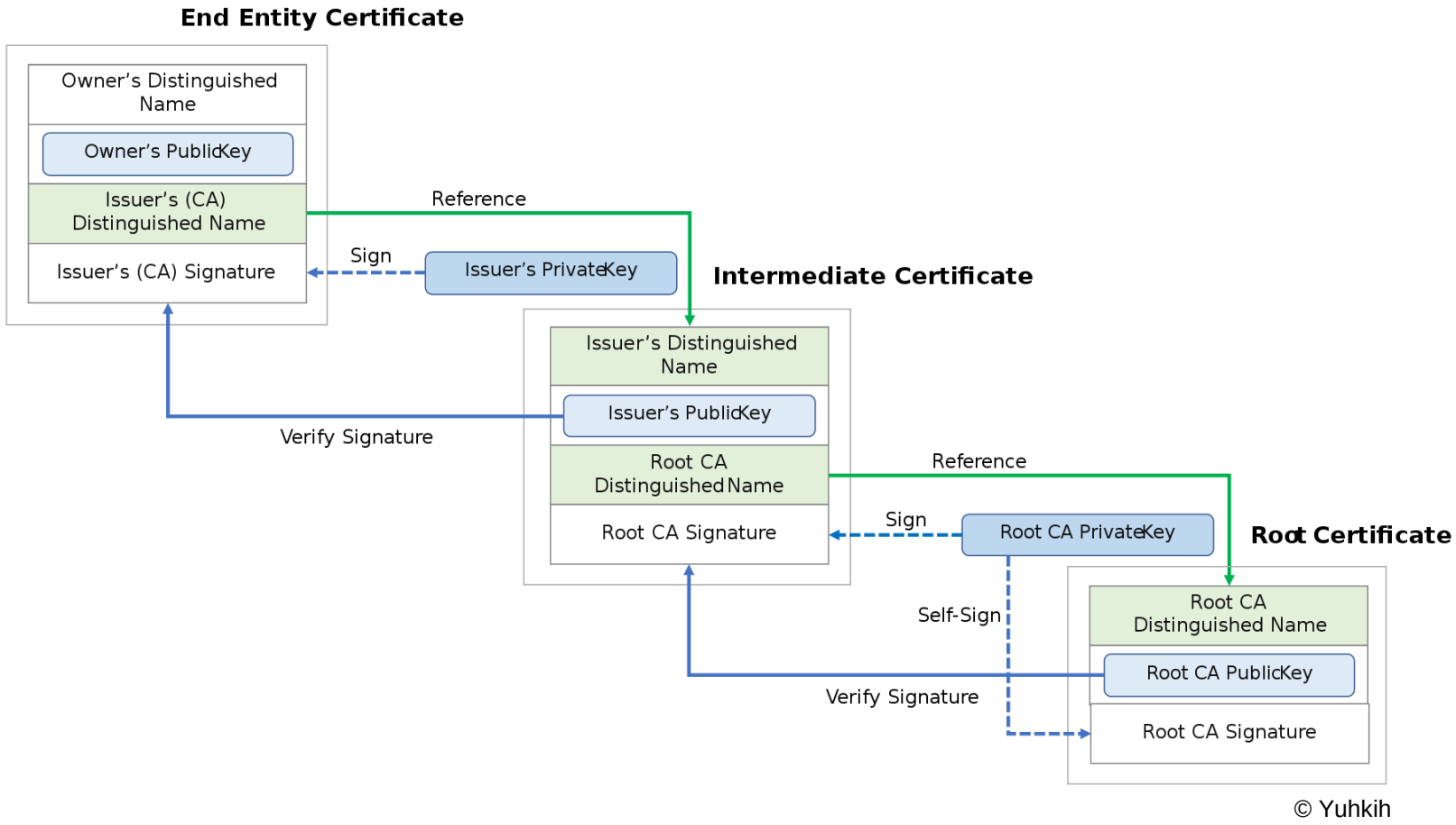
Mirko Mollik, TrustCerts GmbH

Web of Trust

- Keine Hierarchie oder Regeln
- Vertrauen durch Bestätigung anderer Teilnehmer
- Ungeeignet für kritische Anwendungsfälle

© XKCD

Chain of Trust

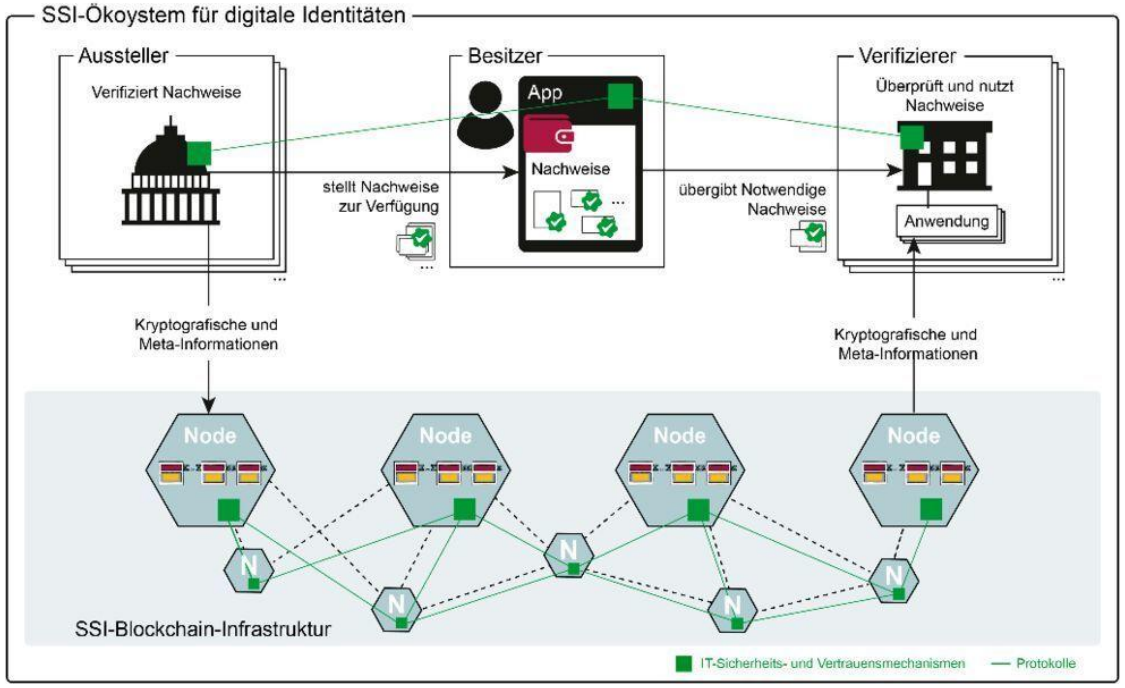


Heutige Nutzung

- Bekannte Protokolle: TLS/SSL für HTTPS
- Standardisierte Zertifikate: X.509
- Klare Definition der Verantwortung = hohe Sicherheit

Grundgedanke von SSI

- Selbstbestimmung bei der Datenweitergabe
- Verifizierung der Daten durch Prüfer
- Nutzt Verifiable Data Registry
  - Dezentrales Key Management System



© Norbert Pohlmann

Validierung der Signatur

- Ist die Signatur gültig?
  - Sicherheitsniveaus der Algorithmen (JWS, BBS+, CL) sind unterschiedlich
- Prüfung der Signatur mit öffentlichem Schlüssel
  - Algorithmus muss lokal unterstützt sein

Validierung der Signatur

- Ist der Schlüssel noch gültig?
  - Did Dokumente sind dynamisch
  - Updates statt Sperrregister

- Abfrage des Dokumentes gegen die Blockchain
  - did:trust:tc:prod:id:HWyGj5NtDH5zx5hUFHZCae?versionTime=2017-06-18T21:19:10Z

Validierung der Signatur

- Sind Issuer und Signer identisch?
  - JSON-LD macht keine Validierungs-Logik
- Vergleich der Werte
  - Falls ungleich, gibt es eine Policy dafür?

Validierung der Signatur

- Wurde der korrekte Schlüssel verwendet?

- Prüfung der Verification Relation im Did Dokument
  - Schlüssel mit Attestation-Relation

Validierung der Signatur

- Hat der Aussteller das Recht diesen Nachweis auszustellen?
  - 1 Blockchain = 1 Use Case ist zu teuer!

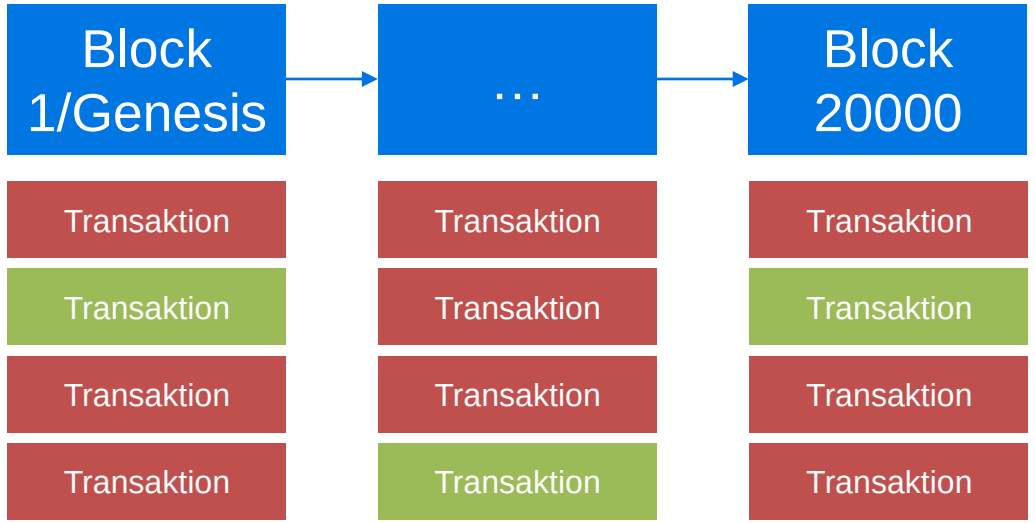
- Autorisierungs-Register
  - Chained-Credentials als Alternative

Validierung der Signatur

- Wer hat die Identität des Ausstellers bestätigt?
  - Blockchain wird nicht privat, sondern im Konsortium betrieben
- Validierung des Ausstellers des Ausstellers
  - Wer im Konsortiums hat die Identität bestätigt?

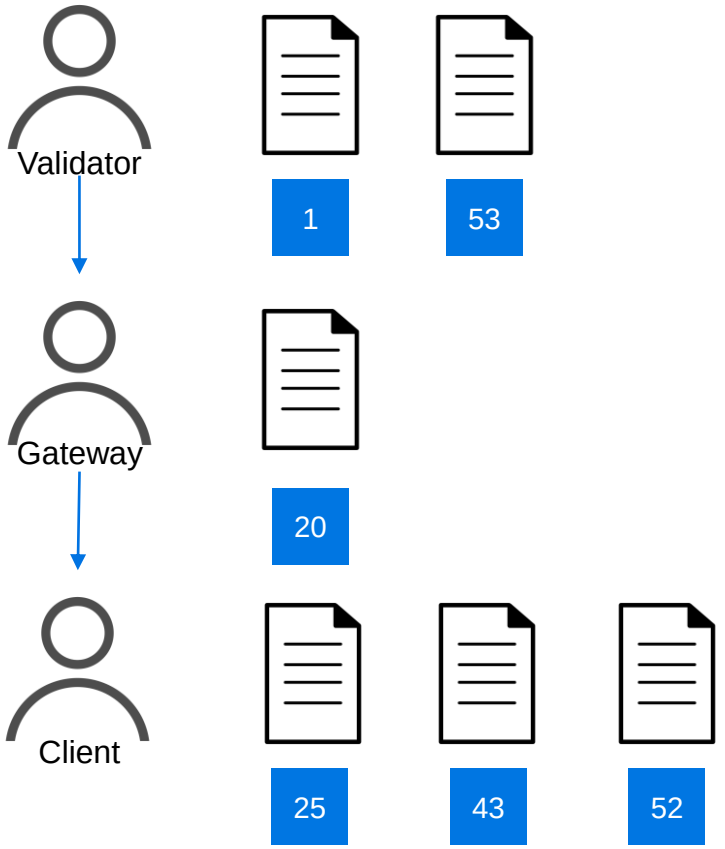
Herleitung der Chain of Trust

- Trust Anker: Genesis Block
  - Muss lokal vorliegen
- Ziel: Weg von Behauptung zum Genesis Block
  - Ganze Blockchain lokal validieren ist möglich, jedoch ineffizient
- Idee: Validierung der relevanten Transaktionen



Validierung der Identitäten der Kette

- Validierung aller Transaktionen
  - Client > Gateway > Validator
- Überprüfung der Validatoren
  - Ersteller der Blöcke, wo die Transaktionen enthalten sind
  - Prüfer der Transaktionen



Validierungs-Performance

- Identitäten können viele Transaktionen verursachen
  - Key-Rotation
- Transaktion-Signatur
  - Signiert die Änderungen
- Did Doc Signatur
  - Signiert IST-Zustand

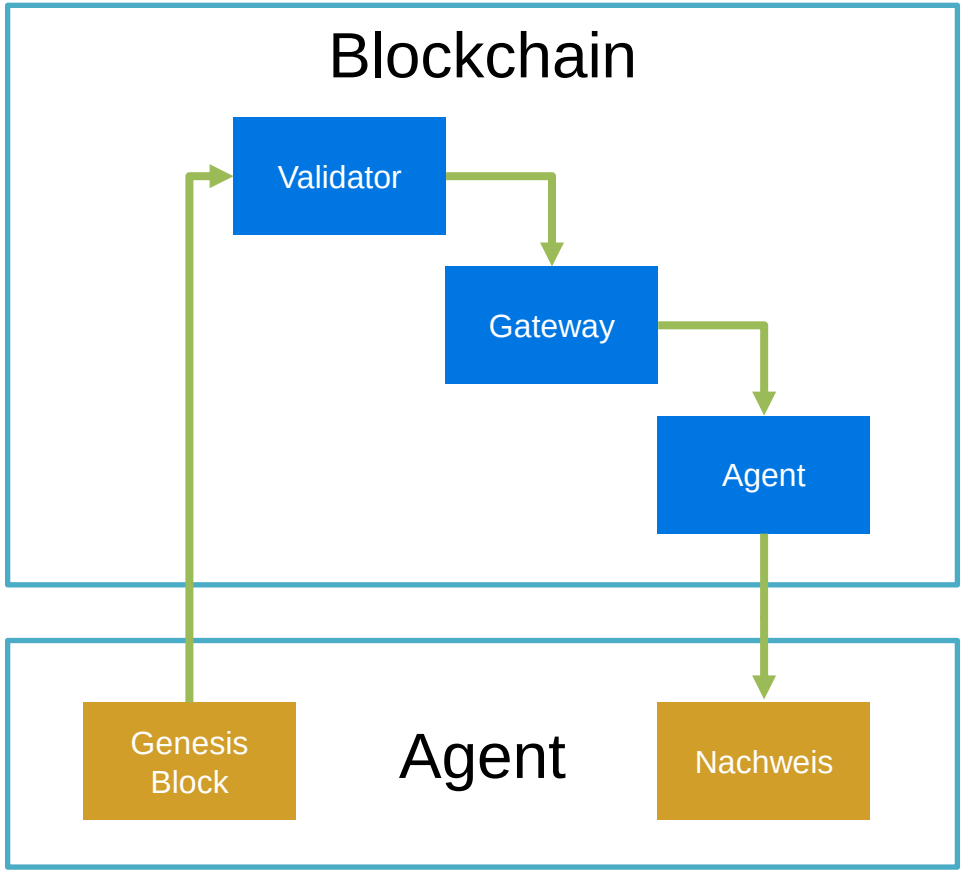

```
"signature": [
  {
    "identifier": "did:trust:tc:dev:id:HWyGj5NtDH5zx5hUFHZCae#9wYcm6qBk2L5JNRnzbiGLvyd1vkBWArTuUeC9JYGHcNd",
    "signature": "2ieLpfpUM81Zf6WD59VZemW6JacgkSjhP1EGvRqZtvEx78vnpsKf3Ye73coBKx4EdEdowLjnzDjkhfeW6a3rYZPnJ8V
cJ5dAxTP9kVbNCdxzyeX5e5jADn8zmGr88vzZrm3KMsL4kT1KGxV27S5iACMiKV9NF9q3qNZxsgP2S5q6Ds6ZsTaSHYtpyHiyXbzS6pFV6HepM
  }
],
"didDocumentSignature": [
  {
    "identifier": "did:trust:tc:dev:id:HWyGj5NtDH5zx5hUFHZCae#9wYcm6qBk2L5JNRnzbiGLvyd1vkBWArTuUeC9JYGHcNd",
    "signature": "35e7vUXeu717YM5uRj9YpyHFM7zAmUTDczRmz5C6psHzffbecoy5LxrS9mJnRwey8CS5f1H6JqGHrwFeHJQwtm6n73V
h6kgvrYogmiB6aR9YwQty3jXYqPASiE116kCFZ74YJt8evbd5DVTnJeZbWZ5acvr9GDoW5mJns1Ni2FWs8zZZBbLgLkKCgmLHqp8ao6UNAiM6v
  }
],
"values": {
  "id": "did:trust:tc:dev:id:HWyGj5NtDH5zx5hUFHZCae",
  "role": {
    "add": [
      "validator"
    ]
  },
  "service": {
    "add": [
      {
        "id": "did:trust:tc:dev:id:HWyGj5NtDH5zx5hUFHZCae#name",
        "endpoint": "undefined/did/resolve/did:trust:tc:dev:id:HWyGj5NtDH5zx5hUFHZCae",
        "type": "resolver"
      }
```

Chain of Trust

Genesis-Block = Root-Zertifikat

Nachweis = Behauptung

Falls gültige Chain of Trust =
Nachweis > Verifizierbarer Nachweis



Passende Blockchains

Bitcoin

- Größtes Netzwerk
- keine Ablage von Identitäten möglich

Ethereum

- Ablage von freien Daten
- Herleitung nur innerhalb des Smart-Contracts

Passende Blockchains

Hyperledger Indy

- Ablage der DIDs in Registern
- keine Chain of Trust

TrustChain

- Register für DIDs für alle Teilnehmer
- Überprüfbare Vertrauenskette

Alternativen

- Full Node
  - Daten werden bei Erhalt einmalig validiert
  - Jeder Stakeholder muss die ganze Blockchain haben

- Mehrere Knoten nach Ergebnis fragen
  - „Wenn X redundante Systeme die gleiche Antwort geben, muss es stimmen“
  - Nicht robust gegen MITM Angriff

Zusammenfassung

- Root Zertifikat = Genesis Block
- Komplette Validierung durch Signaturprüfung möglich
- (Noch) nicht eIDAS kompliant

Vielen Dank für
Ihre Aufmerksamkeit!