

TeleTrust/VOI-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 20.09.2022

SSI mit Blockchain in Deutschland - ein Review der letzten Monate und Ausblick

Mirko Mollik, TrustCerts

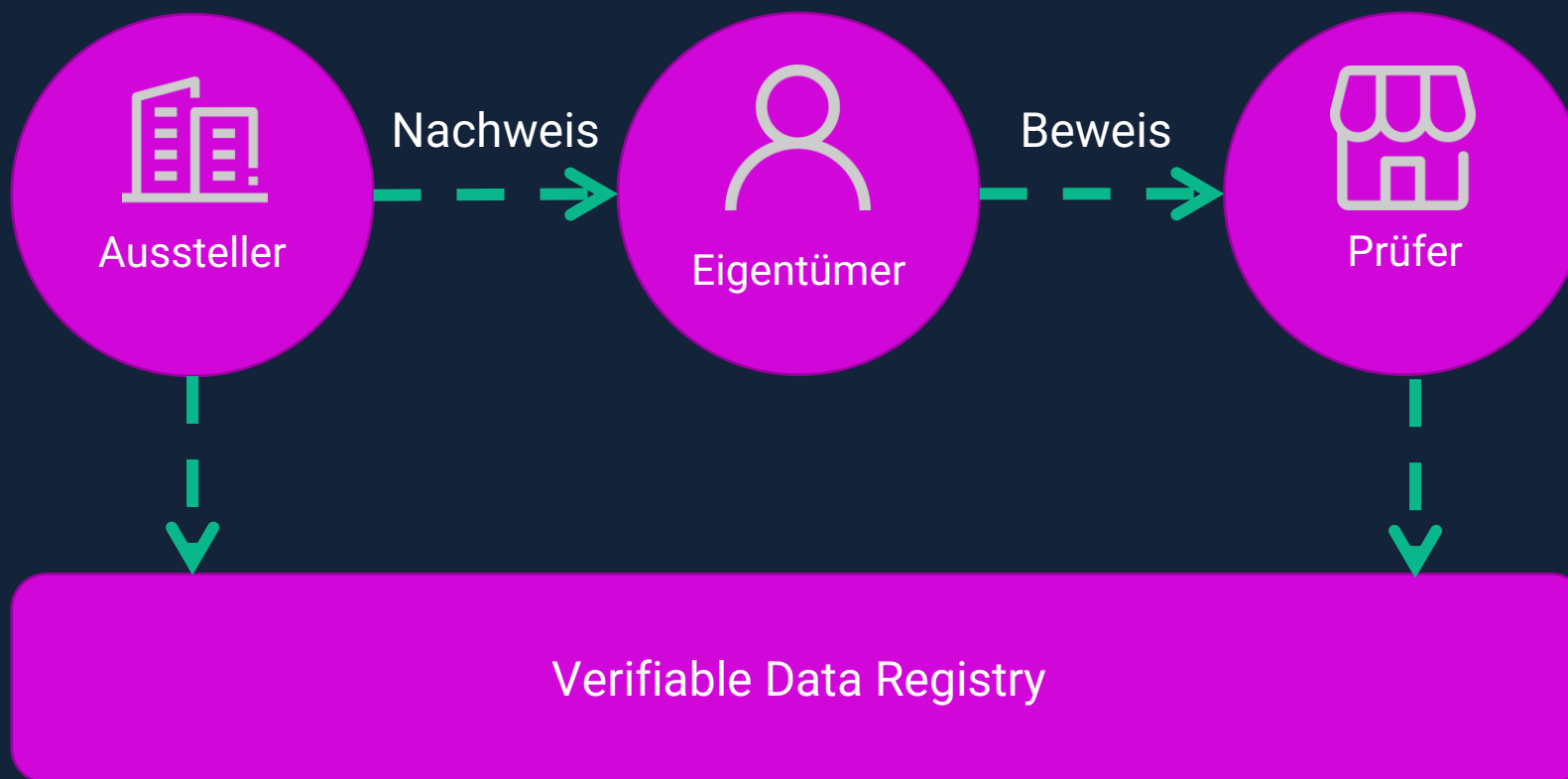


Self Sovereign Identity



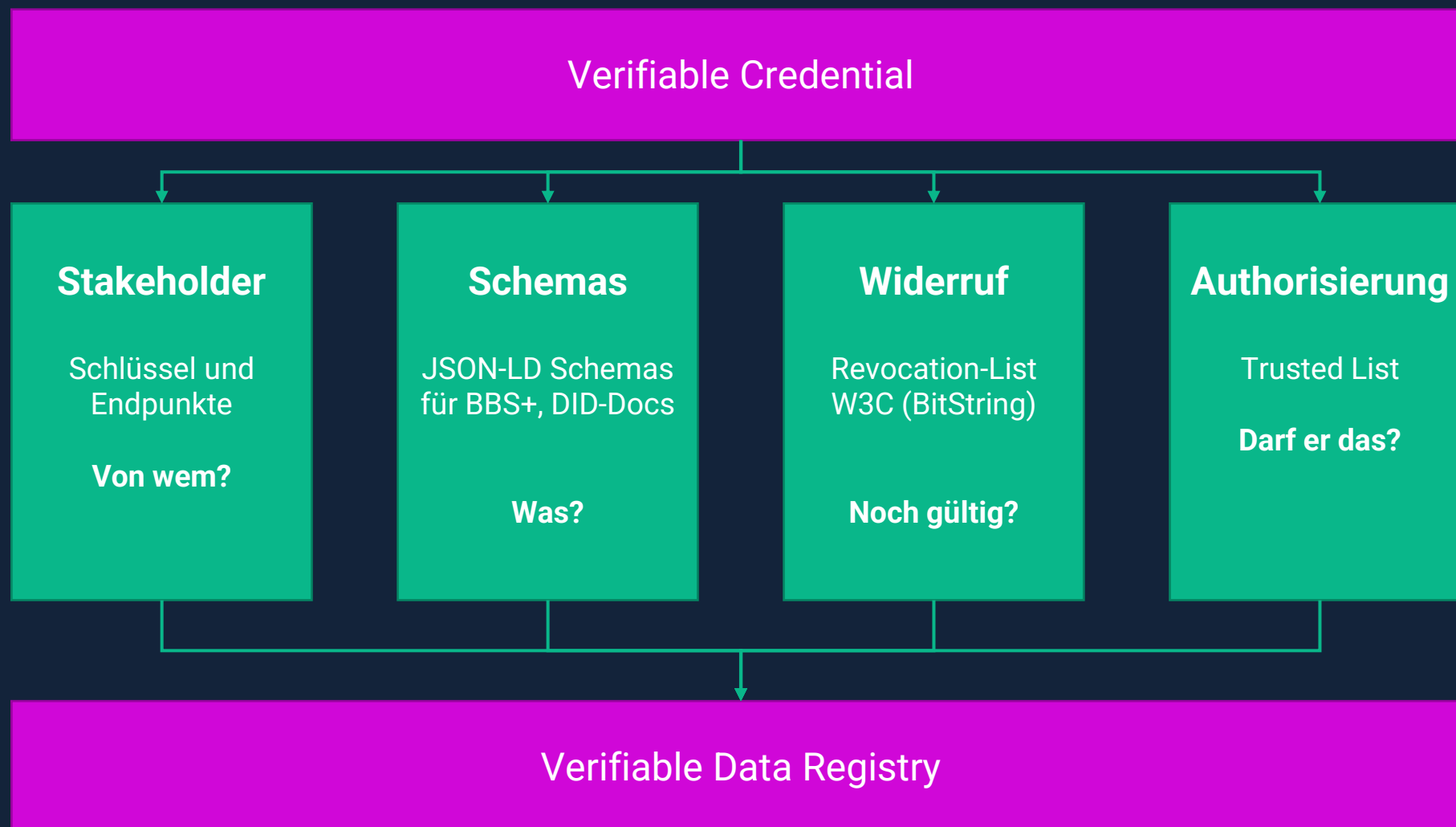


Verifiable Data Registry





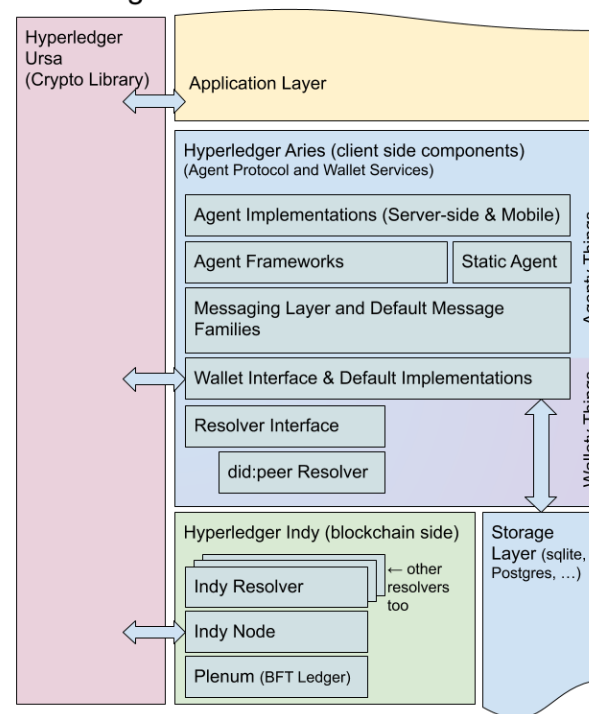
SSI Komponenten





Blockchain ist kein Muss für SSI

Hyperledger as a Verifiable Information Exchange Platform





Soll es genutzt werden?

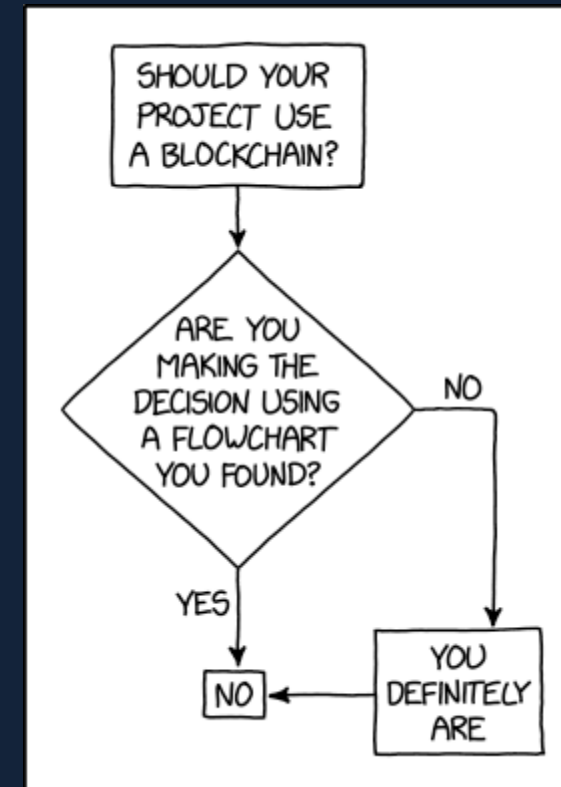
Pros

Kein Single Point of Control/Failure

Hoher Schutz der Privatsphäre

Interoperabel

Cons



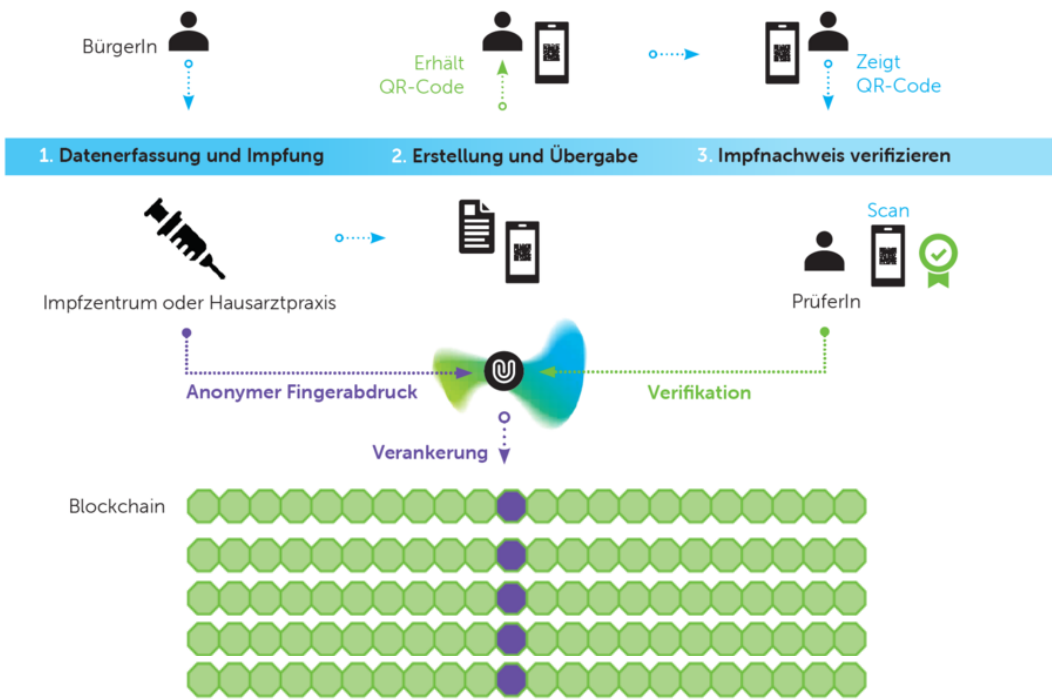


Q1 2020: wir brauchen Impfpass

Let's use blockchain!



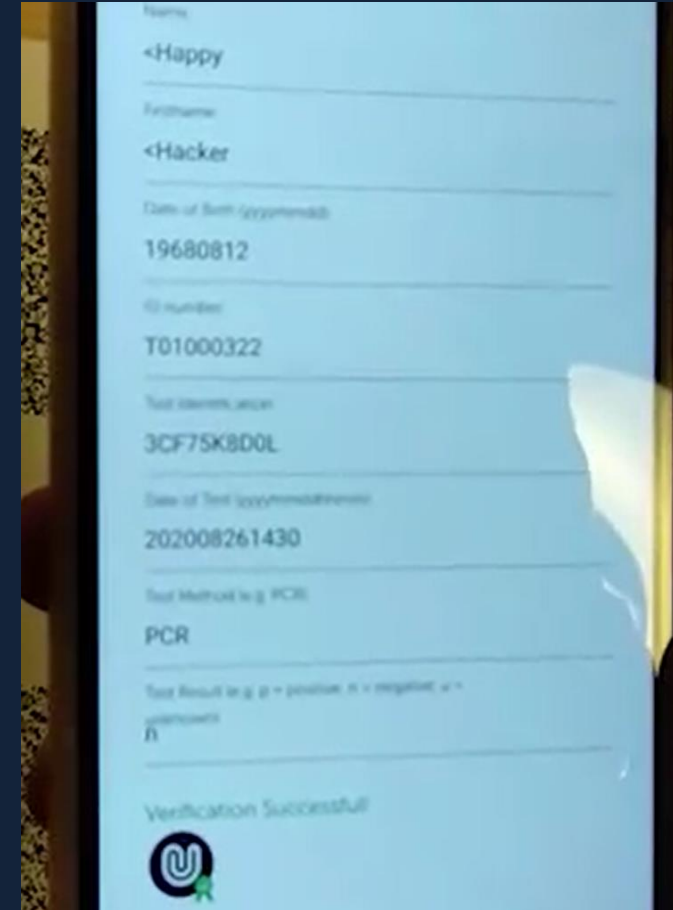
Single point of failure vor der Redundanz





Vaccinated by:

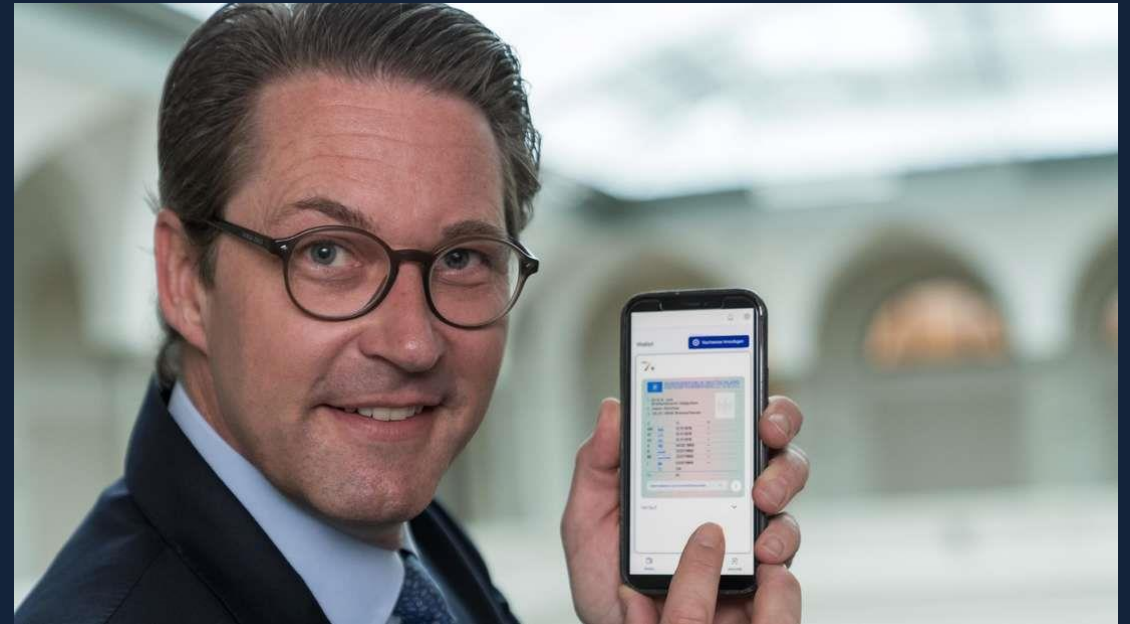
- needle injection
- code injection





Q3 2021: wir
brauchen einen
mobilen
Führerschein

Let's use
blockchain!





Kontrolliere die Weitergabe deiner Daten, die übertragen werden





Keine Verifizierung des Empfängers

```
{
  "@type":
  "did:sov:BzCbsNYhMrjHiqZDTUASHg;spec/connections/1.0/invitation",
  "@id": "a0074e30-9249-4455-b74e-2ca1328586e1",
  "label": "Teletrust",
  "serviceEndpoint": "https://demo-agent.institutional-agent.hacker.com/didcomm/",
  "imageUrl":
  "https://routing.example.io/api/Image/demoMusterhausen",
  "recipientKeys": [

    "3hb8MYnMjGY5EoAAmnmvA9jjiqacxFgAax4eXvmJuiG9mC"

  ]
}
```



Massive Sicherheitslücken in der BC

DOS des Netzwerkes

- CVE-2022-31006 (7.5/10)
- Ausnutzung der Firewallregel

1 Smartphone vs. mehrere leistungsstarke
Server

Distributed code execution

- CVE-2022-31020 (10/10)
- Fehler in der Implementierung der Validierung

Automatische Lösung aller Datensätze



Q1 2022: wir
brauchen digitale
Zeugnisse!

Let's use
blockchain!

DIGITALES ZEUGNIS

**Einfach,
fälschungssicher und
datenschutzkonform**



bdr.

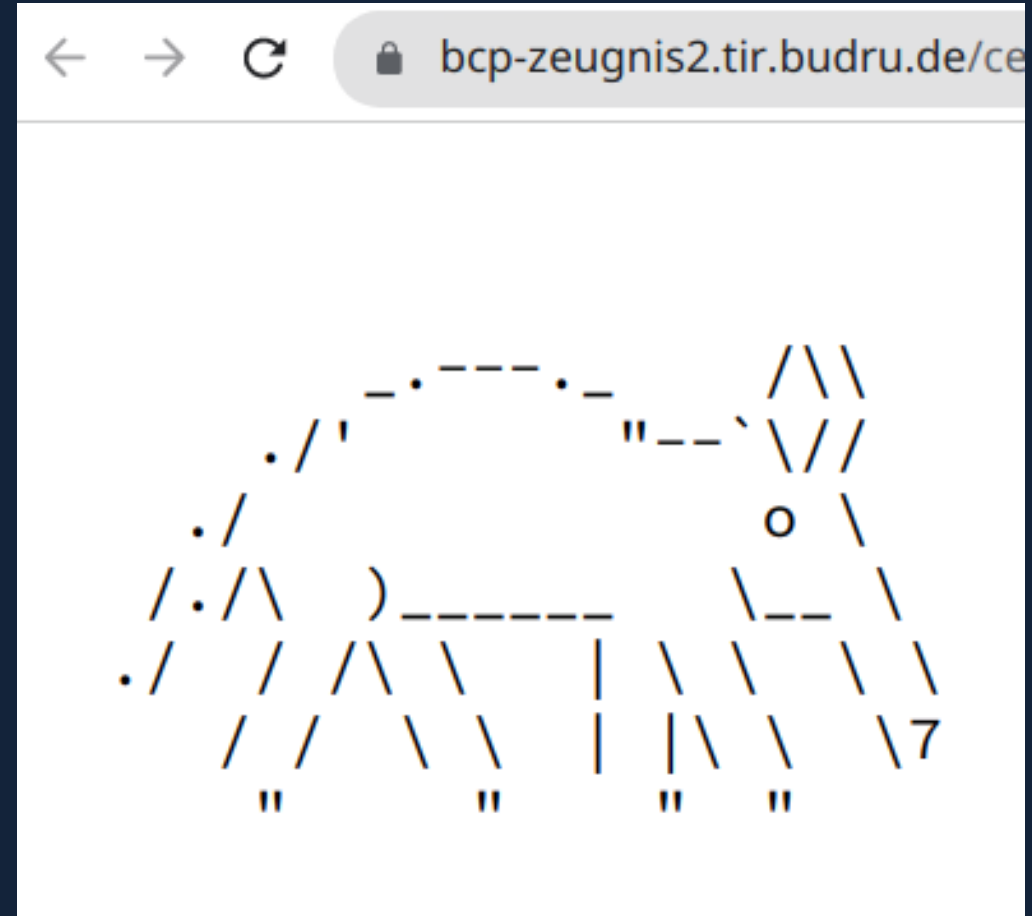




Inkl. XSS

```
https://bcp-  
zeugnis2.tir.budru.de/central/v2/authority/ge  
tAuthority?authorityAddress=<script>alert('bl  
ockhain.wtf');</script>
```

The fix:





Learnings

Veröffentlichen Sie keine
Testumgebung für die ganze Welt!

Ist es nützlich oder Buzzword?

Verstehen der Technologie

BC ist nicht battle proved



Ein neuer Ansatz



founding members



further founding members in 2022s



interested partners



Build on standards





Vielen Dank für Ihre Aufmerksamkeit



Mirko Mollik

+49 (0) 209 883 067 51

mollik@trustcerts.de