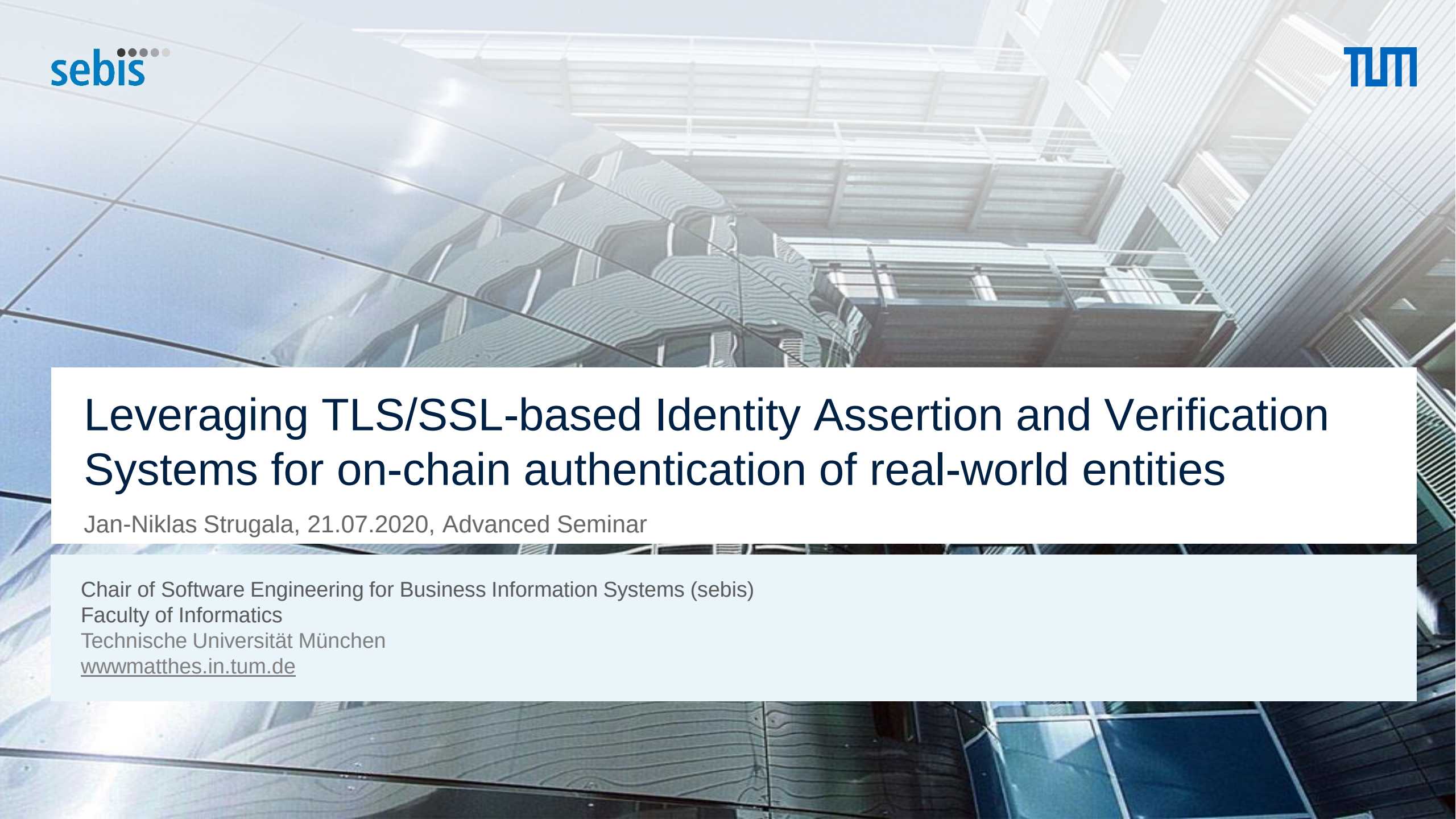


Leveraging TLS/SSL-based Identity Assertion and Verification Systems for on-chain authentication of real-world entities

Jan-Niklas Strugala, 21.07.2020, Advanced Seminar

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
wwwmatthes.in.tum.de

Outline

1. Motivation
2. Background
3. Research Objective & Questions
4. Roadmap

Motivation

Goal of Authentication
Identify an individual that wants to sign into a restricted application

Web 2.0
Many standards as OpenID Connect

Blockchain
No authentication standards

Motivation

Goal of Authentication
Identify an individual that wants to sign into a restricted application

Web 2.0
Many standards as OpenID Connect

Blockchain
No authentication standards

…but
who endows **the application** the user is authenticating at with trust

Web 2.0
TLS/SSL certificate infrastructure

Blockchain
No trust endowment

Motivation

Goal of Authentication
Identify an individual that wants to sign into a restricted application

Web 2.0
Many standards as OpenID Connect

Blockchain
No authentication standards

…but
who endows **the application** the user is authenticating at with trust

Web 2.0
TLS/SSL certificate infrastructure

Blockchain
No trust endowment

Problem Statement

No sophisticated standard for authenticating third parties on the blockchain

TLS/SSL certificate were not developed to actively authenticate entities

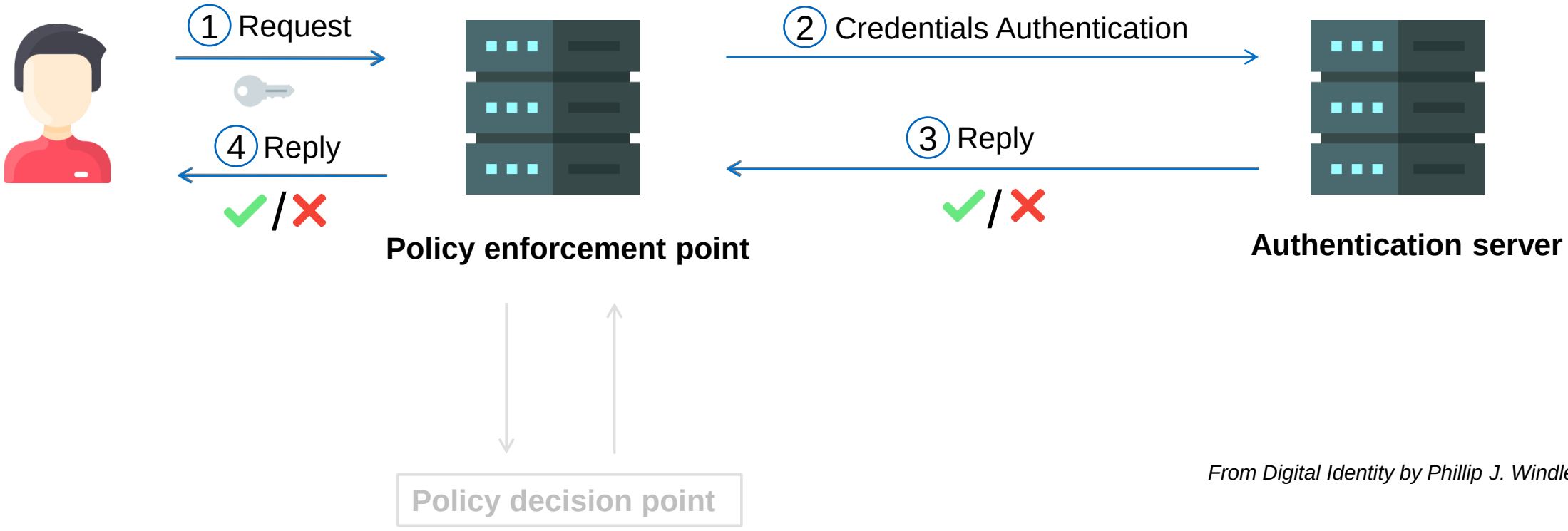
Outline

1. Motivation
2. Background
3. Research Objective & Questions
4. Roadmap

Authentication

Authentication:
"The act of proofing who you are"

Authorization:
"The act of granting someone access"

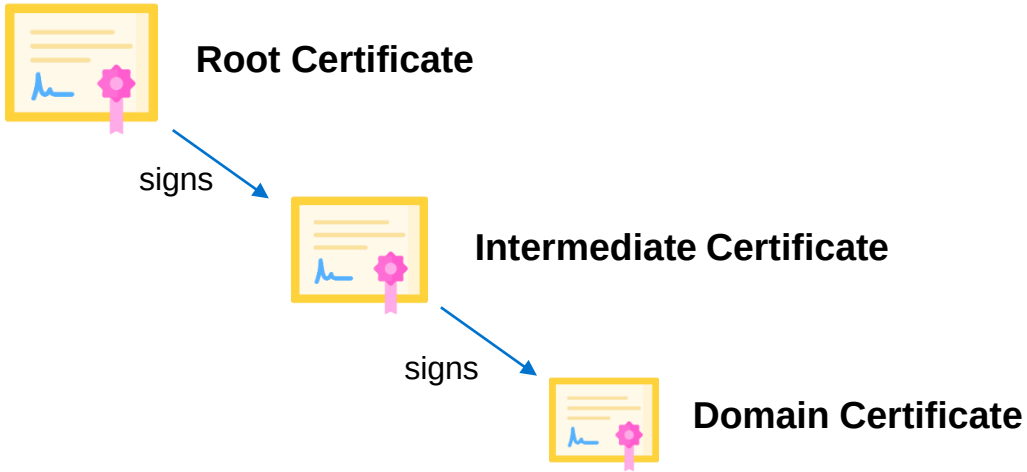


From Digital Identity by Phillip J. Windley

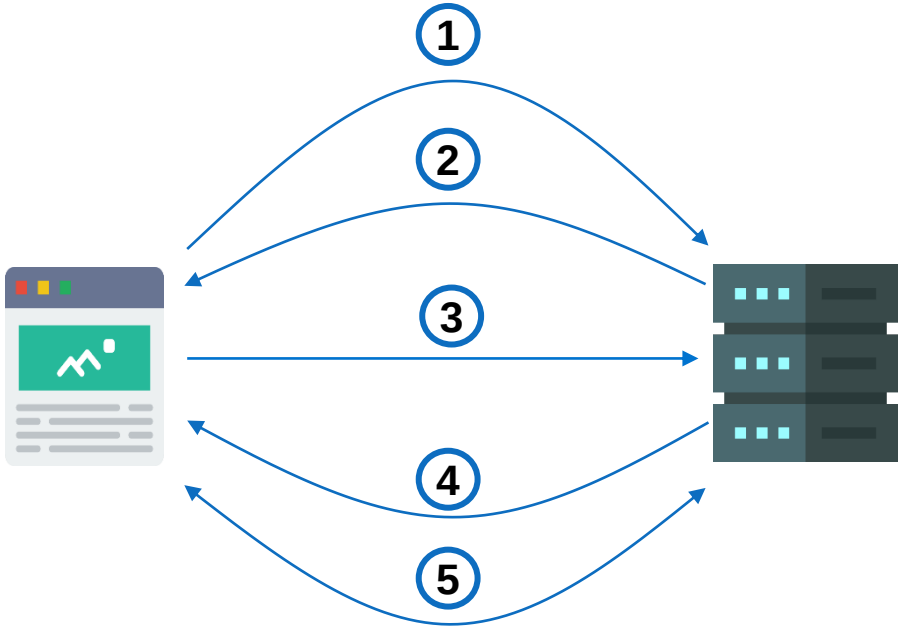
Secure connections with TLS, X.509 Certificates and PKI

1. Browser requests identification
2. Server provides TLS/SSL certificate + public key
3. Browser checks certificate
   - **Root Cert** on list of **trusted Root Certs?**
   - Matching domains?
   - Current date < Expiry date?
   - Certificate not revoked?

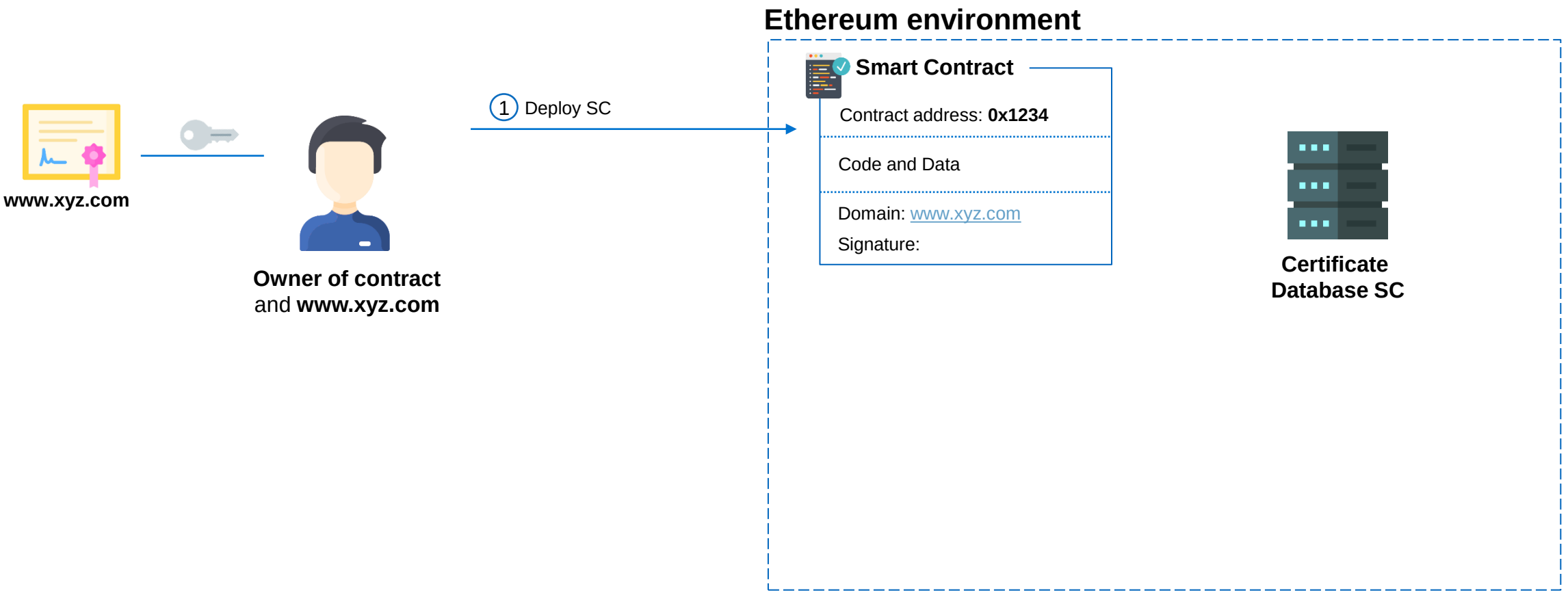
   Responds with encrypted session key by public key



4. Server decrypts message + responds with message encrypted by the session key
5. Encrypted session

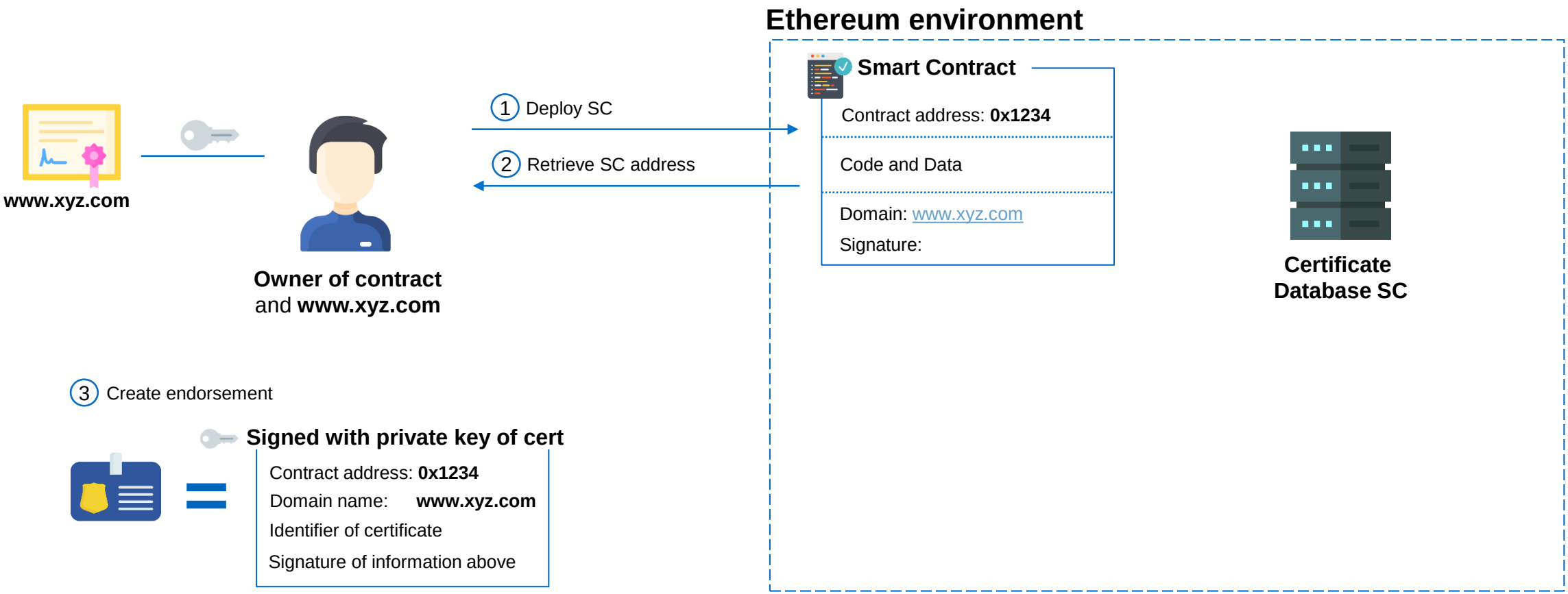


Current System: TLS/SSL-based Identity Assertion and Verification System



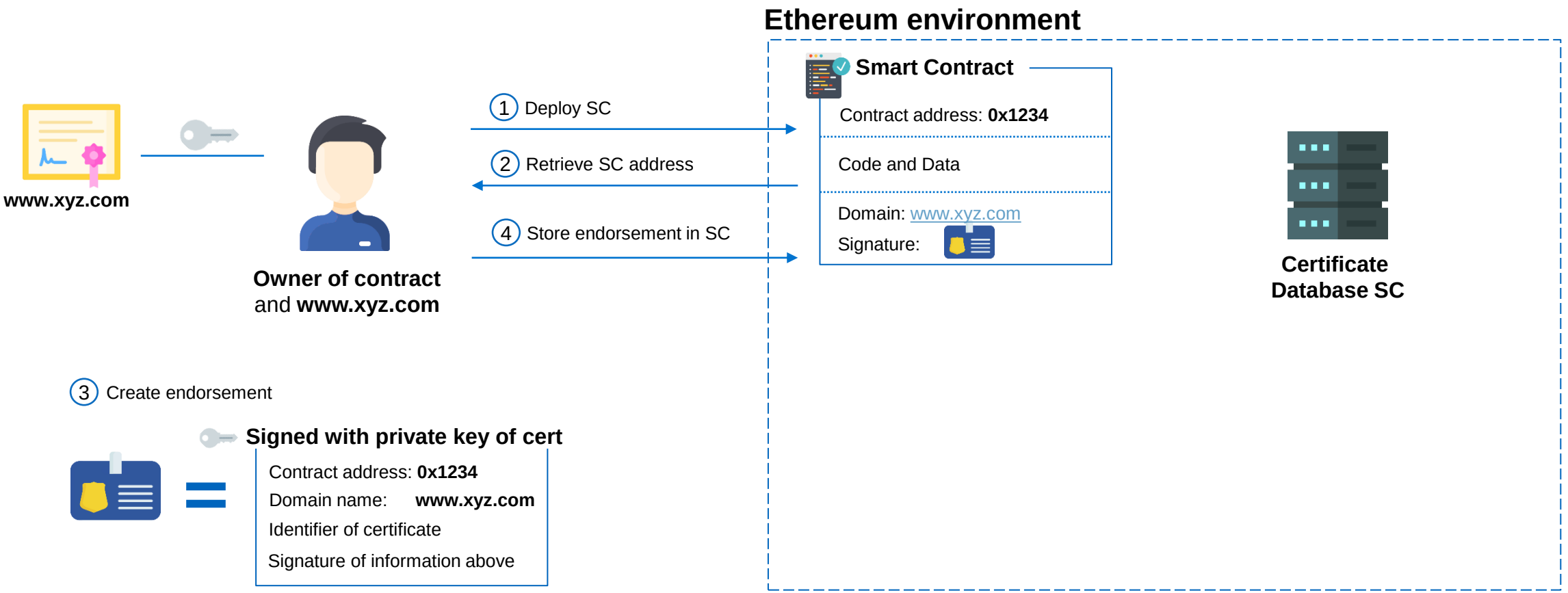
From MT Friederike Groschupp

Current System: TLS/SSL-based Identity Assertion and Verification System



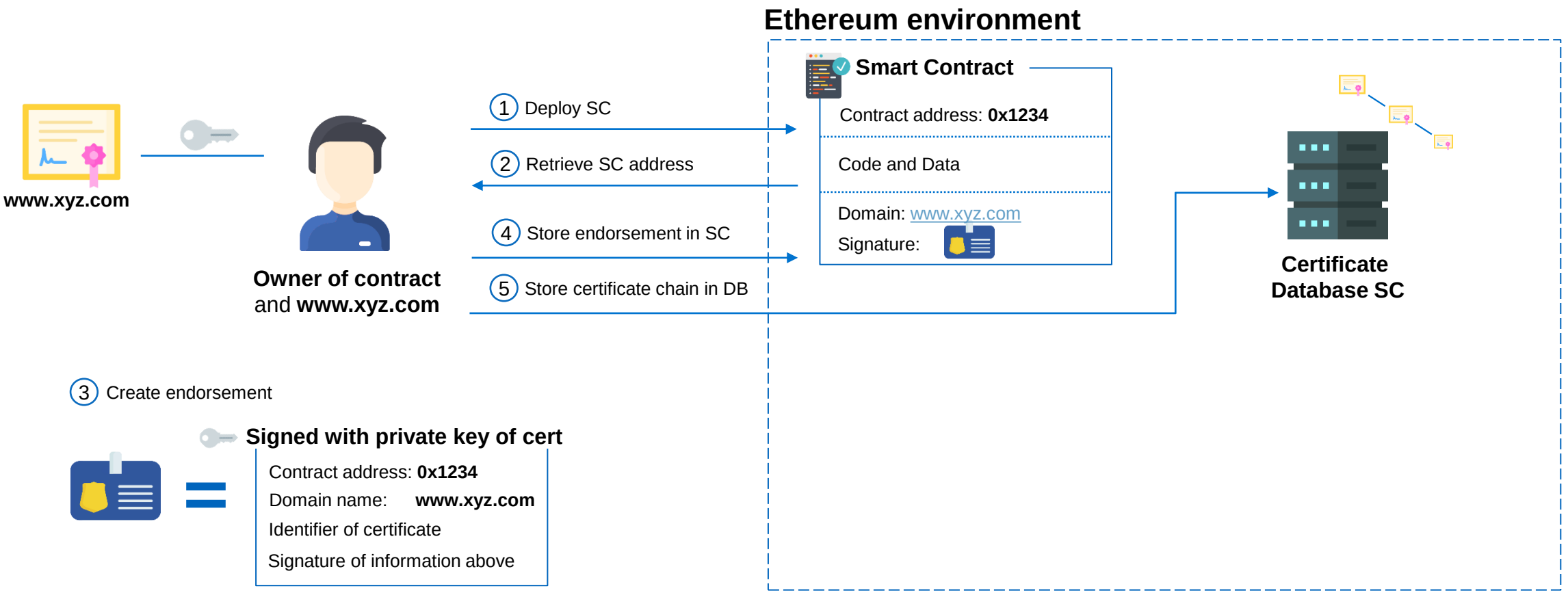
From MT Friederike Groschupp

Current System: TLS/SSL-based Identity Assertion and Verification System



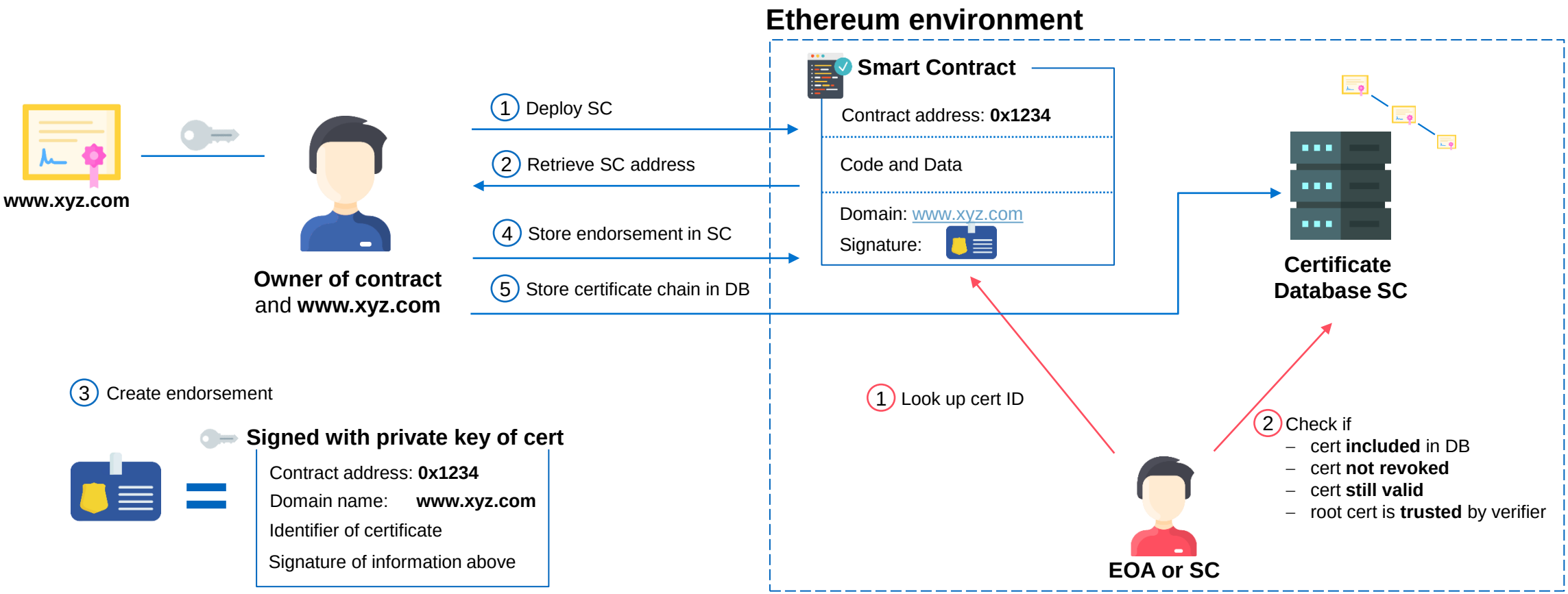
From MT Friederike Groschupp

Current System: TLS/SSL-based Identity Assertion and Verification System



From MT Friederike Groschupp

Current System: TLS/SSL-based Identity Assertion and Verification System



From MT Friederike Groschupp

Outline

1. Motivation
2. Background
3. Research Objective & Questions
4. Roadmap

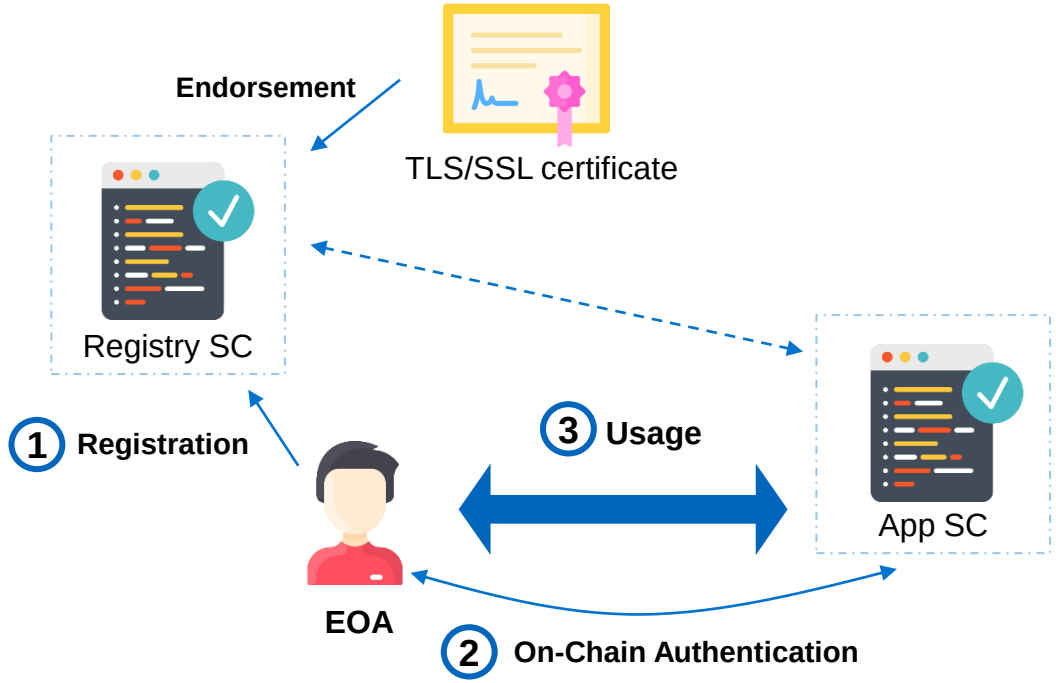
Research Objectives

Improve the **TLS/SSL-based Identity Assertion and Verification System** by adding trustless authentication

A. Exploration and analysis of the Web 2.0 and Blockchain authentication protocols and applications

B. Development of a system which allows:

- **registration** of identities at SC endorsed by TLS/SSL certificates
- **authentication** of identities at App SC, which is **related** to the Registry SC
- **trustless**, **on-chain** authentication



C. Evaluation of System

Research Questions

R1 Which are the major authentication practices and technologies?

R2 How can a TLS/SSL-based identity assertion and verification system contribute trust to authentication?

R3 How can we achieve on-chain authentication of real-world identities considering the constraints of Blockchain?

Research Questions

R1 Which are the major authentication practices and technologies?

R1.1 Which authentication practices and technologies are relevant in the Web 2.0?

- Login with username and password
- Application of tokens for user sessions
- Federated solutions enabled by OAuth 2.0 and OpenID Connect (e.g. “Login with Google”)
- Centralization of user data at “trusted” 3rd parties
- Enhanced security through multi-factor authentication

R 1.2 Which authentication practices and technologies are relevant in Blockchain?

- Login with Username and password
- Whitelisting of accounts
- Few attempts to trustless authentication

Research Questions

R2 How can a TLS/SSL-based identity assertion and verification system contribute trust to authentication?

R2.1 How do existing systems which apply TLS/SSL-based identity assertion execute authentication?

R2.2 Which of its properties endow a TLS/SSL certificate with an increased level of trust?
- Link to a chain of trust?

R2.3 What are challenges of bootstrapping a TLS/SSL-based identity assertion and verification system?

Research Questions

R3 How can we achieve on-chain authentication of real-world identities considering the constraints of Blockchain?

R3.1 What is the application life-cycle of a potential on-chain authentication solution?

R3.2 Which are the constrains of Blockchain that affect the development of our solution?
- Limited transaction throughput?
- Transaction costs?

R3.3 What are potential system designs for an on-chain authentication solution?

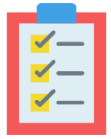
R3.4 What are the advantages and disadvantages of the different system designs?

Outline

1. Motivation
2. Background
3. Research Objective & Questions
4. Roadmap

Methodology

Literature Review with focus on Web 2.0 authentication protocols, considering emergent developments in the Blockchain environment



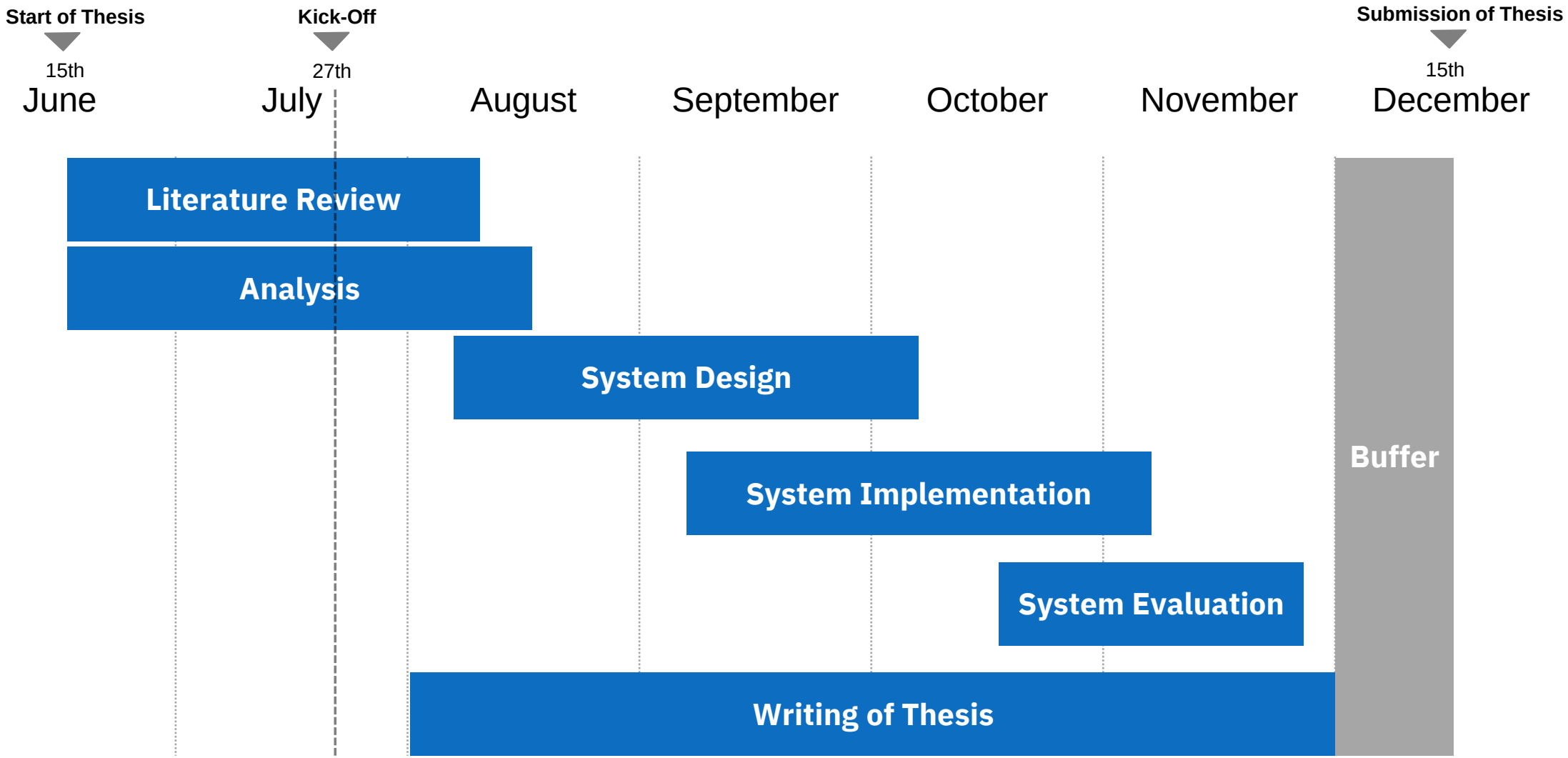
Analysis of authentication environment and definition of system requirements

System Design

System Implementation

System Evaluation

Timeline



Prof. Dr.

Florian Matthes

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289. 17132
Fax +49.89.289.17136

matthes@in.tum.de
wwwmatthes.in.tum.de

Motivation

Web 2.0

Authentication of real-world identities online is dominated by **isolated** and **centralized** solutions

Challenges

Privacy issue

Single-Point of Failure

Centralization of Power

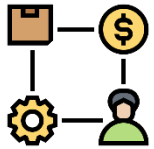
Idea
Leverage the Blockchain

Blockchain

Authentication on the Blockchain is not straight forward

Challenges

Limited Trust



High set-up cost

Barriers of entry

Potential Solution
Use the established TLS/SSL certificate infrastructure to overcome the limited trust and usability in a decentralized system

Problem Statement

No sophisticated standard for authenticating third parties at smart contracts

No registration and authentication of third parties in the current system

The developers of the TLS/SSL certificate infrastructure did not have our use-case in mind