

# Exploring the Use of SSL/TLS Certificates for Identity Assertion and Verification in Ethereum

Friederike Groschupp, December 16, 2019, Kick-Off Presentation

Chair of Software Engineering for Business Information Systems (sebis)  
Faculty of Informatics  
Technische Universität München  
[www.matthes.in.tum.de](http://www.matthes.in.tum.de)

1. Motivation

2. Background Information and Current System

3. Problem Statement and Goal of Thesis

4. Research Questions

5. Approach



Identification of entity and address owners on Ethereum promotes trust in information and services provided



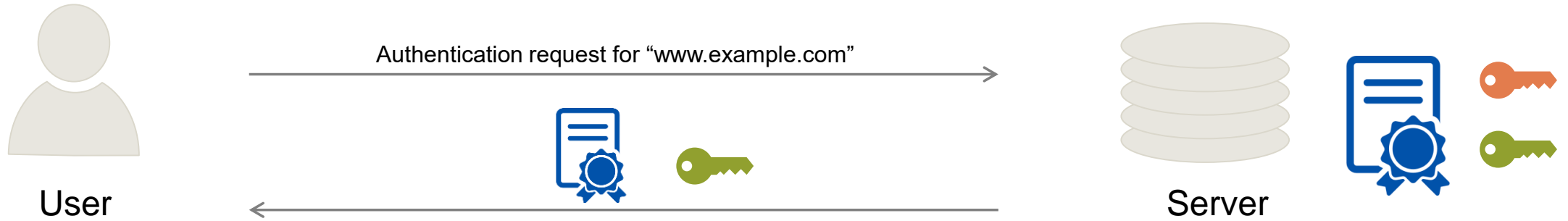
Identity solutions for Ethereum are adopted only slowly

- High entry costs
- Dependence on network effects

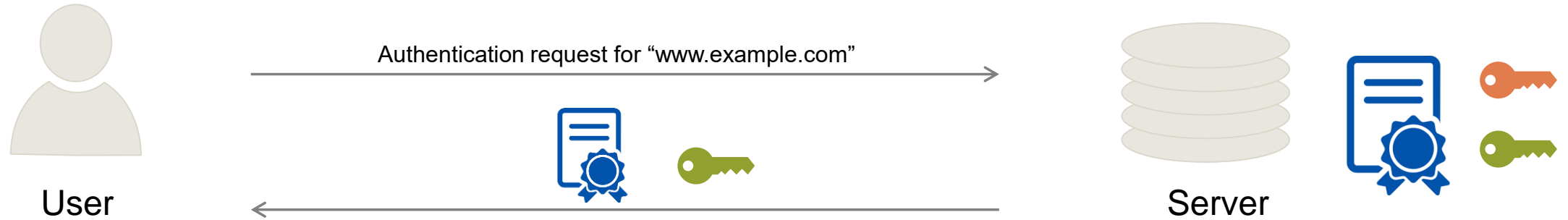


**Use the trust infrastructure providing authenticity of the world wide web – X.509 certificates for TLS and their public key infrastructure (PKI)**

# Background Information: TLS, X.509 certificates, and PKI




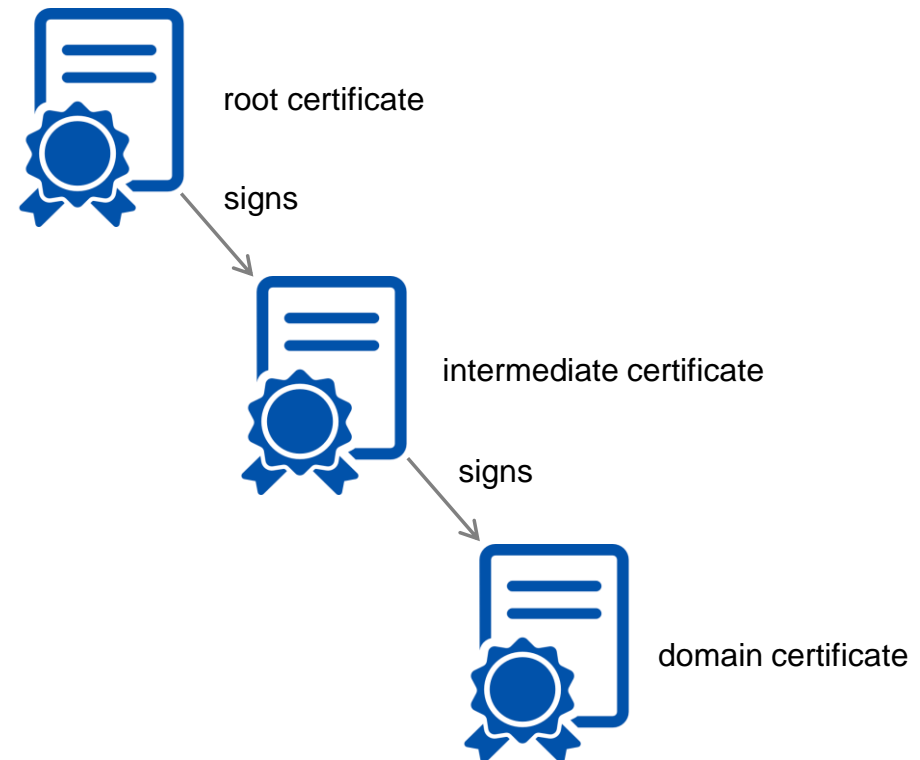
# Background Information: TLS, X.509 certificates, and PKI



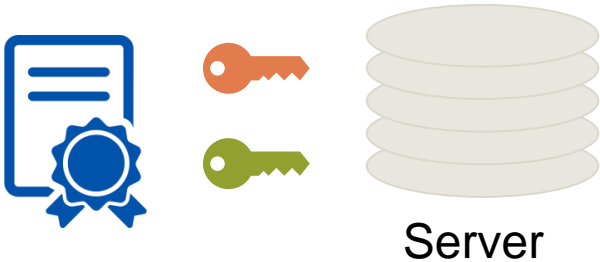
User validates the certificate:

- ✓ Matching domain
- ✓ Validity period valid now
- ✓ Valid certificate chain
- ✓ Root certificate trusted

Server is authenticated once it can proof possession of private key .



# Current System: BldAV [1]

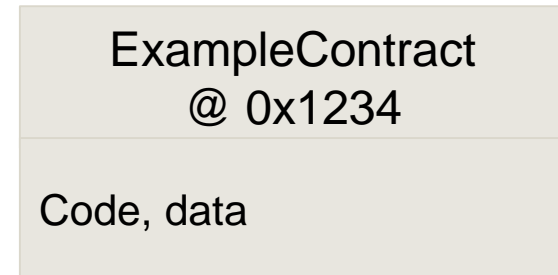
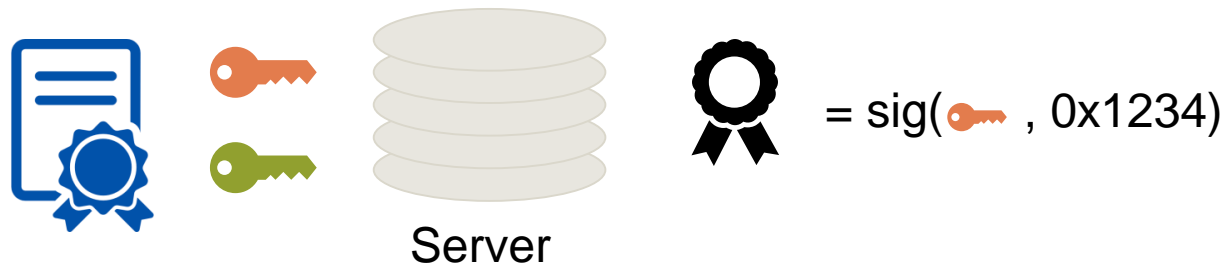


ExampleContract @ 0x1234
Code, data

[1] Gallersdörfer, U: BldAV: Blockchain-based Identity Assertion and Verification for Smart Contracts using SSL-Certificates

# Current System: BldAV [1]

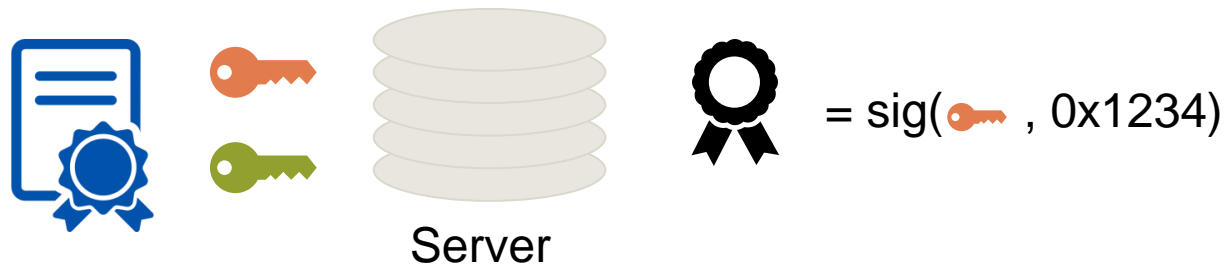
- Owner of a domain can endorse a smart contract by signing its address with the private key



[1] Gallersdörfer, U: BldAV: Blockchain-based Identity Assertion and Verification for Smart Contracts using SSL-Certificates

## Current System: BldAV [1]

- Owner of a domain can endorse a smart contract by signing its address with the private key
- The signature and the domain name are stored in the smart contract



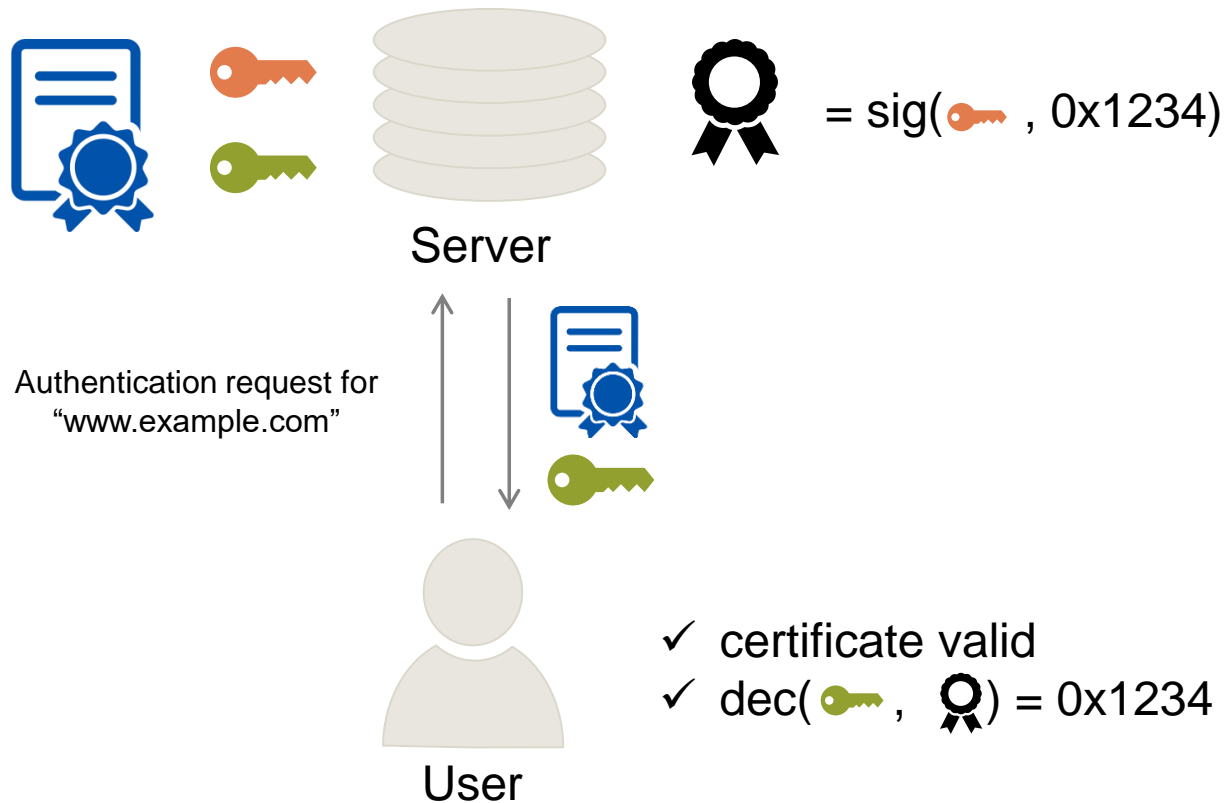
ExampleContract @ 0x1234
Code, data
Name: www.example.com Signature: 

[1] Gellersdörfer, U: BldAV: Blockchain-based Identity Assertion and Verification for Smart Contracts using SSL-Certificates



# Current System: BIdAV [1]

- Owner of a domain can endorse a smart contract by signing its address with the private key
- The signature and the domain name are stored in the smart contract
- Parties interested in SC identity retrieve this information and validate it by retrieving certificate from the domain server



ExampleContract @ 0x1234
Code, data
Name: www.example.com Signature:

[1] Gellersdörfer, U: BIdAV: Blockchain-based Identity Assertion and Verification for Smart Contracts using SSL-Certificates



**No on-chain** decisions, as not deterministic: Decision on validity of signature depends on external factors



**Participation** only open to owners of TLS certificates



Possible **mismatch** between certificate that signed address and that is provided by the server



TLS certificate system was **not designed with our use case in mind**

Explore the opportunities and limitations of using TSL certificates for address identification on Ethereum

The final artifact should be a TLS-certificate-based identity management system for Ethereum, that

- Allows on-chain decisions
- Is open to as many organizations and individuals as possible
- Does not require any onboarding
- Does not require action by current stakeholders other than the identity owner

**R1:** How can we enable on-chain decisions on identity using TLS certificates?

**R2:** How can we ensure trust in identities endorsed by TLS certificates?

**R3:** Which measures can be taken to allow open participation in the system?

# R1 How can we enable on-chain decisions on identity using TLS certificates?



## R1.1 What are possibilities to provide determinism for the validity-decision?

- Generate a proof of certificate validity once and store it on the chain
- Use an oracle service that is queried every time a transaction is to be made

## R1.2 What are the associated costs of the approaches?

## R1.3 How can proofs/certificates be revoked?

## R1.4 What are inherent problems of the TLS PKI and how can we mitigate them?

- Security flaws of the PKI can be mitigated e.g. with Certificate Transparency and TLS notaries
- Design decisions made for TLS PKI might prove problematic for us

## R2 How can we ensure trust in identities endorsed by TLS certificates?

### R2.1 What level of trust is required for different applications?

- How do we quantify trust?
- Which application scenarios exist?

### R2.2 Which measures can an address owner take to increase the trust in their identity claim?

### R2.3 How can policies be specified to enable automated decisions?

### R2.4 What properties of a certificate play a role in deciding on the validity of an identity claim?

- Type of certificate, validity period, root properties, chain length, ...






## R3 Which measures can be taken to allow open participation in the system?



- CAs could start issuing certificates for individual people
- Organizations can issue certificates for their clients, employees, or products
- Organizations could endorse identities on Ethereum

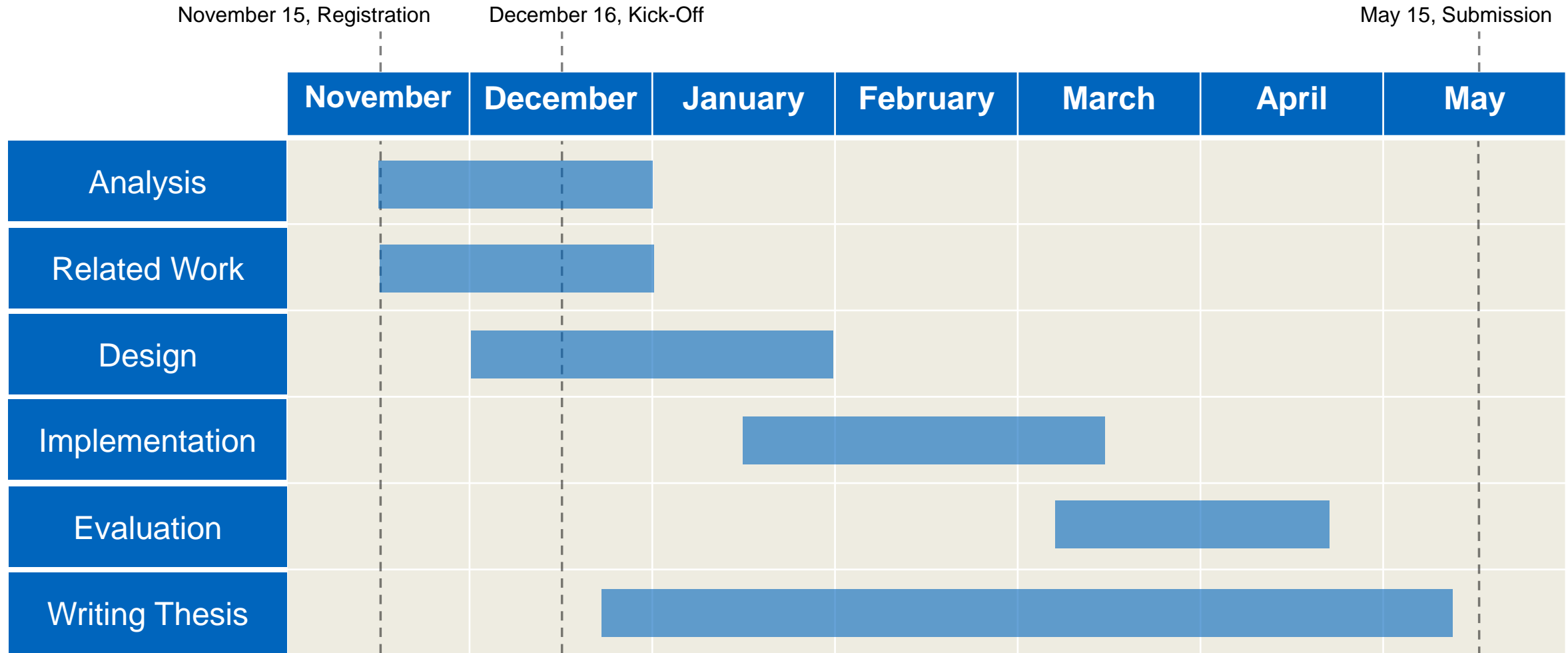
R3.1 In which use case scenarios would the scheme be helpful?

R3.2 How secure are the properties provided by the scheme?

-  Thorough analysis of the "TLS certificate world"
-  Literature review: related work on identity and certificate management with blockchain
-  Design of a system complying with the requirements
-  Implementation of the system
-  Evaluation of the system



# Timeline





## **Friederike Groschupp**

friederike.groschupp@tum.de

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

Boltzmannstraße 3  
85748 Garching bei München

