Trust and Privacy in a Heterogeneous World

PhD Defense

Stefan More

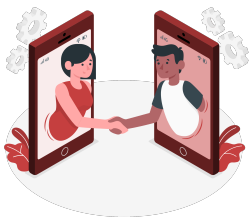
30. November 2023

Graz University of Technology

Trust and Privacy

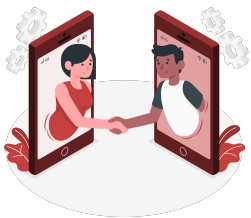
Trust and Privacy

Trust



Trust (noun); to **trust** (verb):

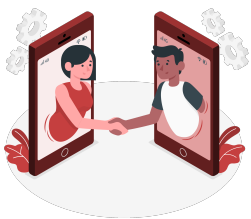
Trust



Trust (noun); to **trust** (verb):

- to rely on the truthfulness or accuracy of ...
- *assured* reliance on the truth of someone or something

Trust



Trust (noun); to **trust** (verb):

- to rely on the truthfulness or accuracy of ...
- *assured* reliance on the truth of someone or something

Trust is an enabler!

Trust as Enabler

Without trust:

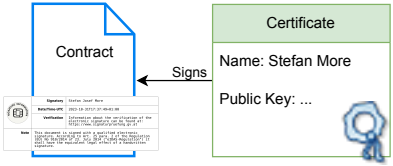
Trust as Enabler

Without trust:

- no reliance on person/document possible
  - need for (manual) verification
  - assessment of reputation, insurance, ...

Computational Trust?

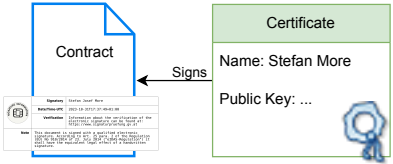
Computational Trust?



Certificate

- contains identity and public key
- used to sign other data

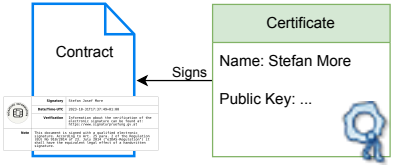
Computational Trust?



Certificate

- contains identity and public key
- used to sign other data

Computational Trust?



Certificate

- contains identity and public key
- used to sign other data

Credential

- contains attributes

Cryptography

Cryptographic signatures can provide:

- Integrity

Cryptography

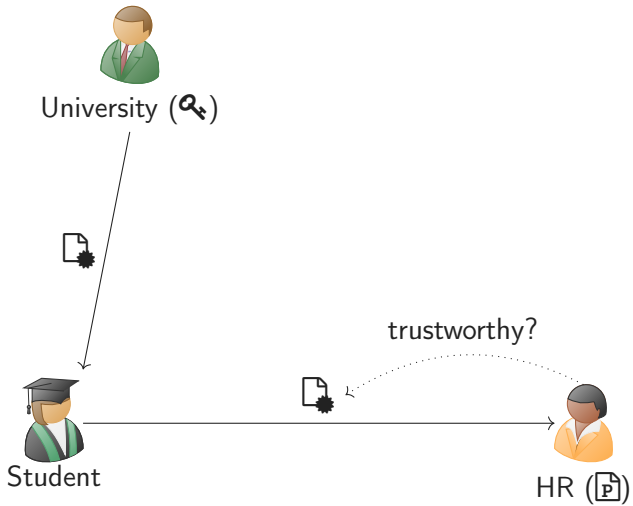
Cryptographic signatures can provide:

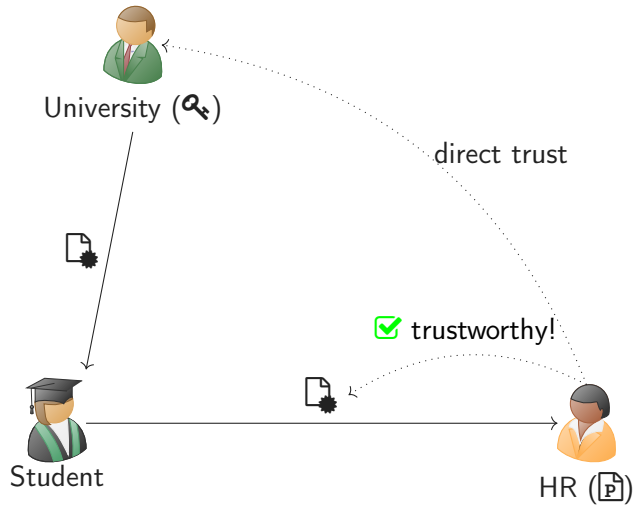
- Integrity
- Authenticity?

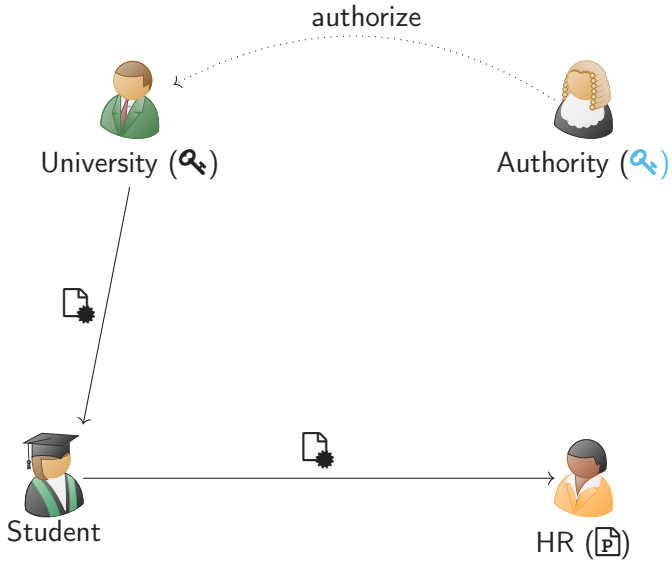
Cryptography

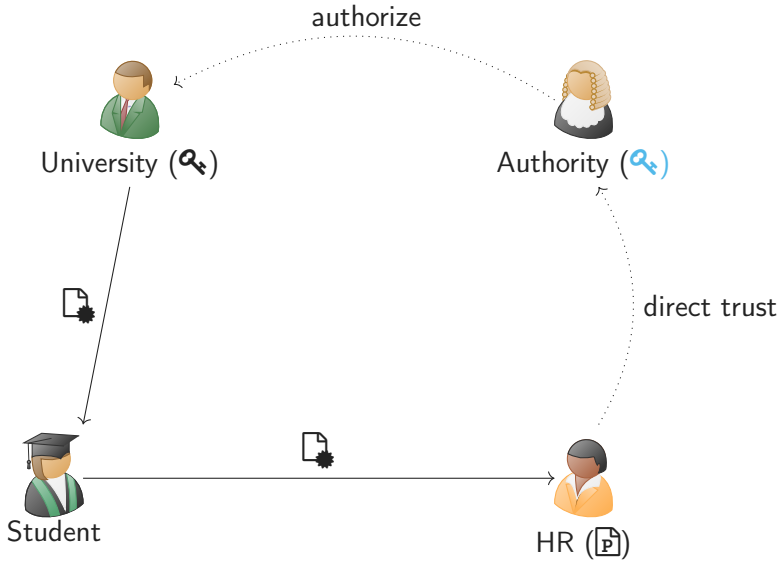
Cryptographic signatures can provide:

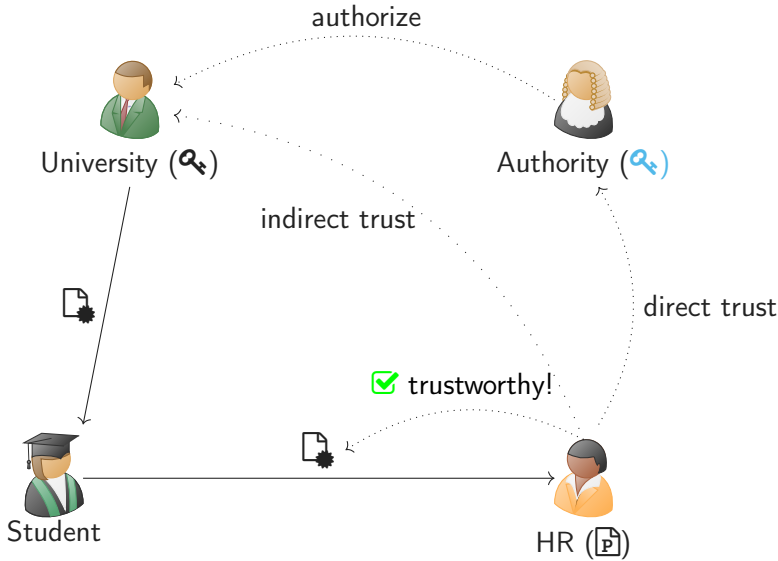
- Integrity
- Authenticity?
  - Data was signed by specific cryptographic key. But ...
    - is this key really the issuer's key?
    - is this issuer qualified to issue that information?


University (🔑)
trustworthy?
Student
HR (P)


University ( )
direct trust
trustworthy!
Student
HR ( )


authorize
University ( )
Authority ( )
Student
HR ( )


authorize
University ( )
Authority ( )
direct trust
Student
HR ( )


authorize
University ( )
Authority ( )
indirect trust
direct trust
trustworthy!
Student
HR ( )

Trust Scheme

- Legal regulations, technical standards, infrastructure, and organizations

Trust Scheme

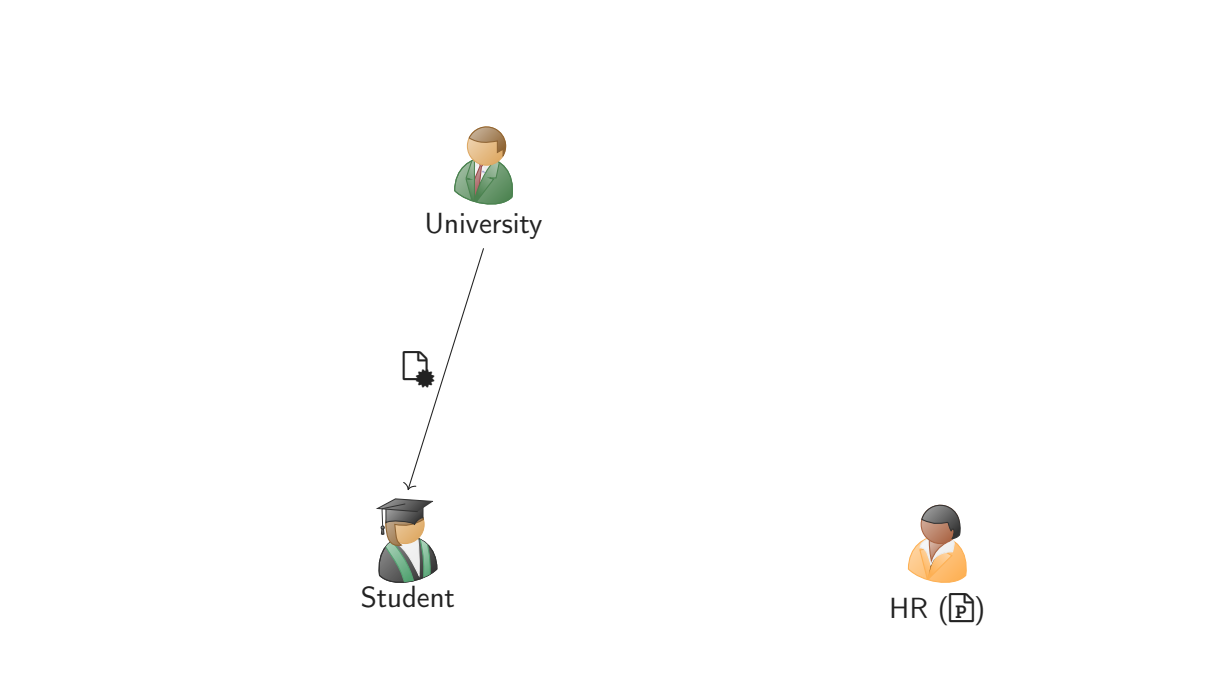
- Legal regulations, technical standards, infrastructure, and organizations
- Authorize qualified issuers

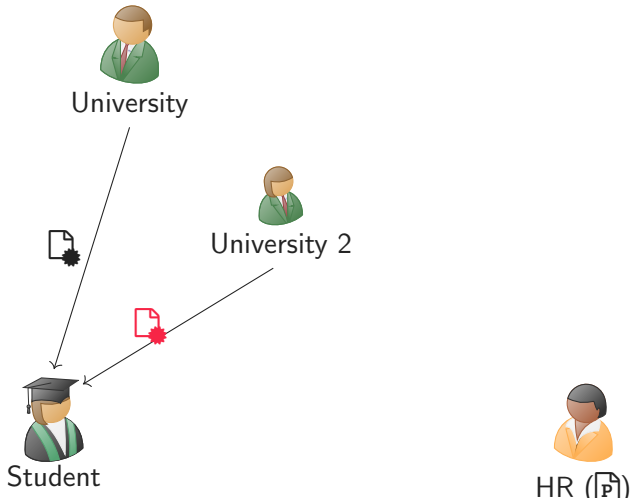
Trust Scheme

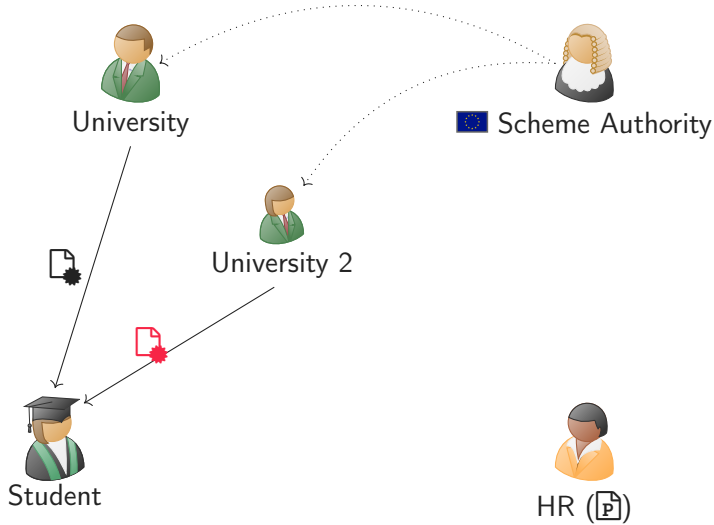
- Legal regulations, technical standards, infrastructure, and organizations
- Authorize qualified issuers
- Verifier trusts the Trust Scheme
  (direct trust in scheme, indirect trust in issuer)

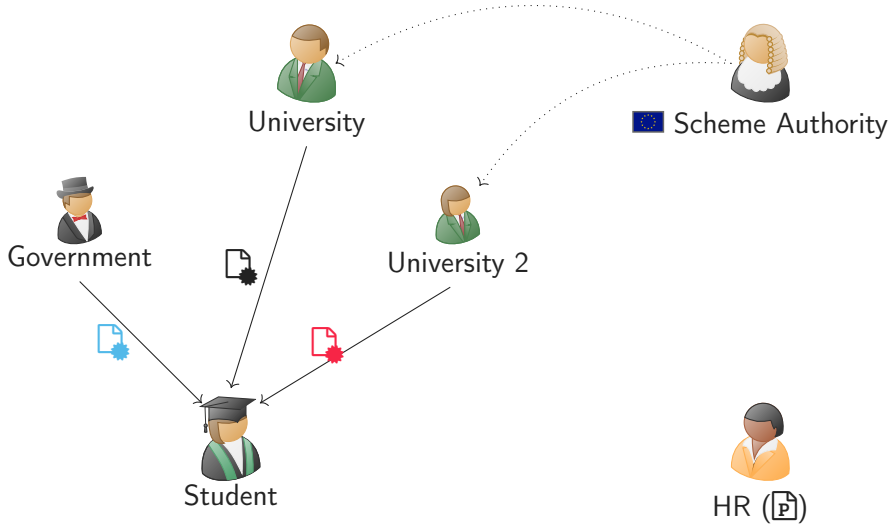
Examples:

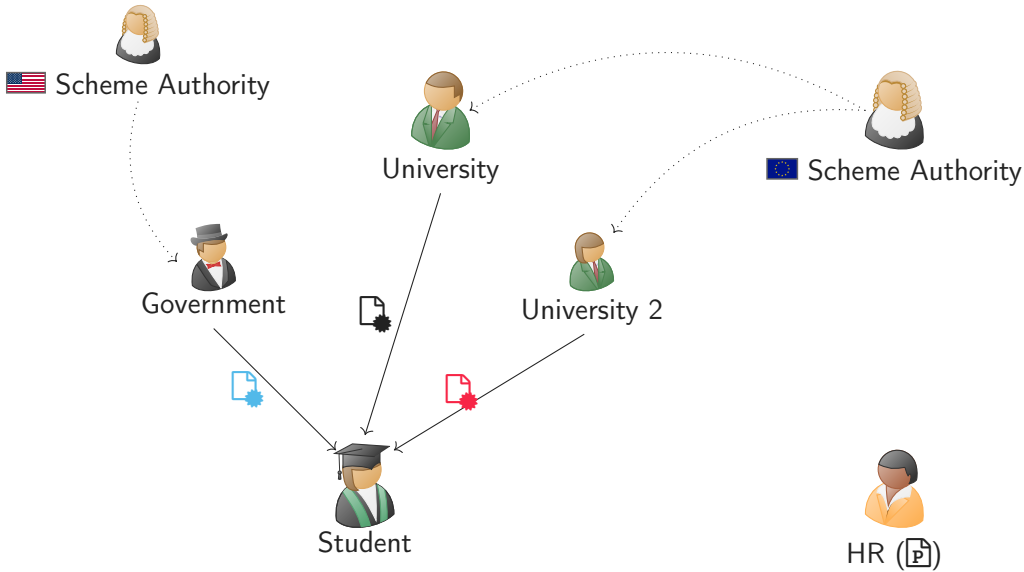
- Web PKI: CA/Browser Forum, list of trusted root CAs
- EU: eIDAS regulation, EU Trusted List

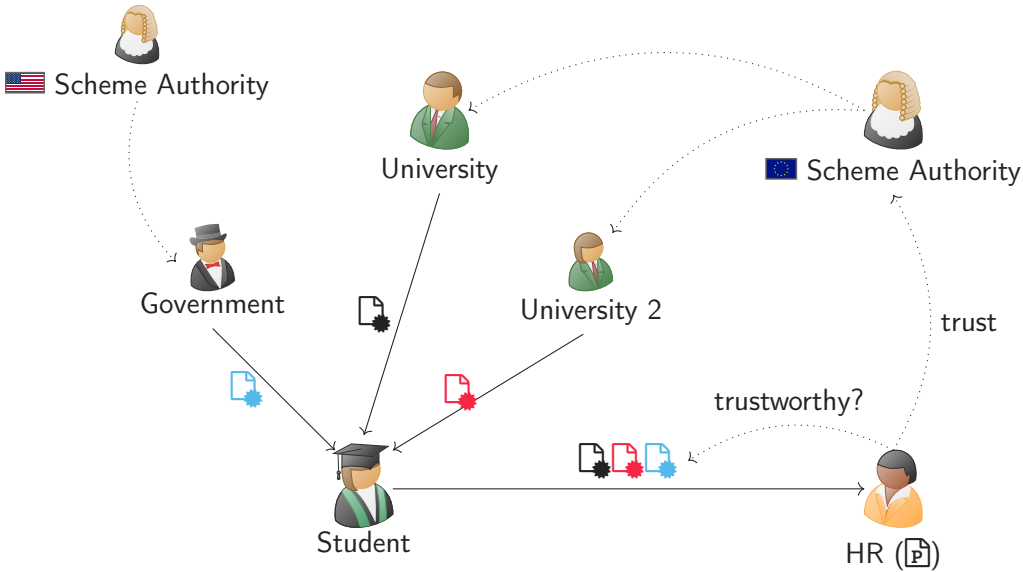

University
Student
HR (P)


University
University 2
Student
HR (P)


University
Scheme Authority
University 2
Student
HR (P)


University
Scheme Authority
Government
University 2
Student
HR (P)


Scheme Authority
University
Scheme Authority
Government
University 2
Student
HR (P)


Scheme Authority
University
Scheme Authority
Government
University 2
trust
trustworthy?
Student
HR (P)

Challenges of *going global in a heterogeneous world:*

- Complex transactions: many credentials

Challenges of *going global in a heterogeneous world:*

- Complex transactions: many credentials
- Multiple issuers, qualified in different schemes

Challenges of *going global in a heterogeneous world:*

- Complex transactions: many credentials
- Multiple issuers, qualified in different schemes
- Different trust requirements: no "meta scheme" possible

Challenges of *going global in a heterogeneous world:*

- Complex transactions: many credentials
- Multiple issuers, qualified in different schemes
- Different trust requirements: no "meta scheme" possible

Technical Challenges of supporting multiple schemes:

- Need to setup cryptographic material for each scheme

Challenges of *going global in a heterogeneous world:*

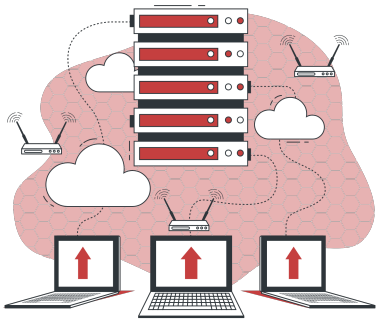
- Complex transactions: many credentials
- Multiple issuers, qualified in different schemes
- Different trust requirements: no "meta scheme" possible

Technical Challenges of supporting multiple schemes:

- Need to setup cryptographic material for each scheme
- Different encoding of trust





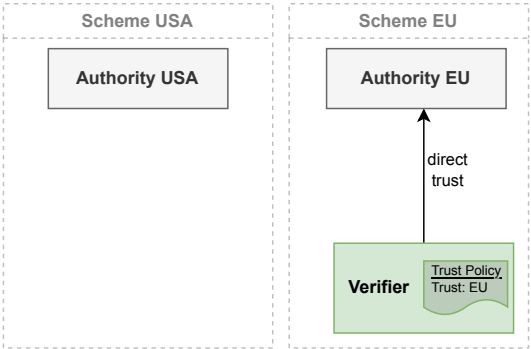


Global Trust Infrastructure

Trust Scheme Recognition

Many different schemes

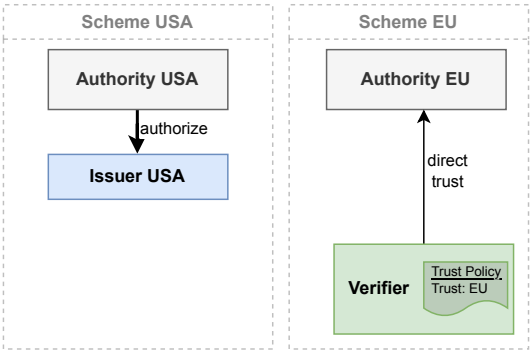
- Verifier only trusts few directly



Trust Scheme Recognition

Many different schemes

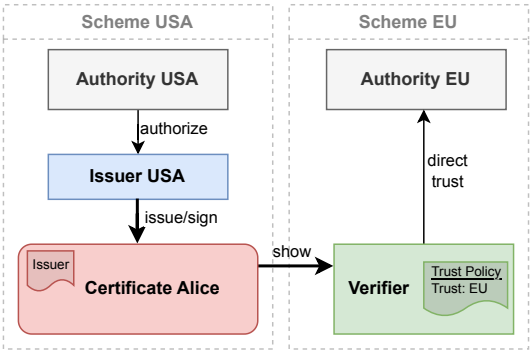
- Verifier only trusts few directly



Trust Scheme Recognition

Many different schemes

- Verifier only trusts few directly



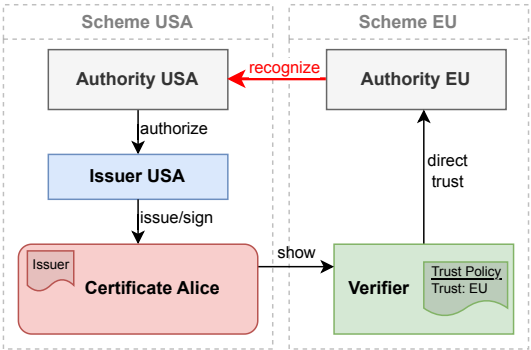
Trust Scheme Recognition

Many different schemes

- Verifier only trusts few directly

Trust Scheme Recognition:

- Trust Schemes identified by human-readable name
- Recognition:
  list of names of other schemes



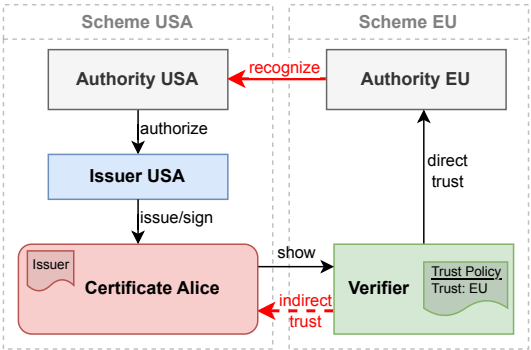
Trust Scheme Recognition

Many different schemes

- Verifier only trusts few directly

Trust Scheme Recognition:

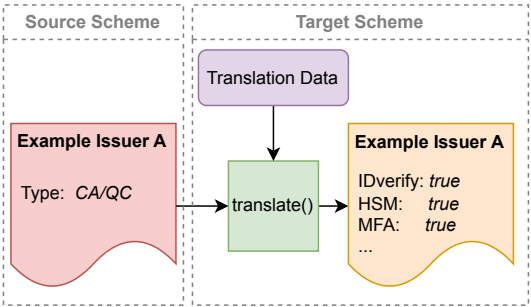
- Trust Schemes identified by human-readable name
- Recognition:
  list of names of other schemes

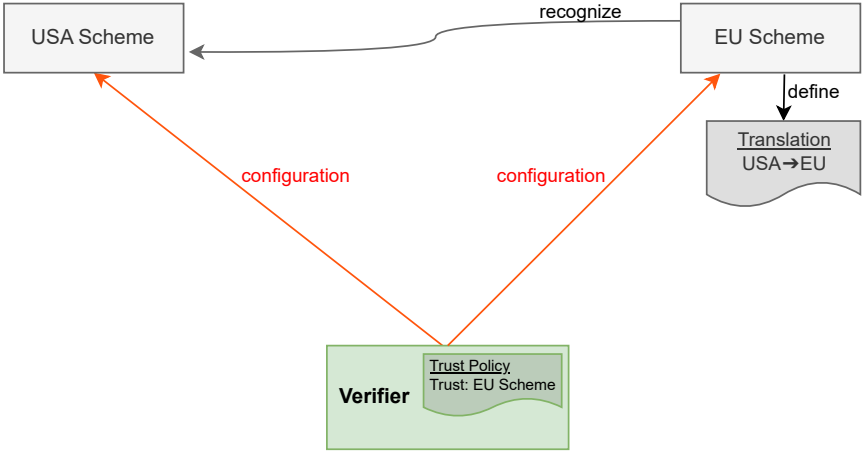


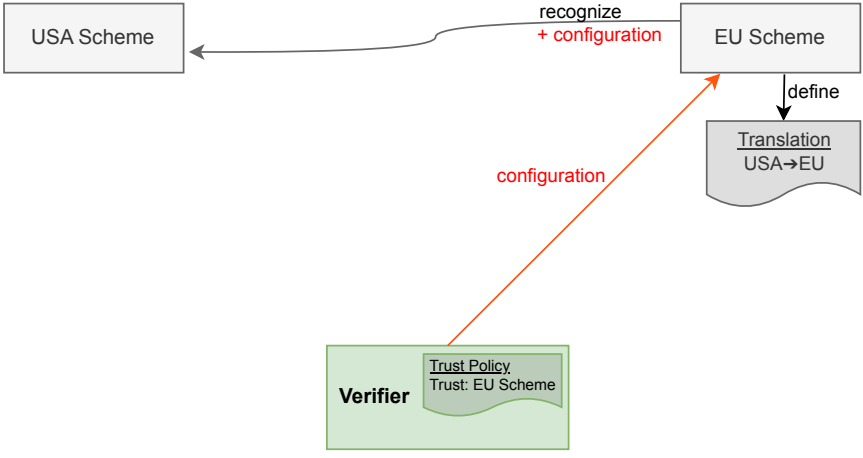
Trust Translation

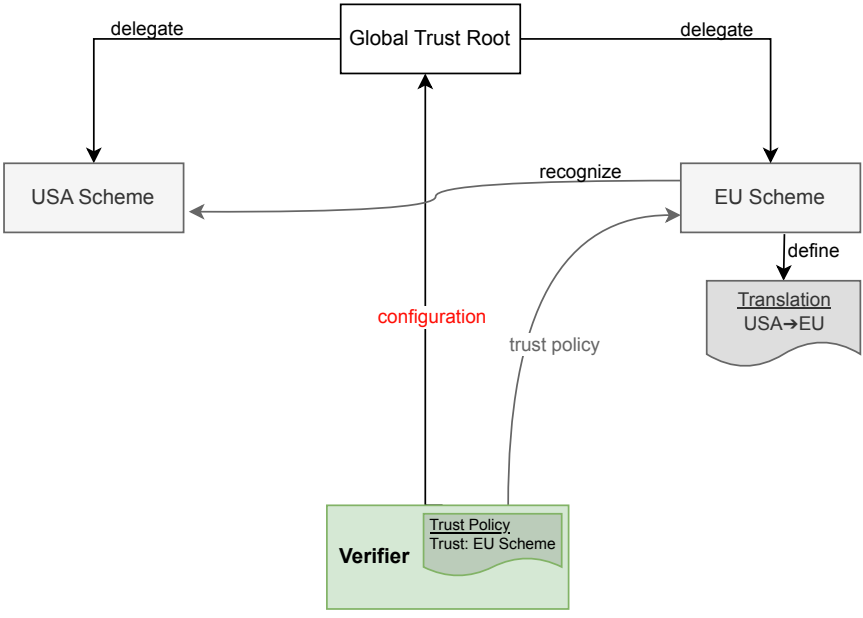
Varying understanding of trust

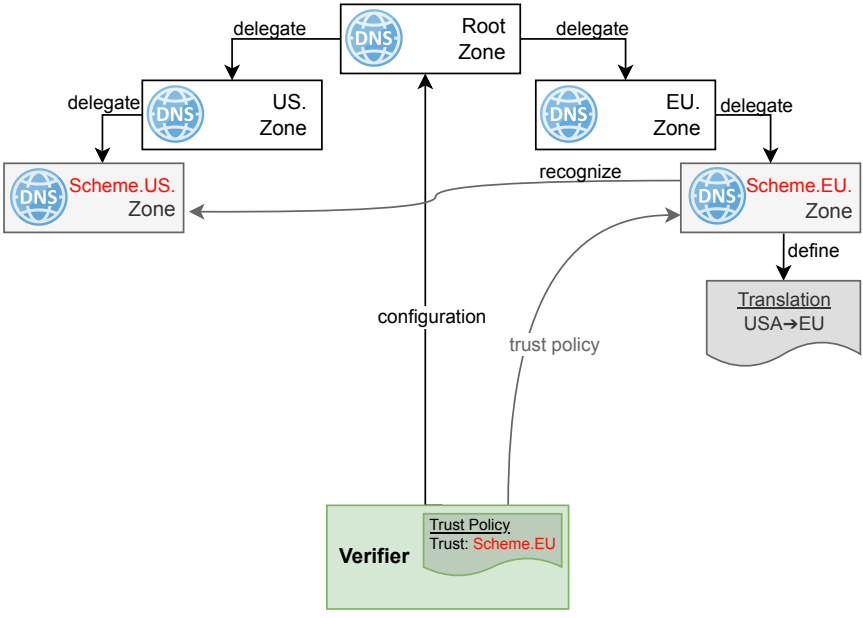
- Trust character of a credential
- Boolean, Ordinal, Tuple-based

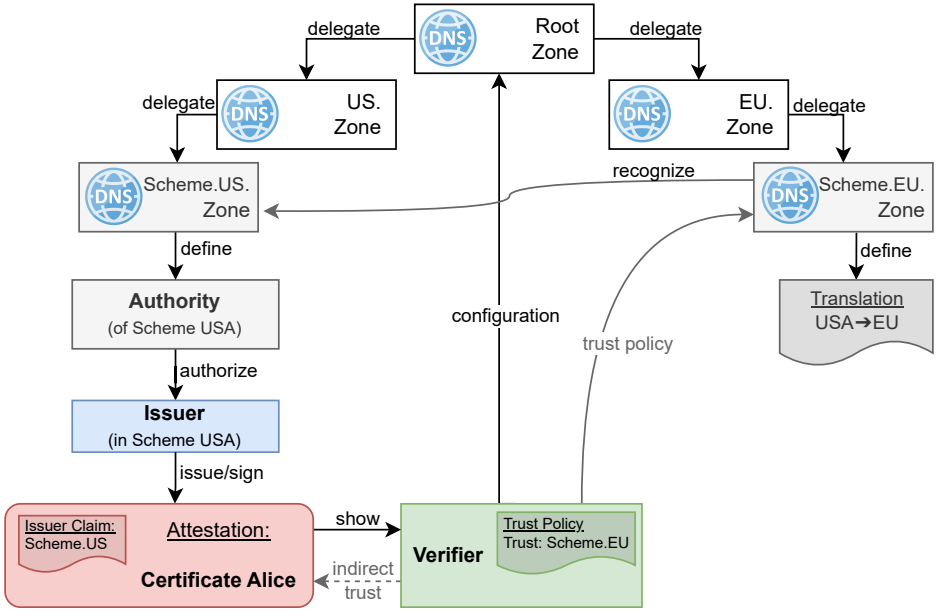



USA Scheme
recognize
EU Scheme
define
Translation
USA➔EU
configuration
configuration
Verifier
Trust Policy
Trust: EU Scheme


USA Scheme
recognize
+ configuration
EU Scheme
define
Translation
USA→EU
configuration
Verifier
Trust Policy
Trust: EU Scheme


delegate
Global Trust Root
delegate
USA Scheme
recognize
EU Scheme
define
Translation
USA→EU
configuration
trust policy
Verifier
Trust Policy
Trust: EU Scheme


delegate
Root Zone
delegate
delegate
US. Zone
delegate
EU. Zone
delegate
Scheme.US. Zone
recognize
Scheme.EU. Zone
define
Translation USA→EU
configuration
trust policy
Verifier
Trust Policy
Trust: Scheme.EU


delegate
Root Zone
delegate
delegate
US. Zone
delegate
EU. Zone
delegate
recognize
Scheme.US. Zone
Scheme.EU. Zone
define
define
Authority
(of Scheme USA)
Translation
USA➔EU
configuration
trust policy
authorize
Issuer
(in Scheme USA)
issue/sign
Issuer Claim:
Scheme.US
Attestation:
Certificate Alice
show
indirect
trust
Verifier
Trust Policy
Trust: Scheme.EU

Discussion

- Governance
  - eIDAS Article 14
  - DNS / DNSSEC (ICANN/IANA)
  - LIGHTest provides legal framework: [GJ19]

Discussion

- Governance
  - eIDAS Article 14
  - DNS / DNSSEC (ICANN/IANA)
  - LIGHTest provides legal framework: [GJ19]

- Requirements Evaluation
  - 🔨 DNS governance for legal *liability*
  - ☑ Support for different scheme types
  - ☑ Single cryptographic root

Publications

DNS-based Trust Scheme Publication
+ Trust Recognition + Trust Translation

Wagner, G., Wagner, S., **More, S.**, Hoffmann, M., "DNS-based Trust Scheme Publication and Discovery". In: *Open Identity Summit*. 2019

More, S. "Trust Scheme Interoperability: Connecting Heterogeneous Trust Schemes". In: *ARES*. 2023

Going global in a heterogeneous world:

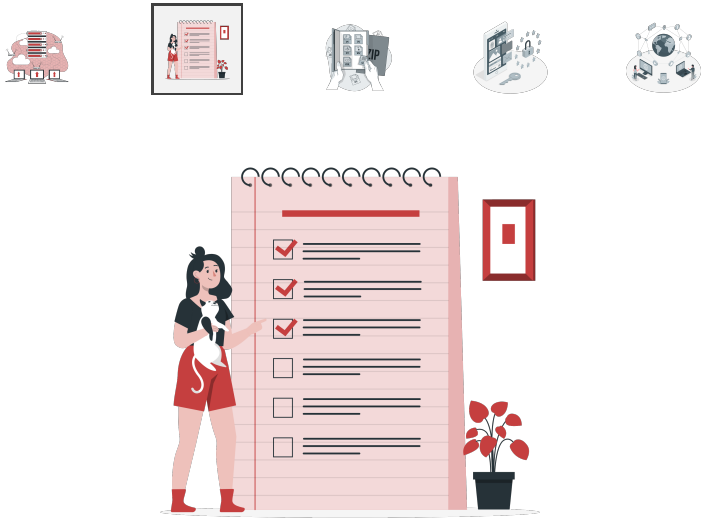
- ☑ Complex transactions: many credentials
- ☑ Multiple issuers, qualified in different schemes

Going global in a heterogeneous world:

- ☑ Complex transactions: many credentials
- ☑ Multiple issuers, qualified in different schemes
- Local perception of trust
  - Different verifiers trust different entities/schemes/regulations
  - No meta-scheme
  - Need to enable verifiers to define their own trust rules

Going global in a heterogeneous world:

- ☑ Complex transactions: many credentials
- ☑ Multiple issuers, qualified in different schemes
- Local perception of trust
  - Different verifiers trust different entities/schemes/regulations
  - No meta-scheme
  - Need to enable verifiers to define their own trust rules



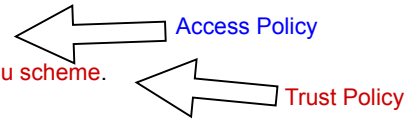
TPL: Trust- & Access-Policies

Example rule:

Accept any application
from CS master-level graduates
with a diploma qualified in EU-Edu scheme.

Example rule:

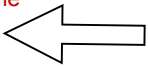
Accept any application
from CS master-level graduates
with a diploma qualified in EU-Edu scheme.



Motivation / Goals

Example rule:

Accept any application
from CS master-level graduates
with a diploma qualified in EU-Edu scheme
or any scheme recognized by EU-Edu.



Trust Recognition/Translation

Example rule:

Accept any application
  from CS master-level graduates
  with a diploma qualified in EU-Edu scheme
  or any scheme recognized by EU-Edu
and a recommendation letter
  issued to the same student
  by a person qualified in the EU-Sci scheme.

} Second Credential
with Inter-credential constraint

The *TPL* System

The ***TPL* Trust- and Access-Policy System**:

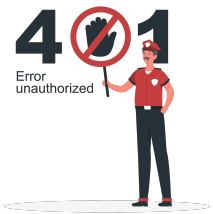
Enable Service Providers to encode their own rules

The *TPL* System

The ***TPL* Trust- and Access-Policy System**:
Enable Service Providers to encode their own rules

- Support of expressive constraints for trust & access rules

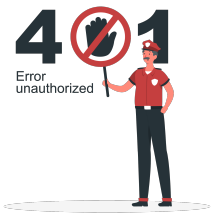
The *TPL* System



The ***TPL* Trust- and Access-Policy System**:
Enable Service Providers to encode their own rules

- Support of expressive constraints for trust & access rules
- Integration with our global trust infrastructure

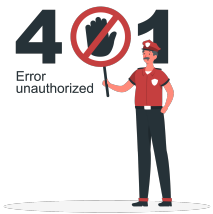
The *TPL* System



The ***TPL* Trust- and Access-Policy System**:
Enable Service Providers to encode their own rules

- Support of expressive constraints for trust & access rules
- Integration with our global trust infrastructure
- Modularity
  - Formats (e.g., credential schemata)
  - Predicates (use-case: integration with SSI)

The *TPL* System

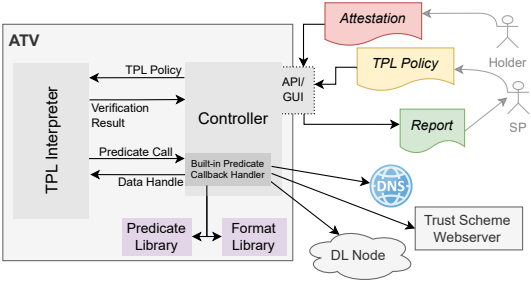


The ***TPL* Trust- and Access-Policy System**:
Enable Service Providers to encode their own rules

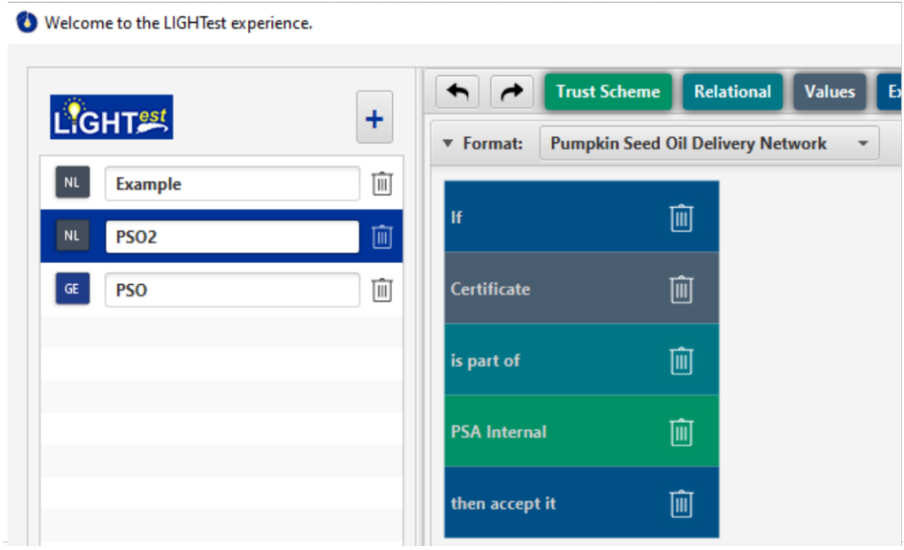
- Support of expressive constraints for trust & access rules
- Integration with our global trust infrastructure
- Modularity
  - Formats (e.g., credential schemata)
  - Predicates (use-case: integration with SSI)

TPL Components

- TPL Policy Language
- TPL Interpreter
- Automated Trust Verifier (ATV)



Bonus: graphical *TPL* editor



Publications

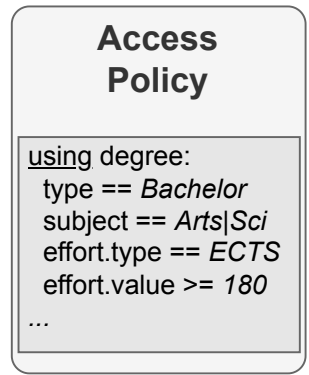
Mödersheim, S., Schlichtkrull, A., Wagner, G., **More, S.**, Alber, L., "TPL: A Trust Policy Language". In: *IFIPTM*. 2019

Alber, L., **More, S.**, Mödersheim, S., Schlichtkrull, A., "Adapting the TPL Trust Policy Language for a Self-Sovereign Identity World". In: *Open Identity Summit*. 2021

More, S., Alber, L., "YOU SHALL NOT COMPUTE on my Data: Access Policies for Privacy-Preserving Data Marketplaces and an Implementation for a Distributed Market using MPC". In: *ARES*. 2022

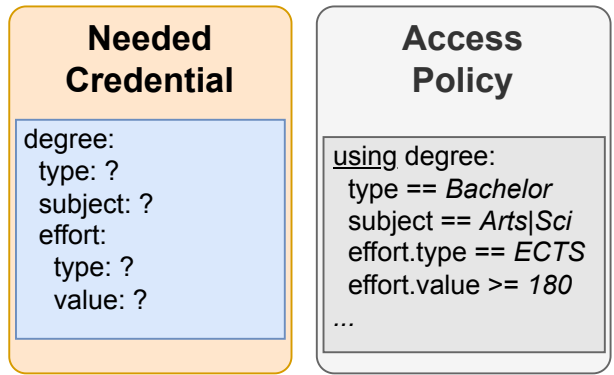
Going global in a heterogeneous world

Problem: Different Credential Schemata



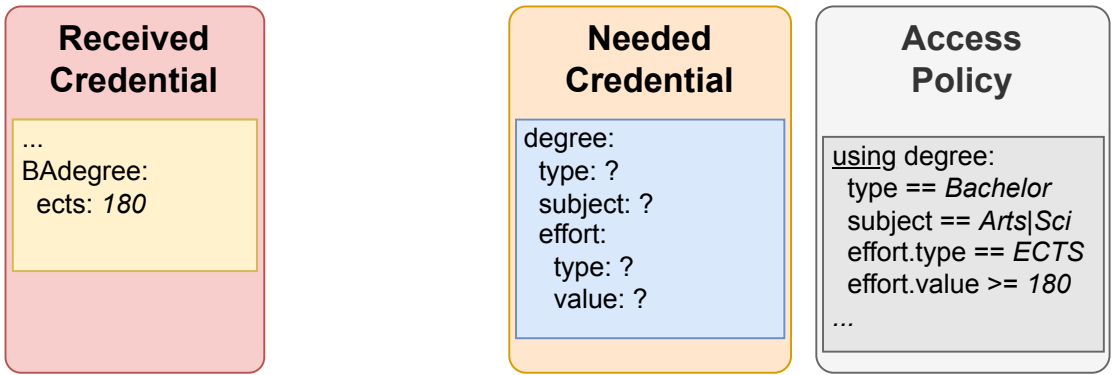
Going global in a heterogeneous world

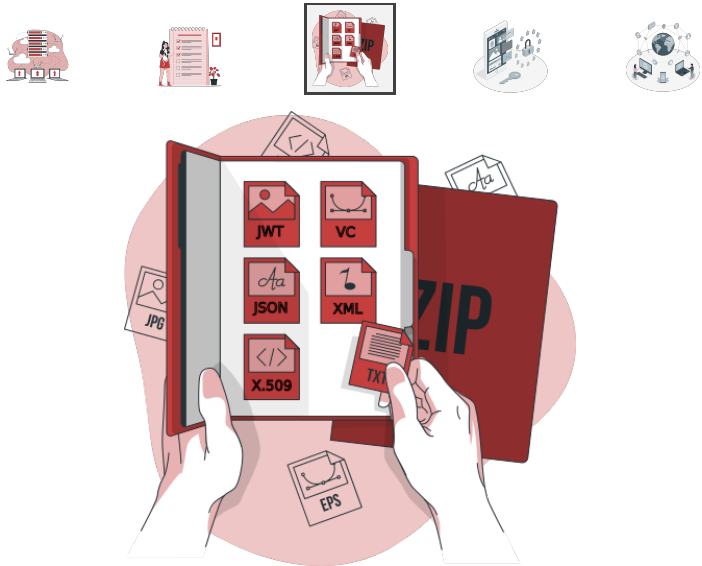
Problem: Different Credential Schemata



Going global in a heterogeneous world

Problem: Different Credential Schemata

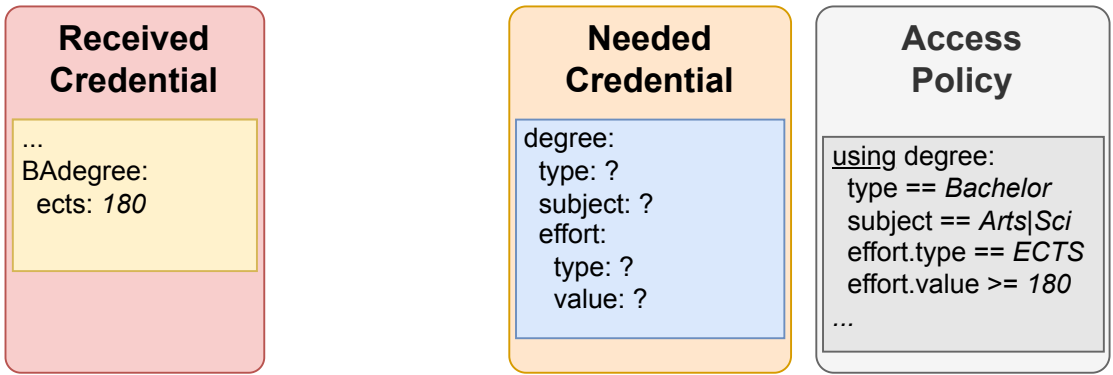




Credential Format Interoperability

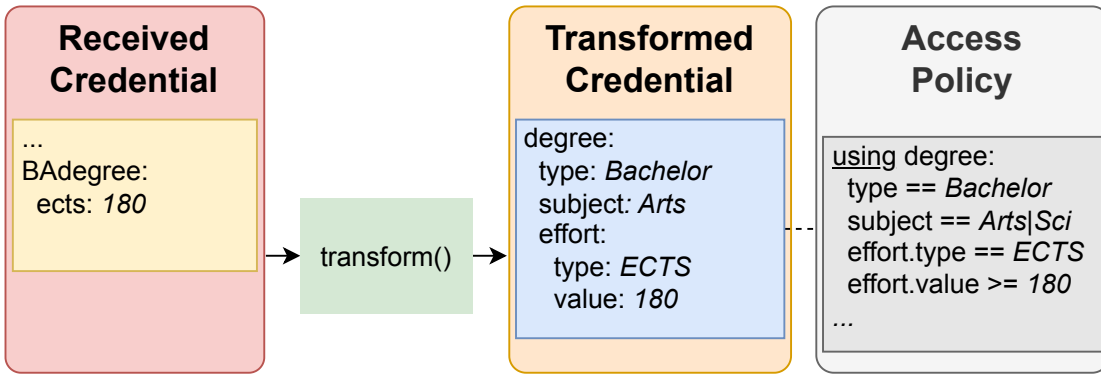
Going global in a heterogeneous world

Problem: Different Credential Schemata



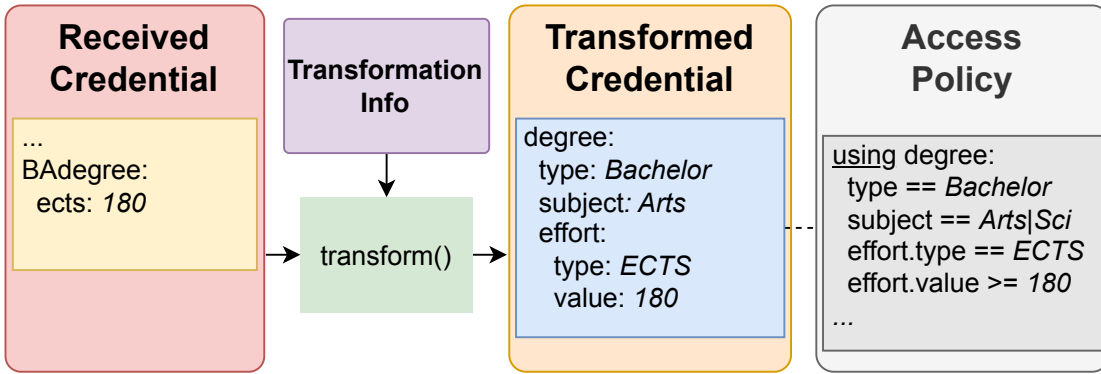
Going global in a heterogeneous world

Problem: Different Credential Schemata

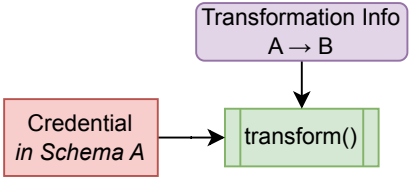


Going global in a heterogeneous world

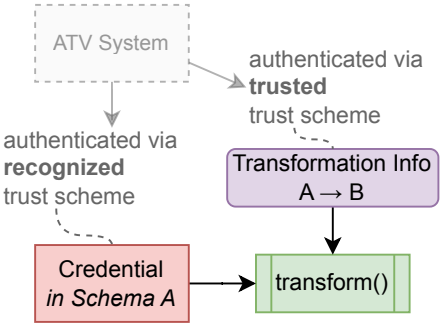
Problem: Different Credential Schemata



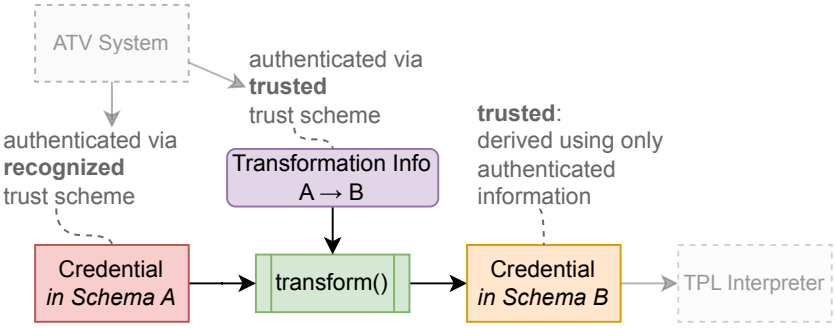
Trusted Credential Transformation



Trusted Credential Transformation

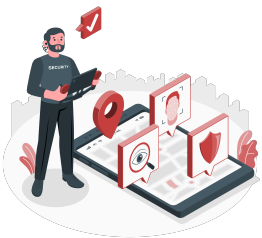


Trusted Credential Transformation



Publication

More, S., Grassberger, P., Hörandner, F., Abraham, A., Klausner, L. D., "Trust Me If You Can: Trusted Transformation Between (JSON) Schemas to Support Global Authentication of Education Credentials". In: *SEC*. 2021



Going global in a heterogeneous world:

- Service Provider is happy about trustworthy information
- What about the User?

Trust and Privacy

Computers

- Computers are omnipresent and interconnected
  - $\Rightarrow$ A lot of sensitive data
  - Behavior, medical, political preferences, personality profiles, ...

Computers

- Computers are omnipresent and interconnected
  - $\Rightarrow$ A lot of sensitive data
  - Behavior, medical, political preferences, personality profiles, ...
- Computers are powerful
  - $\Rightarrow$ Possible to collect, process, and store an unthinkable amount of data

Computers

- Computers are omnipresent and interconnected
  - $\Rightarrow$ A lot of sensitive data
  - Behavior, medical, political preferences, personality profiles, ...
- Computers are powerful
  - $\Rightarrow$ Possible to collect, process, and store an unthinkable amount of data

Various actors (mis-)use these data, e.g.

- Targeted advertising
- Surveillance capitalism
- Disinformation campaigns

Privacy

Privacy (noun):

- from Latin *Privatus*: what is private

Privacy

Privacy (noun):

- from Latin *Privatus*: what is private
- *the claim of individuals [...] to determine for themselves when, how, and to what extent [any] information about them is communicated to others*

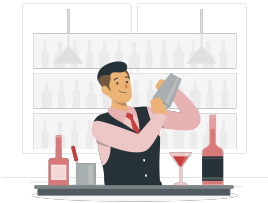
Privacy

Privacy (noun):

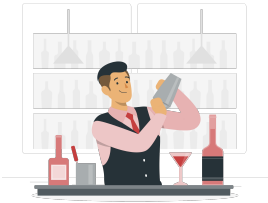
- from Latin *Privatus*: what is private
- *the claim of individuals [...] to determine for themselves when, how, and to what extent [any] information about them is communicated to others*

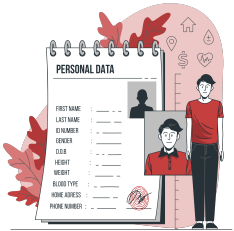
Privacy is a right!

European Convention on Human Rights (Article 8):
Everyone has the right to respect for his private and family life, his home and his correspondence.

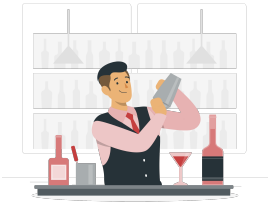


Bar Visit: Age Check

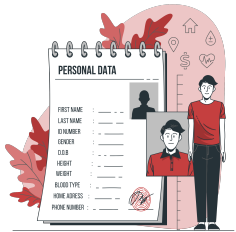




Bar Visit: Age Check



Bar Visit: Age Check



A lot of data revealed

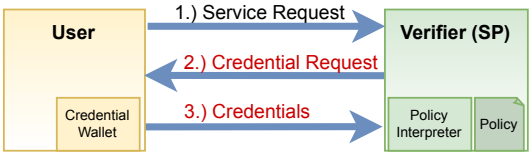
Privacy !?

Privacy-enhanced Access Policies

Privacy in Access Control: Challenges

Privacy:

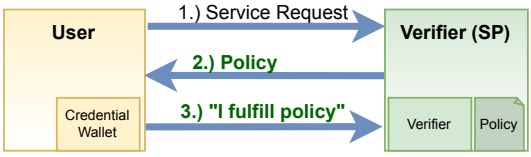
- To prove they fulfill a policy, users need to send full credentials and reveal all attributes



Privacy in Access Control: Challenges

Privacy:

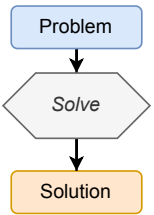
- To prove they fulfill a policy, users need to send full credentials and reveal all attributes



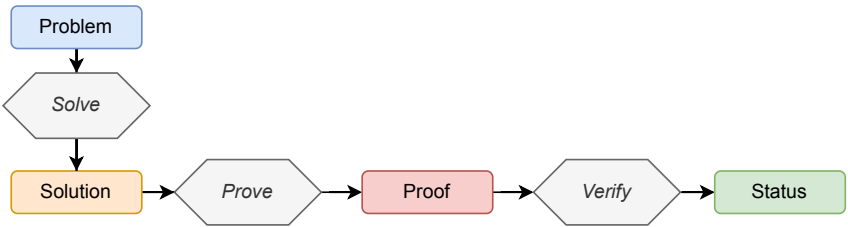
Background: Zero-knowledge Proofs

(Non-interactive) Zero-knowledge Proof:

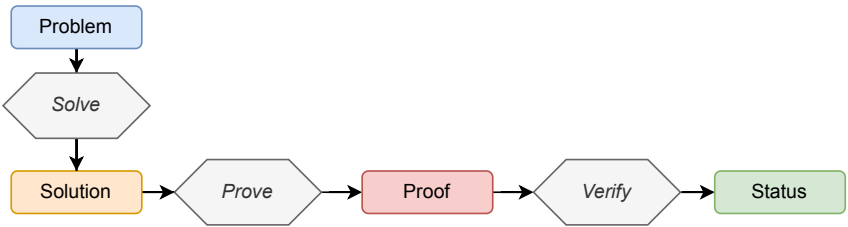
(Non-interactive) Zero-knowledge Proof:



(Non-interactive) Zero-knowledge Proof:

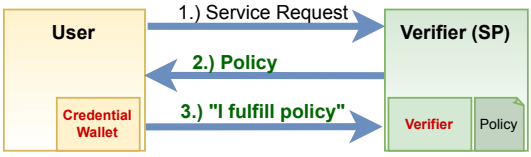


(Non-interactive) Zero-knowledge Proof:



We extend policy language systems
with privacy features using zero-knowledge proofs.

Privacy in Access Control: Challenges

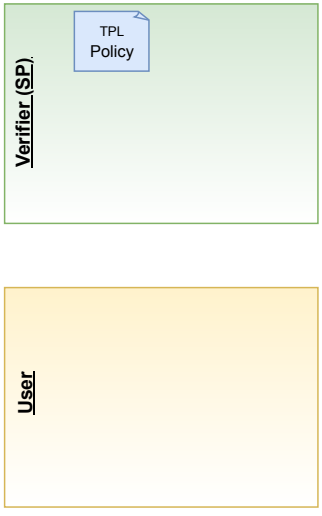


Integration Gap:

- Use of privacy features with existing technologies

Privacy-preserving Policy System:

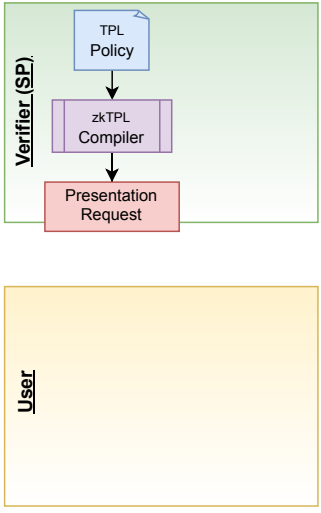
1. Policy author defines which attributes need to be revealed (and for which proof of statement is enough)



Contribution

Privacy-preserving Policy System:

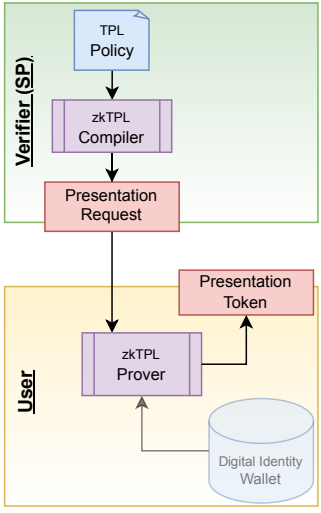
1. Policy author defines which attributes need to be revealed (and for which proof of statement is enough)
2. Policy compiler derives ZKP presentation request



Contribution

Privacy-preserving Policy System:

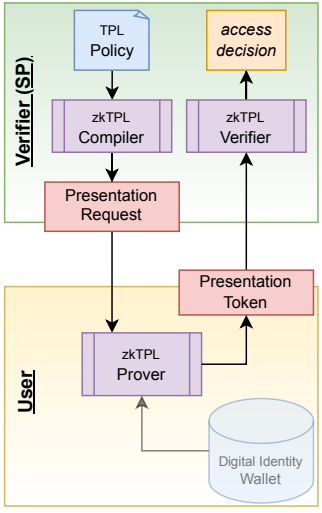
1. Policy author defines which attributes need to be revealed (and for which proof of statement is enough)
2. Policy compiler derives ZKP presentation request
3. User creates ZKP presentation token based on request



Contribution

Privacy-preserving Policy System:

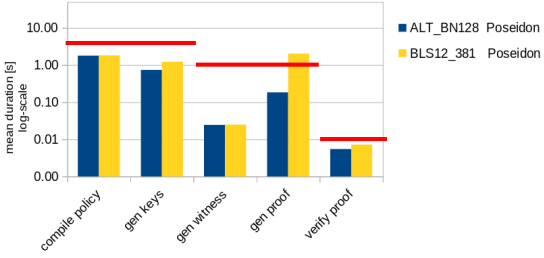
1. Policy author defines which attributes need to be revealed (and for which proof of statement is enough)
2. Policy compiler derives ZKP presentation request
3. User creates ZKP presentation token based on request

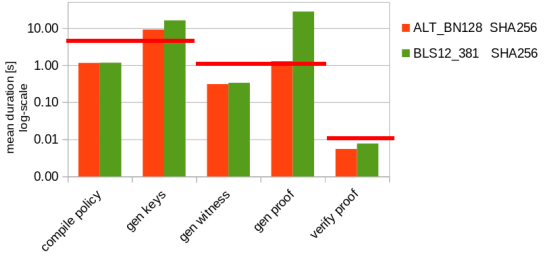


Evaluation

- Performance
  - 2 curves, 2 commitments
  - One-time: *compile*, *gen keys*
  - Repeated: *witness*, *proof*, *verify*

Evaluation





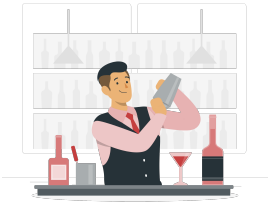
- Performance
  - 2 curves, 2 commitments
  - One-time: *compile*, *gen keys*
  - Repeated: *witness*, *proof*, *verify*

Evaluation

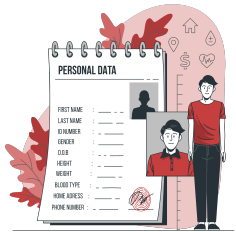
- Performance
  - 2 curves, 2 commitments
  - One-time: *compile*, *gen keys*
  - Repeated: *witness*, *proof*, *verify*
- Future Work
  - Linkability
  - ZKP Setup & NIZK Toolchains
  - Policy Authoring Tools & UX

Publication

More, S., Ramacher, S., Alber, L., Herzl, M., "Extending Expressive Access Policies with Privacy Features". In: *TrustCom*. 2022

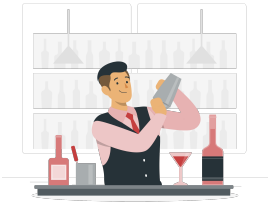


Bar Visit: Age Check

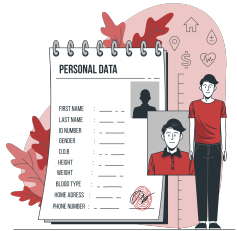


A lot of data revealed

☑ zkTPL

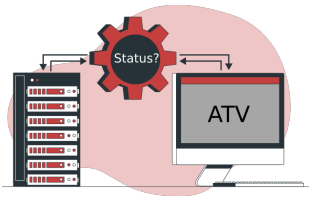


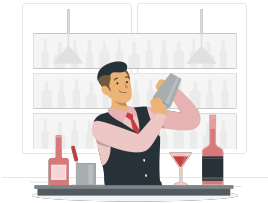
Bar Visit: Age Check



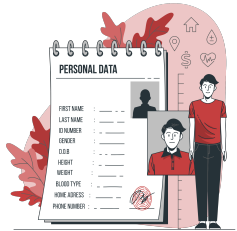
A lot of data revealed

☑ zkTPL



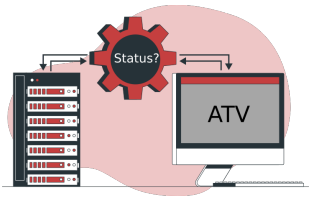


Bar Visit: Age Check



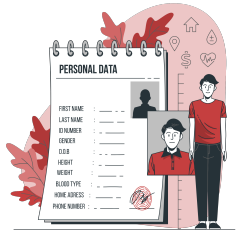
A lot of data revealed

☑ zkTPL



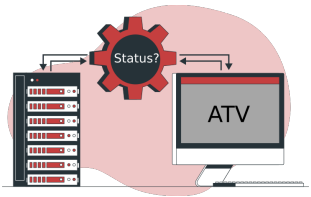
State learns about visit

Bar Visit: Age Check



A lot of data revealed

☑ zkTPL

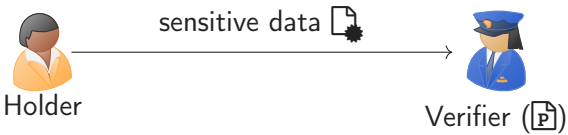


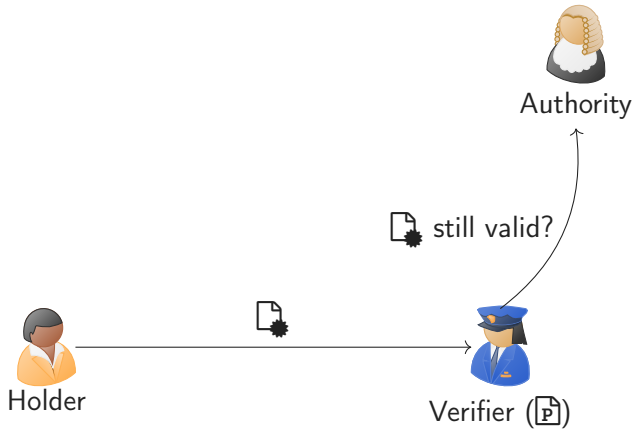
State learns about visit

Privacy !?

Ledger State Attestations

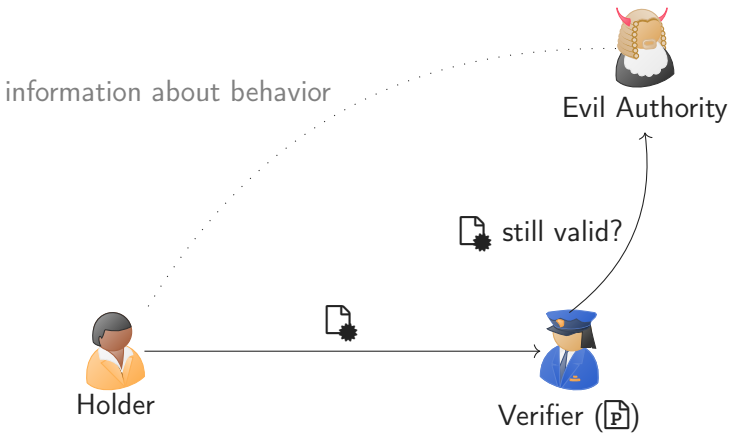
Challenges:





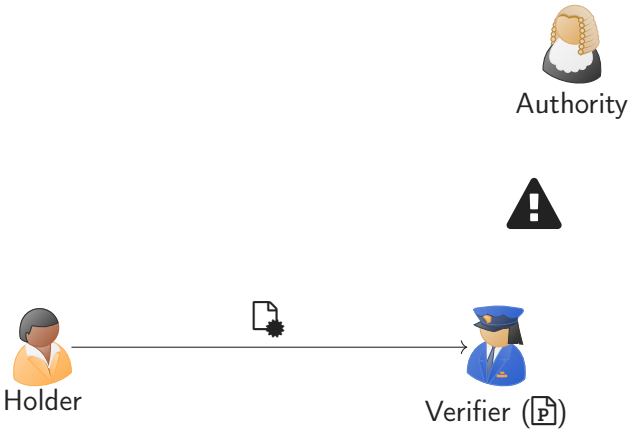
Challenges:

- Verification leaks information about the user's behavior to registry



Challenges:

- Verification leaks information about the user's behavior to registry



Challenges:

- Verification leaks information about the user's behavior to registry
- Registry might be unavailable
- Verifier needs to be online

Challenge

Status Registry involved in Status checks

Challenge

Status Registry involved in Status checks

Solution: Remove communication between Verifier and DL

Challenge

Status Registry involved in Status checks

Solution: Remove communication between Verifier and DL

Context: Distributed Ledger-based Registries

Challenge

Status Registry involved in Status checks

Solution: Remove communication between Verifier and DL

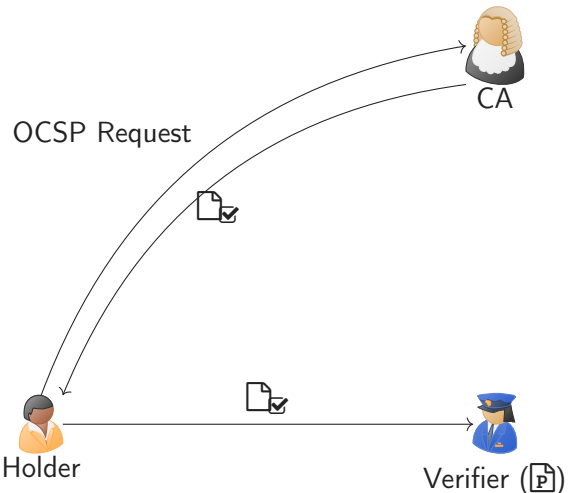
Context: Distributed Ledger-based Registries

Challenges:

- Many DL nodes: Who signs a response/attestation?
- Not just revocation: Need for generic query system

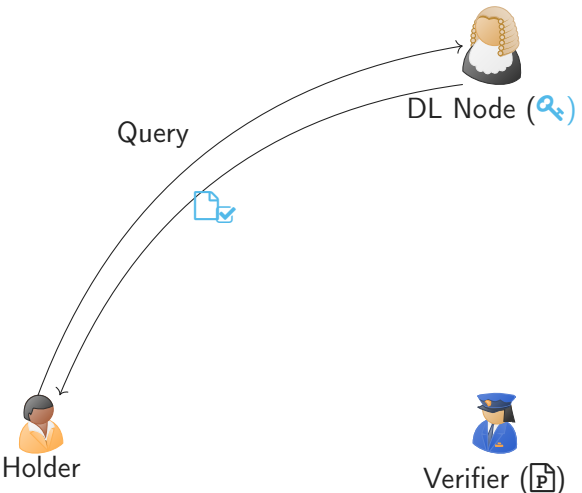
Ledger State Attestations: Concept

Contribution: *We augment DL data to be trustable by an offline verifier.*



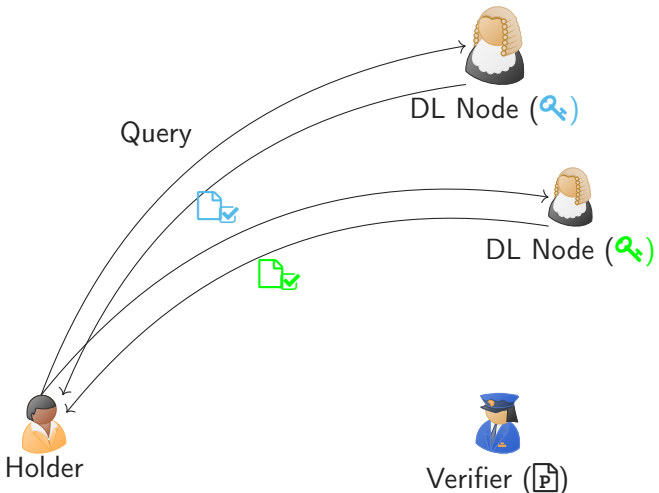
Ledger State Attestations: Concept

Contribution: *We augment DL data to be trustable by an offline verifier.*



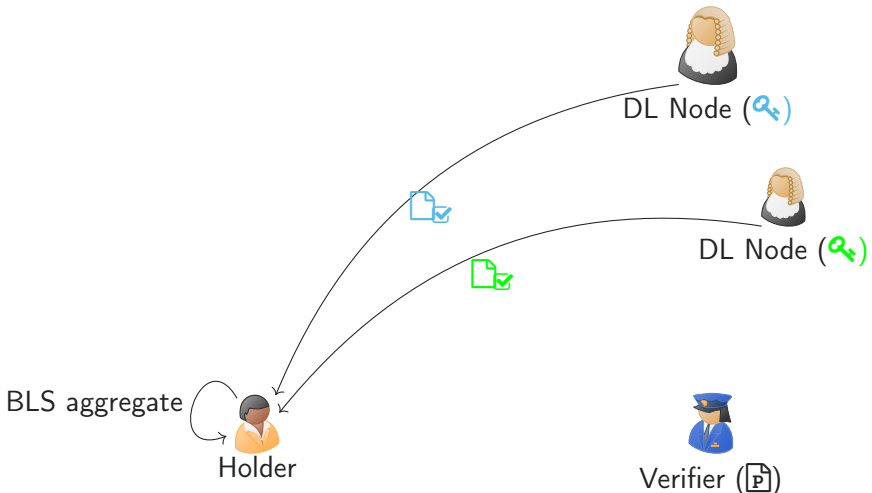
Ledger State Attestations: Concept

Contribution: *We augment DL data to be trustable by an offline verifier.*



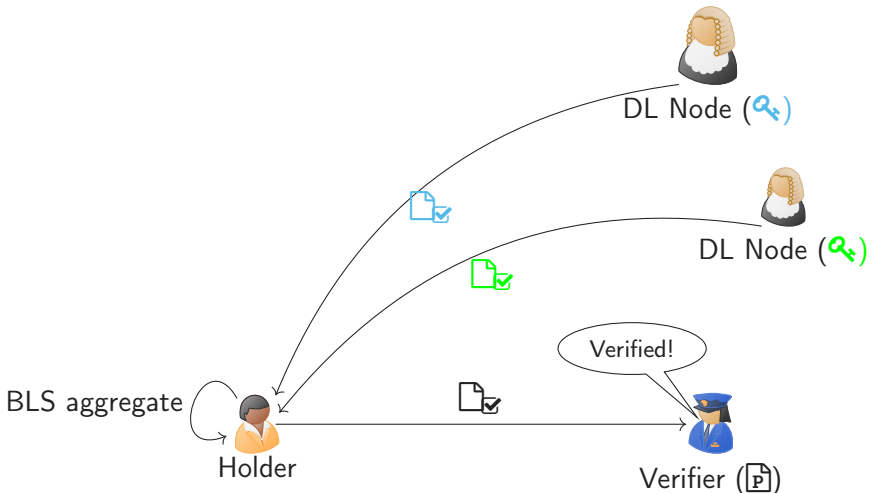
Ledger State Attestations: Concept

Contribution: *We augment DL data to be trustable by an offline verifier.*



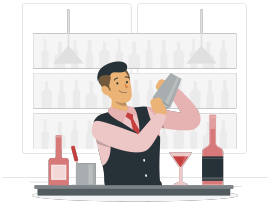
Ledger State Attestations: Concept

Contribution: *We augment DL data to be trustable by an offline verifier.*

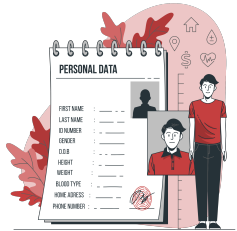


Publication

More, S., Heher, J., Walluschek, C., "Offline-verifiable Data from Distributed Ledger-based Registries". In: *SECRYPT*. 2022

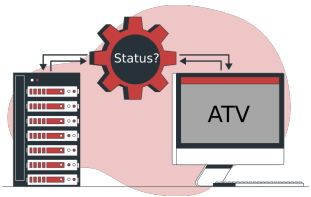


Bar Visit: Age Check



A lot of data revealed

☑ zkTPL



State learns about visit

☑ LSA

Overall Summary

Global
Trust Infrastructure

Overall Summary

Global
Trust Infrastructure

TPL Trust- &
Access-Policies

Overall Summary

Global
Trust Infrastructure

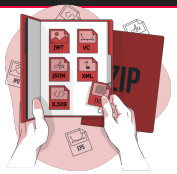
TPL Trust- &
Access-Policies

Credential Format
Interoperability

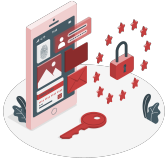
Overall Summary

Global
Trust Infrastructure

TPL Trust- &
Access-Policies



Credential Format
Interoperability

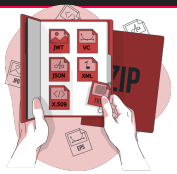


Privacy-enhanced
Access Policies

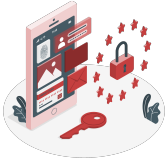
Overall Summary

Global
Trust Infrastructure

TPL Trust- &
Access-Policies



Credential Format
Interoperability



Privacy-enhanced
Access Policies

Ledger State
Attestations

Contribution Summary

18 Publications

+1 under submission

8 First Author

Contribution Summary

18 Publications

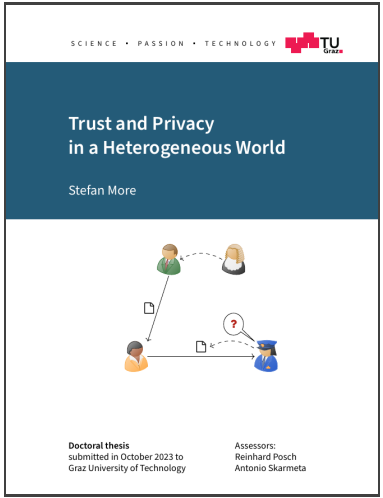
+1 under submission

8 First Author

Service & Community

- PC (OID, ARES SECPID)
- Session Chairing

- 3 Horizon 2020 Projects
- CTF Team Coordinator
- CryptoParty Founder



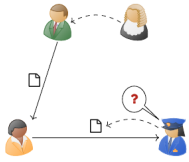
Thank you for your attention!

And your support!

SCIENCE • PASSION • TECHNOLOGY

Trust and Privacy in a Heterogeneous World

Stefan More



Doctoral thesis
submitted in October 2023 to
Graz University of Technology

Assessors:
Reinhard Posch
Antonio Skarmeta

- Illustrations by Storyset.com
- LaTeX icons: tikzsymbols, tikzpeople, fontawesome, worldflags

[AMM+21] Alber, L. "Adapting the TPL Trust Policy Language for a Self-Sovereign Identity World". In: *Open Identity Summit*. Vol. P-312. LNI. Gesellschaft für Informatik e.V., 2021, pp. 107–118.

[GJ19] Graux, H., Jacobs, E., *LIGHTest D4.7 Cross-Border Legal Compliance and Validity of Trust Scheme Translation*. https://www.lightest.eu/static/deliverables/D4.7.pdf. online, accessed on 17 February 2023. LIGHTest Consortium, 2019.

[MA22] **More, S.**, Alber, L., "YOU SHALL NOT COMPUTE on my Data: Access Policies for Privacy-Preserving Data Marketplaces and an Implementation for a Distributed Market using MPC". In: *ARES*. ACM, 2022, 137:1–137:8.

[MGH+21] **More, S.** "Trust Me If You Can: Trusted Transformation Between (JSON) Schemas to Support Global Authentication of Education Credentials". In: *SEC*. Vol. 625. IFIP Advances in Information and Communication Technology. Springer, 2021, pp. 19–35.

[MHW22] **More, S.**, Heher, J., Walluschek, C., "Offline-verifiable Data from Distributed Ledger-based Registries". In: *SECRYPT*. SCITEPRESS, 2022, pp. 687–693.

[Mor23] **More, S.** "Trust Scheme Interoperability: Connecting Heterogeneous Trust Schemes". In: *ARES*. ACM, 2023, 124:1–124:9.

[MRA+22] **More, S.** "Extending Expressive Access Policies with Privacy Features". In: *TrustCom*. IEEE, 2022, pp. 574–581.

[MSW+19] Mödersheim, S. "TPL: A Trust Policy Language". In: *IFIPTM*. Vol. 563. IFIP Advances in Information and Communication Technology. Springer, 2019, pp. 209–223.

[WWM+19] Wagner, G. "DNS-based Trust Scheme Publication and Discovery". In: *Open Identity Summit*. Vol. P-293. LNI. GI, 2019, pp. 49–58.