Self-Sovereign Identity: Proving Power over Legal Entities

Master’s Thesis Defense

Tim Speelman

KVK

TU Delft

POLITIE

Kopie

EENHEID OOST-NEDERLAND
DISTRICT GELDERLAND-ZUID
BASISTEAM TWEESTROMENLAND
Telefoon 0900 8844

Proces-verbaalnummer : [redacted]

PROCES-VERBAAL
aangifte

Feit	: Gekwalificeerde diefstal in/uit bedrijf/kantoor
Plaats delict	: [redacted]
Pleegdatum/tijd	: Tussen vrijdag 29 mei 2020 om 17:30 uur en maandag 1 juni 2020 om 16:00 uur

Ik, verbalisant, [redacted], hoofdagent van politie Eenheid Oost-Nederland, verklaar het volgende:

Op dinsdag 2 juni 2020 om 07:47 uur, kwam ik ter plaatse van het misdrijf op de locatie [redacted] Nijmegen, bij een persoon die mij opgaf te zijn:[2]

What is identity?

- Latin *identitas: sameness.*
- These claims are about the *same* subject:
  - .. is 28 years old,
  - .. is male,
  - .. has Master's degree
  - .. is named *Tim Speelman*
  - .. has BSN *209051251*
  - .. has e-mail *timspeelman@live.nl*

Attributes

Identifiers

Attributes

What is identity?

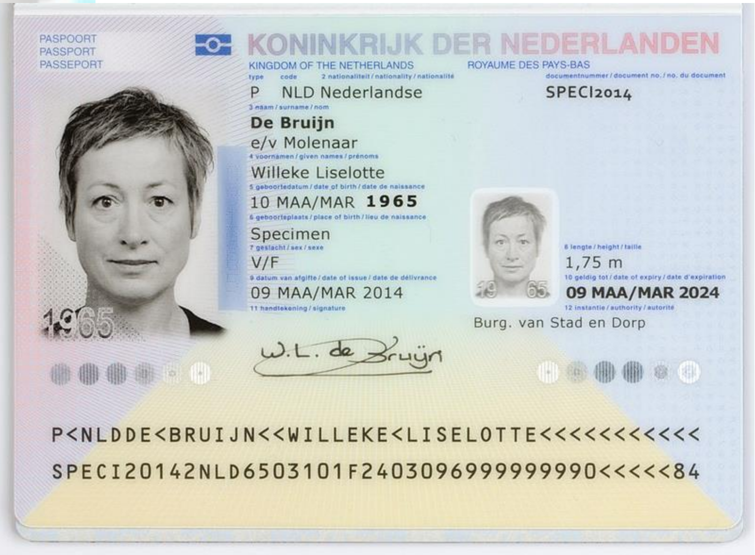
Person

Identifier

Tim

Attribute

Has Master’s degree



PASPOORT
PASSPORT
PASSEPORT

KONINKRIJK DER NEDERLANDEN
KINGDOM OF THE NETHERLANDS ROYAUME DES PAYS-BAS

type code 2 nationaliteit / nationality / nationalité
P NLD Nederlandse

documentnummer / document no. / no. du document
SPECI2014

3 naam / surname / nom
De Bruijn
e/v Molenaar

4 voornamen / given names / prénoms
Willeke Liselotte

5 geboortedatum / date of birth / date de naissance
10 MAA/MAR **1965**

6 geboorteplaats / place of birth / lieu de naissance
Specimen

7 geslacht / sex / sexe
V/F

8 lengte / height / taille
1,75 m

9 datum van afgifte / date of issue / date de délivrance
09 MAA/MAR 2014

10 geldig tot / date of expiry / date d'expiration
09 MAA/MAR 2024

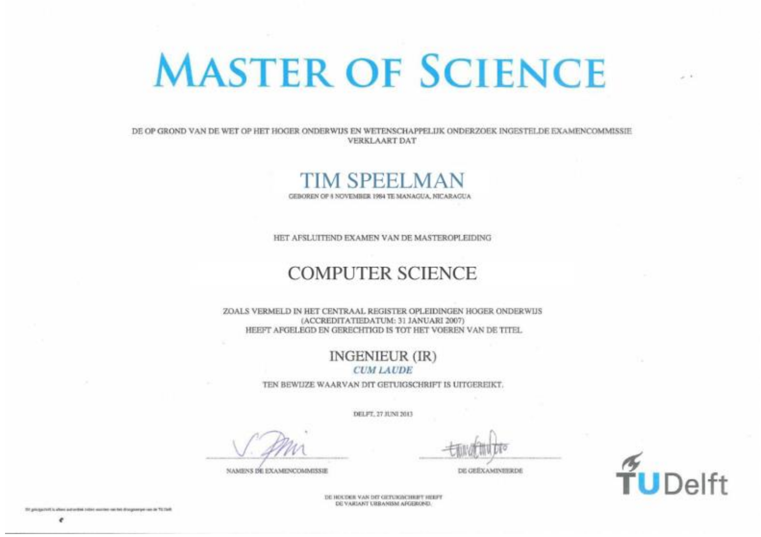
11 handtekening / signature
W.L. de Bruijn

12 instantie / authority / autorité
Burg. van Stad en Dorp

1965

19 65

```
P<NLDDE<BRUIJN<<WILLEKE<LISELOTTE<<<<<<<<<<<
SPECI20142NLD6503101F2403096999999990<<<<<84
```



MASTER OF SCIENCE

DE OP GROND VAN DE WET OP HET HOGER ONDERWIJS EN WETENSCHAPPELIJK ONDERZOEK INGESTELDE EXAMENCOMMISSIE
VERKLAART DAT

TIM SPEELMAN
GEBOREN OP 8 NOVEMBER 1984 TE MANAGUA, NICARAGUA

HET AFSLUITEND EXAMEN VAN DE MASTEROPLEIDING

COMPUTER SCIENCE

ZOALS VERMELD IN HET CENTRAAL REGISTER OPLEIDINGEN HOGER ONDERWIJS
(ACCREDITATIEDATUM: 31 JANUARI 2007)
HEEFT AFGELEGD EN GERECHTIGD IS TOT HET VOEREN VAN DE TITEL

INGENIEUR (IR)
CUM LAUDE

TEN BEWIJZE WAARVAN DIT GETUIGSCHRIFT IS UITGEREIKT.

DELFT, 27 JUNI 2013

NAMENS DE EXAMENCOMMISSIE

DE GEËXAMINEERDE

DE HOUDER VAN DIT GETUIGSCHRIFT HEEFT
DE VARIANT URBANISM AFGEROND.

[illegible]

TU Delft

What is identity?

Communication between trusted party and a relying party (Bob)

1. Direct communication:

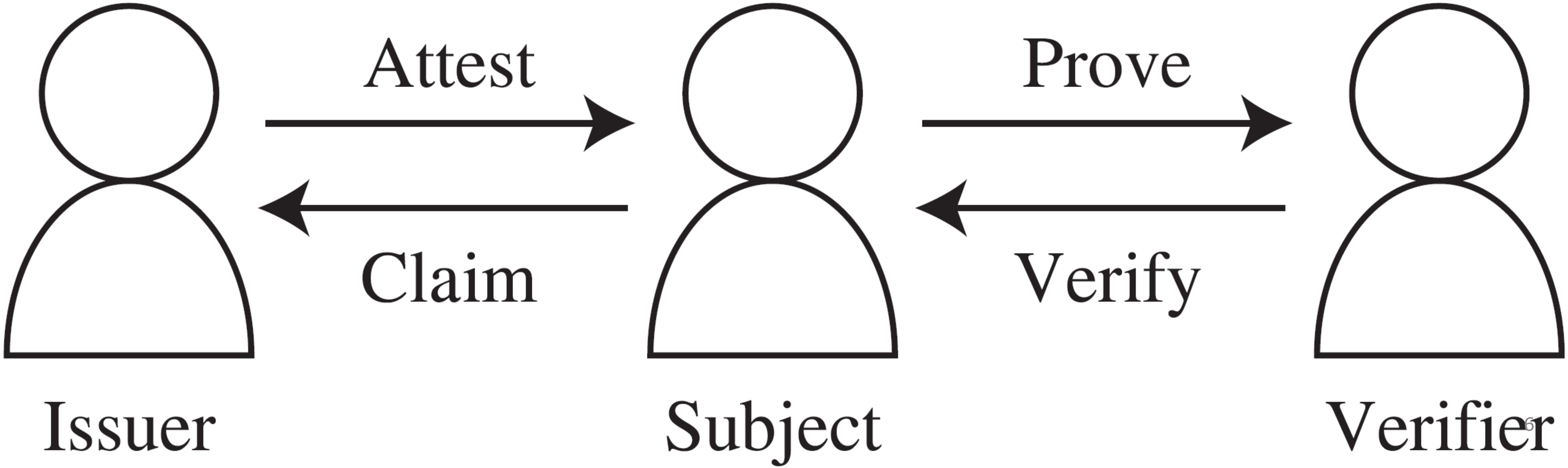
    harms independence and privacy

2. Alternative: Tamper-proof credential (unforgeable)

[Use one example]

Intro / Self-Sovereign Identity

- User in control with one app: agent (or *wallet*).
  - Agent manages identifiers (and secrets)
  - Agent manages attributes (linked to those identifiers)
  - Interoperability: one app in all cases



Research Challenge

Universal identity infrastructure with validity across **wide range** of identity problems, for natural persons and legal entities.

Methodology

Incremental approach. [immersed in practice]

1. Create **theoretical framework** for self-sovereignty.
2. Design and prototype **infrastructure** for one use case.
3. Experimentally validate resulting technology.

Intro

Research Challenge

Methodology

> Starting Point: TrustChain

Case Study

Universal SSI infrastructure

Experimental Validation

Conclusion

Starting Point: TrustChain (1/2)

- Academic peer-to-peer networking stack supporting SSI.

- Ongoing experiment by TU Delft, Dutch government, IDEMIA.
- Next phase: integration with third parties.

Starting Point: TrustChain (2/2)

- Create pseudonyms: public/private keypairs.
- Secure peer to peer networking
  - Identity based: send to public key.
  - Android to Android, without servers
- Attesting to attributes
- Verifying attributes

- What binds a pseudonym to a real person?
  - 1st factor: holds the private key
- **Passport-grade authentication** using real time facial recognition (selfie).

Intro

Research Challenge

Methodology

Starting Point: TrustChain

> Case Study

Problem

Step 1: Entrepreneur Passport

Step 2: Peer-to-peer authorisation

Universal SSI infrastructure

Experimental Validation

Conclusion

Problem

Use Self-Sovereign Identity to ..

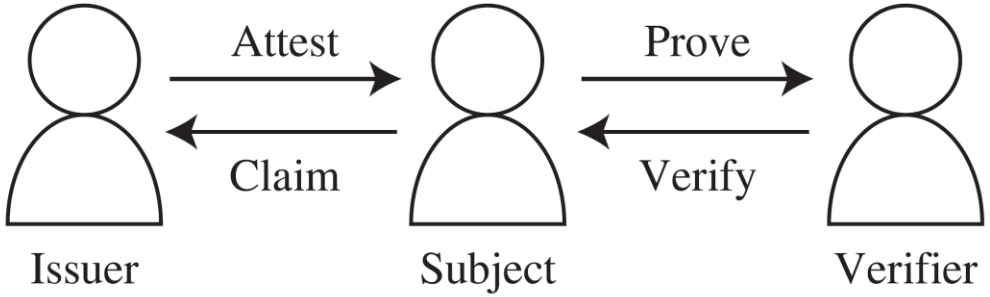
prove that a person is authorised to act on behalf of some legal entity (organisation).

KVK

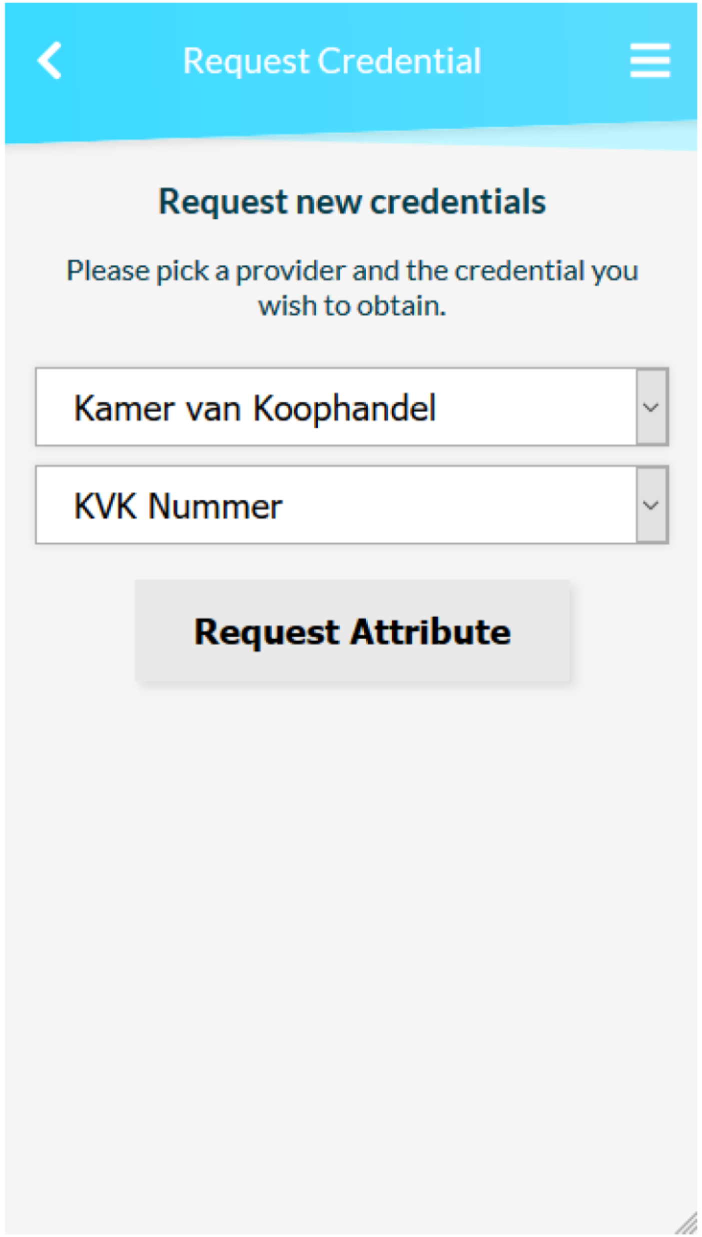
Scope: Netherlands, Dutch legal system

Step 1. Entrepreneur Passport

- Trade Register (KVK):
  - Stores legal entities by KVK number.
  - Maps natural persons (BSN) to legal entities (KVKNR)
- Issuing procedure:
  1. Verify $\mathtt{Nym:BSN(x)}_{\mathtt{NL}}$
  2. Look up $\mathtt{KVKNR}$ $\mathtt{L}$ belonging to $\mathtt{BSN}$ $\mathtt{x}$
  3. Attest $\mathtt{Nym:FULL(L)}_{\mathtt{KVK}}$



- Authentication Risk (both when issuing and when verifying)
  - $\mathtt{Nym:FULL(L)}_{\mathtt{KVK}}$ conditional on $\mathtt{Nym:BSN(x)}_{\mathtt{NL}}$ blinded

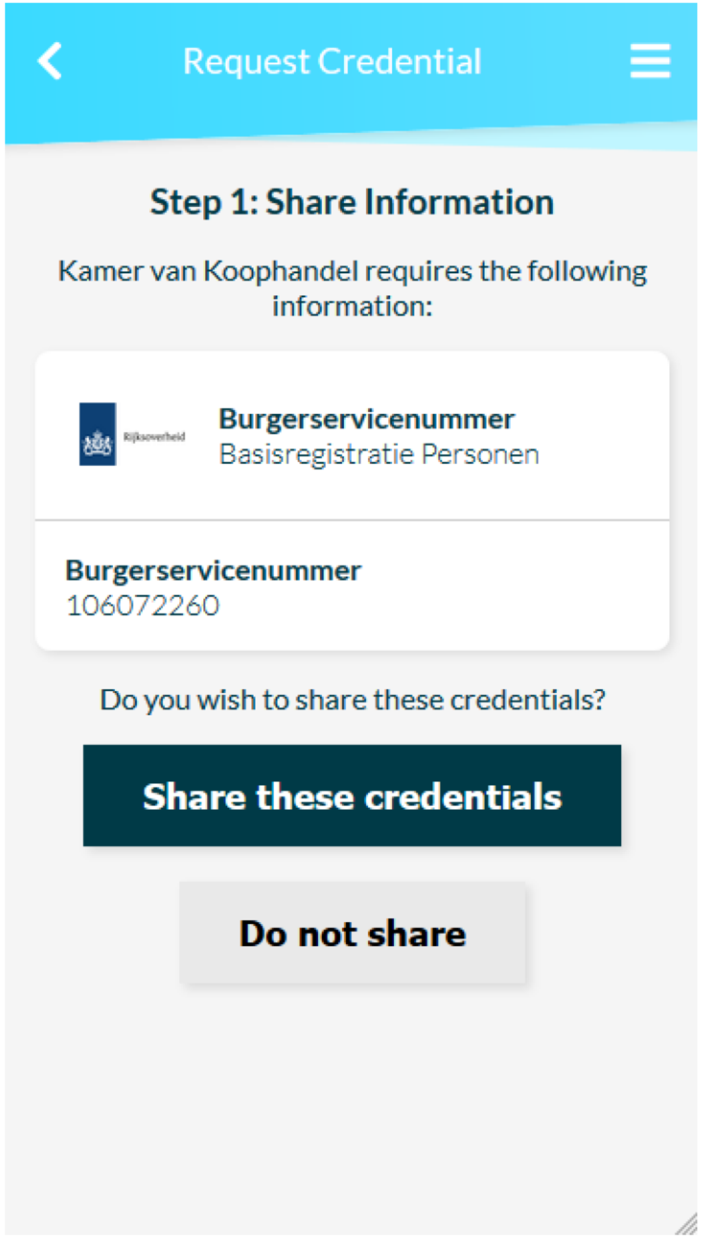


Request new credentials

Please pick a provider and the credential you wish to obtain.

Kamer van Koophandel

KVK Nummer



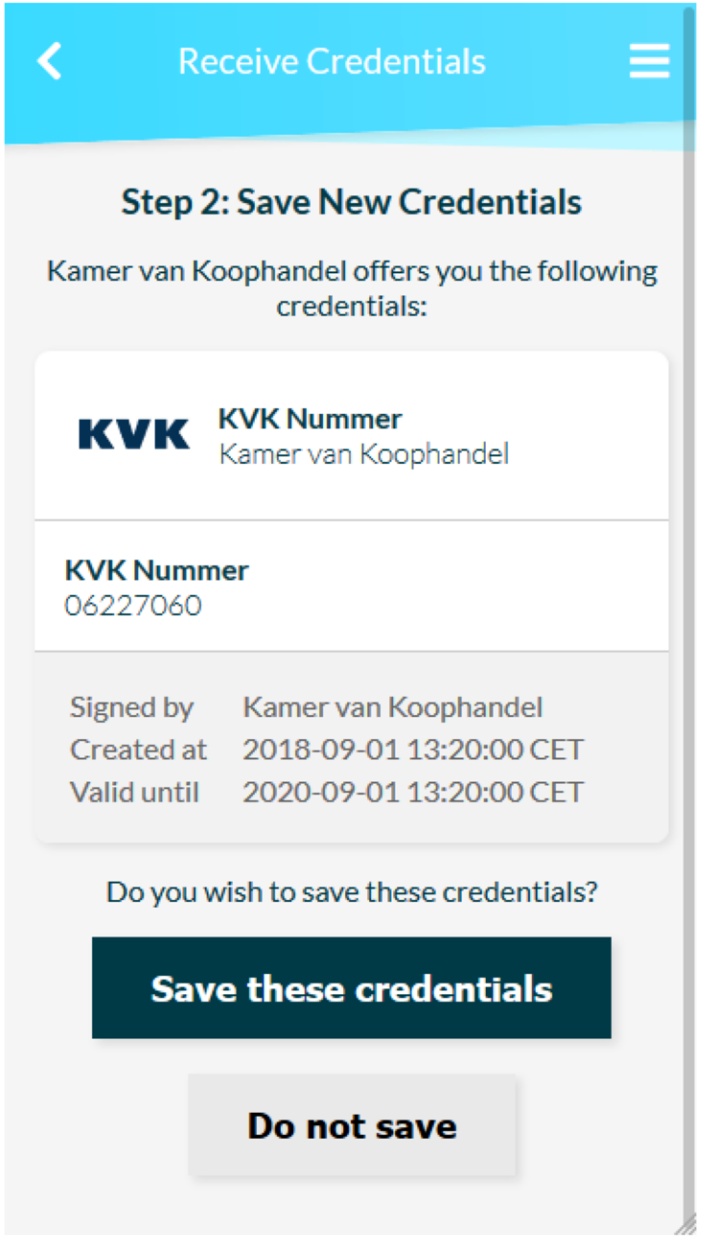
Step 1: Share Information

Kamer van Koophandel requires the following information:

Burgerservicenummer
Basisregistratie Personen

Burgerservicenummer
106072260

Do you wish to share these credentials?



Step 2: Save New Credentials

Kamer van Koophandel offers you the following credentials:

KVK Nummer
Kamer van Koophandel

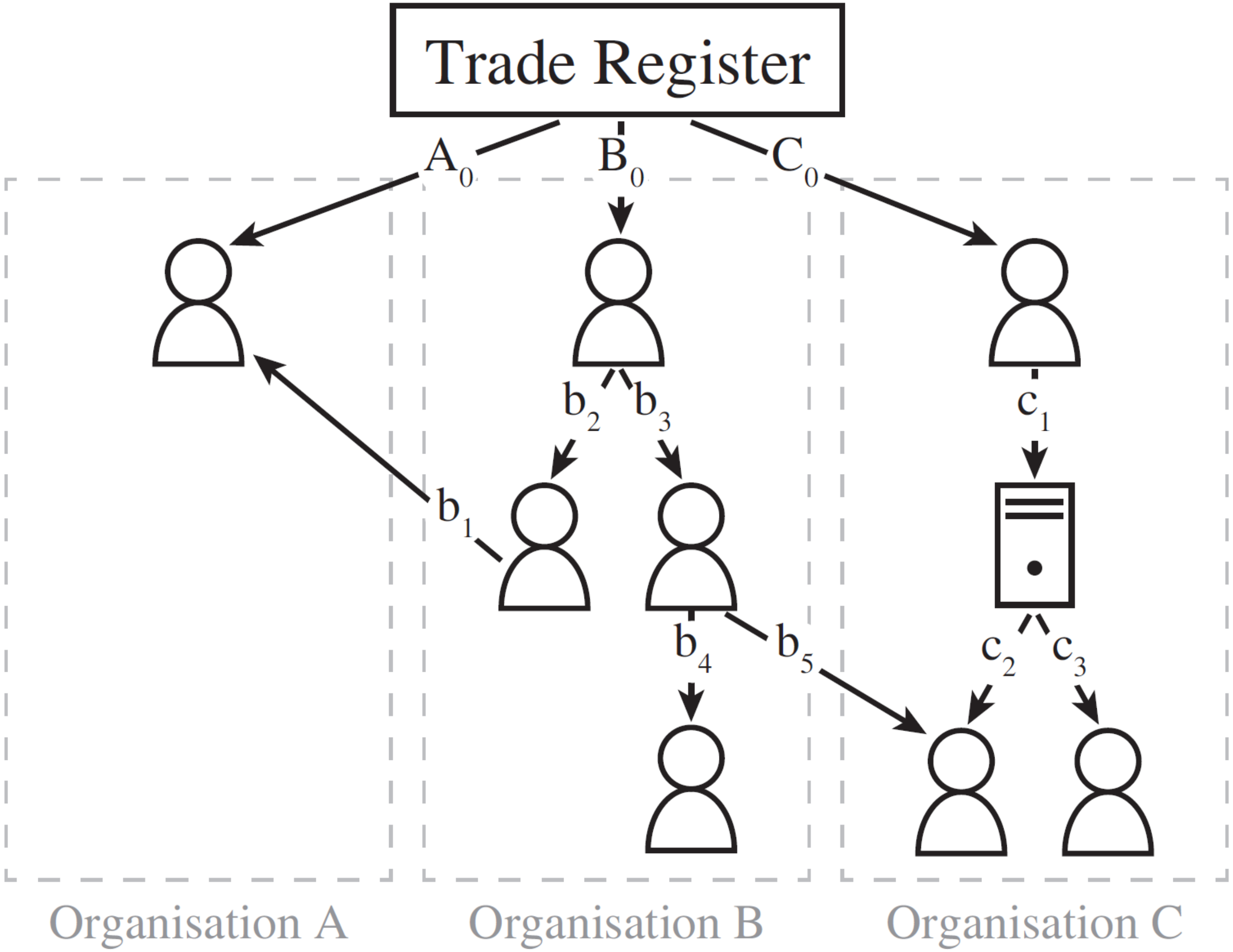
KVK Nummer
06227060

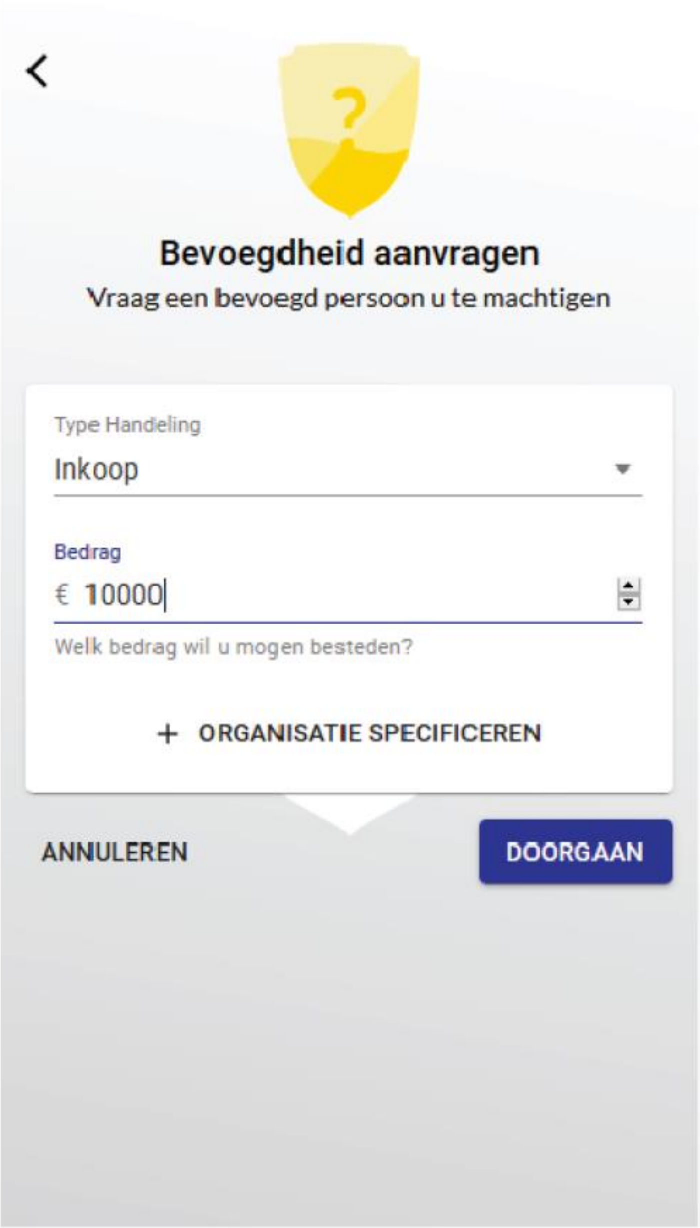
Signed by	Kamer van Koophandel
Created at	2018-09-01 13:20:00 CET
Valid until	2020-09-01 13:20:00 CET

Do you wish to save these credentials?

Step 2. Peer-to-peer authorisation

- Attributes
  - `Auth(P,L)`: Authorized
- Issuing procedure:
  1. Verify `Nym` belongs to Bettie.
  2. Attest `Nym`:`FULL(L)`$_{x}$
- Authentication Risk
  - `Nym`:`FULL(L)`$_{x}$ conditional on `Nym`:`BSN(x)`$_{NL}$





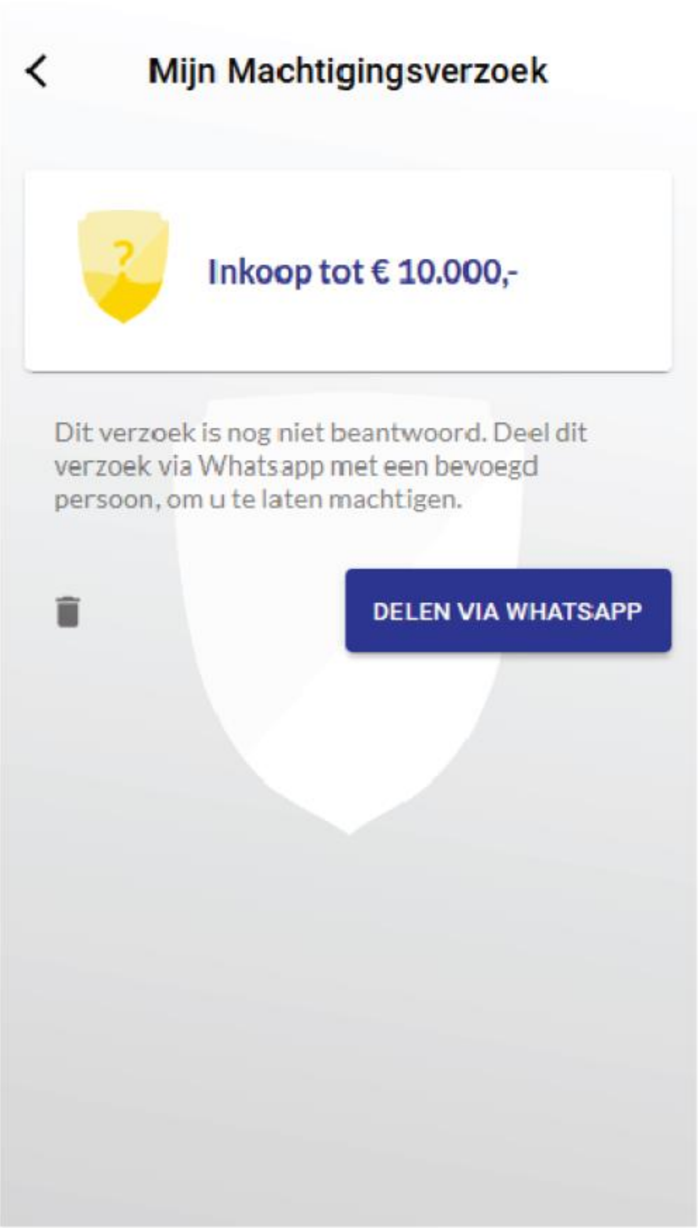
Bevoegdheid aanvragen

Vraag een bevoegd persoon u te machtigen

Type Handeling: Inkoop

Bedrag: € 10000

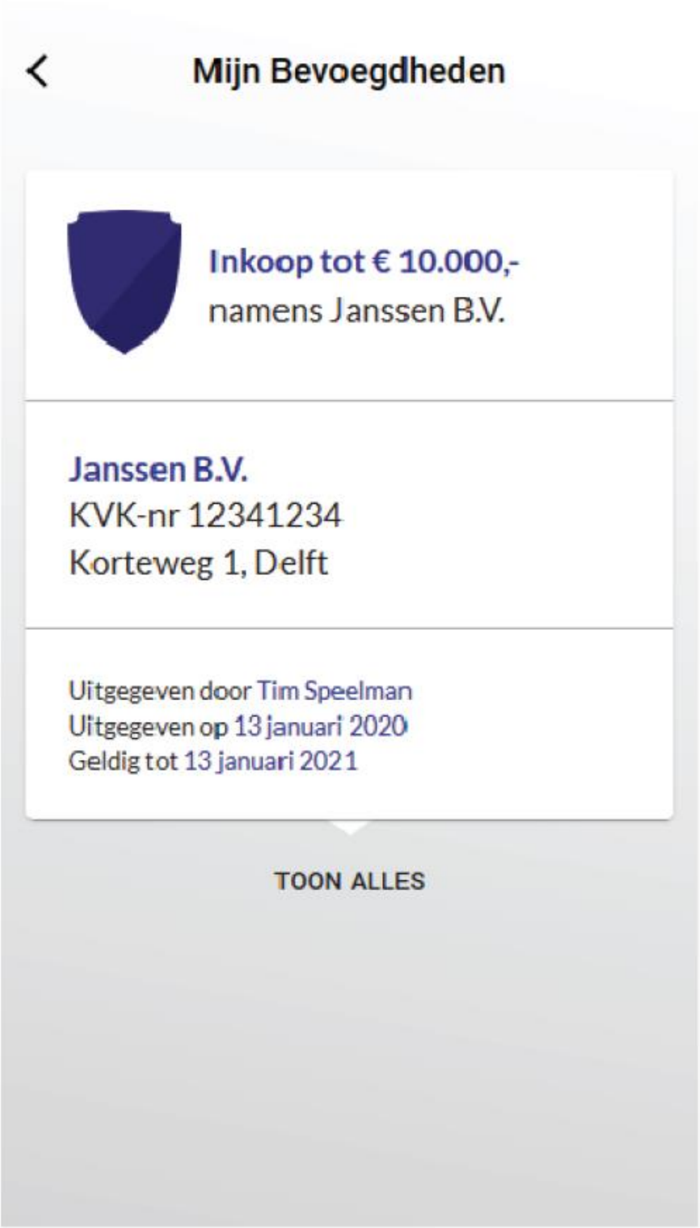
Welk bedrag wil u mogen besteden?



Mijn Machtigingsverzoek

Inkoop tot € 10.000,-

Dit verzoek is nog niet beantwoord. Deel dit verzoek via Whatsapp met een bevoegd persoon, om u te laten machtigen.



Mijn Bevoegdheden

Inkoop tot € 10.000,-
namens Janssen B.V.

Janssen B.V.
KVK-nr 12341234
Korteweg 1, Delft

Uitgegeven door Tim Speelman
Uitgegeven op 13 januari 2020
Geldig tot 13 januari 2021

Step 2. Peer-to-peer authorisation

Verification

A person S proves to a verifier V that he has power P over legal entity L.

Requirements:

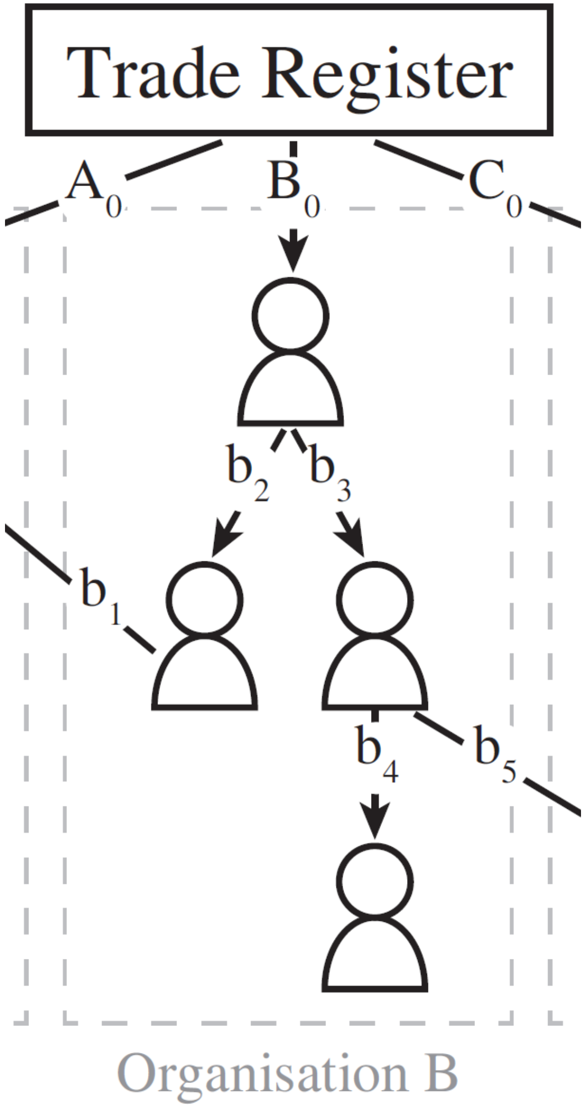
1. V needs attributes of entire chain.
2. V must trust these attributes.
3. Attributes must provide power P.

Step 2. Peer-to-peer authorisation

Verification: Collecting Attributes

- Interactive (online)
- Passive (public, offline)
- Proxy (via subject)

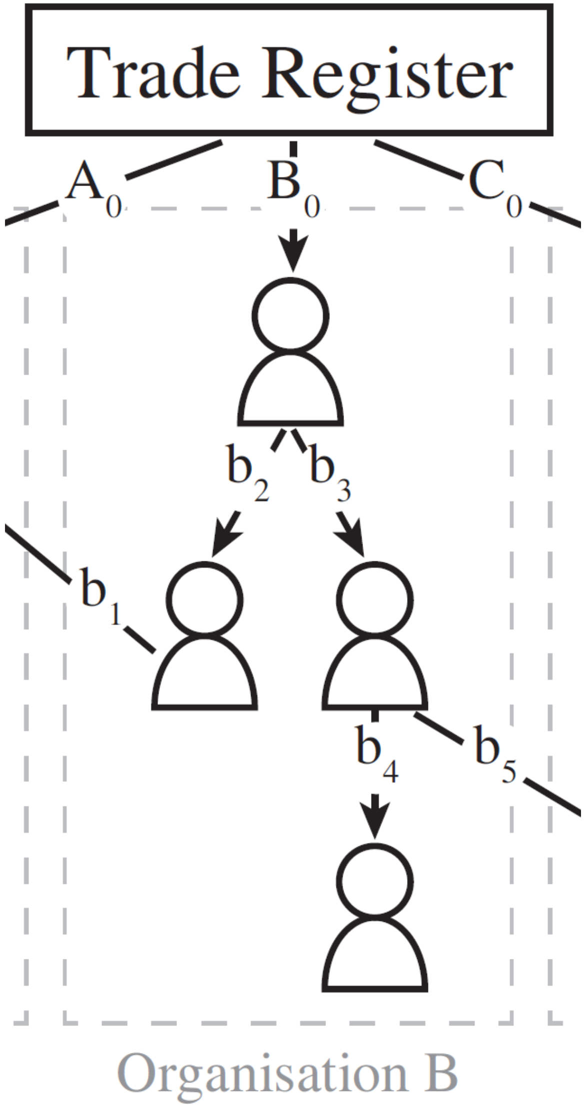
Preferred: Proxy or Passive



Step 2. Peer-to-peer authorisation

Verification: Power Evaluation

- Pow(): S_2 assigned power P over L to S_1
- Trust(): S is trusted to have power P over L
- Q(S,P,L): *S has power P over L*
    - A trusted root S_n for which hold Trust(Sn, Pn, L),
    - Attributes satisfy Pow(S_i , P_i , L, S_{i+1}) for i in N<n
    - P_i <= P_{i+1} for all i



Step 2. Peer-to-peer authorisation

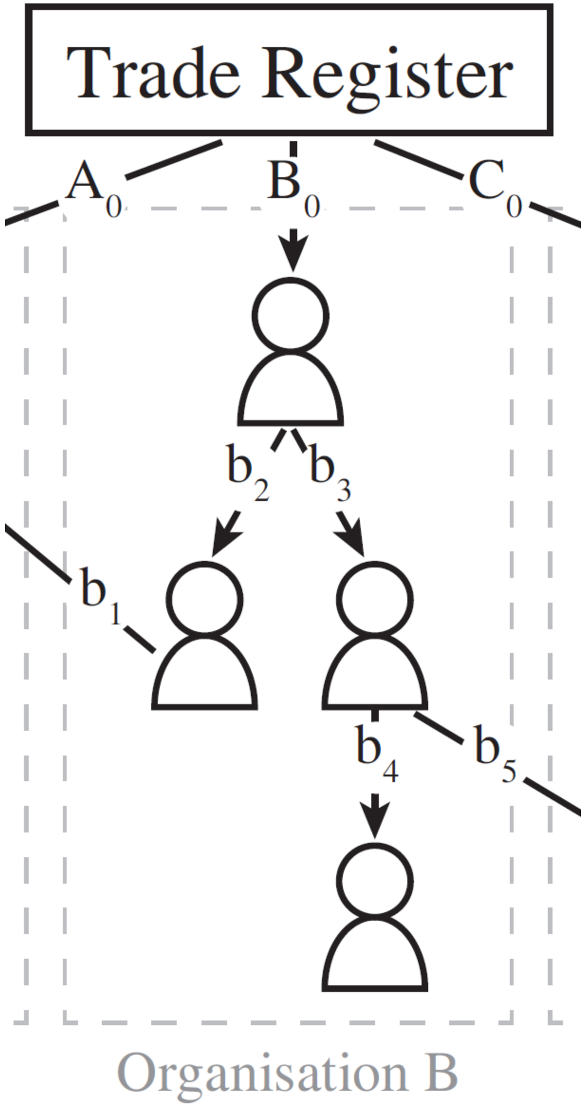
Verification: conditions for Trust

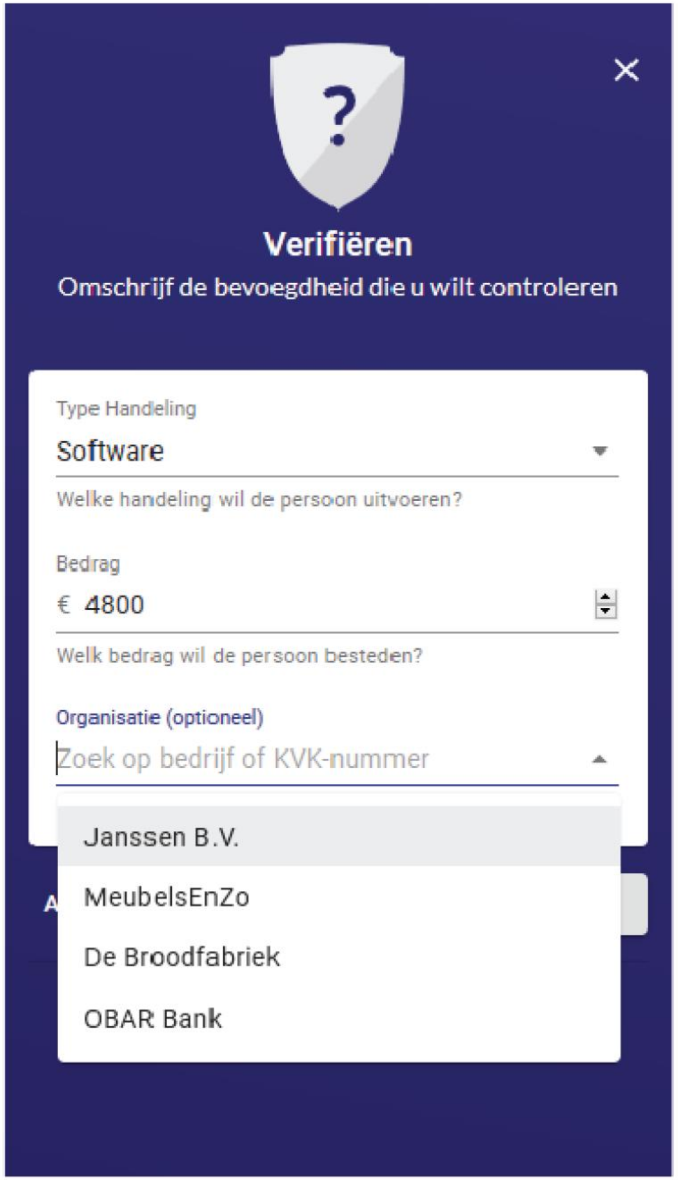
Individual responsibility

Authentication

System Integrity

Requires (missing) revocation.





Verifiëren

Omschrijf de bevoegdheid die u wilt controleren

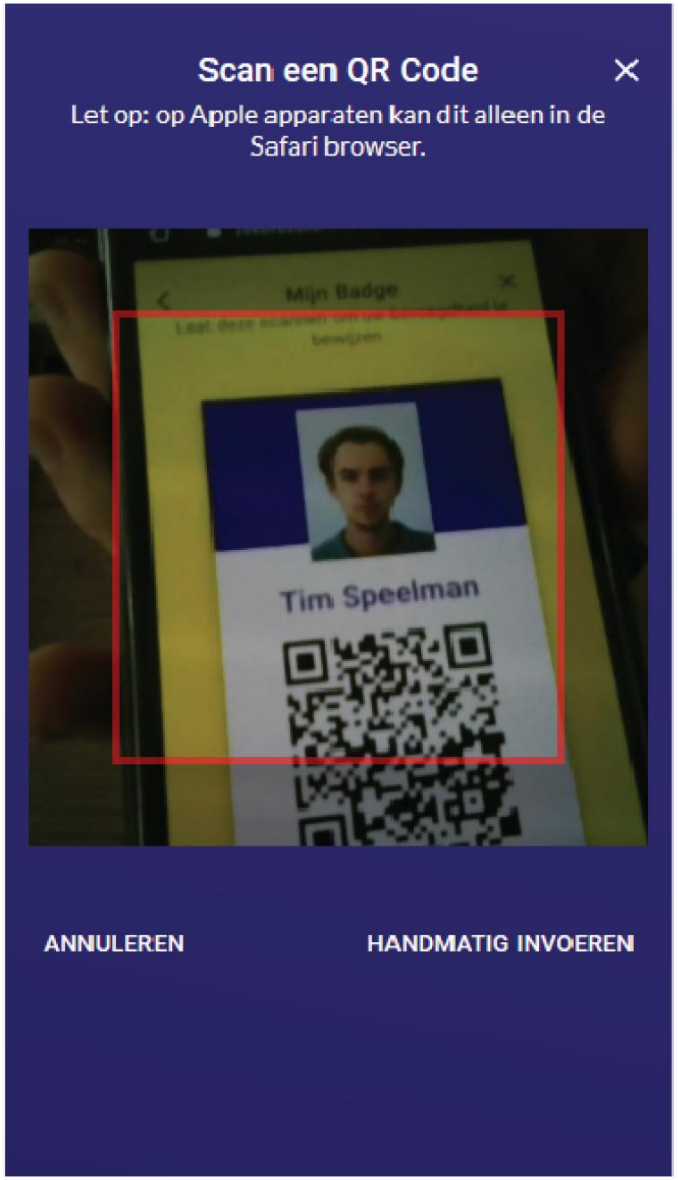
Type Handeling: Software

Welke handeling wil de persoon uitvoeren?

Bedrag: € 4800

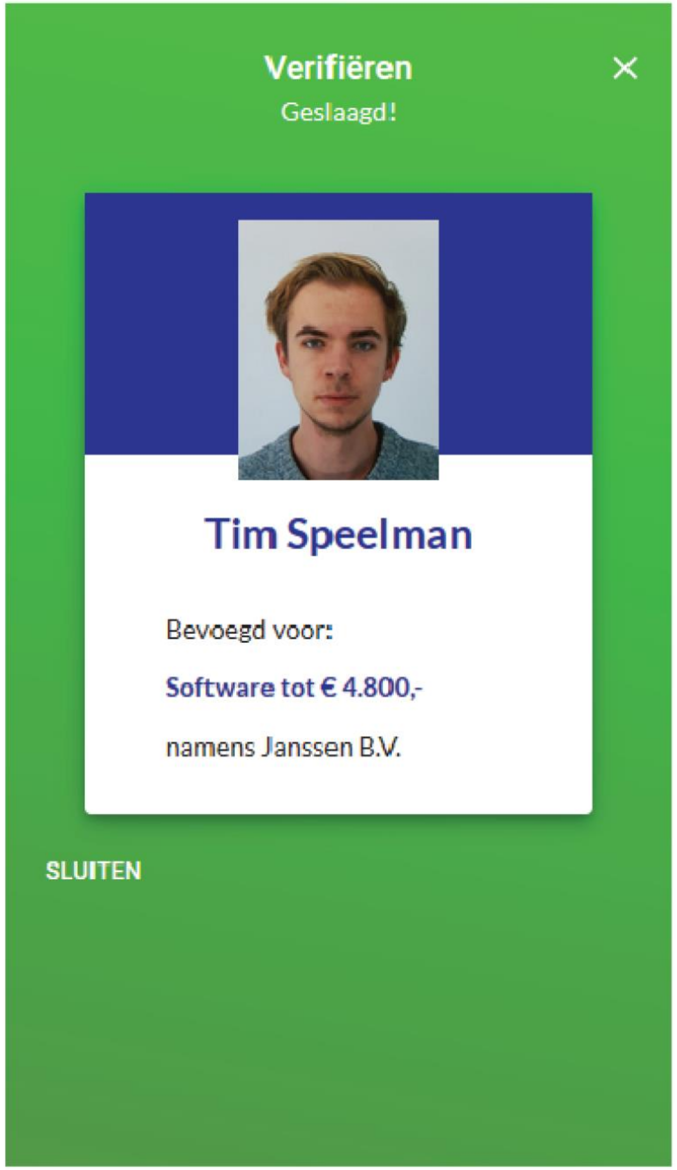
Welk bedrag wil de persoon besteden?

Organisatie (optioneel): Zoek op bedrijf of KVK-nummer



Scan een QR Code

Let op: op Apple apparaten kan dit alleen in de Safari browser.



Verifiëren

Geslaagd!

Tim Speelman

Bevoegd voor:

Software tot € 4.800,-

namens Janssen B.V.

Attribute Actuality

- Trade Register frequently changes.
- Authorisations should be revocable any time.
- Existing method: Attribute expiration.
- Alternate method: Public single-sided revocation.
    - New requirement for TrustChain

Intro

Research Challenge

Methodology

Starting Point: TrustChain

Case Study

> Universal SSI infrastructure

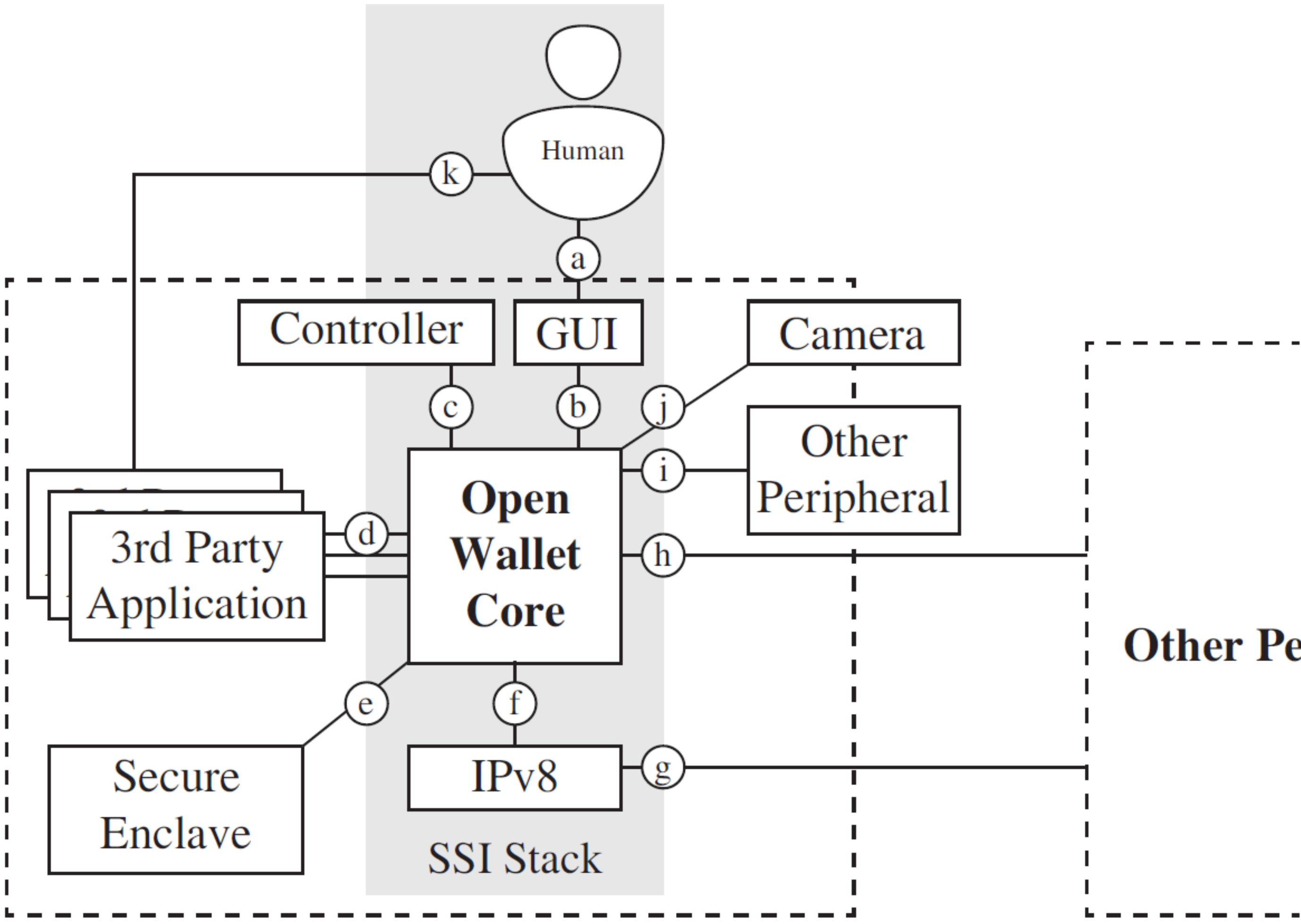
- Architecture
- Authentication

Experimental Validation

Conclusion

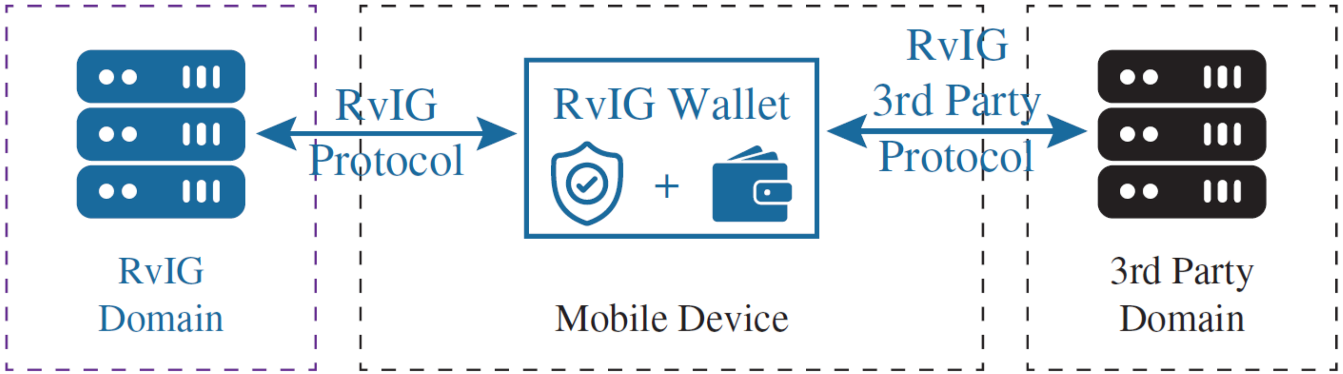
Universal SSI infrastructure

- Universal Wallet
- Collects keys and attributes
- Human interface
- Programmable Controller: KVK
- 3rd party apps
- Communicate via OW/IPv8



Peer Device

Current Architecture (Authentication + Wallet)



RvIG Domain

RvIG Protocol

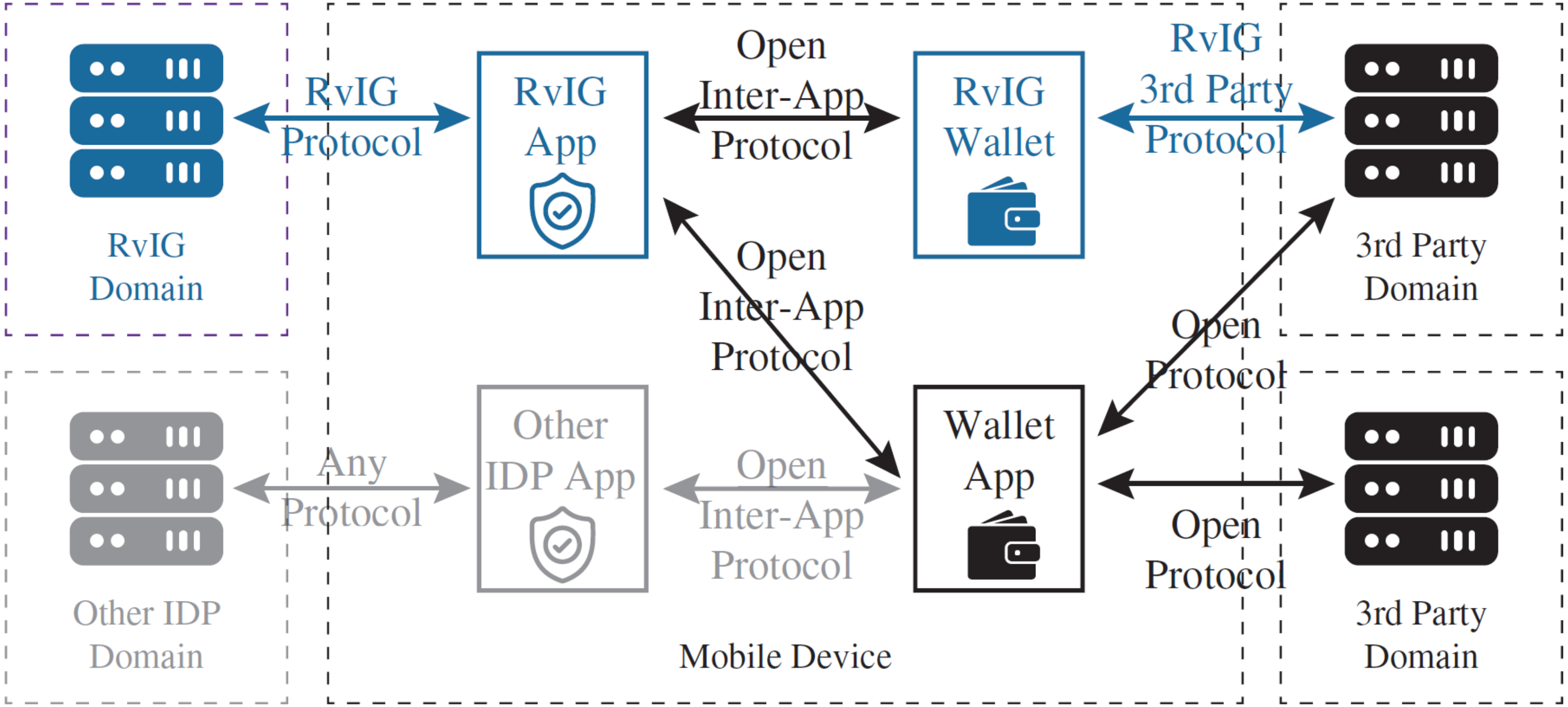
RvIG Wallet +

Mobile Device

RvIG 3rd Party Protocol

3rd Party Domain

Alternative Architecture (Separate Authentication from Wallet)



RvIG Domain

RvIG Protocol

RvIG App

Open Inter-App Protocol

RvIG Wallet

RvIG 3rd Party Protocol

3rd Party Domain

Open Inter-App Protocol

Open Protocol

Other IDP Domain

Any Protocol

Other IDP App

Open Inter-App Protocol

Wallet App

Open Protocol

3rd Party Domain

Mobile Device

Intro

Research Challenge

Methodology

Starting Point: TrustChain

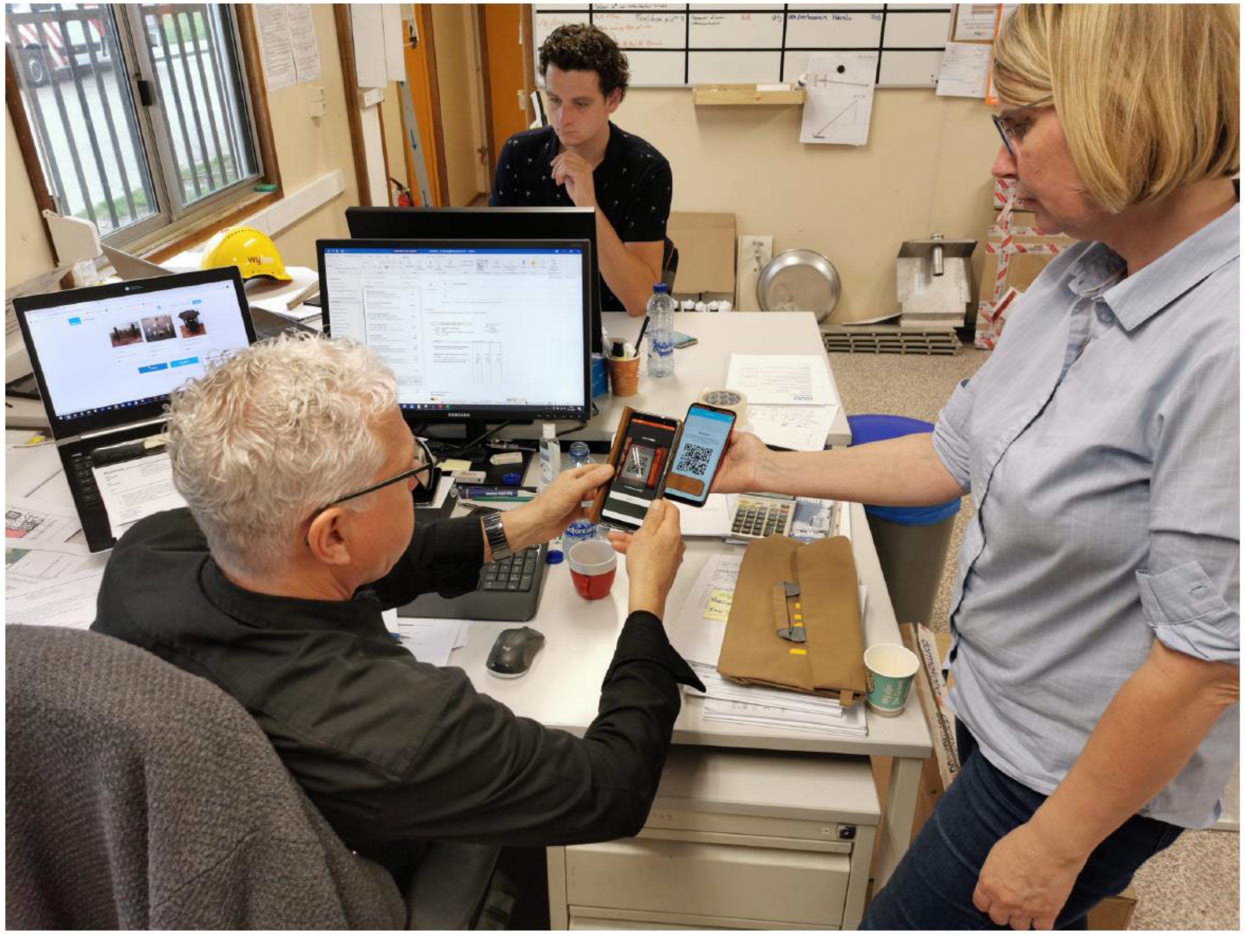
Case Study

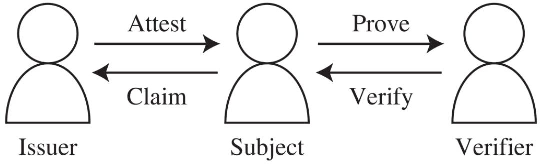
Universal SSI infrastructure

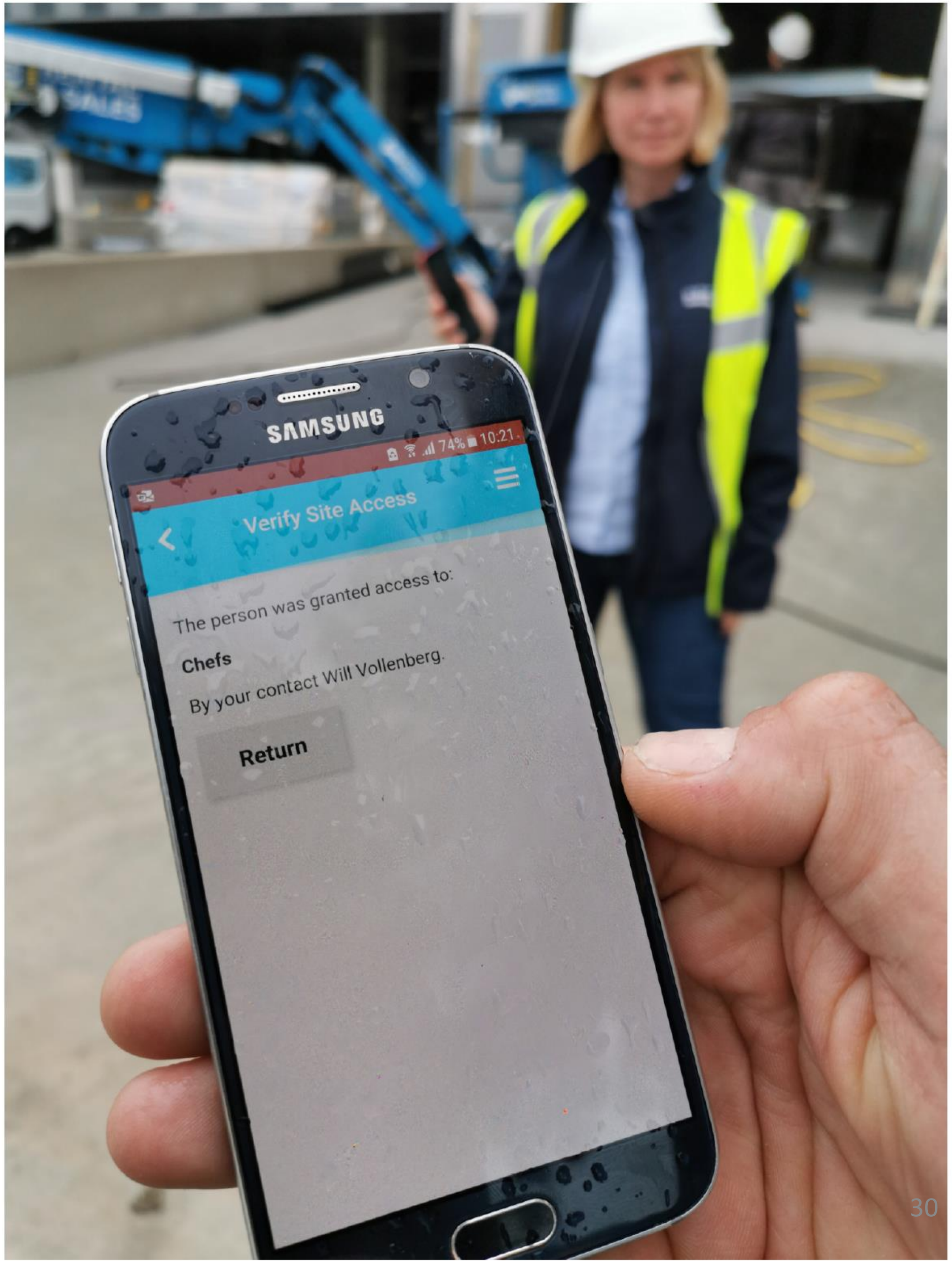
> Experimental Validation

Conclusion

UITVOERDER
UITVOERDER
Zien wij iets over het hoofd?
Meld hinder en tips
www.verbeterdeboom.nl
LEVERANCIERS
CHAUFFEURS
BEZOEKERS
Contactpersoon
DKC: 06-51139153
DE GROOT: 06-20050757
JWR:
MUCON: 06-21987051
ZND NEDICOM: 06-43011039
KKP: 491777065103
Wijnen Bouw: 06 – 10 24 99 10




Attest
Claim
Prove
Verify
Issuer
Subject
Verifier



The person was granted access to:

Chefs

By your contact Will Vollenberg.

Conclusions (1/2)

- Problem**: Use Self-Sovereign Identity to prove that a person is authorised to act on behalf of some legal entity (organisation).**
- New requirements elicited for TrustChain:
    - Public single-sided revocation required for actuality
    - Passive/Proxy Verification mechanism required for chains of issuers
- App will be further developed by KVK
- KVK can be valuable issuer (entrepreneur passport), but may be restricted by legal framework and business model

Conclusions (2/2)

- Contributions to **Research Challenge:**

  Universal identity infrastructure with validity across **wide range** of identity problems, for natural persons and legal entities.

- Semantic Layer Design
  - Independent Wallet application needed to serve user.
  - Integration with UC-specific third party apps is needed for a complex case such as authorisation by legal entities.
  - Integration with third party authentication apps is needed.
- Developed prototype contributes to interoperable SSI infrastructure.
- Theoretical framework improves discourse by adding under-emphasized principles, providing structure and elaborating on the boundaries of sovereignty.