

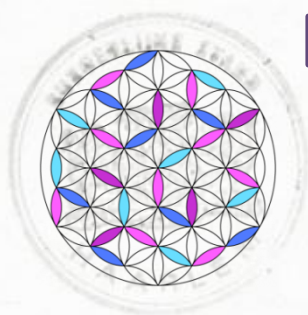


# BURGERLIJKE STAND HAARLEM

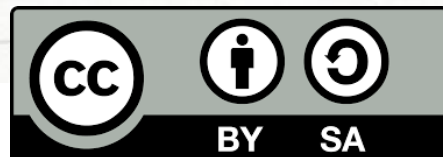
Nr. A 659

Op zeventien augustus negentienhonderd vijfenzeventig,  
te 23 uur, 55 minuten, is in de gemeente Haarlem overleden:  
Moison, Cornelis, geboren te 's-Heer-Arendskerke op  
19 juni 1886, wonende te Haarlem, echtgenoot van: Stokx,  
Adriana Johanna, zoon van: Moison, Louis en van: Verbart,  
Cornelia.

## Proofs of being registered Digital through Discipl

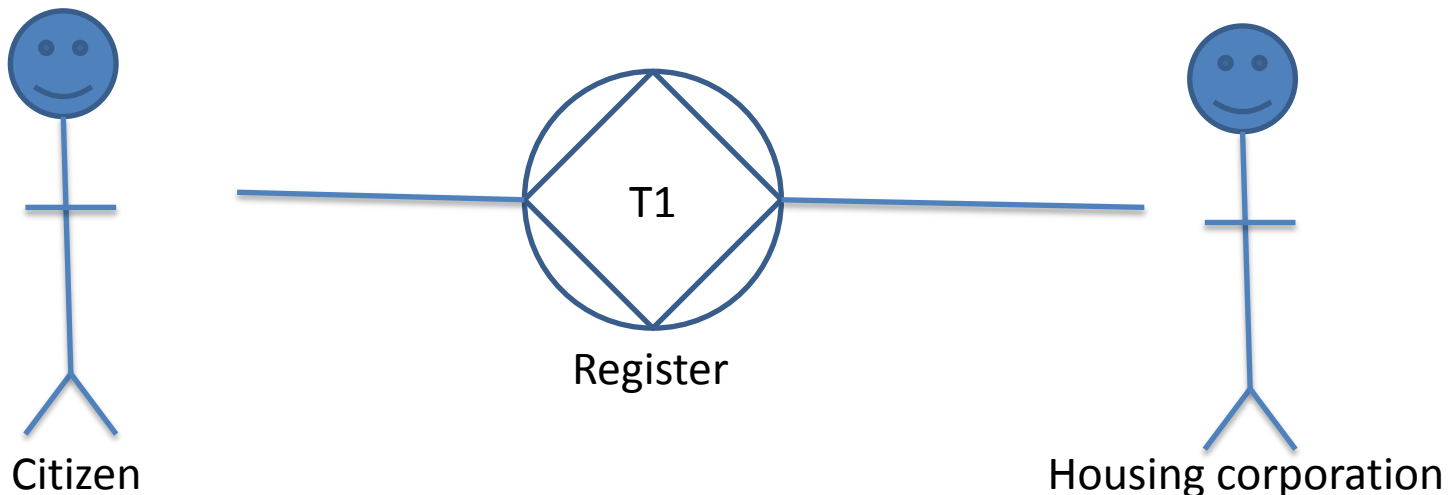


*De afgeschreven tekst stemt overeen met het origineel.*  
Haarlem, 19 AUG. 1925  
De ambtenaar van de burgerlijke stand,



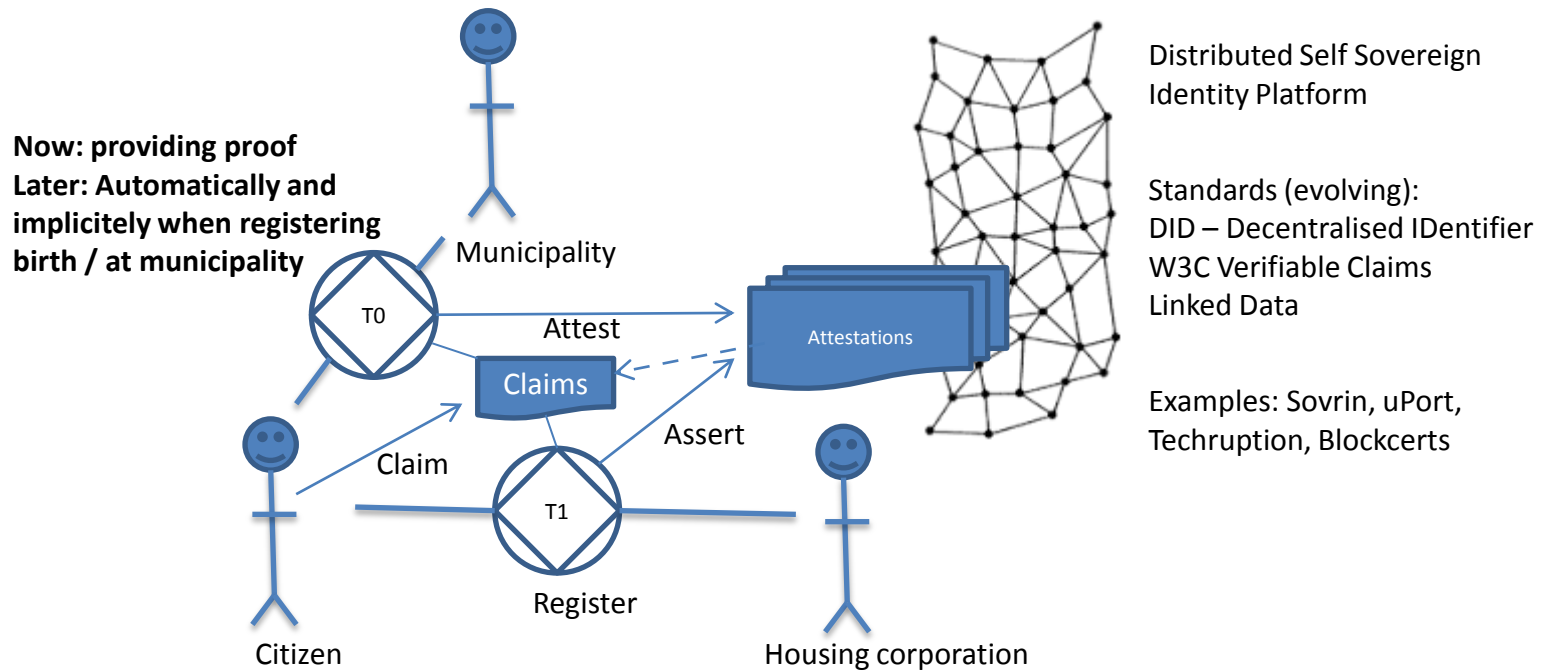
# Providing proofs

- It is a step preceding a broader use case with a corresponding universal transaction between for example a citizen and a housing corporation



# Providing proofs

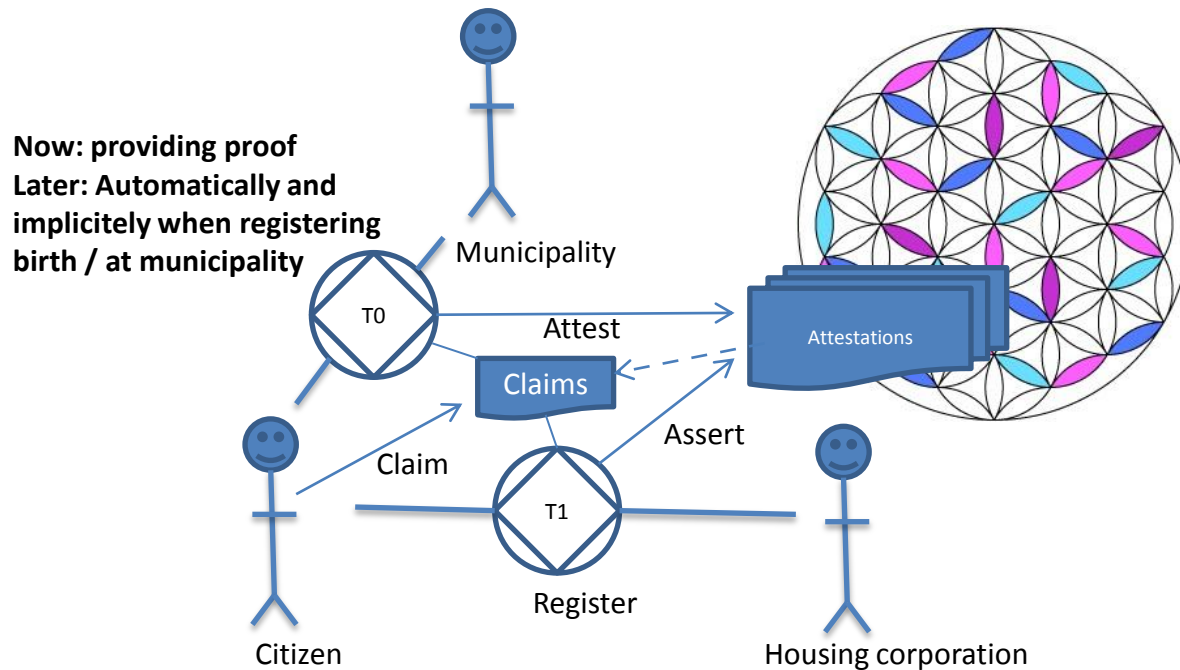
Citizen claims (claim) data to be proofed, municipality attests claim (attest), housing corporation verifies attestation on claim (assert)



- This is the same pattern as can be found in Self Sovereign Identity Platforms (SSIP)

# Providing Proofs

Citizen claims (claim) data to be proofed, municipality attests claim (attest), housing corporation verifies attestation on claim (assert)



- **Discipl is a new innovative architecture for society. Within this Discipl Core is an API for, amongst other functions, leveraging a distributed SSIP**

# About Discipl

← → ↻ ⓘ discipl.org



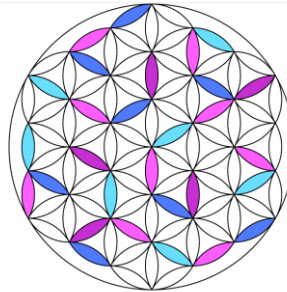
**DISCIPL**

[Discipl](#)

[Whitepaper](#)

[Github](#)

[Contact](#)



## D I S C I P L

DIStributed Collaborative Information PLaform



READY FOR A NEW  
WORLD

Based on love, not fear.



SMART  
DATASOURCES

Globally identifiable data at single



PRIVACY

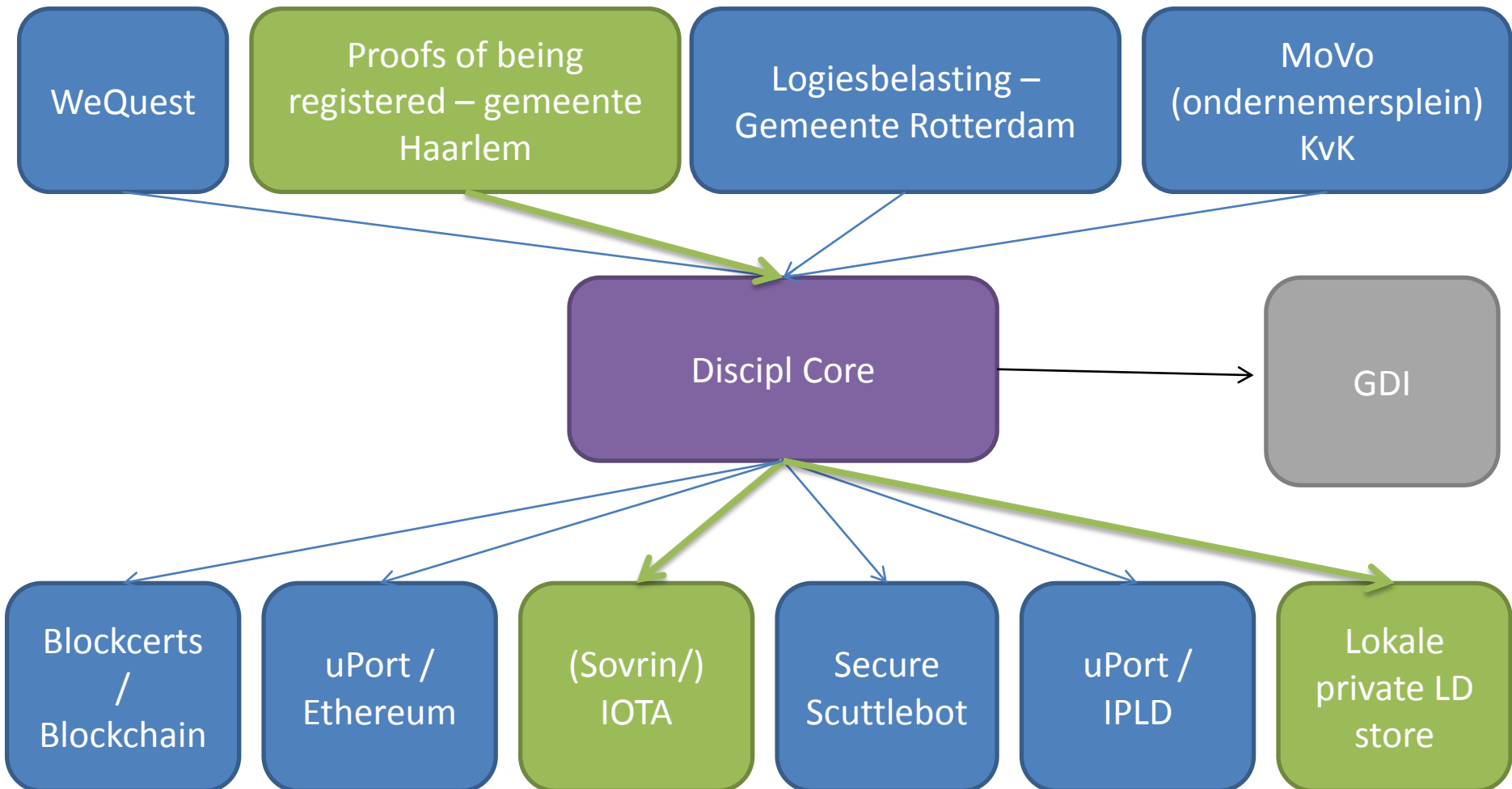
Self Sovereignty. Smart  
Datasources as Private Data



LEGAL


Making legal sources  
comprehensible for man and

# Discipl Core Context



# About IOTA

- No blockchain but Tangle
- No fees, no miner's
- Scalable: more nodes, more transactions: more throughput
- Quantum safe

 domschiener / **ICTU.md** Secret  
Created 8 days ago

★ Star 0    🍴 Fork 0

Code    Revisions 1    Embed    <script src="https://gist."    Download ZIP

ICTU.md    Raw

## ICTU + IOTA: Test Environment

In order to kickstart some early prototyping around IOTA, we have provided you with some resources to get easily started. Please find all the necessary information here:

- Blog Post on IOTA: <https://blog.iota.org/a-primer-on-iota-with-presentation-e0a6eb2cc621>
- Documentation for Developers: <https://domschiener.gitbooks.io/iota-guide/>

At @MyData2017 @wilfriedpimenta of @iotatoken announces partnership between IOTA and @evernym to create a new digital identity. #sovrin



8/31/17, 3:58 AM

# About IOTA

## Masked Authenticated Messaging (MAM) Channels

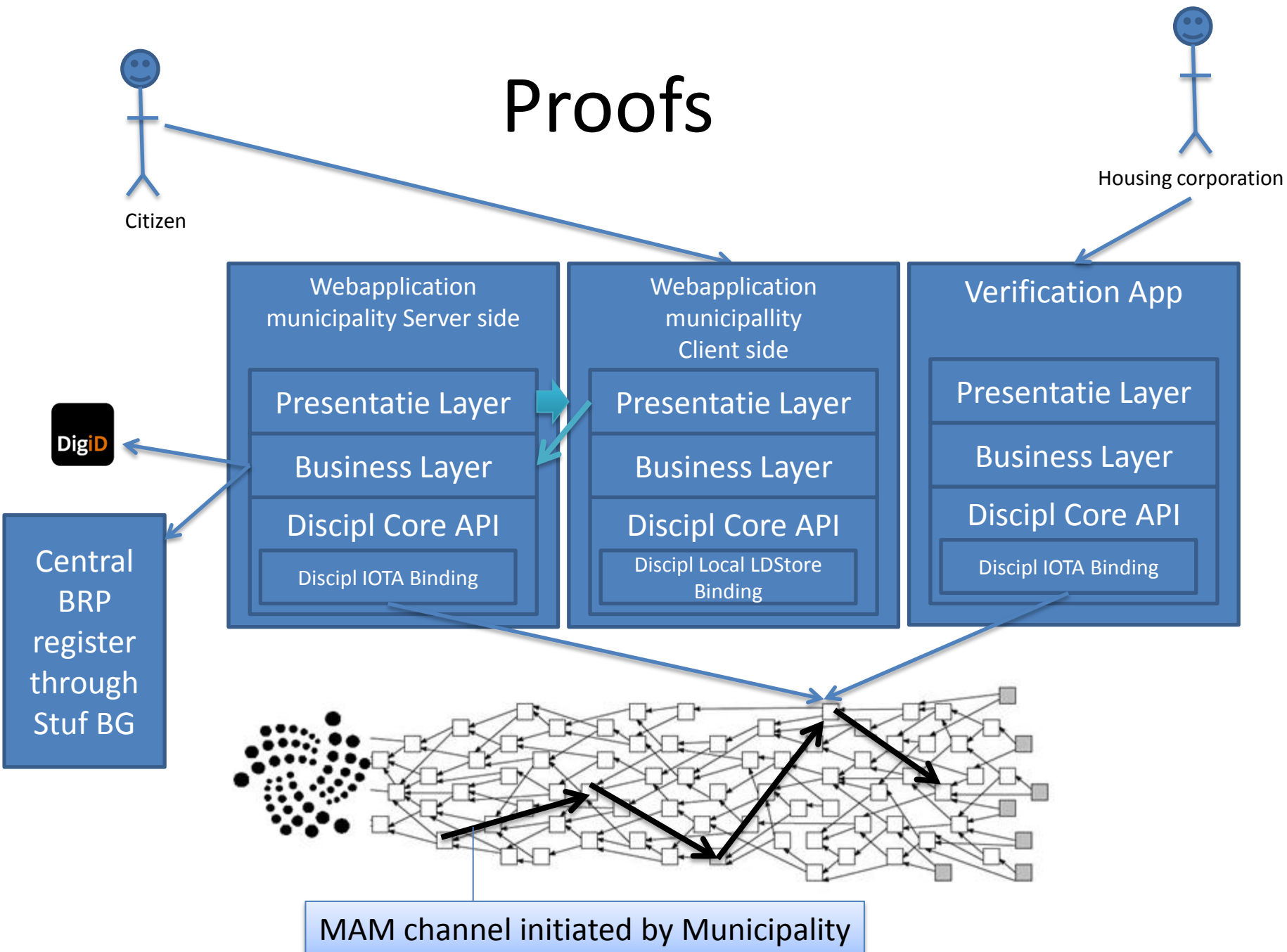
- Initiating party generates random address under which an encrypted message is published referring to a next random address (that can only be generated with the private key of the initiating party) and where the next message will be found.
- Others need to get a reference to a message in the channel (within the Tangle) along with an appropriate key for decryption
- Now still a beta release add on module, being verified by team of cryptologists september 2017



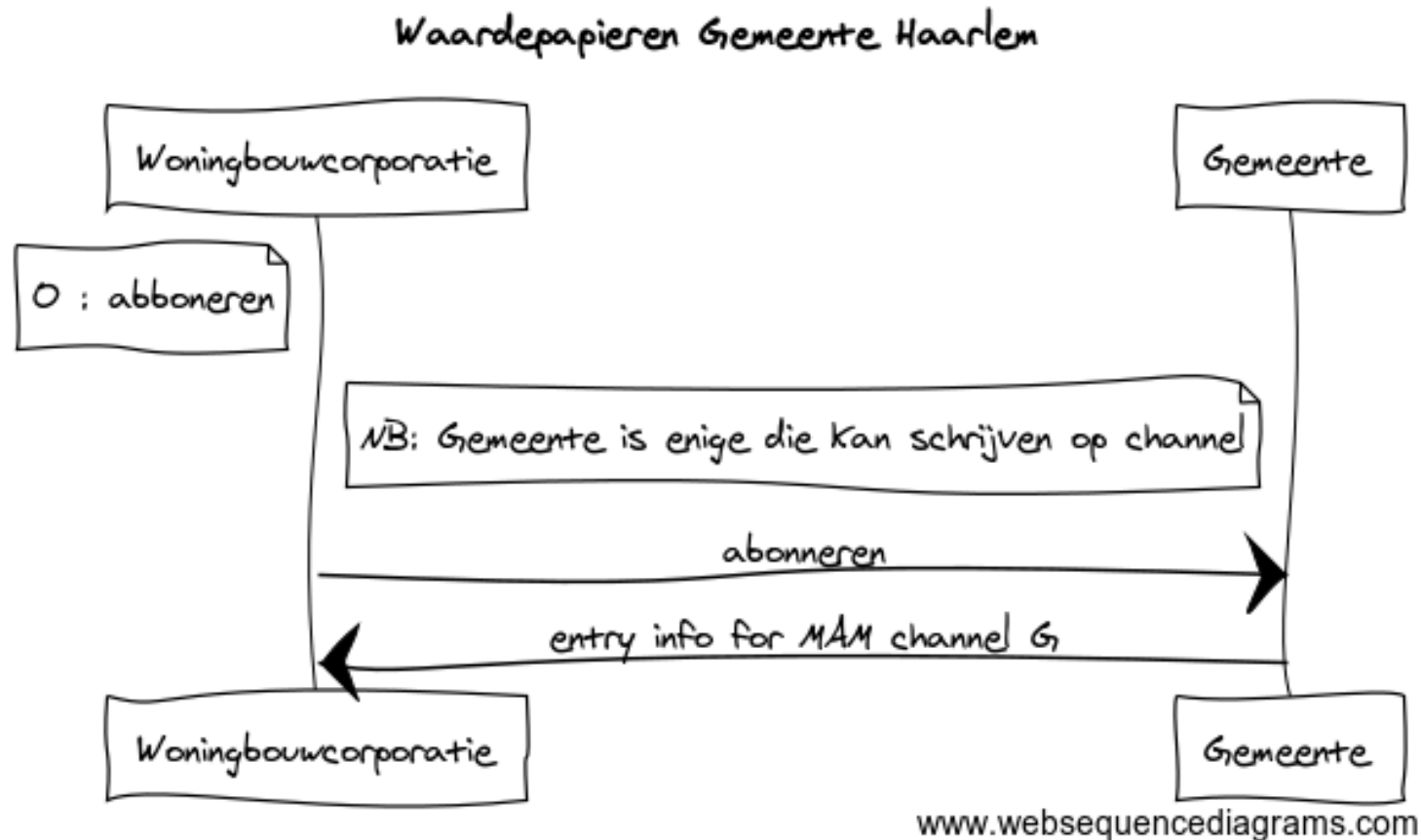
# Proofs

- Housing corporation subscribes to MAM channel of municipality (can be done at a later moment too).
- Website for providing information out of central register, citizen claiming this information and attesting of these claims on MAM channel of municipality. Claim and attestation provided as QR code.
- App for asserting (assert) of claim (through QR code scan)
- Information itself is not put on a public distributed ledger platform, only the hash of the hash of it, and also in encrypted form

# Proofs

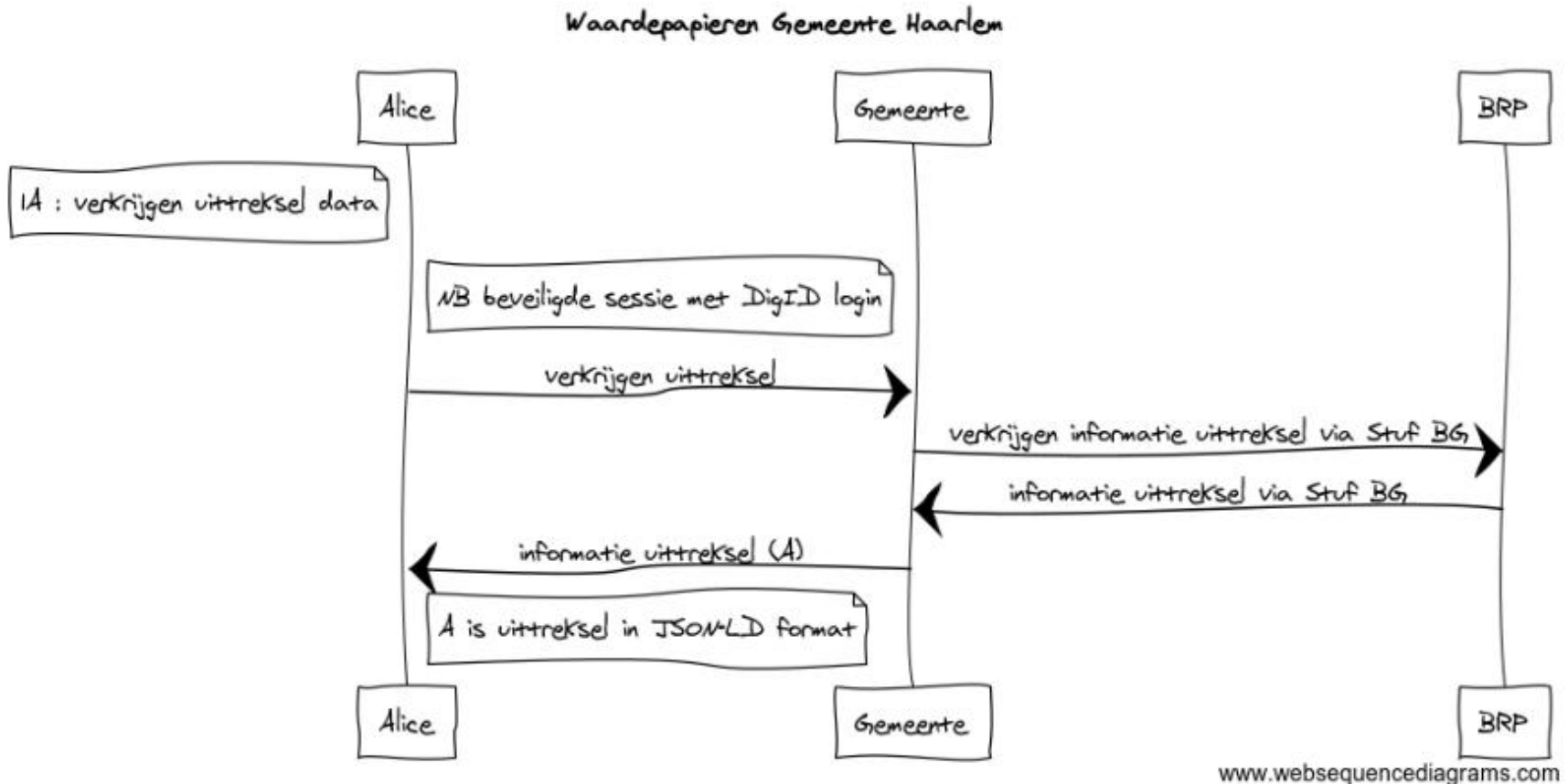


# Step 0 : subscribe



Subscription can be realised in multiple ways. For better security a relying party like a housing corporation needs to identify itself in a secured session through a website or even better: the verification-app.

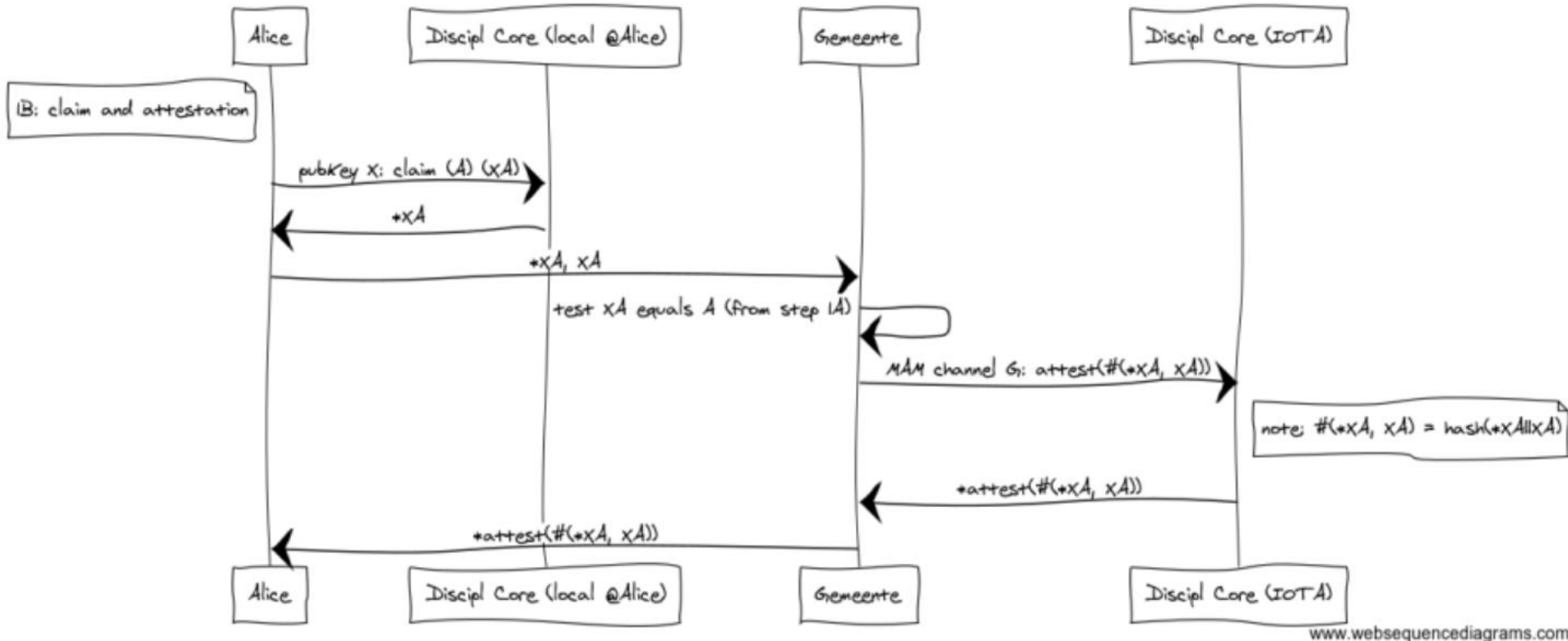
# Step 1A : retrieving information



NB: Alice uses the client side of the webapplication of the municipality.  
It could also be a smartphone App compatible with SSIP standards.  
Signing takes place in the next step.

# Step 1B : claim and attestation

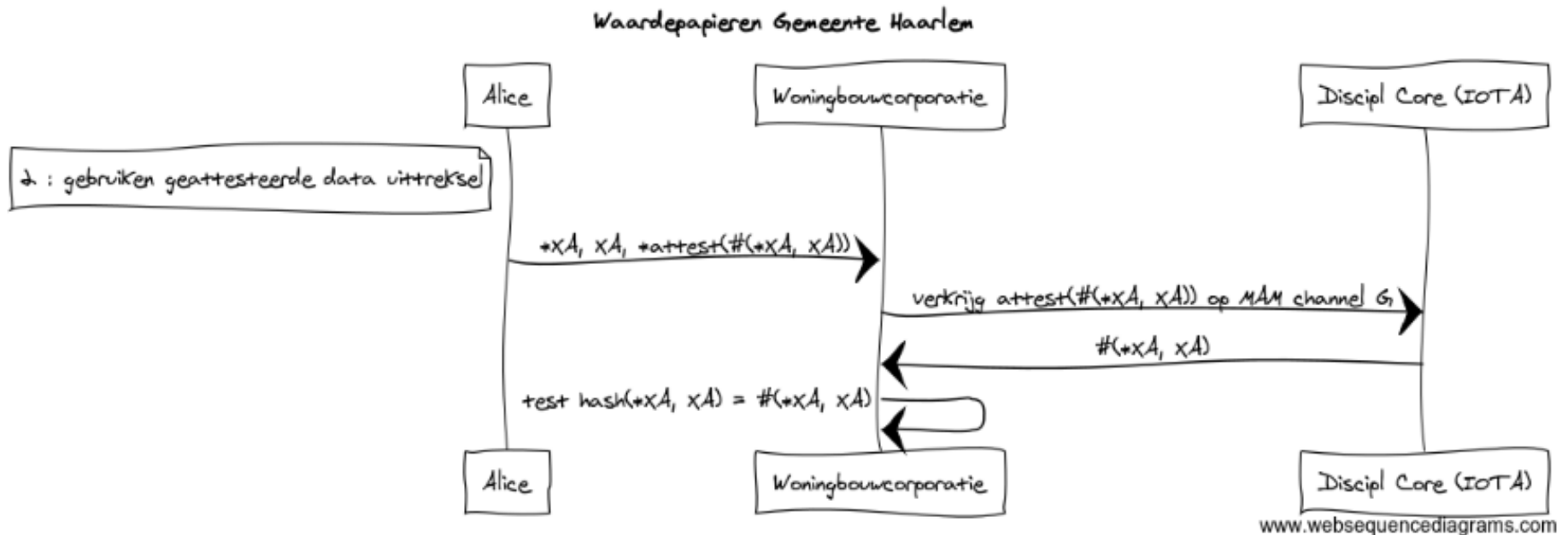
Waardepapieren Gemeente Haarlem



www.websequencediagrams.com

Alice claims locally (temporarily) the information to be proved and doing so adds a secret code. The municipality publishes the hash of information+secret on MAM channel. A reference to this message together with the information and secret is rendered in a QR code for Alice to keep safe (op paper or digitally). It might be easier and more safe for Alice to keep it in a dedicated App instead of fetched from the client side webapplication. In the end Discipl will probably allow for safely sharing claims through a DLT, for example through MAM channels.

# Step 2 : verification



The verification app supports subscription (step 0) and crawls the channel until the attestation claim referenced by Alice has been found. The App tests whether the hash of the information provided by Alice equals the hash in the attestation claim found on the channel.

The fact that the hash of information and secret exists in the channel in which only the municipality can add messages proves that the municipality earlier identified a person with the same information and knowledge of the same secret code (which is not being stored elsewhere than with that person.) as provided by the person now in contact with the housing corporation.

# Security en Privacy

- Open Source and GPLv3.0, Privacy By Design
- No real information on the ledger, also not in encrypted form, only encrypted one way hashes
- **Non-transferability** : attestations are linked to personal identifiable information as name and adres; these can not be altered and therefore used when keys of the citizen are stolen, or the citizen deliberately shares keys with others.
- **Issuer unlinkability** : The municipality will not be aware of the verification the housing corporation performs.
- **Multi show unlinkability** : the information claimed in this use case will always be linkable by comparing information when housing corporations share this info (which is probably not permitted). There will never be a way to prevent this, but that's not different in the current situation. An attestation can be used only once by the citizen to make this more hard
- **Revocation** : in the current situation the municipality will have to publish a revocation on the MAM channel. In the future when the claim is a real registration itself, the citizen publishes the revocation him/her selves (though that would mean he/she unregisters).  
When the keys of the municipality are stolen the municipality can invalidate the whole channel when noticing a first fraudulent message by adding a kill-message together with revocations of fraudulent attestations and move to a new channel.  
Revocation will be out of scope in the first demo.

# Roadmap

1. Octobre 2017: Functional and technical design,  
Proof of technology on IOTA Sandbox
2. December 2017: Demo website and App  
(without DigId en BRP)
3. 2018: Production version (with DigId en BRP)



# Technical Design

Components ICTU / Discipl community with support IOTA Foundation :

1. Discipl Core (Claim(), Attest(), Assert())
2. Discipl Local binding
3. Discipl IOTA binding (with MAM support)

<http://github.com/discipl/core>

Components Municipality of Haarlem (development: Xurux):

1. Demo Website server/client side
2. Demo Verification App

<http://github.com/Haarlem/Digitale-waardepapieren>

(later in “App Store”: <http://github.com/discipl/projects/waardepapieren>)