Update on BRSKI-AE – Support for asynchronous enrollment

draft-ietf-anima-brski-async-enroll-03

Steffen Fries, Hendrik Brockhaus, Elliot Lear, Thomas Werner

IETF 111 – ANIMA Working Group

Problem to solve

- Limited or no connectivity between Pledge and Registrar.
- Distinction between operational modes of the pledge
  - Pledge-initiator-mode (use case 1): Pledge acts as client and follows the BRSKI approach for the voucher exchange, but allows for alternative enrollment protocols
  - Pledge-responder-mode (use case 2): Pledge acts as server and communicates with registrar via a registrar-agent. Pledge is triggered (pushed) to generate and receive bootstrapping data. → main changes made this use case
- Draft addresses these issues by defining the call flow and objects to be exchanged. To be independent of the transport security authenticated self-contained objects (signature-wrapped objects) for the certificate enrolment to bind proof of possession and poof of identity to the exchanged objects (similar to existing voucher exchanges with pledge)

BRSKI-AE Status
History of (main) changes from version 01 to version 02

- Defined detailed call flow and exchanged objects for interactions in UC2 between pledge – registrar-agent – registrar and MASA. Object format aligns with draft JOSE signed voucher artifacts (Section 5.2.3).
- Removed TLS-PSK approach between pledge and registrar-agent to allow transport security independent object exchange and also to avoid relying on PSK.
- Included enhancements in voucher-request content and handling to allow registrar to verify agent-proximity to the pledge (enhancements in voucher-request and handling on registrar) in Section 5.2.3.
- Defined enhancements in voucher-request YANG to allow for additional parameters to be transported (Section 6).
- Terminology alignment (pledge-agent -> registrar-agent; PULL/PUSH -> pledge-initiator-mode and pledge-responder-mode).

BRSKI-AE Status
History of changes from version 02 to version 03

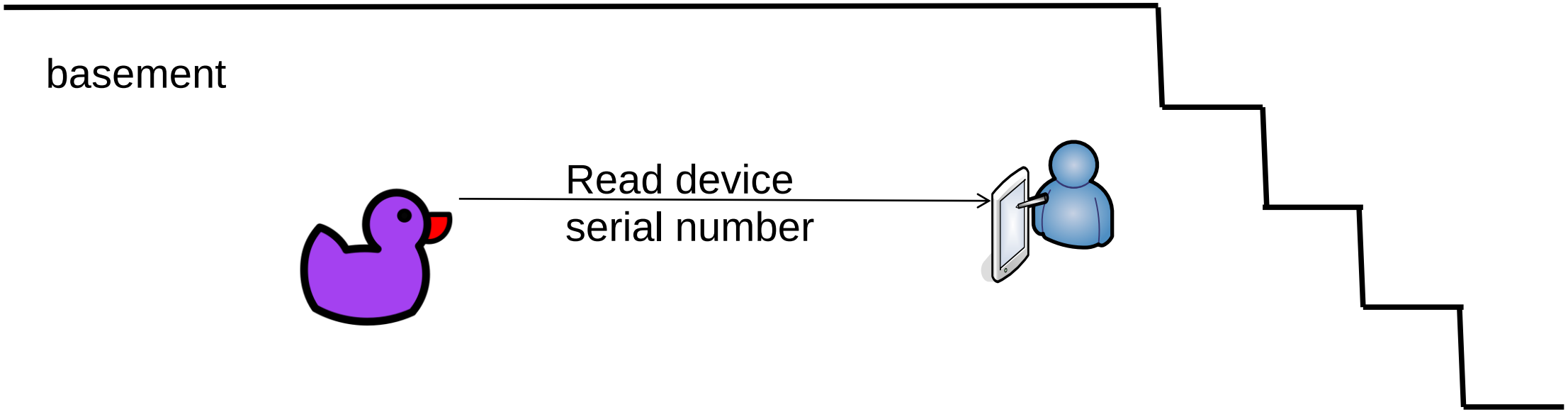
- Discussion of open issues discovered in the currently applied YANG definitions:
  - YANG doctors were informed to have an early review on
    - the enhanced voucher-request from RFC 8995
    - the enhancement of the assertion enum of the voucher to include new value agent-proximity (section 5.2) → relates to RFC 8366bis discussion

    No feedback received, yet
  - YANG module for CSR (for the enrollment request): draft currently reuses SZTP-CSR defined sub module: turns out to be not possible as the complete module must be used.
    → Proposal provided on mailing list to define csr types independent of the embedding protocol as part of SZTP-CSR is currently discussed

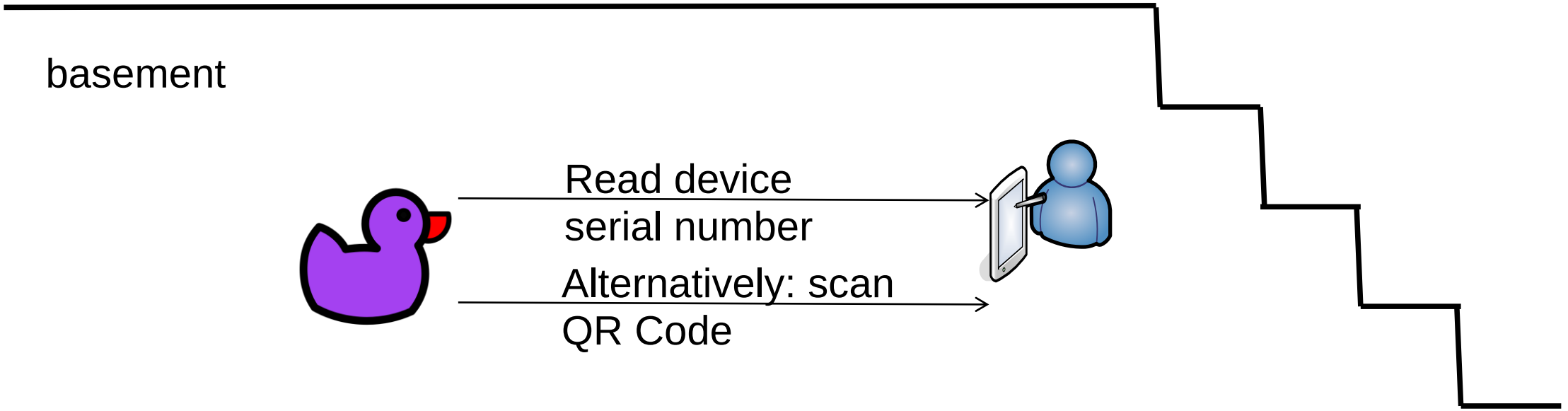
BRSKI-AE
Abstract view on use case 2 call flow

First Trip

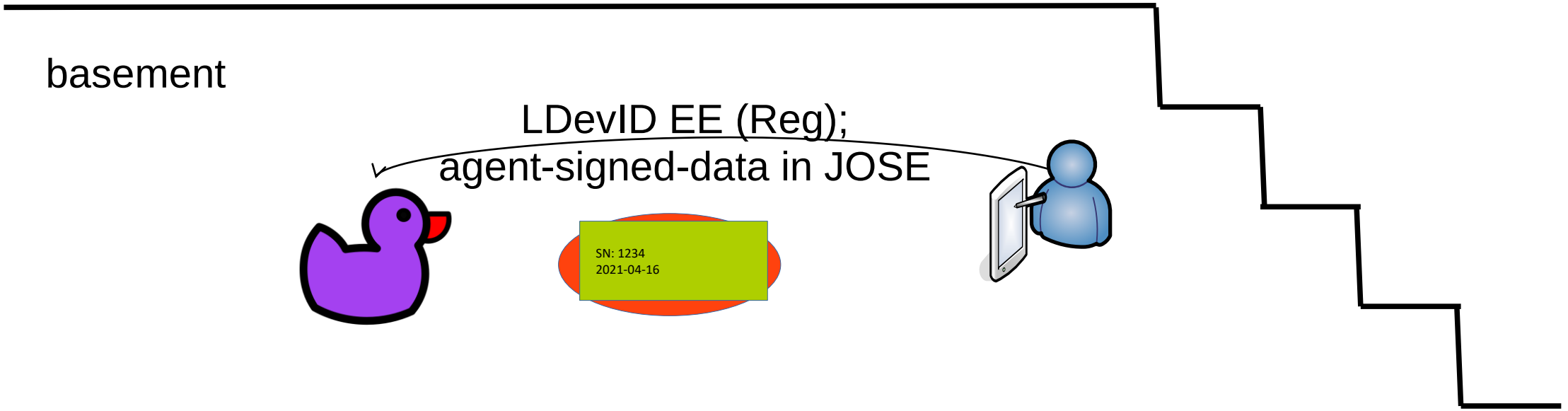
First Trip



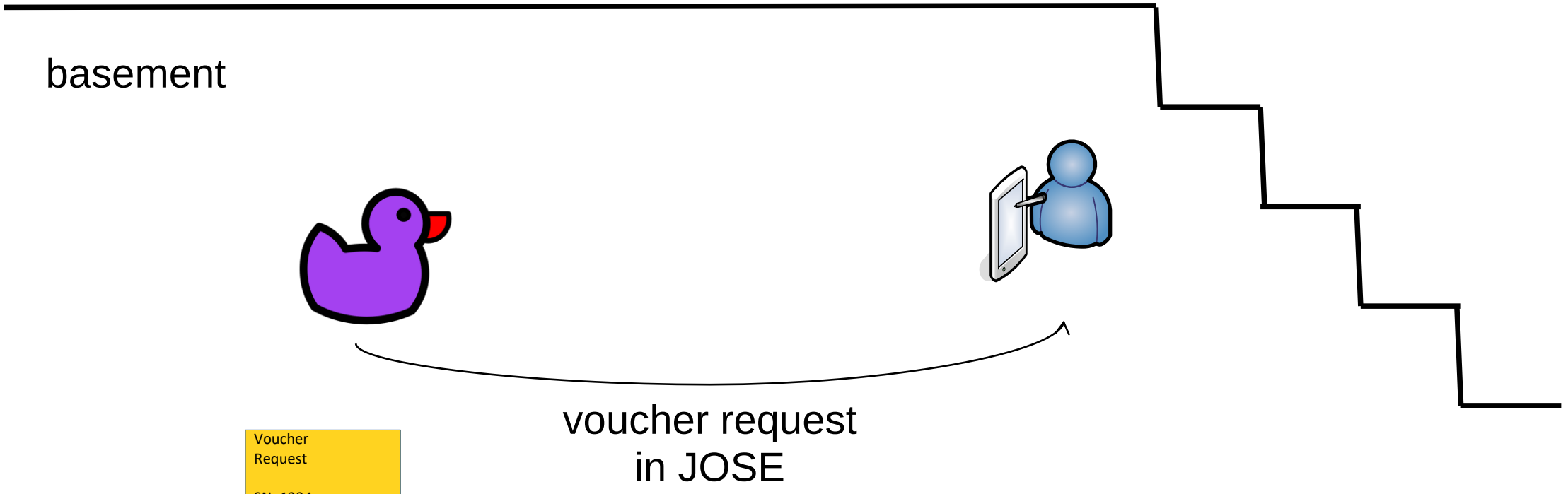
First Trip


basement
Read device
serial number
Alternatively: scan
QR Code

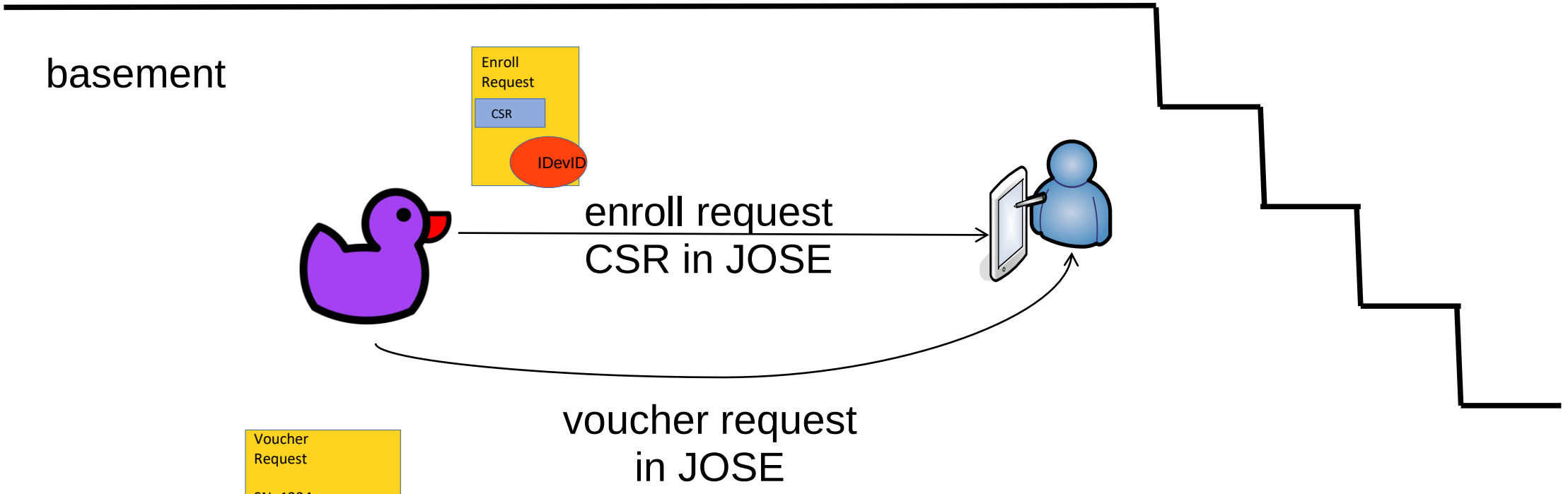
First Trip


basement
LDevID EE (Reg);
agent-signed-data in JOSE
SN: 1234
2021-04-16

First Trip


basement
voucher request
in JOSE
Voucher
Request
SN: 1234
LDevID EE (Reg)
Assertion:
agent-prox
SN: 1234
2021-04-16

First Trip


basement
Enroll
Request
CSR
IDevID
enroll request
CSR in JOSE
voucher request
in JOSE
Voucher
Request
SN: 1234
LDevID EE (Reg)
Assertion:
agent-prox
SN: 1234
2021-04-16

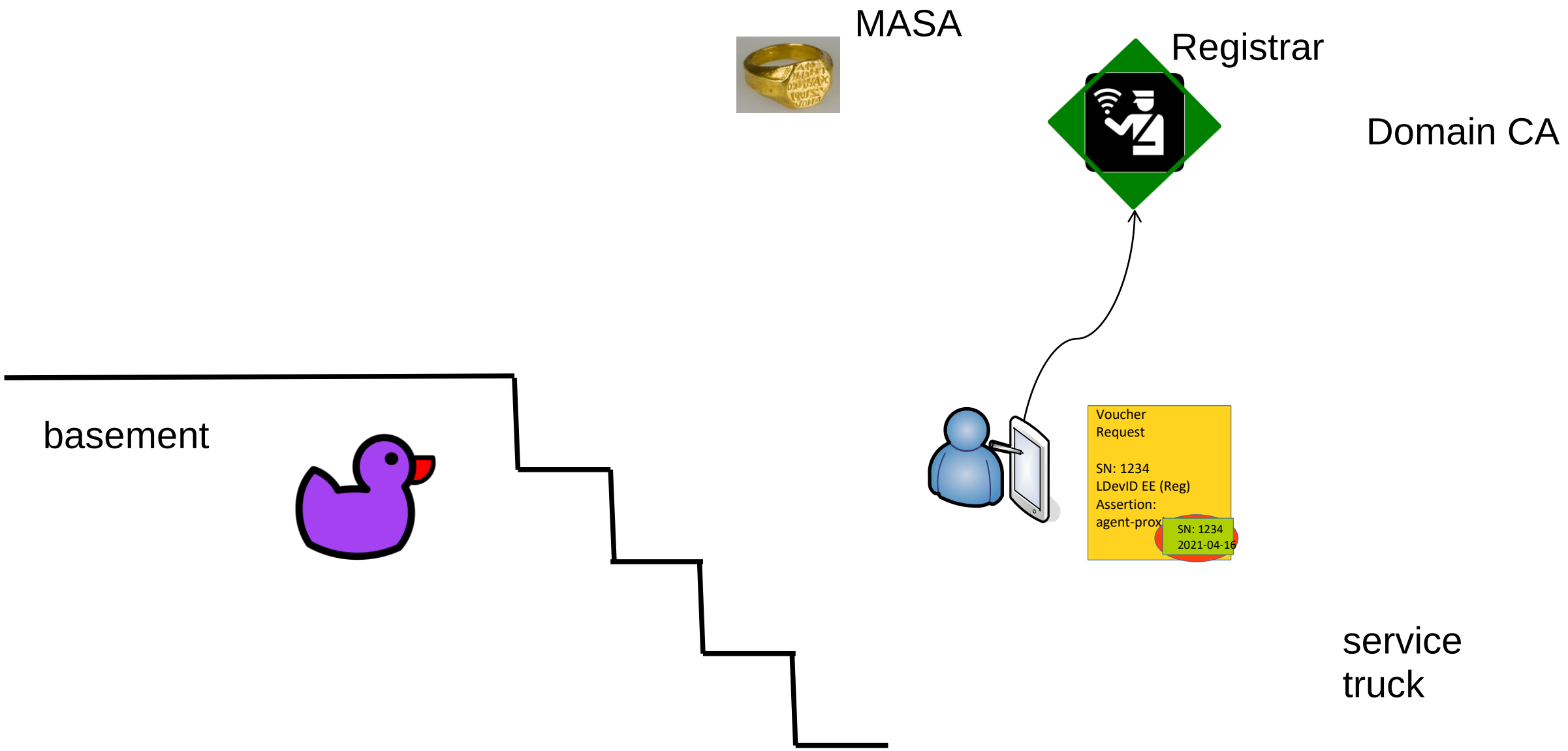
MASA

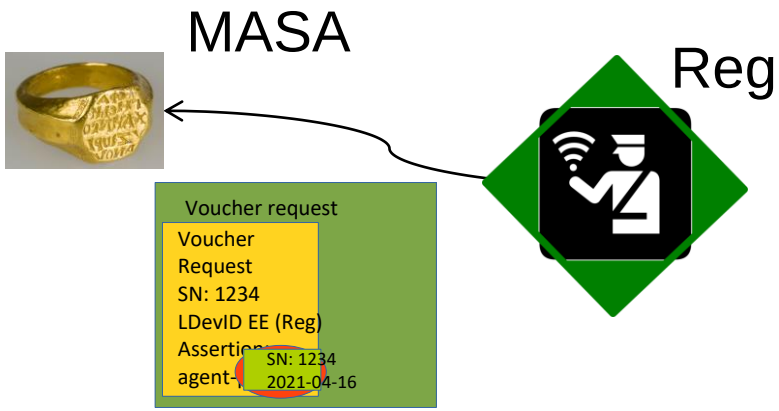
Registrar

Domain CA

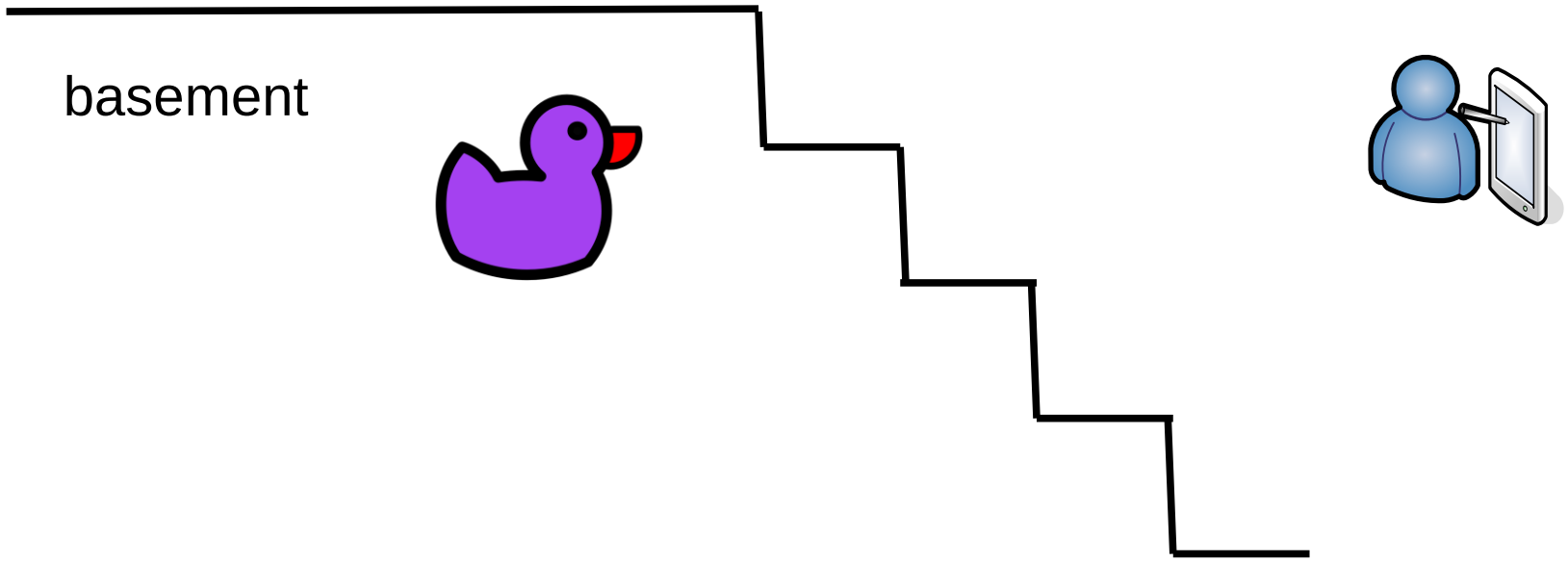
basement

service
truck


MASA
Registrar
Domain CA
basement
Voucher
Request
SN: 1234
LDevID EE (Reg)
Assertion:
agent-prox
SN: 1234
2021-04-16
service
truck



Domain CA



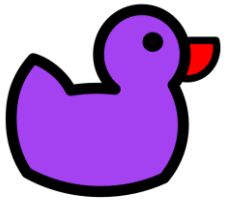
service
truck

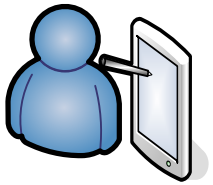
MASA

Registrar

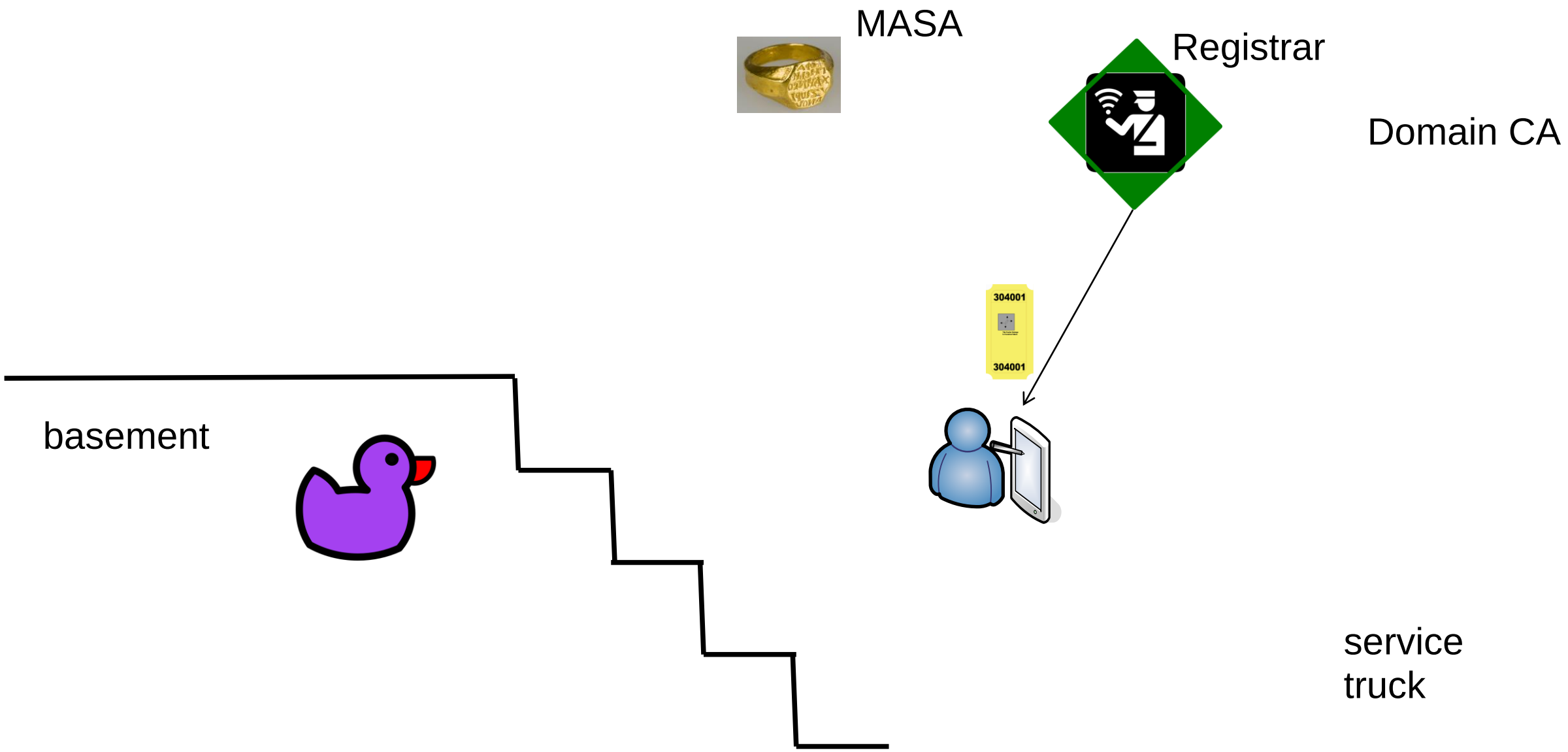
Domain CA

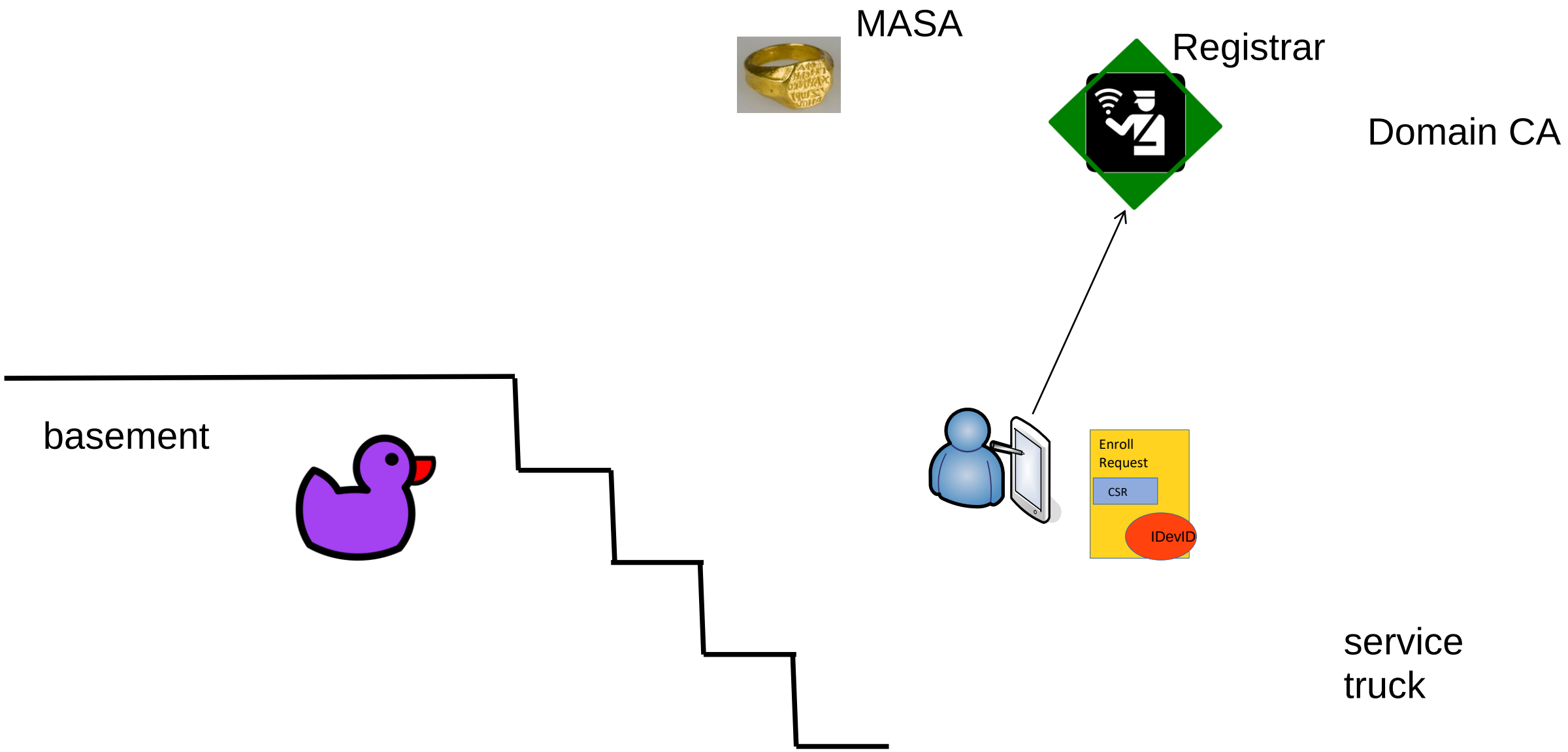
basement





service truck


MASA
Registrar
Domain CA
304001
304001
basement
service
truck


MASA
Registrar
Domain CA
basement
Enroll
Request
CSR
IDevID
service
truck

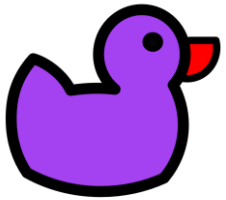
MASA

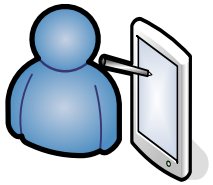
Registrar

Domain CA

CSR

basement





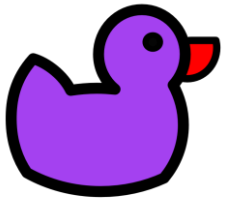
service truck

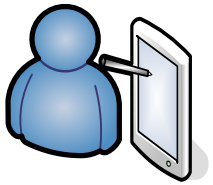
MASA

Registrar

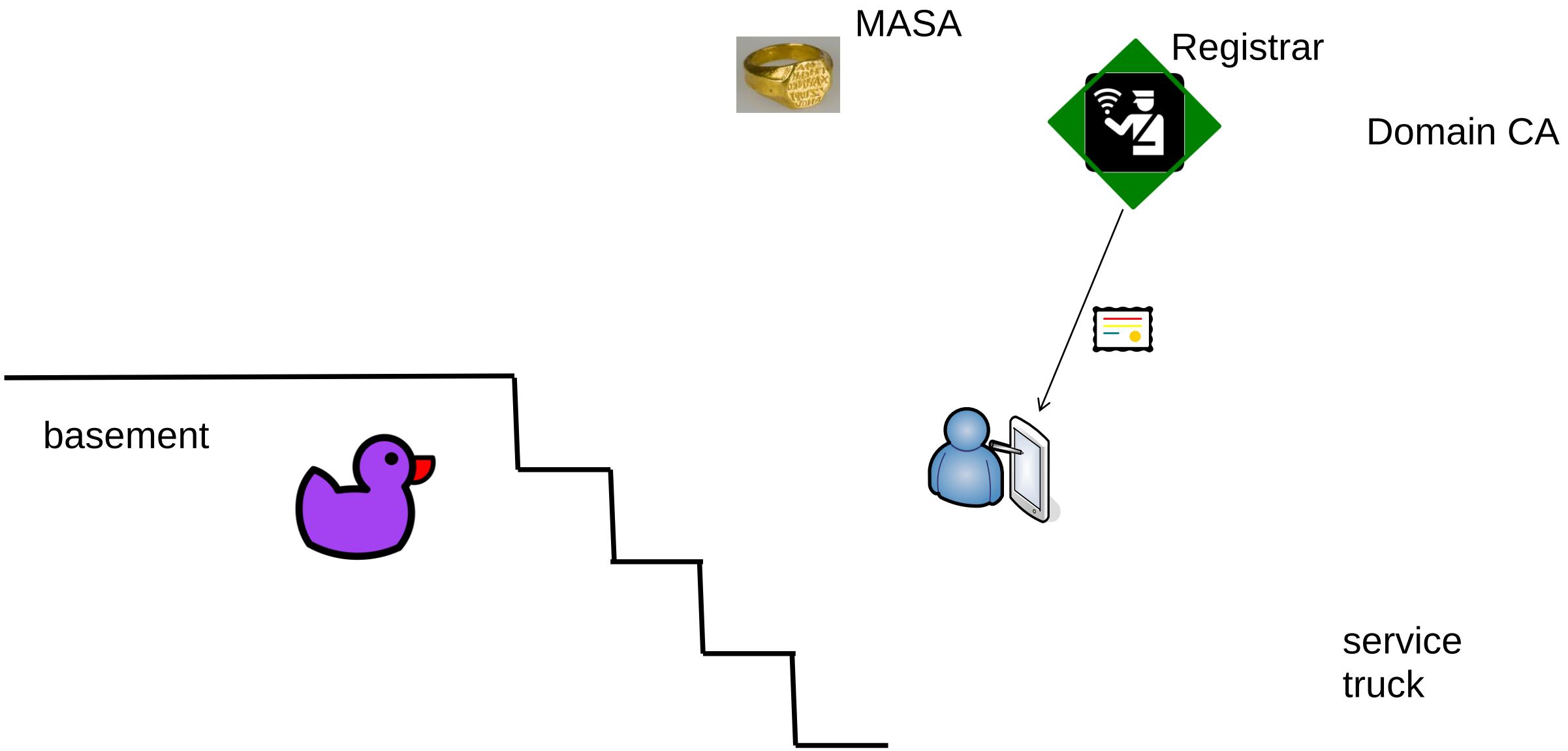
Domain CA

basement



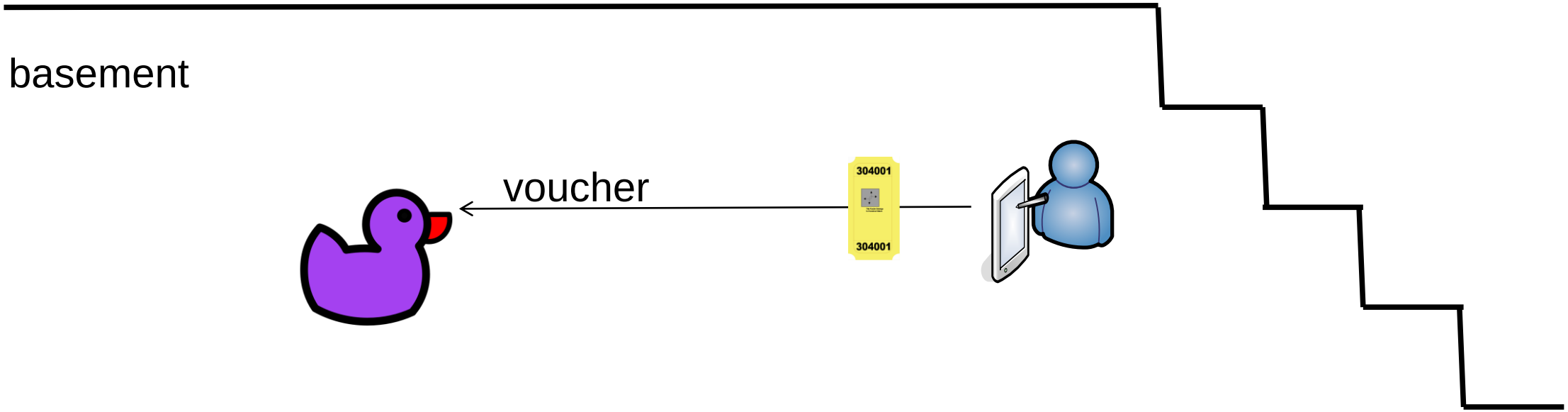


service
truck

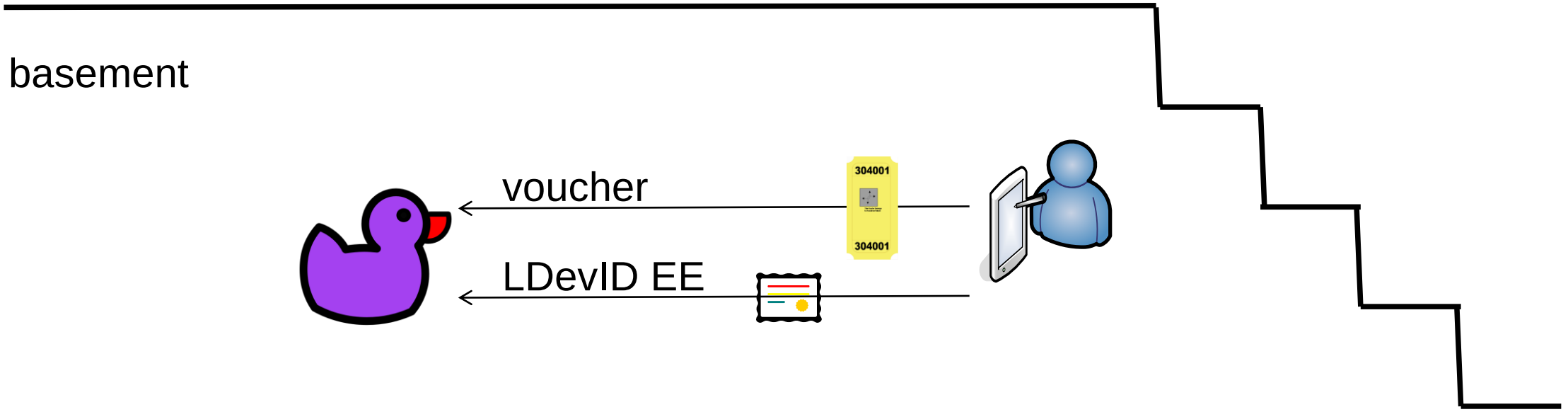

MASA
Registrar
Domain CA
basement
service
truck

Second Trip

Second Trip



Second Trip



BRSKI-AE, Use Case 2
Verification of agent-proximity

- Data exchange between registrar-agent and pledge based on signed objects (no TLS)
- Enhancements in pledge voucher-request with a signed statement from registrar-agent
- Allows registrar to identify, which registrar-agent is involved in the bootstrapping
- Registrar includes LDevID EE(RegAgt) into registrar-voucher-request.
- As pledge-voucher-request is included in registrar-voucher-request MASA can also verify agent-proximity and trust relation registrar-agent / registrar
- MASA can issue assertion “agent-proximity”, which is weaker than “proximity” but stronger than “logged” or “verified”
  - "agent-proximity" is a statement that the proximity-registrar-certificate was provided via the registrar-agent and that the pledge could not verify proof-of-possession at the time of voucher-request creation
  - “proximity” is a statement that the proximity-registrar-certificate was received directly (via TLS) and that the pledge could verify proof-of-possession during the TLS handshake before voucher-request creation.

Discussion: Open issues

- Version 03 addresses most of the existing issues in the github/anima-wg
- Current open issues
  - Early review of enhanced voucher-request in section 6 by YANG doctor
  - #10: YANG module for CSR to be used in enrollment-request (to allow for P10 and further formats)
  - #18: enhancement of YANG voucher with new assertion “agent-proximity”
    → discussion in the context of revising RFC 8366 to allow for enhancements of assertion types

Discussion: Further draft handling

- Currently, BRSKI-AE addresses two use cases with different target and different level of detail
  - Use Case 1 targets the definition of requirements for a communication architecture using the existing BRSKI components and call model (pledge-initiator-mode, formerly PULL) to enable the use of alternative enrollment protocols for certificate enrollment (voucher handling untouched).
  - Use Case 2 targets the specification of a reversed call model (pledge-responder-mode, formerly PUSH) in which the pledge has no or only limited connectivity to a registrar or cannot initiate requests to a registrar. To facilitate the interaction between pledge and registrar, the registrar-agent component is established. The interaction between pledge and registrar-agent results in new or enhanced data objects (voucher-request-trigger, voucher-request, voucher, enrollment-request-trigger, enrollment-request). Exchanges between registrar-agent and registrar follow~~s~~ BRSKI (RFC8995) and EST (RFC7030), with the enhanced objects.
- Declaration of conformity to „AE“ is difficult, as the use cases have developed in different directions
- Proposal to split the draft into two separate documents for use case 1 and use case 2
- Is this a reasonable approach for the WG?

Next Steps

- Clarification of open issues stated in github/anima-wg and also in the draft
- Split into two drafts concentrating on the distinct use cases, depending on WG view
- Circulate outcome on the mailing list for further discussion
- WG review appreciated

Backup

BRSKI-AE, Use Case 2
Abstract Protocol Overview