The Future of Digital Identity

Kingdom of Cheese

Oktober 2022

ubique

About us

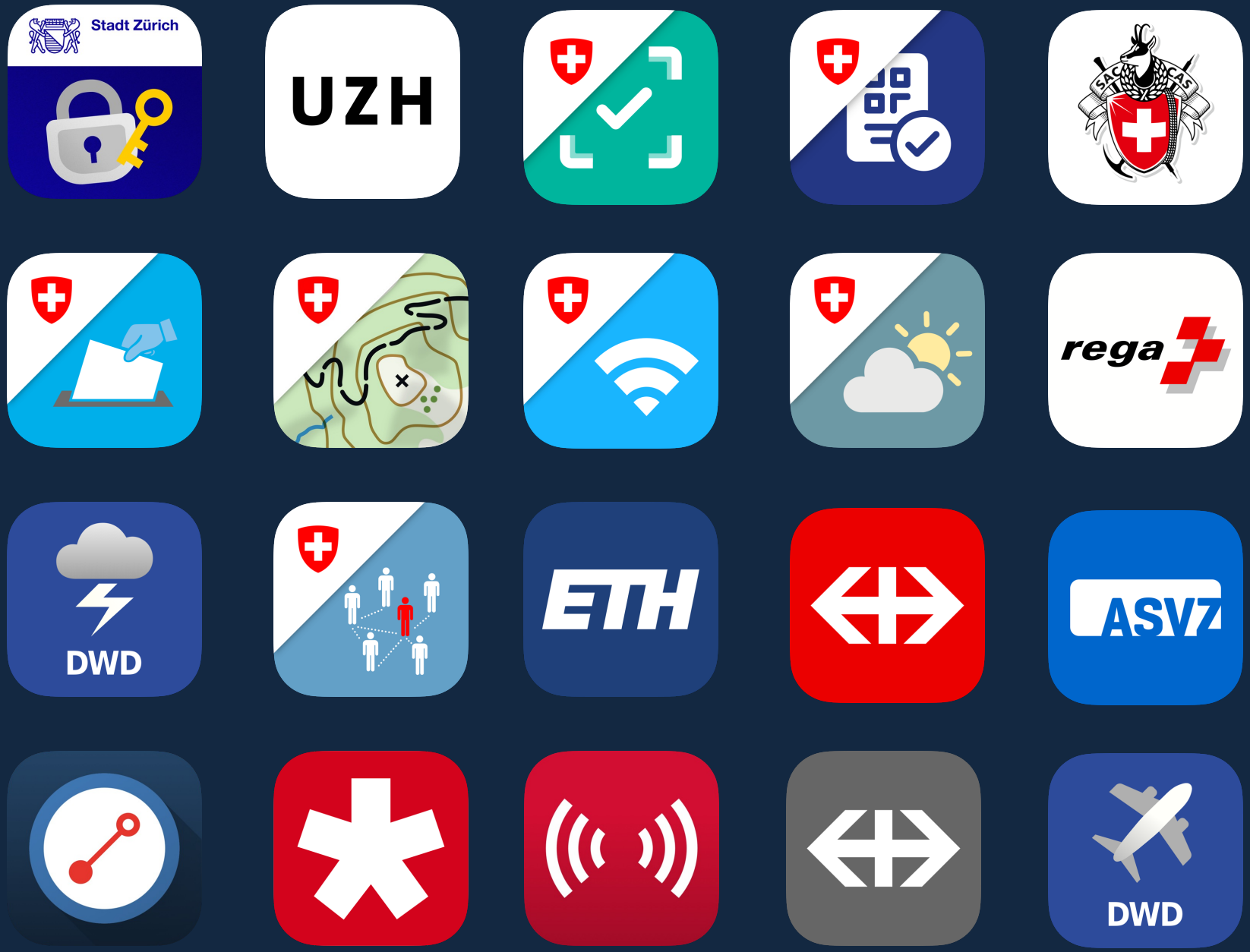
Patrick Amrein
Master in Physics at ETH

Started as a student @Ubique in 2014
Security Engineer

Cléa Benz
Master in CS at ETH

@Ubique since 2017
Android Developer & Project Lead

ubique


Stadt Zürich
UZH
rega
DWD
ETH
ASVZ
DWD

ubique

Founded 2010 in Zürich

47 Employees

100% Swiss Made

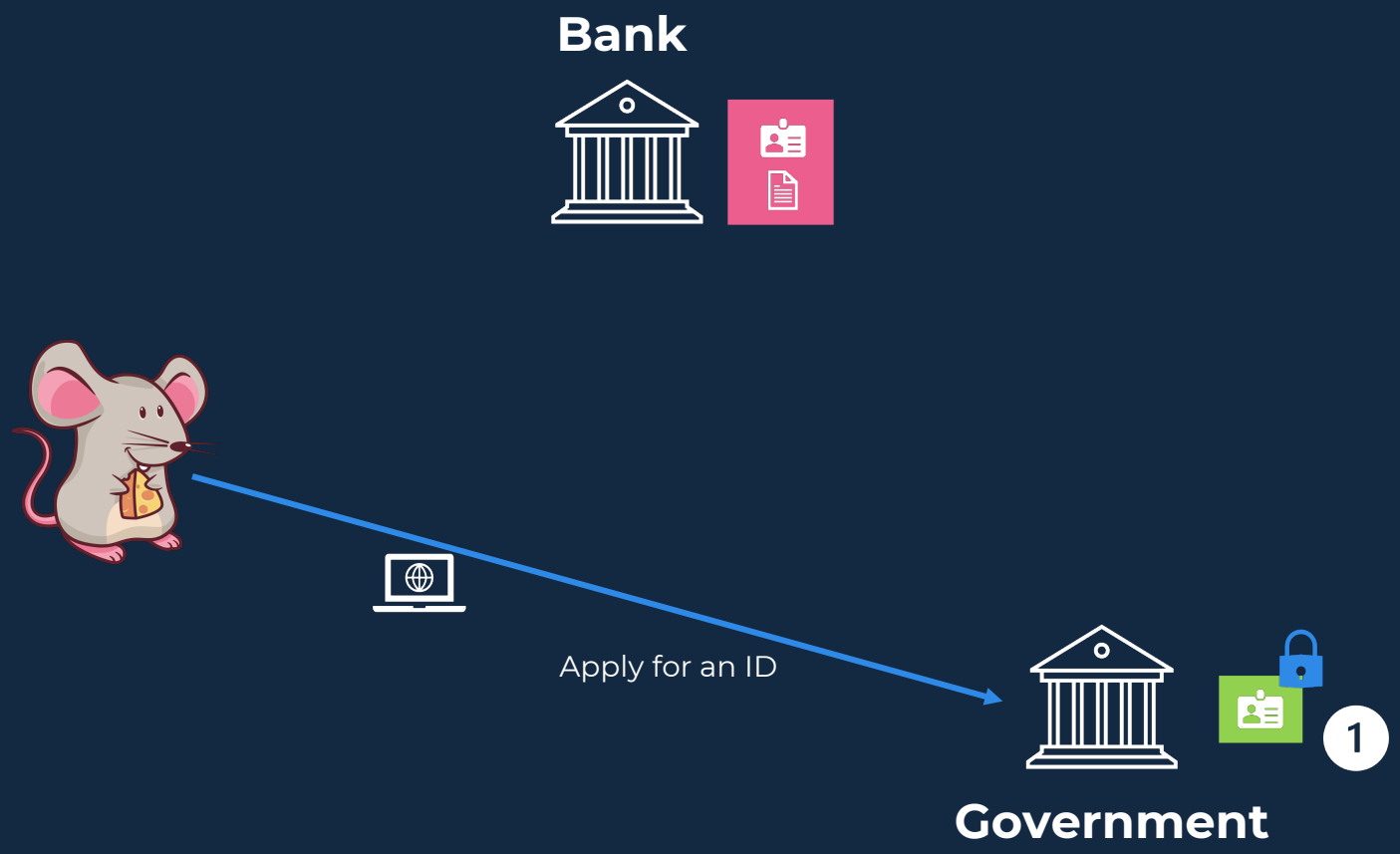
Self-sovereign Identity World

ubique

Kingdom of Cheese

Self-sovereign Identity World

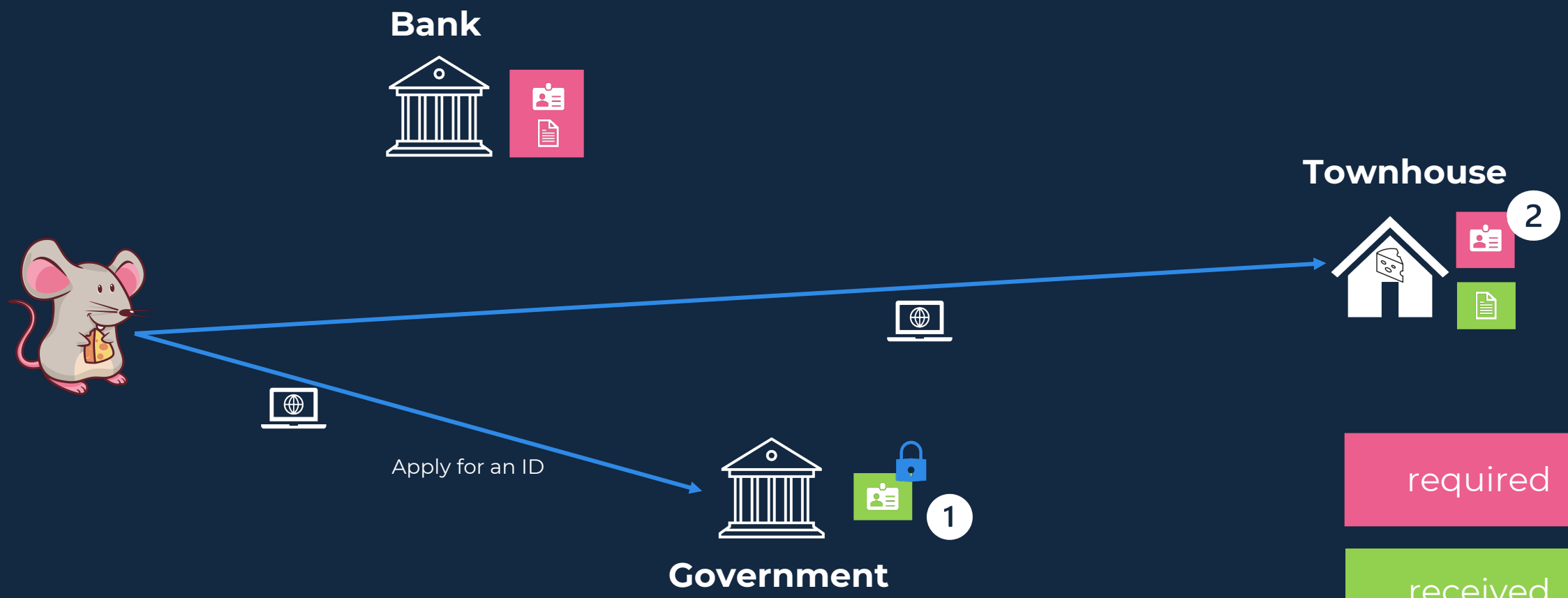
Goal: Jenny wants to open a bank account in the Kingdom of Cheese



Kingdom of Cheese

Self-sovereign Identity World

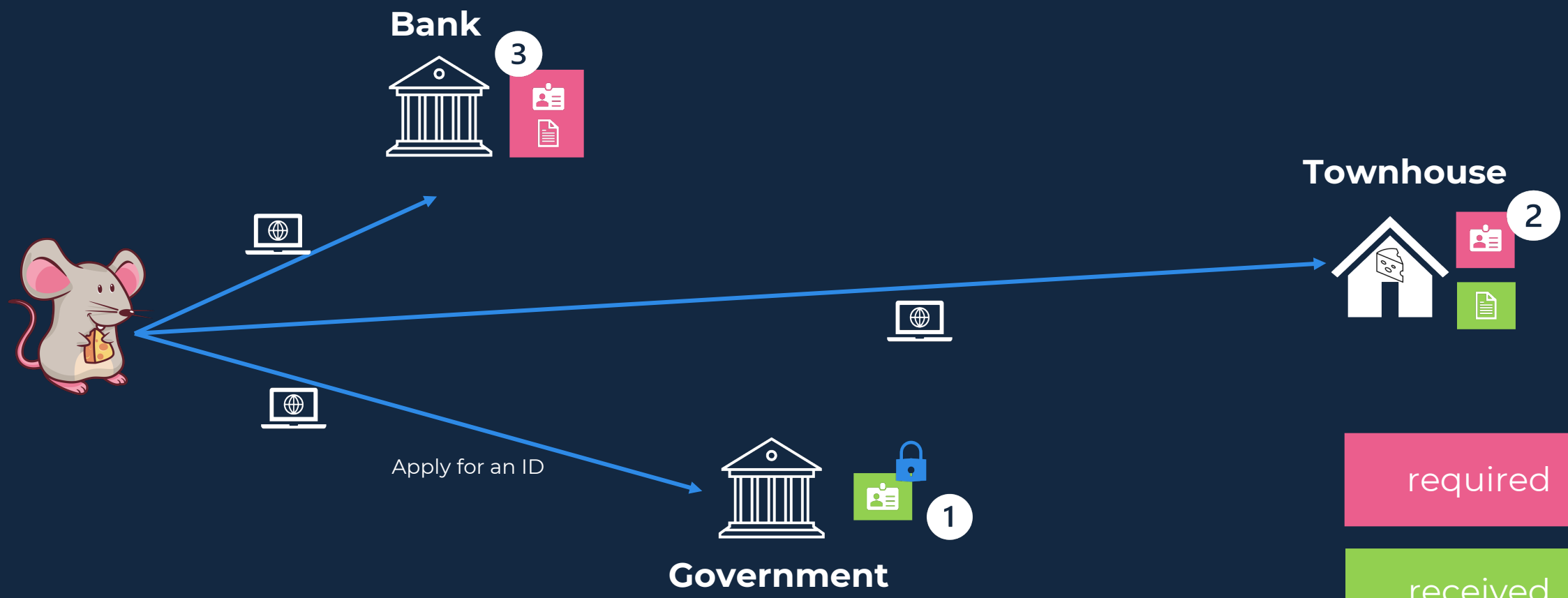
Goal: Jenny wants to open a bank account in the Kingdom of Cheese



Kingdom of Cheese

Self-sovereign Identity World

Goal: Jenny wants to open a bank account in the Kingdom of Cheese



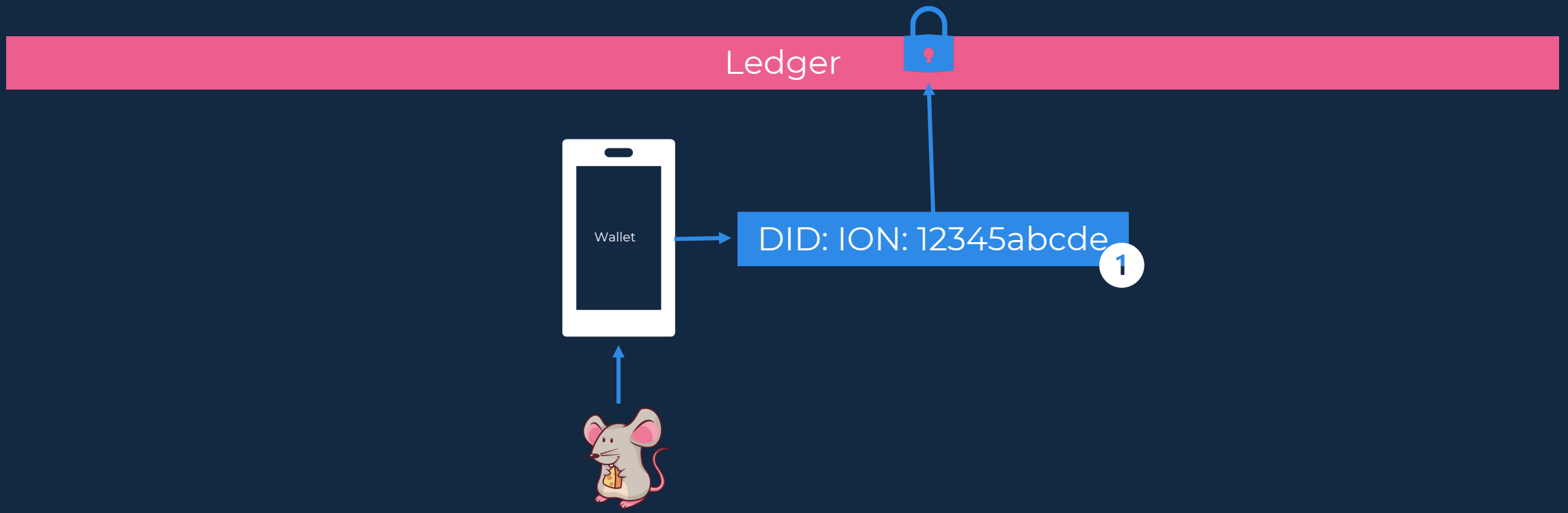
E-Pass

ubique

Kingdom of Cheese

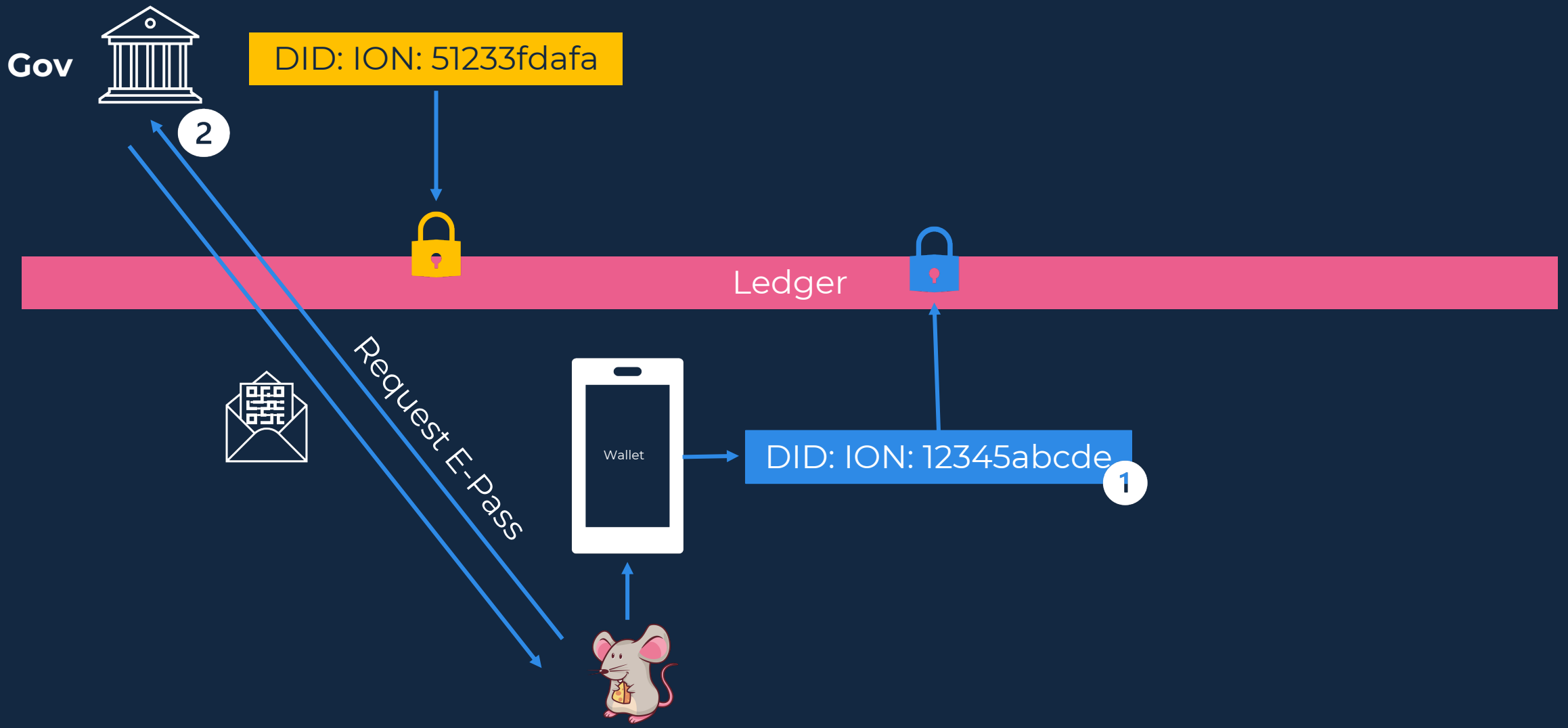
Digitally signed ID

Gov



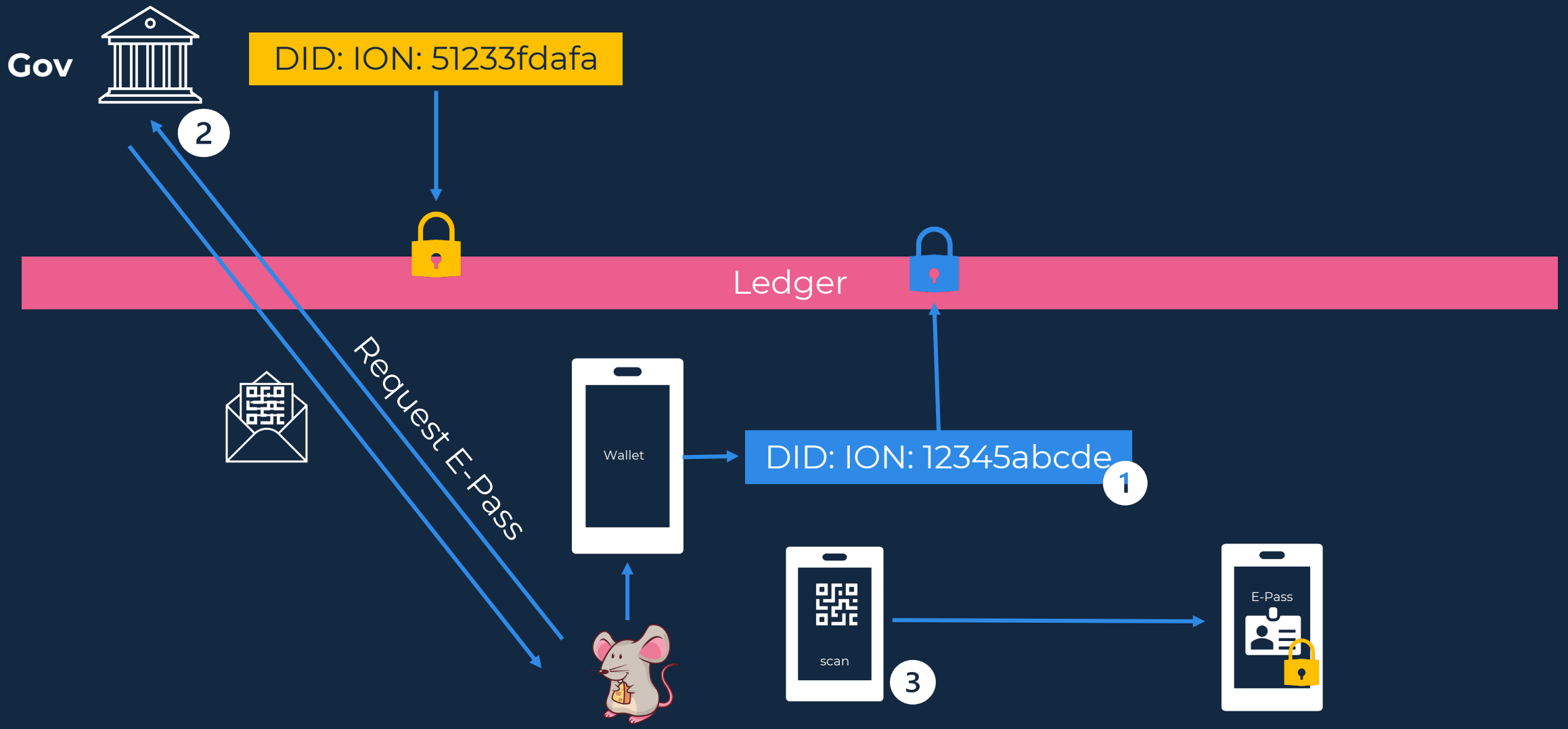
Kingdom of Cheese

Digitally signed ID



Kingdom of Cheese

Digitally signed ID



Kingdom of Cheese

E-Pass in Detail

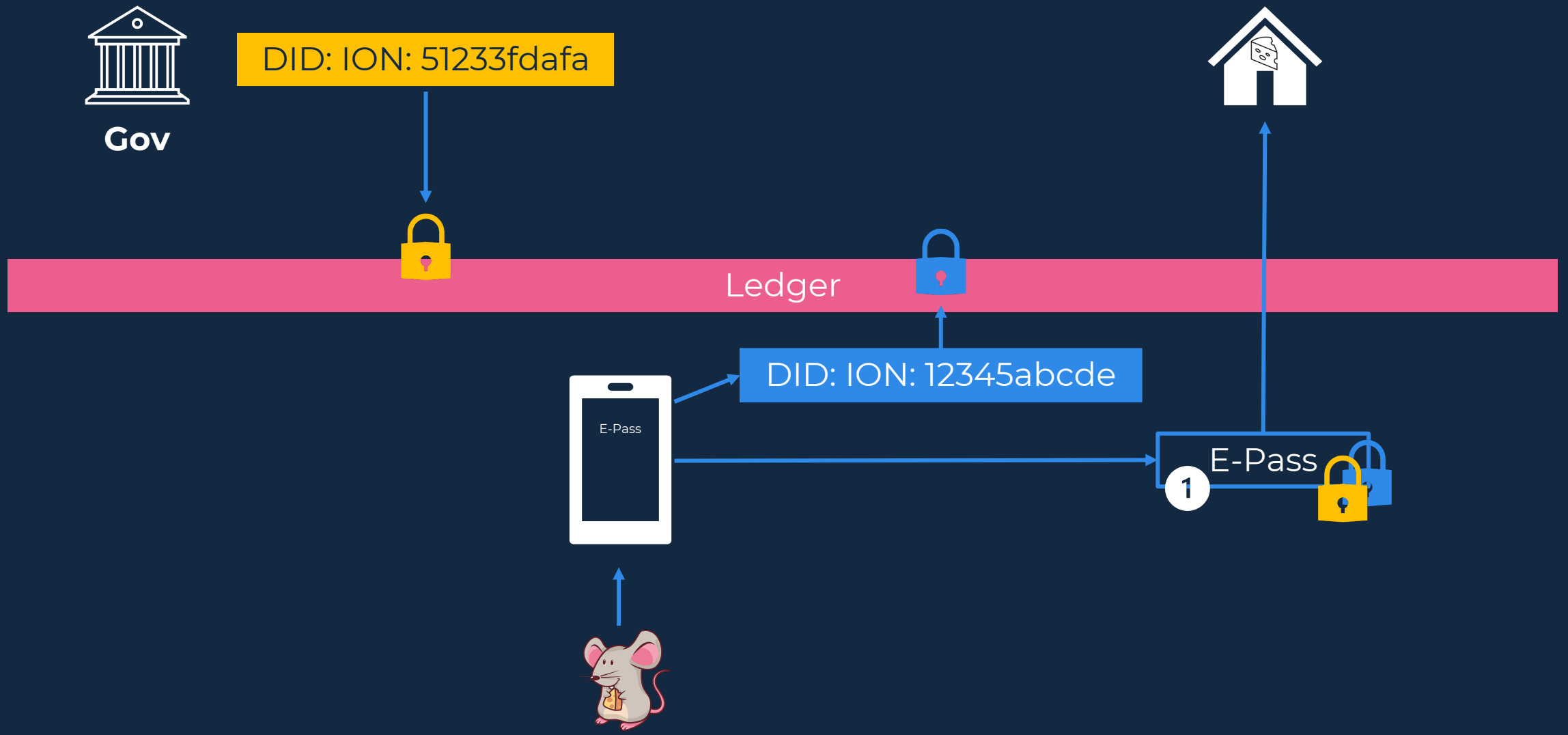
- Signed by government with their did (issuer)
- Contains claims about Jenny (name, Date of Birth, ...)
- Use the government did (public key on ledger) to verify the signature

Residence Confirmation

ubique

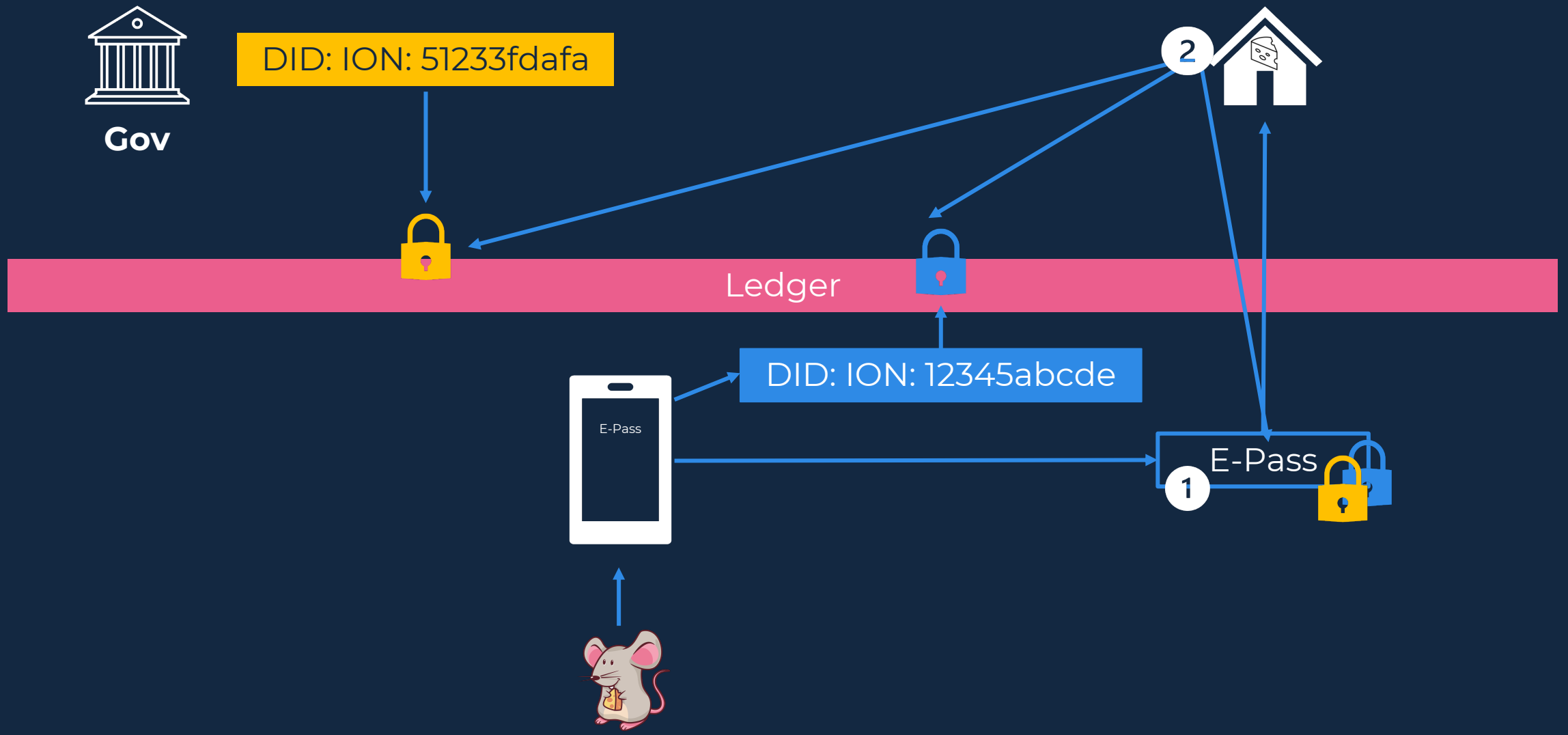
Kingdom of Cheese

Residence Confirmation



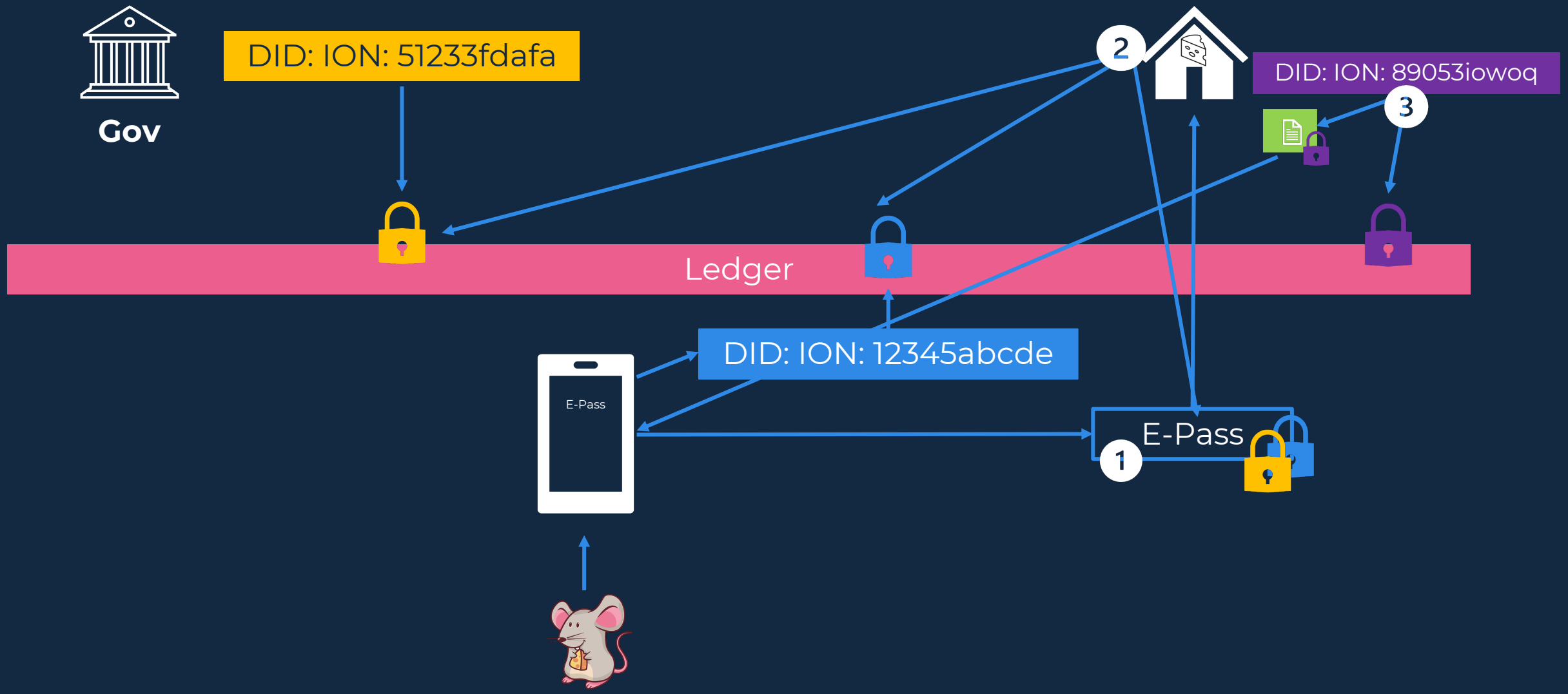
Kingdom of Cheese

Residence Confirmation



Kingdom of Cheese

Residence Confirmation

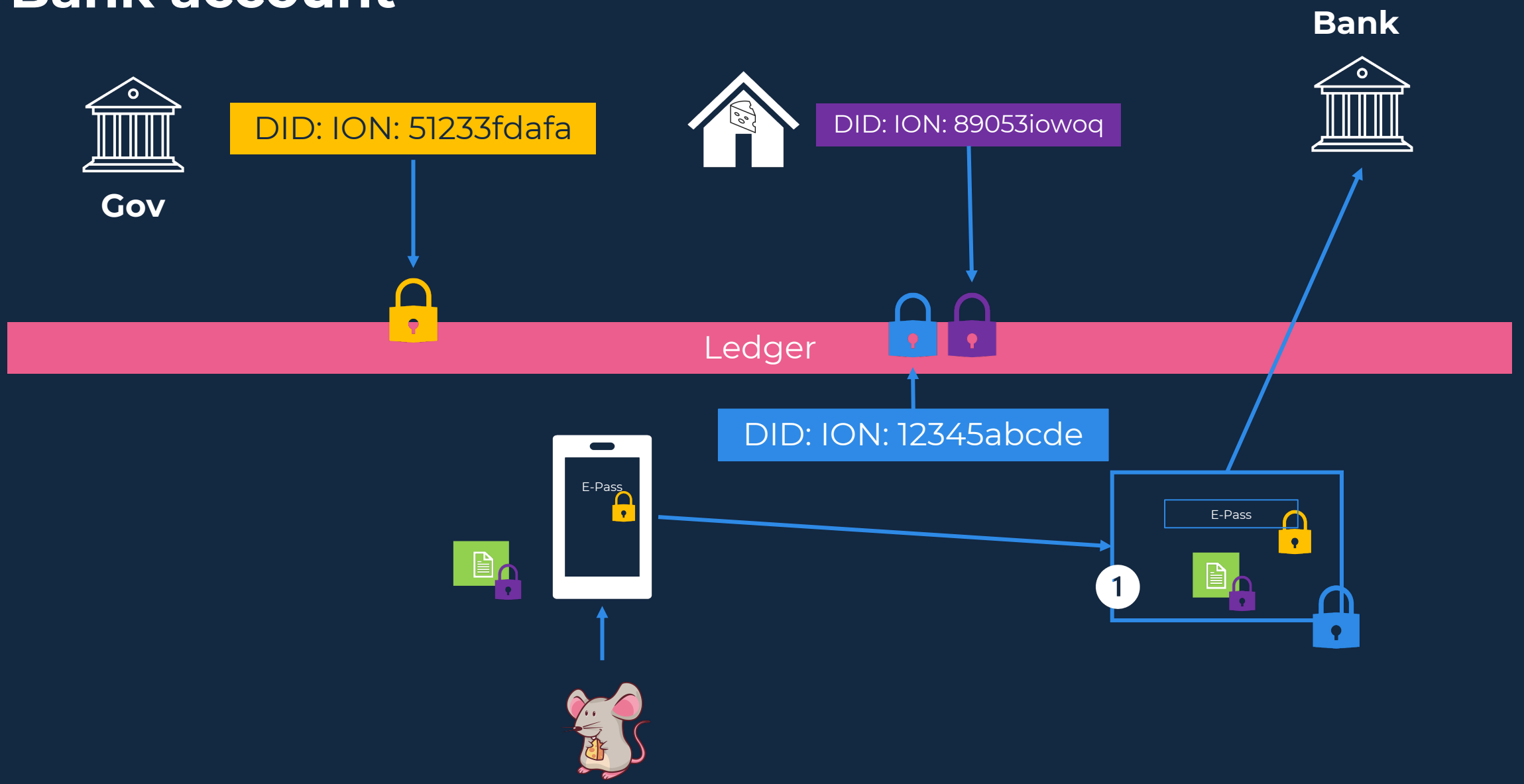


Bank account

ubique

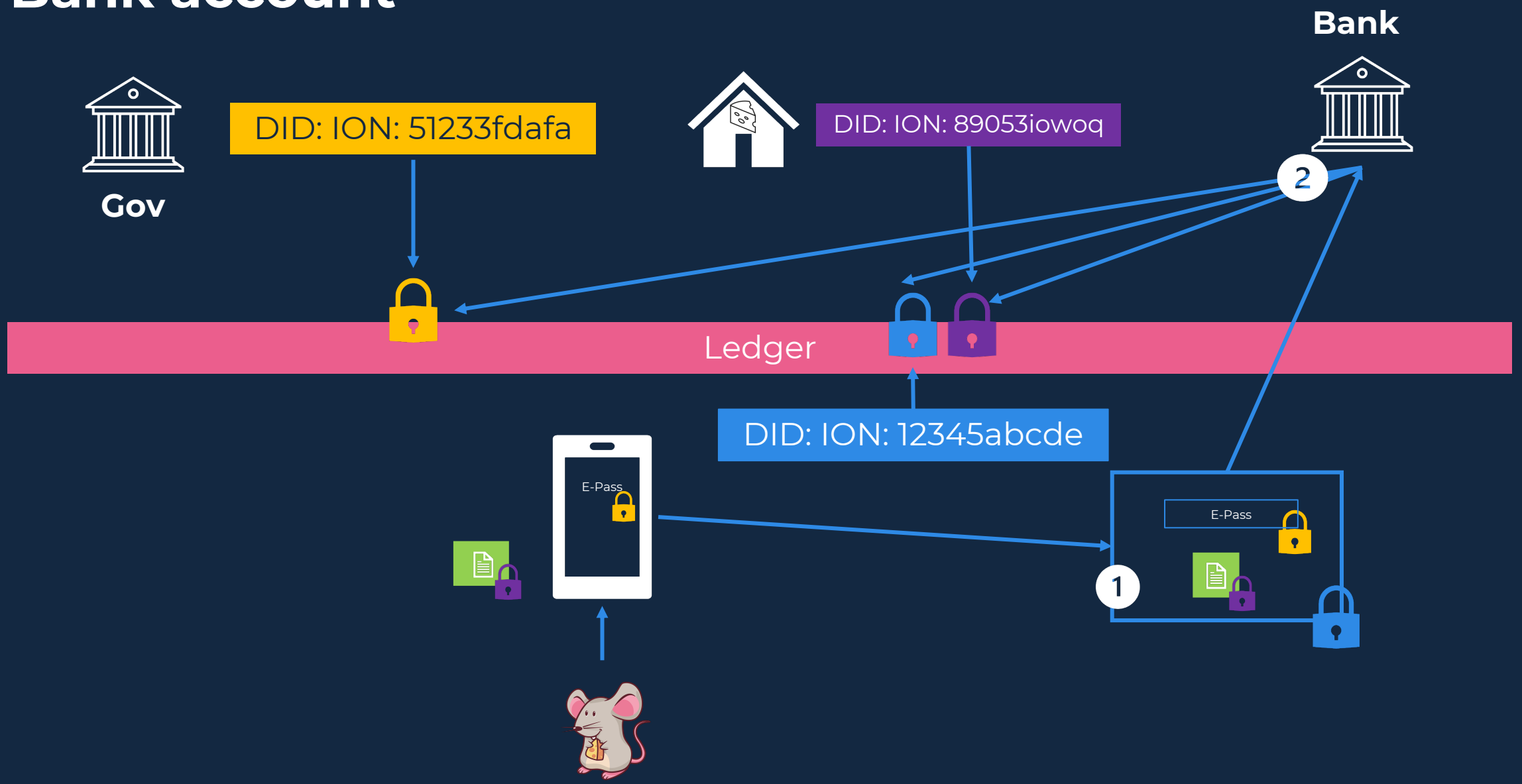
Kingdom of Cheese

Bank account



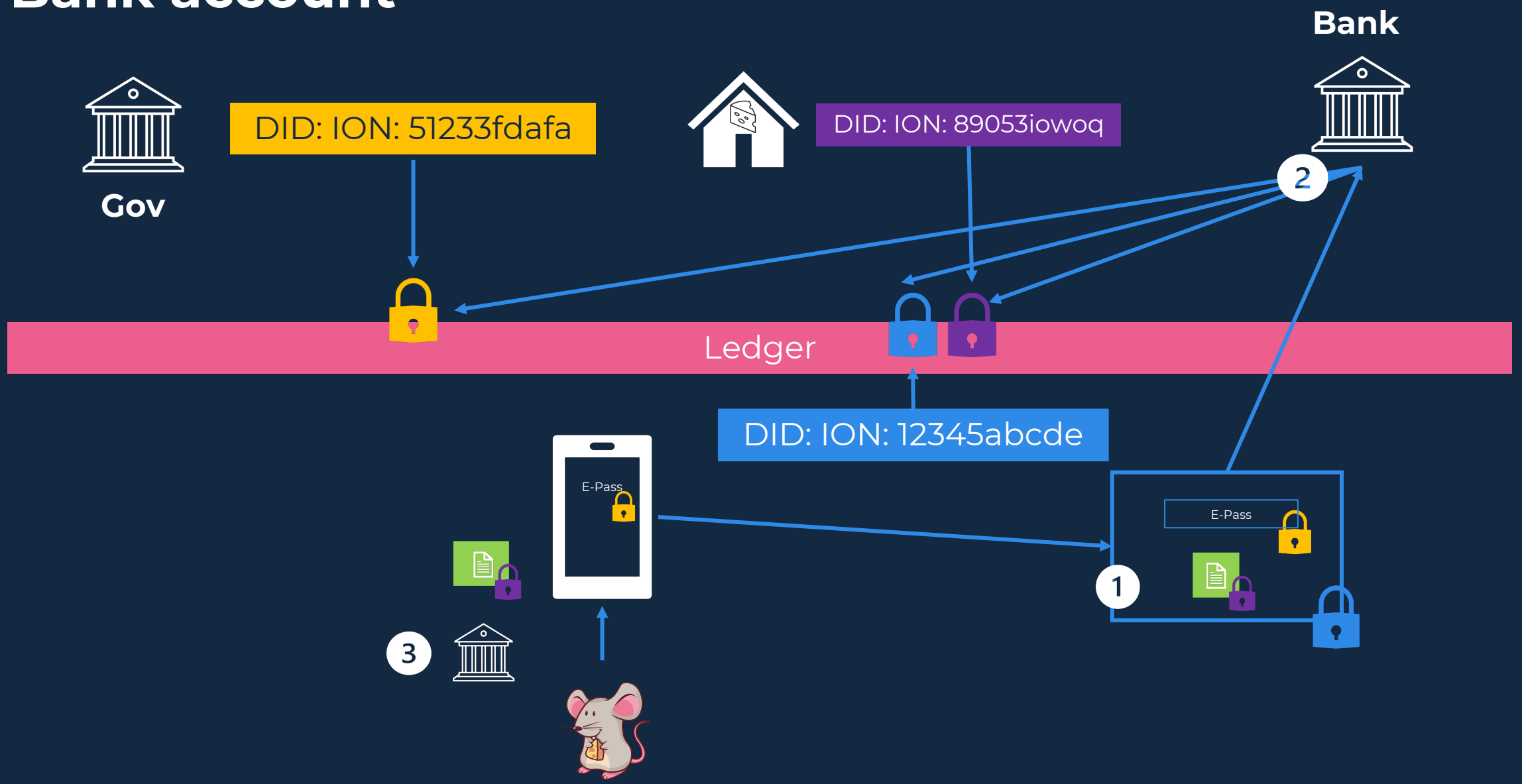
Kingdom of Cheese

Bank account



Kingdom of Cheese

Bank account



Kingdom of Cheese

Problems to solve

1. We share information which is not necessary to share

   → Selective Disclosure

2. DID: government and townhall can match your e-pass with your residency → Hiding the DID

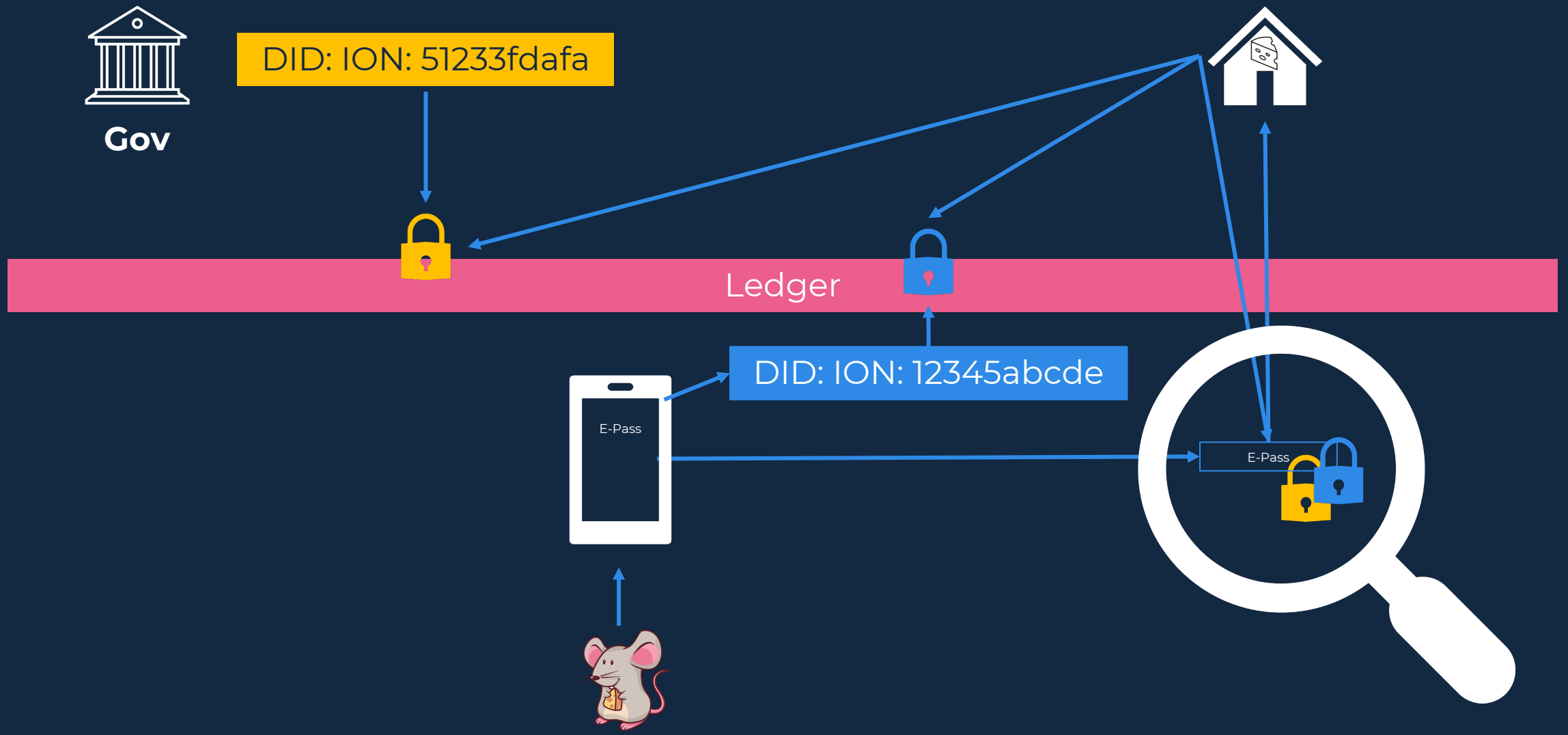
3. With the signature you can correlate information → Hiding signature

Selective Disclosure

ubique

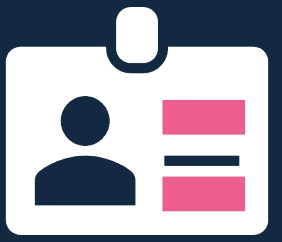
Kingdom of Cheese

Selective Disclosure



Selective Disclosure

- In a selective disclosure scheme, the signature holder can specify, which credential-properties to reveal



- By allowing this, we can improve on data privacy (e.g. an institution does not need to know anything on my passport)

- Selective disclosure for regular RSA or ECDSA signatures can be achieved with atomic signatures

Kingdom of Cheese

Selective Disclosure Issue

Jenny has two wine bottles and a certificate for both

Origin: Bordeaux
Vintage: 1980

Origin: Kingdom of bad wine
Vintage: 1964

Kingdom of Cheese

Selective Disclosure Issue

Works fine but we run into problems

Origin: Bordeaux

Vintage: 1980

4 credential

Origin: Kingdom of bad wine

Vintage: 1964

Kingdom of Cheese

Selective Disclosure Issue

Origin: Bordeaux

Vintage: 1964

Selective Disclosure

Easy solution: The issuer can issue all possible combinations

Number of combinations increases very fast → we would need a lot of signatures:

$$\mathrm{N} + \binom{N}{2} + \binom{N}{3} + \cdots + 1 = \sum_{k=1}^{N} \binom{N}{k} = 2^N - 1$$

Selective Disclosure

We need a signature scheme, where the holder can “modify” the signature (or at least the verification payload)

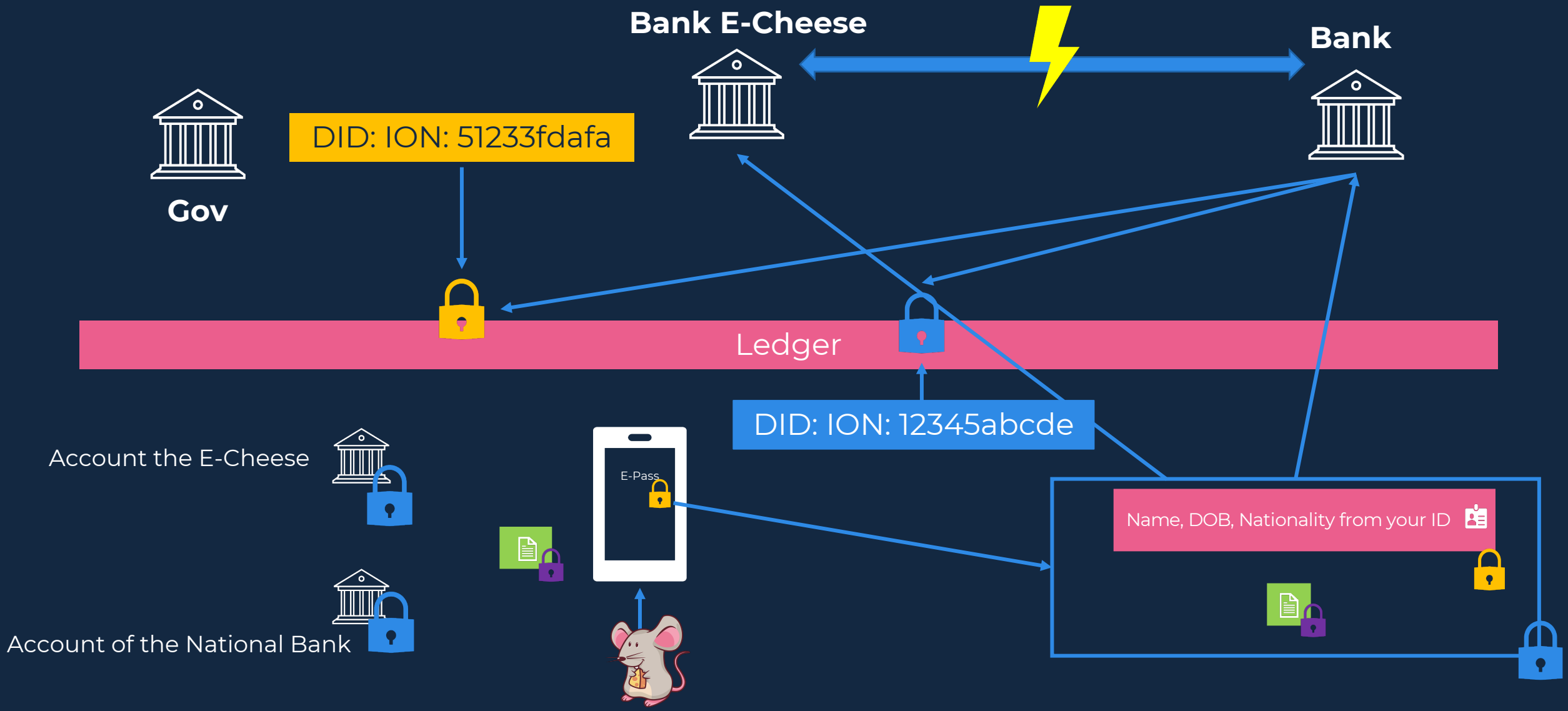
- Camenisch-Lysyanskaya (CL) Signatures (RSA-based) https://cs.brown.edu/people/alysyans/papers/camlys02b.pdf
- Dan Boneh, Xavier Boyen, and Hovav Shacham (BBS+) Signatures (Pairing-based) https://eprint.iacr.org/2016/663.pdf

Hiding the DID

ubique

Kingdom of Cheese

Hiding the DID: Decentralized identifier



Kingdom of Cheese

Hiding the DID

Goal: Hide the identifier → so that the holder can choose when to disclose the link between two credential

Naïve approach: Use different DIDs to get the credentials

→ But how can we now link certain credentials?

Hiding the DID

Solution: linked-secrets (Pedersen Commitment)

Requirements:

- Jenny can “blind” a secret
- Jenny can use the same secret multiple times
- Jenny can proof that she knows the secret (she is the subject)
- Jenny can proof that two or more signature have the same secret

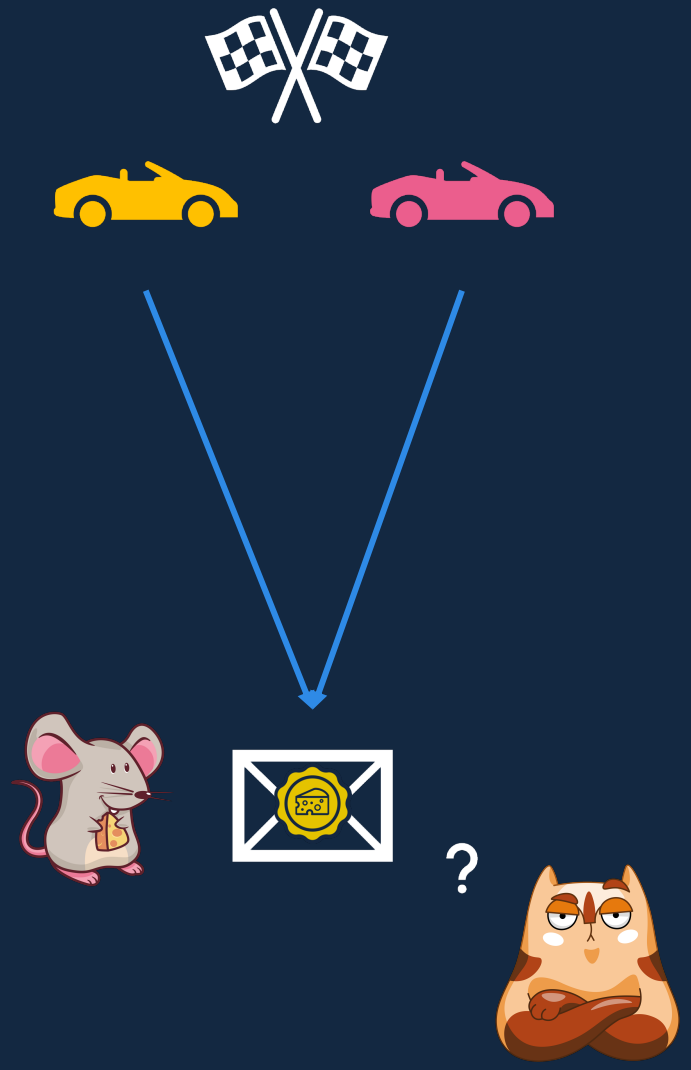
Linked-secrets

Pedersen Commitment

ubique

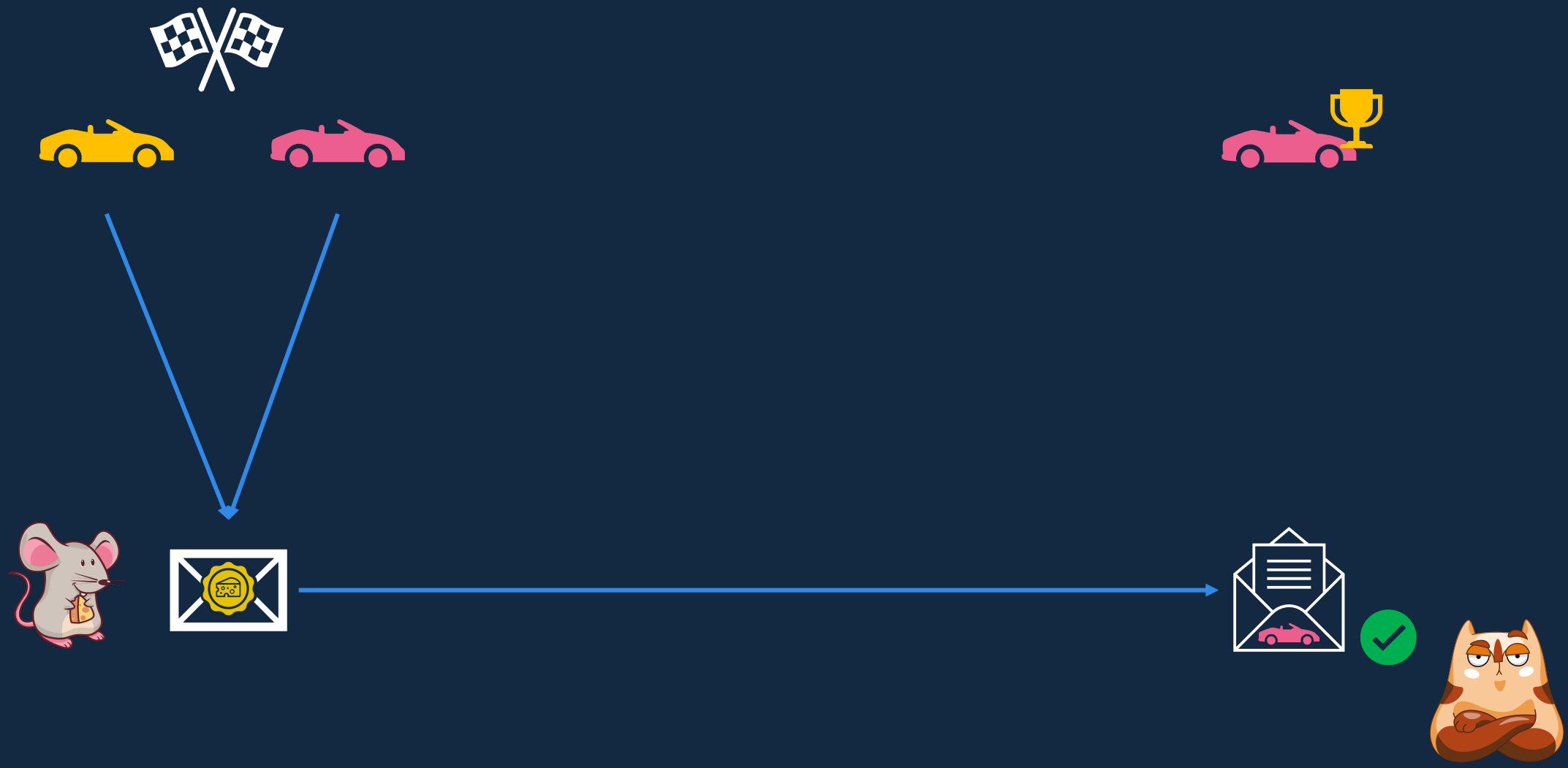
Linked-secrets

Pedersen Commitment



Linked-secrets

Pedersen Commitment



Pedersen Commitment [1] (Algo)

1. Use a cryptographic elliptic Curve $\mathbb{G}$ as our Base-Group
2. We start with two generators ($g, h \in \mathbb{G}$) → public key
3. We call $C = xg + rh$ a **commitment** to secret x with blinding factor r in the basis (g, h)

[1] https://link.springer.com/content/pdf/10.1007/3-540-46766-1_9.pdf

Pedersen Commitment (Properties)

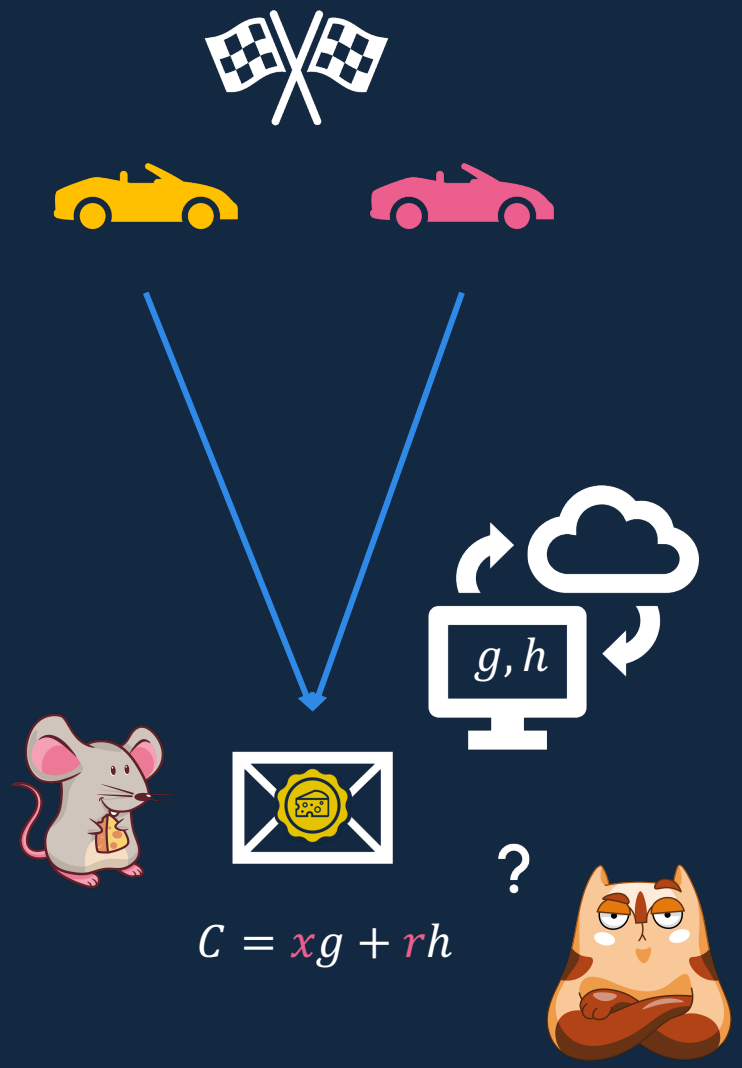
- It is binding $C' \neq C \; for \; x' \neq x$
- It is hiding because C alone does not leak any information about x
- (additive) homomorphic
  - Using the group property of G it can be shown that:

$$C_1 - C_2 = (x_1 g + r_1 h) - (x_2 g + r_2 h) = (x_1 - x_2) g + (r_1 - r_2) h \xrightarrow[x_1 = x_2]{} C_1 - C_2 = (r_1 - r_2) h$$

  - If Jenny reveals $r_1 - r_2$, Tomas can verify that C_1, C_2 are commitments to the same x

Linked-secrets

Pedersen Commitment



Linked-secrets

Pedersen Commitment

Hiding the signature

Kingdom of Cheese

Hiding the signature

Requires a proof that Jenny lives in Kingdom of Cheese (Nationality from E-Pass)

Requires a proof that Jenny is older than 18 (DoB from E-Pass)

- Nationality
- DoB
- ...

Hiding the Signature

Solution: Zero Knowledge Proofs (ZKP)

1. We call them proof of knowledge

2. Like the name suggests, we can prove the ownership of the signature without actually showing it

3. Hence we eliminate the link between different usages (as the Proofs generally have a random element to them)

Proof of knowledge

Schnorr Protocol

ubique

Proof of knowledge

Schnorr Protocol

1. In order to prove the knowledge of a secret value (without revealing it) in a Pedersen commitment we use the Schnorr protocol

2. We basically prove the knowledge of the discrete logarithm

3. The Schnorr protocol is an interactive proof of knowledge

Proof of knowledge

Schnorr Protocol

1. We start with the commitment $C = xg + rh$
2. The prover chooses β and γ randomly and sends $a = a_1 + a_2 = \beta g + \gamma h$ to the verifier
3. The verifier chooses c randomly and sends it to the prover
4. The prover calculates $s_1 = \beta - cx \pmod{q}$, $s_2 = \gamma - cr \pmod{q}$ and sends it to the verifier
5. The verifier calculates

$$C' = s_1 g + s_2 h + cC = \beta g - cxg + \gamma h - crh + cxg + crh = \beta g + \gamma h = a_1 + a_2 = a$$

Selective disclosure

Camenisch-Lysyanskaya

ubique

Kingdom of Cheese

Selective Disclosure Issue

Origin: Bordeaux

Vintage: 1964

Camenisch-Lysyanskaya

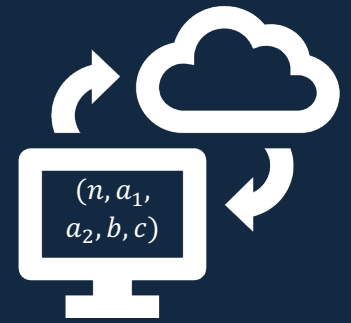
- The security is based on the strong RSA assumption
- It enables:
  - blinded signing
  - partially revealing (selective disclosure)
  - proof of knowledge of the signature

Camenisch-Lysyanskaya

1. Key Generation
2. Signing
3. Verifying

Camenisch-Lysyanskaya

Key Generation



1. The issuer chooses a special RSA modulus n = p*q

2. Choose uniformly at random (a_1, a_2, b, c) from the quadratic residues (QR) ($QR = \{a, b \in \mathbb{Z}_n^* | b^2 = a\}$)

3. Public Key corresponds to (n, a_1, a_2, b, c) and the private key to the factorization of n

Camenisch-Lysyanskaya

Signing

1. On message $m = (m_1, m_2)$, choose at random e (prime) and s
2. Calculate v such that

$$v^e = a_1^{m_1} a_2^{m_2} b^s c \bmod n$$

$$v = \left(a_1^{m_1} a_2^{m_2} b^s c\right)^{\frac{1}{e}} \bmod n$$

3. Output is (s, e, v)

m_1 = Bordeaux

m_2 = 1980

Camenisch-Lysyanskaya

Verifying (showing all properties)

1. Check that $v^e \equiv a_1^{m_1} a_2^{m_2} b^s c \; mod \; n$ and the length requirements on e
2. Tomas needs all properties to verify the signature

Camenisch-Lysyanskaya

Verifying with selective Disclosure

m_1 = Bordeaux

m_2 = *****

Bordeaux Club

For commitment $C = a_2^{m_2} b^r$ we can modify the signature output to $(s - r, e, v)$ →

$$v^e \equiv a_1^{m_1} C b^{s-r} c = a_1^{m_1} a_2^{m_2} b^r b^{s-r} c = a_1^{m_1} a_2^{m_2} b^s c \bmod n$$

Which is still a valid signature on our original triple (s, e, v)

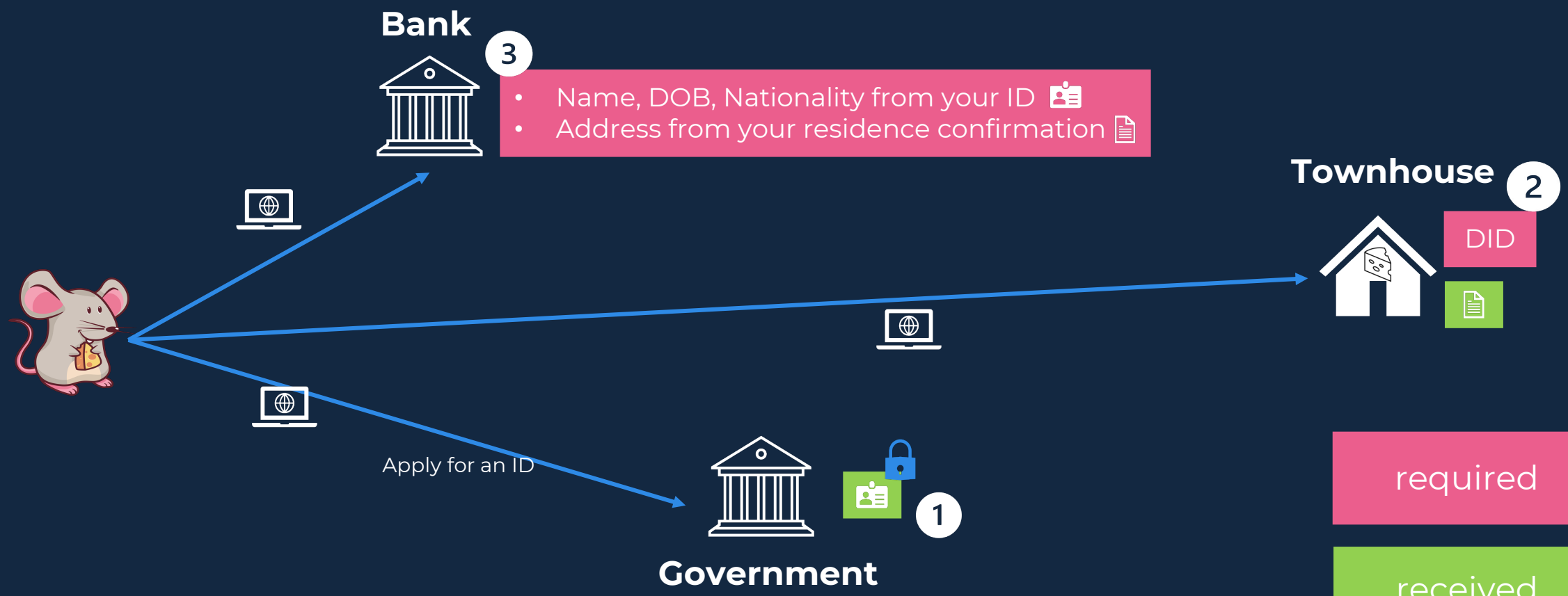
Recap

ubique

Kingdom of Cheese

Self-sovereign Identity World

Goal: Jenny wants to open a bank account in Kingdom of Cheese



Kingdom of Cheese

Recap

Selective Disclosure

Jenny can hide properties

- Name, DOB, Nationality from your ID
- Address from your residence confirmation

Hiding the DID

we can hide the common identifier (secret) from Jenny

Ledger

Hiding the signature

We can hide the signature (no correlation between different proofs)

ubique

www.ubique.ch

Schnorr Protocol

1. For the prover it is important to choose new randoms each time

2. Otherwise, the secret can be derived

$$s_1 = \beta - c_1 x, \qquad s_2 = \beta - c_2 x$$

$$s_1 - s_2 = (c_2 - c_1)x$$

$$x = \frac{s_1 - s_2}{c_2 - c_1}$$

Zero knowledge protocol, non interactive

Fiat Shamir Heuristic

ubique

Fiat Shamir Heuristic

1. The Schnorr protocol is nice to prove knowledge of the discrete logarithm

2. It is an interactive zero knowledge proof though

3. It is interactive, as we need a random unguessable challenge c (otherwise the prover could construct a forged value)

Fiat Shamir Heuristic

1. Note that the challenge c is just a call to a random oracle

2. Further c can be made public → (public-coin)

3. Fiat and Shamir realized that it can be constructed using a cryptographic hash function

Fiat Shamir Heuristic

1. The idea is to produce a challenge by hashing

2. To be a secure challenge, all public parameters have to be hashed

3. For our Schnorr protocol this means H(C,a,g,h)

Fiat Shamir Heuristic

1. We start with the commitment $C = xg + rh$

2. The prover chooses β and γ randomly and sets $\mathrm{a} = \mathrm{a}_1 + \mathrm{a}_2 = \beta g + \gamma h$

3. The prover then calculates $c = H(C||a||g||h)$

4. The prover uses this c to calculate $\mathrm{s}_1 = \beta - cx \pmod{\mathrm{q}}, \mathrm{s}_2 = \gamma - cr \ (mod\ q)$ and sends it together with either c or a to the verifier

5. The verifier calculates and verifies $C' = s_1 g + s_2 h + cC = \beta g - cxg + \gamma h - crh + cxg + crh = a_1 + a_2 = a$ or $H(C||C'||g||h) = c$

Recap

1. We found a scheme to “commit” to a value, the Pedersen commitment

2. Thanks to Schnorr’s protocol, we could prove the knowledge of the secret

3. With the help of the Fiat-Shamir-Heuristic we made it interactive