Building trust for Peer 2 Peer transaction

Cyril Vignet, BPCE

The text and diagrams below represent the personal views of the author and are not necessarily endorsed by his company or any community he represents or is associated with. It is submitted here for discussion only without any commitments or obligations to be derived therefrom.

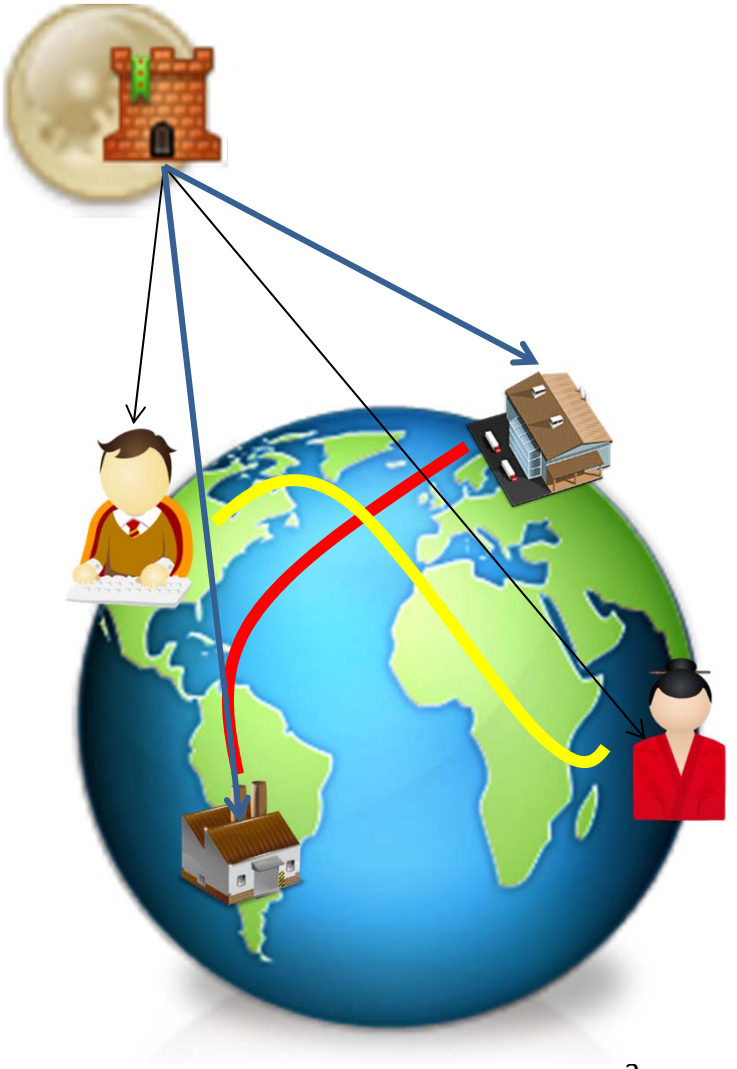
The commercial P2P paradigm

- 2 entities,
  - **At random**
  - **On a worldwide basis**
  - **May know each other but not necessarily**

- A commercial transaction:
  - **Accepted by both parties**
  - **Reliable and impossible to repudiate later by one or the other**
  - **Fair balanced, that is, no party can impose its conditions unilaterally**

The “friend of a friend” solution

- Need for
  - A centralised worldwide company
  - A worldwide PKI
- Operational difficulties with 7 billion people and hundreds millions of companies



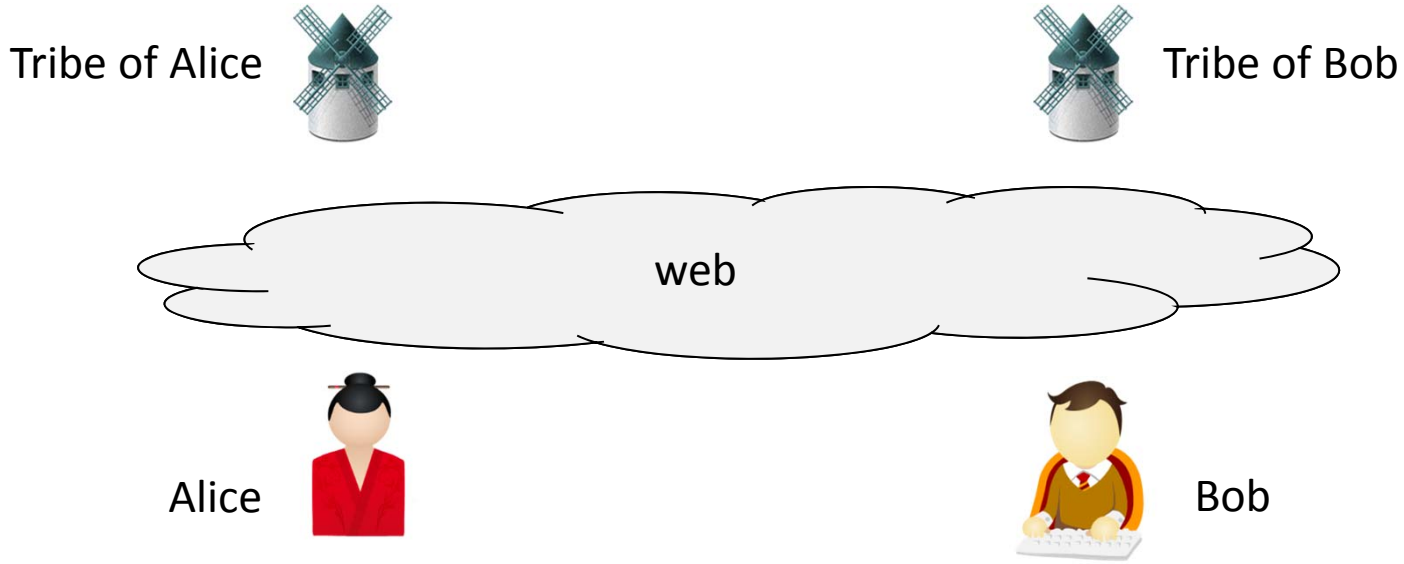
The “my tribe knows your tribe” solution

- Scalability achieved by existing networks of three/four parties (trust parties)
  - Governments, Telcos, banks, notaries, lawyers,…
- Possibility for the « peer » to switch the trust party

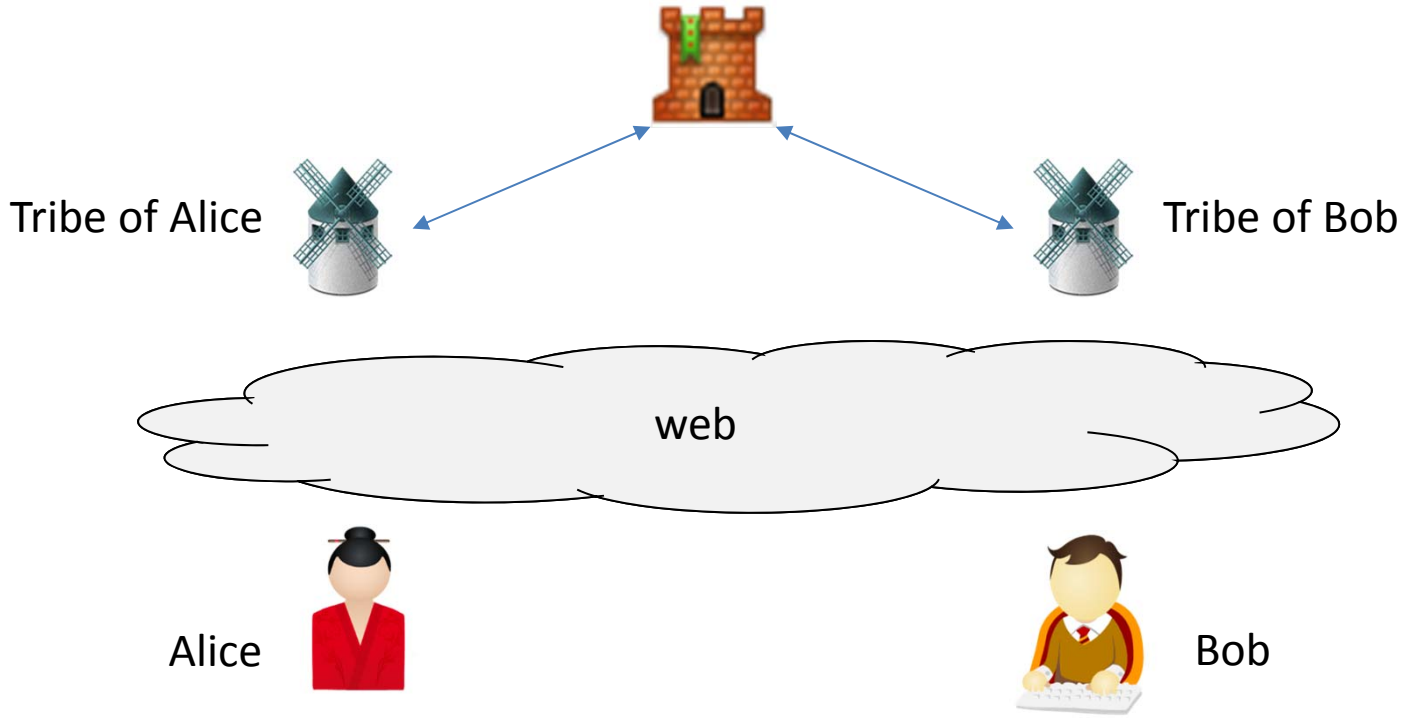
S.C.A.I

A proposal for a web operational model for the « my tribe knows your tribe » solution

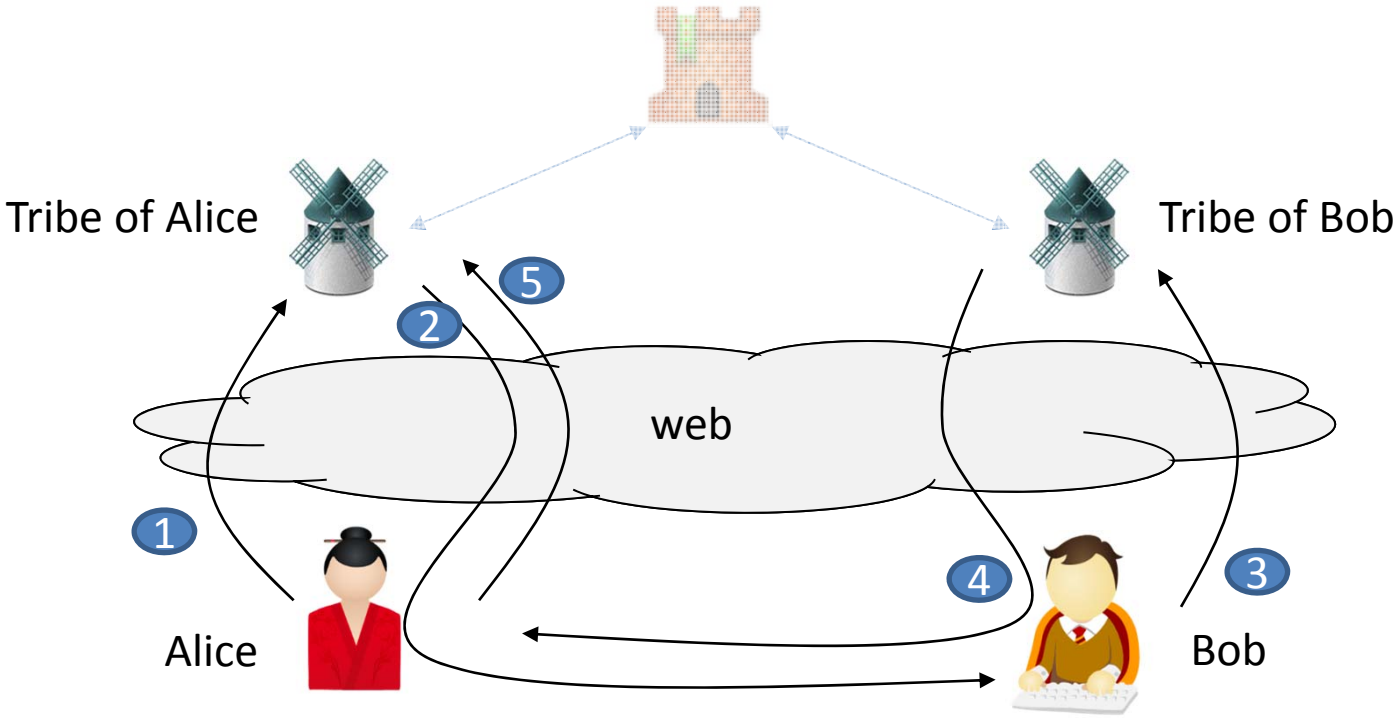
2 peers, 2 Trust parties, the WEB



Prerequisite: a shared PKI amongst trust parties



First structure: a workflow

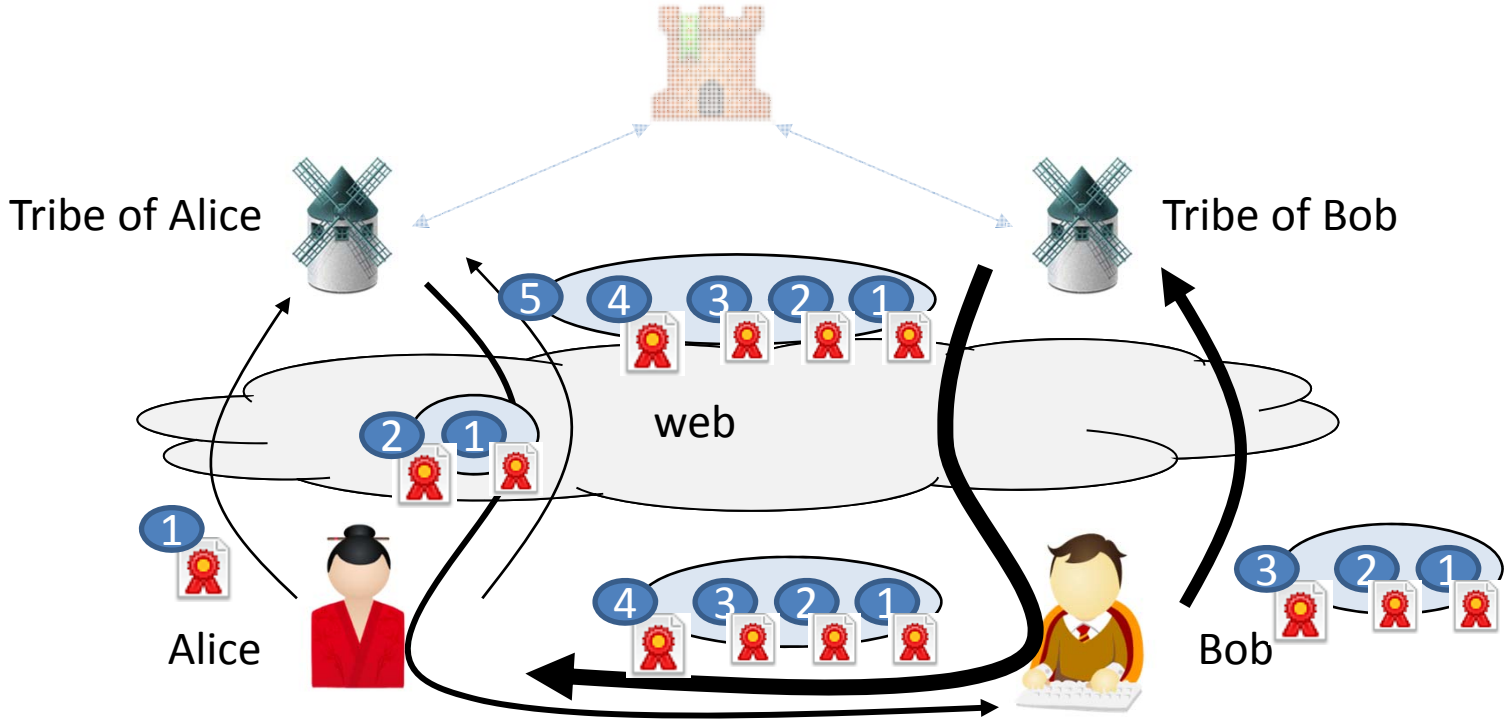


First structure: legend of the workflow

- Alice want to send a message to Bob and receive an answer

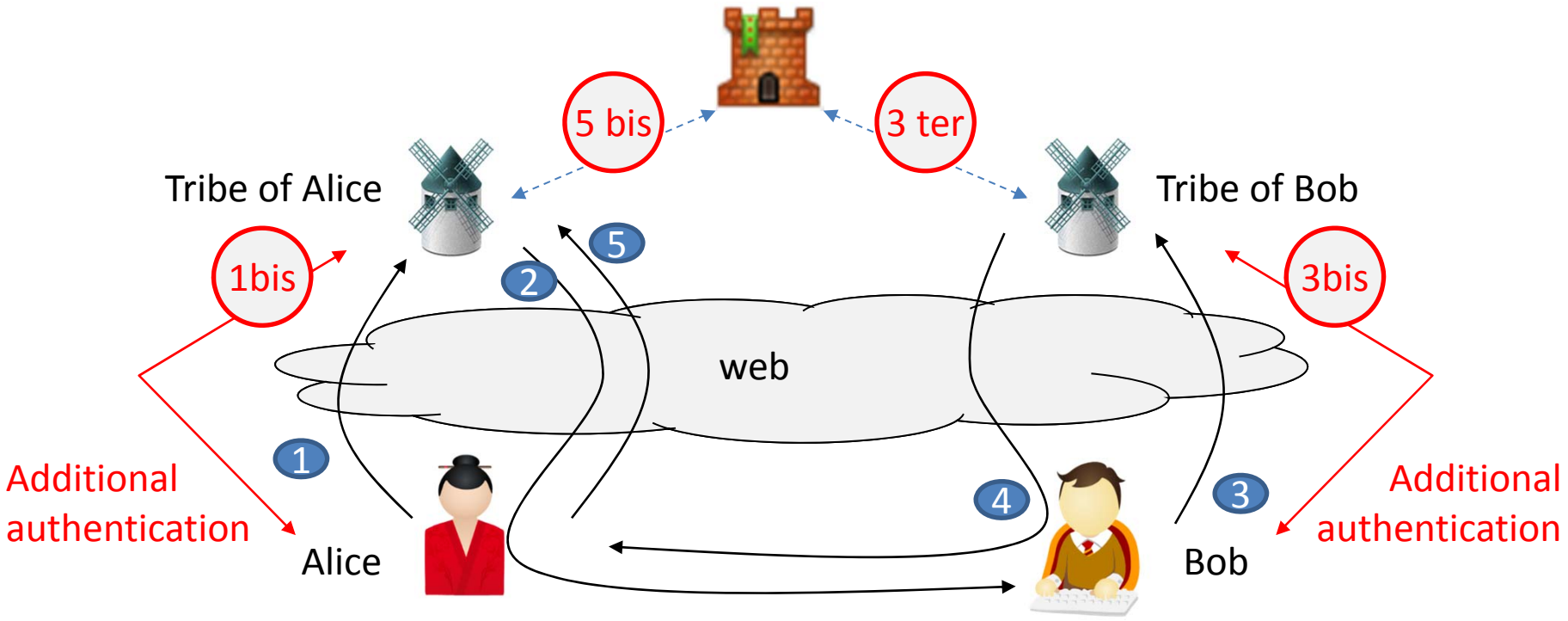
1. Alice writes the message and send it to her Tribe
2. The Tribe of Alice grants Alice to be « The » Alice then send back to Alice. Alice forward to Bob
3. Bob read the message, answers it and send to his Tribe
4. The Tribe of Bob, grants The Tribe of Alice, grants Bob to be Bob and send back to Bob. Bob forwards to Alice
5. Alice read the answer from Bob and forwards to her Tribe to be sure of Tribe of Bob.

Second structure: a SCAI line = 



- Each bilateral flow is signed by the issuer
- The next flow stacks the previous flows and signs the result

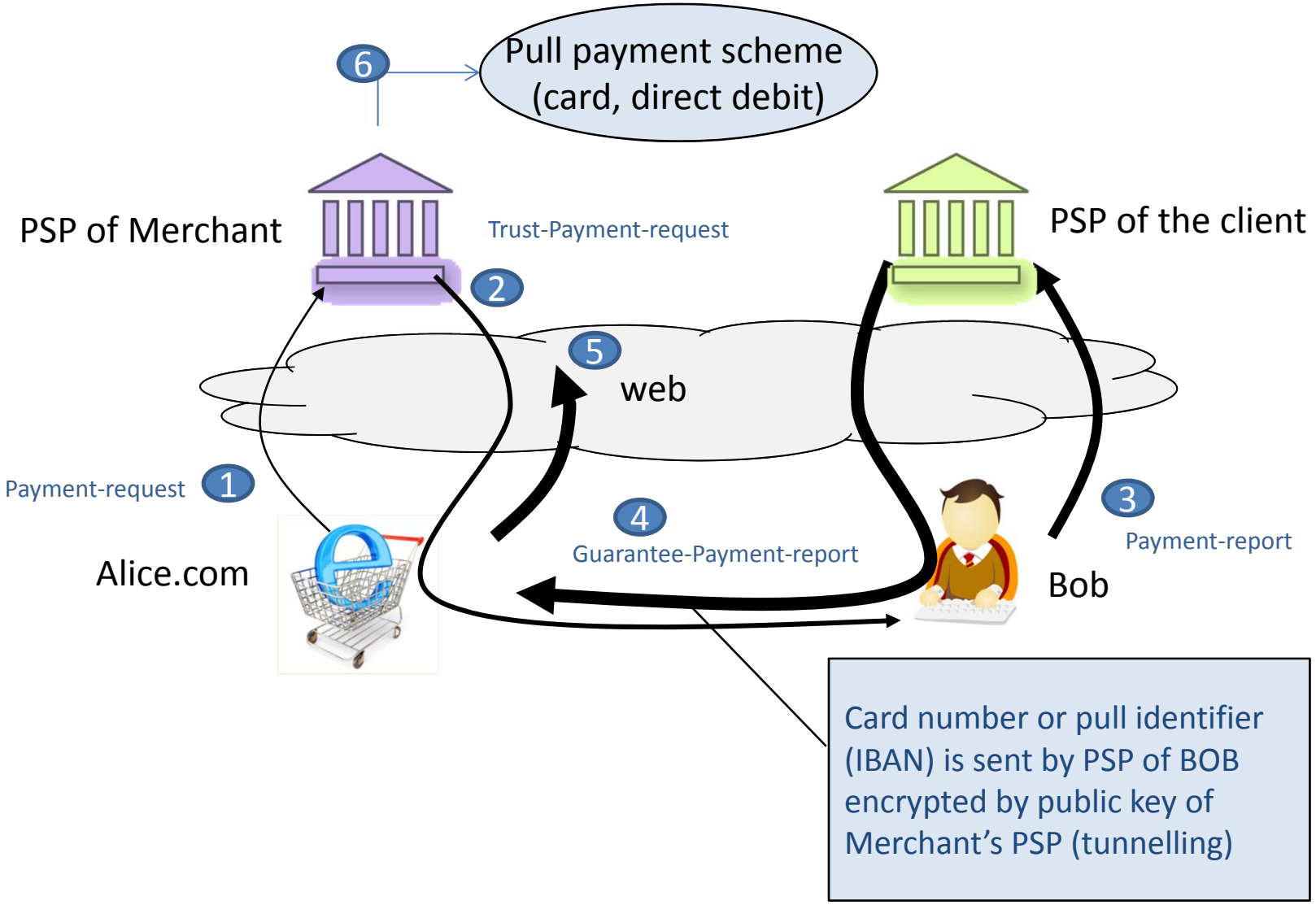
Third structure: additional controls by trust parties



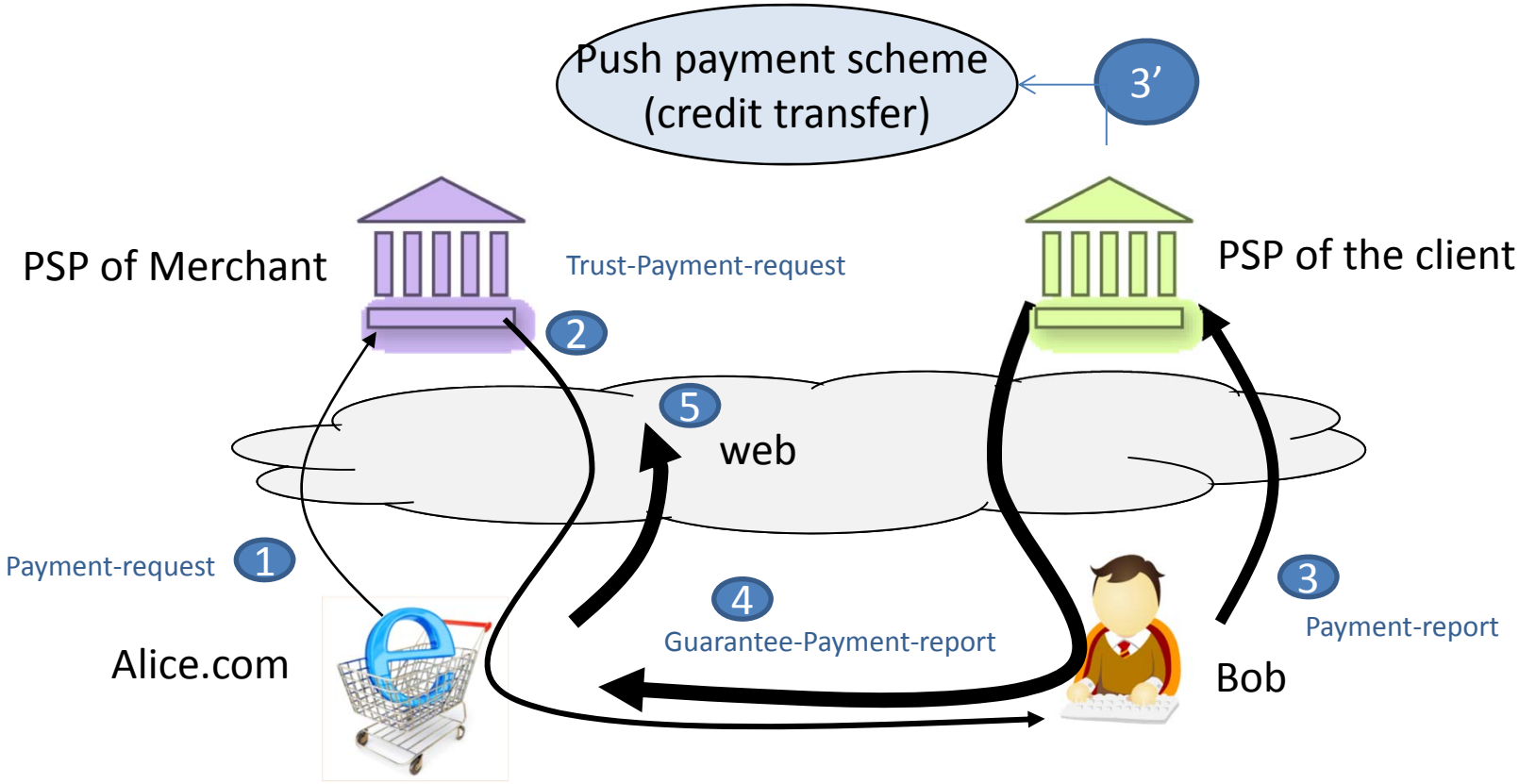
Advantages of SCAI concept

- SCAI should use only state-of-the-art cryptographic signature
- SCAI is balanced because the workflow gives the power to the peers
- Explicit audit trail of successive messages
- Agnostic regarding the transported messages (could be payment, initiation, purchase, information)
- Transparency for all actors, except for some secret data
- SCAI does not enforce certified key on the peer side (but uses session key or self-signed certificate). Nevertheless a peer could use key from existing PKI (corporate)
- 2 peers of a same tribe could use SCAI
- SCAI is neutral versus the data transported and so could be used in a wide range of areas
- SCAI could be extended to more than four actors if really necessary
- SCAI complies with privacy needs by offering tunnelling capabilities and using session key at peer level

Example: Web Commerce pull payment



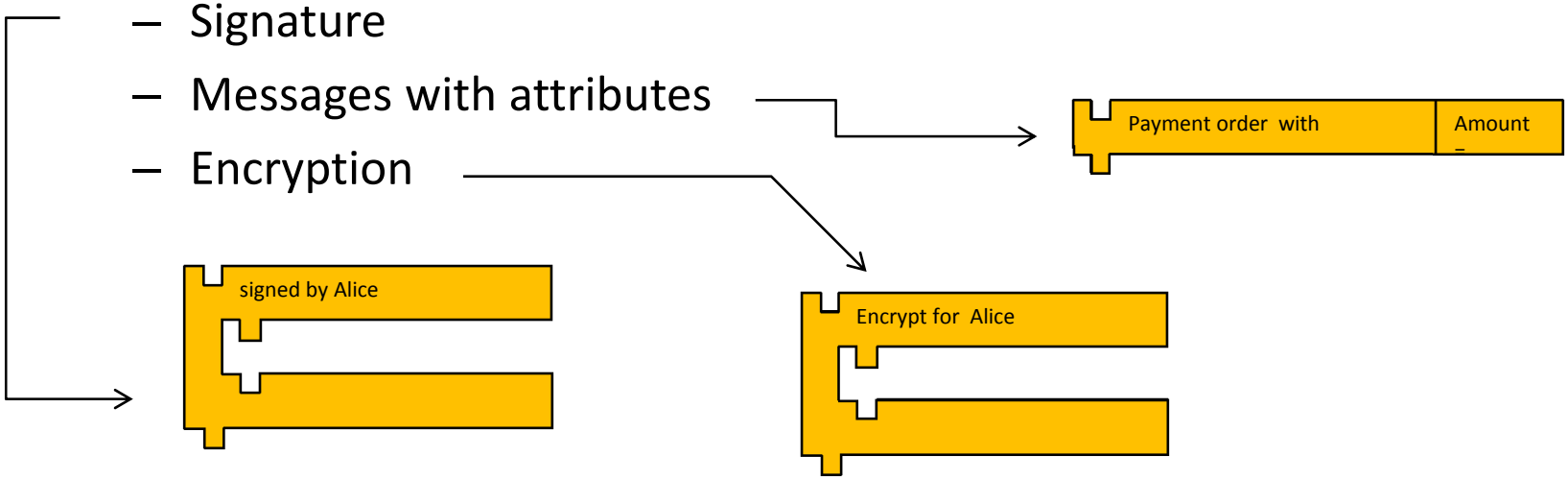
Example: Web Commerce push payment



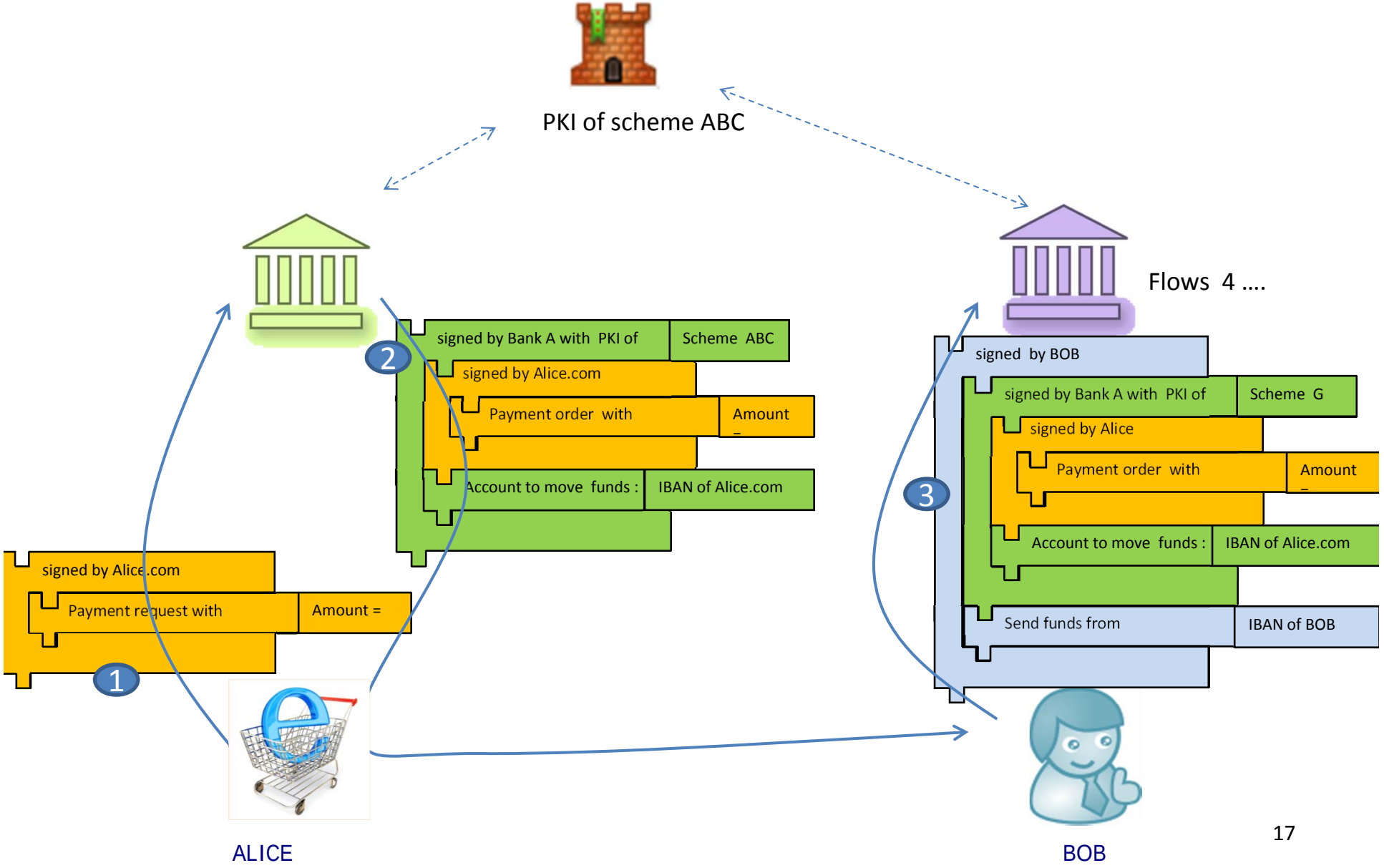
Stacked Countersignatures with Attributes Implementation

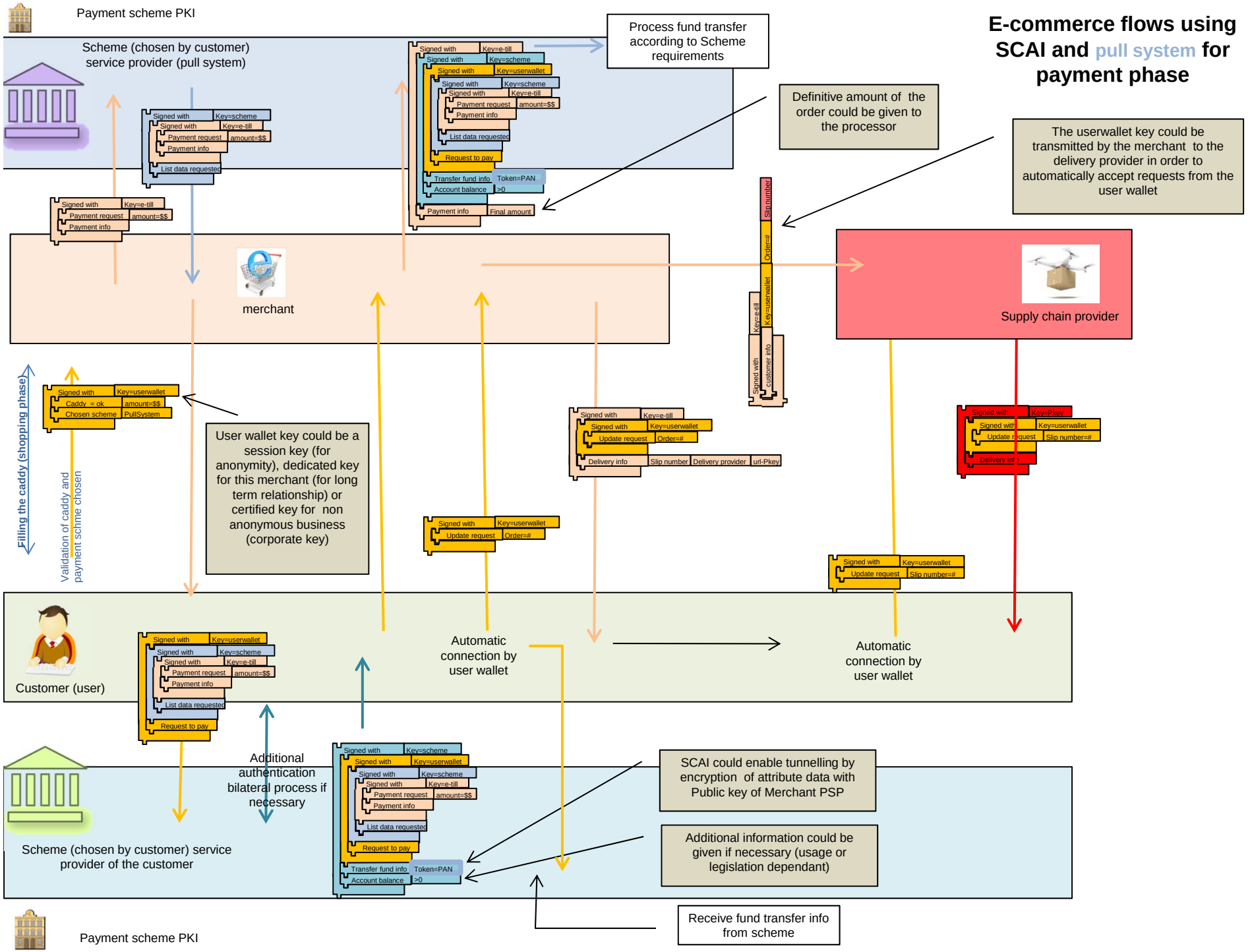
For going into details

- We develop a representation based on the Scratch User Interface concept (https://scratch.mit.edu/) to detailed SCAI capabilities
- we will use three types of blocks, all of them could be stacked:
  - Signature
  - Messages with attributes
  - Encryption



first flows using SCAI template




E-commerce flows using SCAI and pull system for payment phase
Payment scheme PKI
Scheme (chosen by customer) service provider (pull system)
Process fund transfer according to Scheme requirements
Definitive amount of the order could be given to the processor
The userwallet key could be transmitted by the merchant to the delivery provider in order to automatically accept requests from the user wallet
merchant
Supply chain provider
Filling the caddy (shopping phase)
Validation of caddy and payment schme chosen
User wallet key could be a session key (for anonymity), dedicated key for this merchant (for long term relationship) or certified key for non anonymous business (corporate key)
Automatic connection by user wallet
Automatic connection by user wallet
Customer (user)
Additional authentication bilateral process if necessary
Scheme (chosen by customer) service provider of the customer
SCAI could enable tunnelling by encryption of attribute data with Public key of Merchant PSP
Additional information could be given if necessary (usage or legislation dependant)
Receive fund transfer info from scheme
Payment scheme PKI