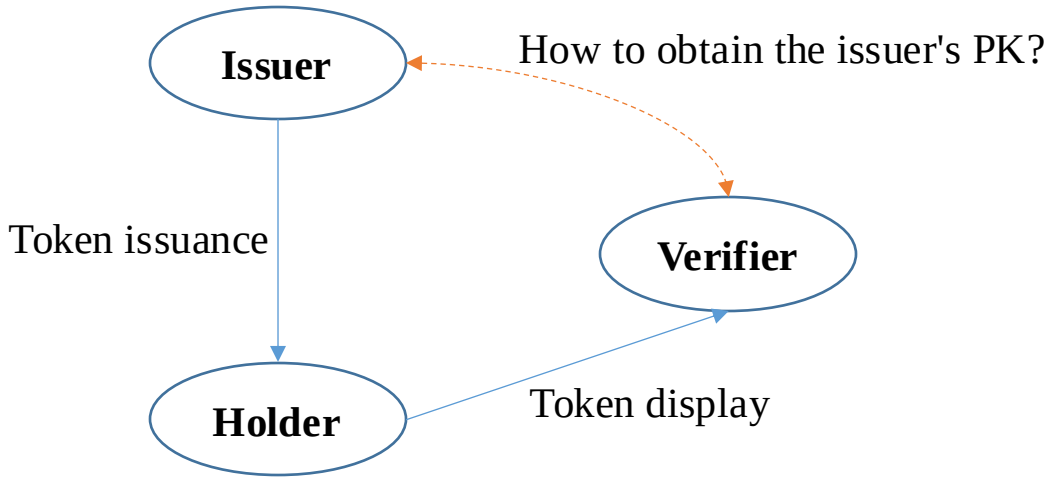
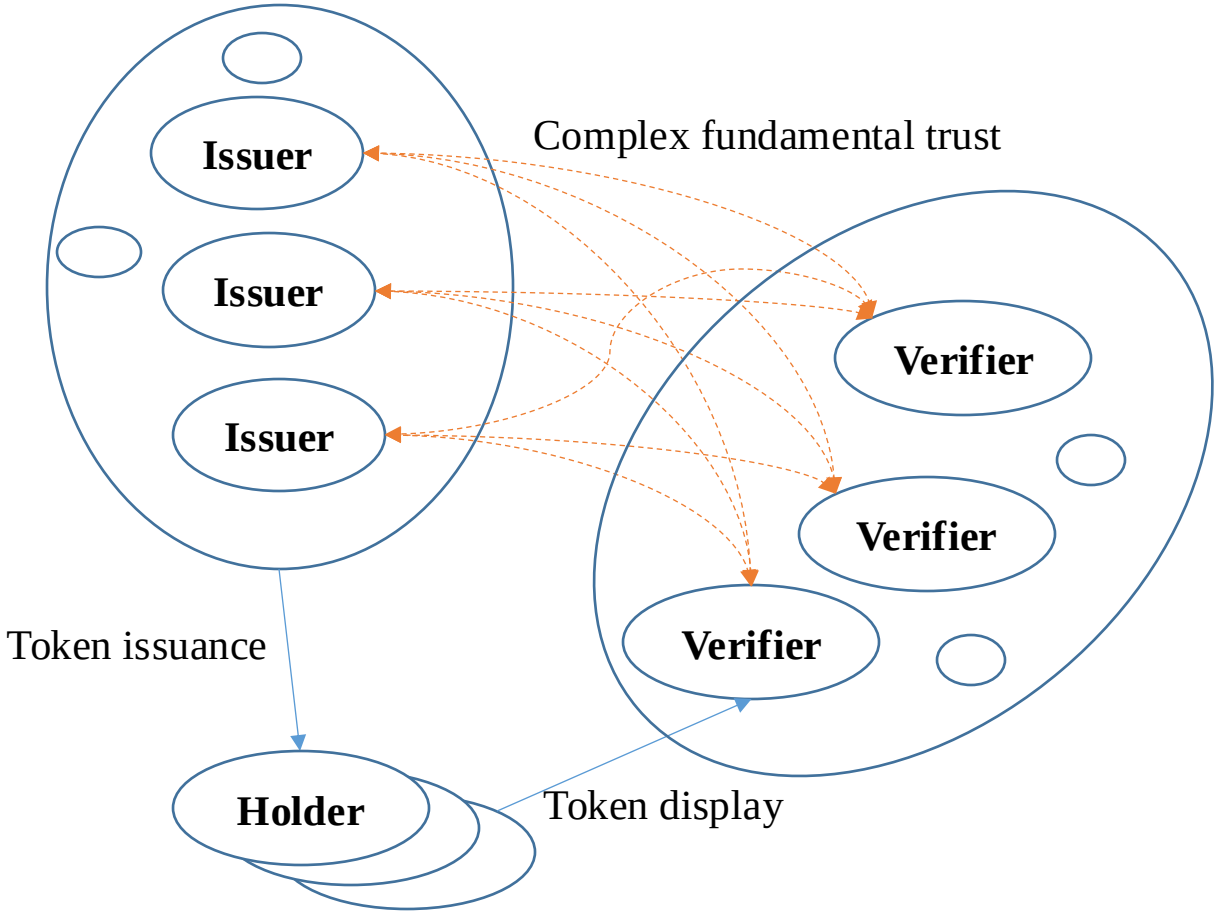
A Public Key Service Provider for Verification in Multiple Issuers and Verifiers

https://datatracker.ietf.org/doc/draft-wang-spice-public-key-service-provider/

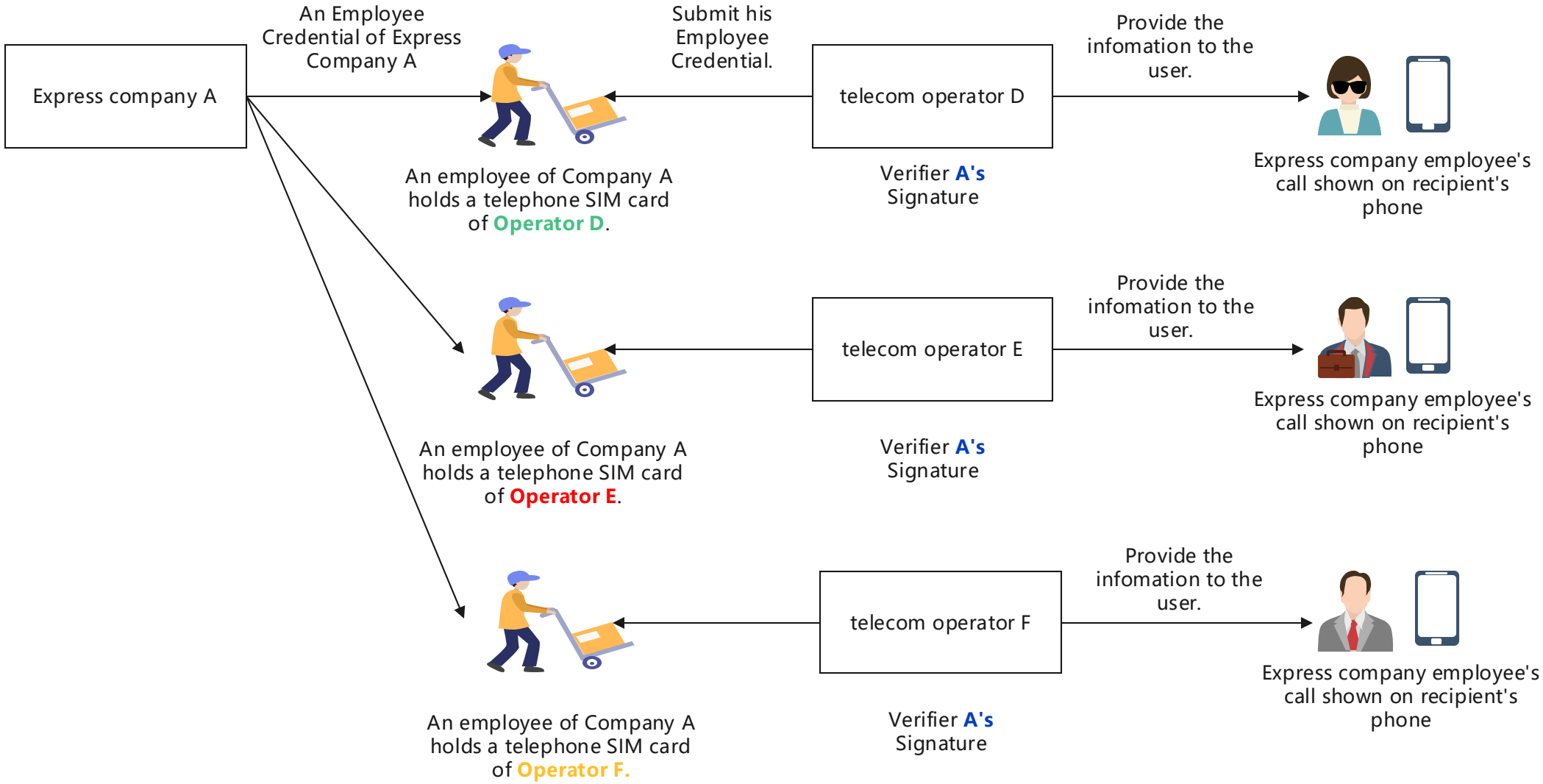
Donghui Wang

Why Public Key Service Provider?

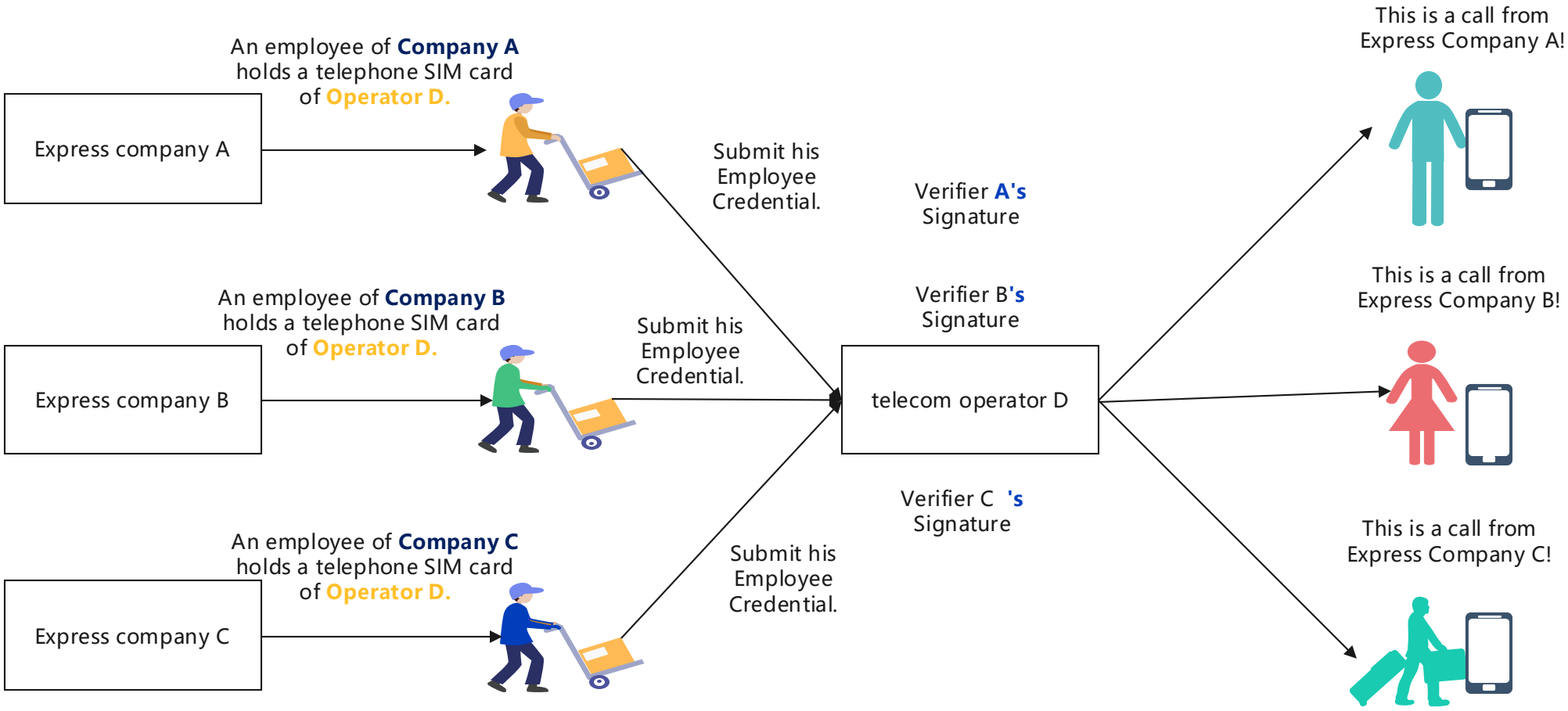




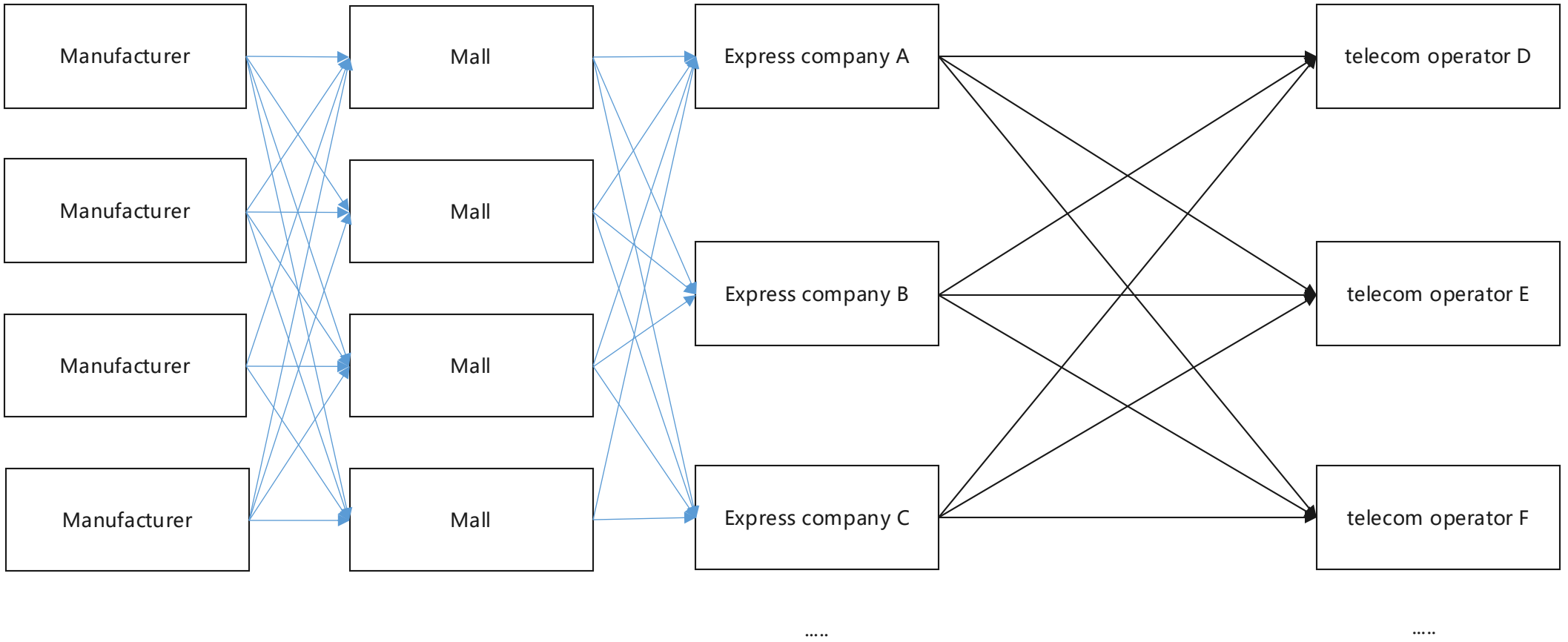
An example...


Express company A
An Employee Credential of Express Company A
Submit his Employee Credential.
telecom operator D
Provide the infomation to the user.
An employee of Company A holds a telephone SIM card of Operator D.
Verifier A's Signature
Express company employee's call shown on recipient's phone
telecom operator E
Provide the infomation to the user.
An employee of Company A holds a telephone SIM card of Operator E.
Verifier A's Signature
Express company employee's call shown on recipient's phone
telecom operator F
Provide the infomation to the user.
An employee of Company A holds a telephone SIM card of Operator F.
Verifier A's Signature
Express company employee's call shown on recipient's phone

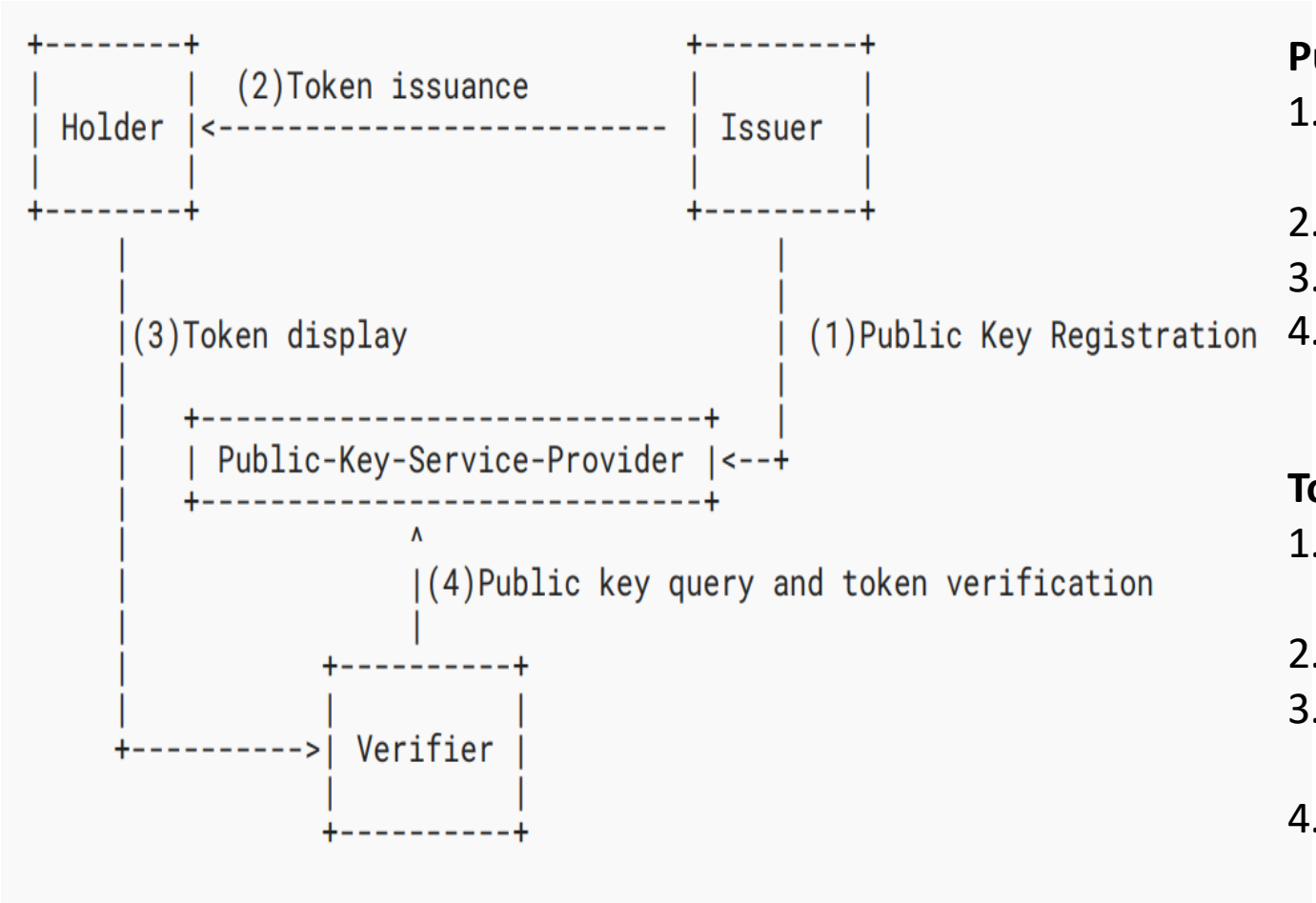
An example…


An employee of **Company A** holds a telephone SIM card of **Operator D.**
Express company A
Submit his Employee Credential.
Verifier **A's** Signature
This is a call from Express Company A!
An employee of **Company B** holds a telephone SIM card of **Operator D.**
Express company B
Submit his Employee Credential.
Verifier B**'s** Signature
This is a call from Express Company B!
telecom operator D
Verifier C **'s** Signature
An employee of **Company C** holds a telephone SIM card of **Operator D.**
Express company C
Submit his Employee Credential.
This is a call from Express Company C!

What’s more?


Manufacturer
Manufacturer
Manufacturer
Manufacturer
Mall
Mall
Mall
Mall
Express company A
Express company B
Express company C
.....
telecom operator D
telecom operator E
telecom operator F
.....

System architecture of a Public-Key-Service-Provider



Public Key Registration

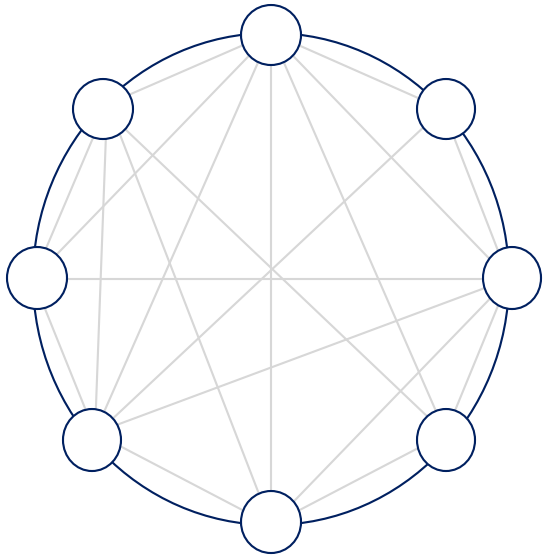
1. The Issuer submits the public key to the PKSP.
2. The PKSP verifies the public key .
3. The issuer gets a response from the PKSP.
4. The registration is completed.

Token verification

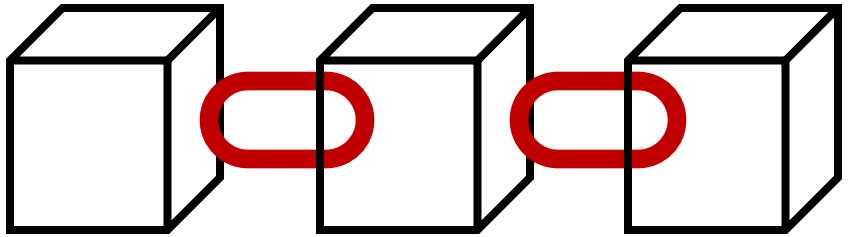
1. Token verification The holder sends the token to the Verifier.
2. The verifier requests the Public Key from the PKSP.
3. The PKSP processes the request and returns the public key.
4. The Verifier uses the public key to verify the token signature.

Public-Key-Service-Provider

PKSP



Multi-party consensus based



Immutable and fault-tolerant storage

programmatically-defined
and automated-executing

Future work

- PKSP service detailed design
- PKSP ledger detailed design

Any comments and discussions are welcomed

Thank you

Contactor: wangdonghui124@huawei.com