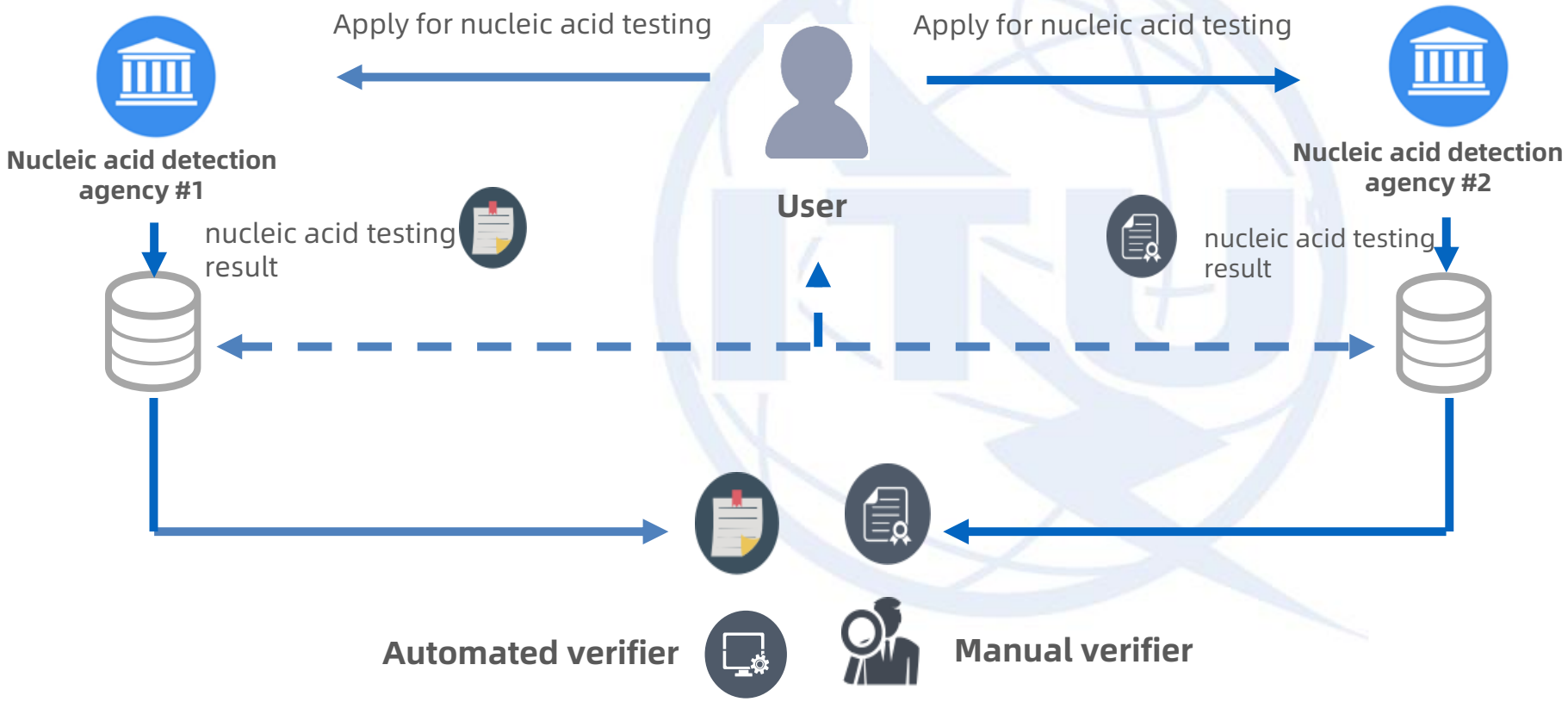
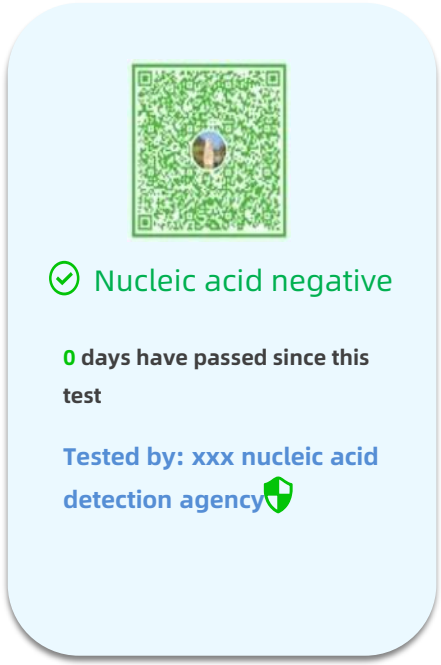
DID : A blockchain based solution to enable controllable and trustable data management

COVID-19 nucleic acid test, certification and it's usage



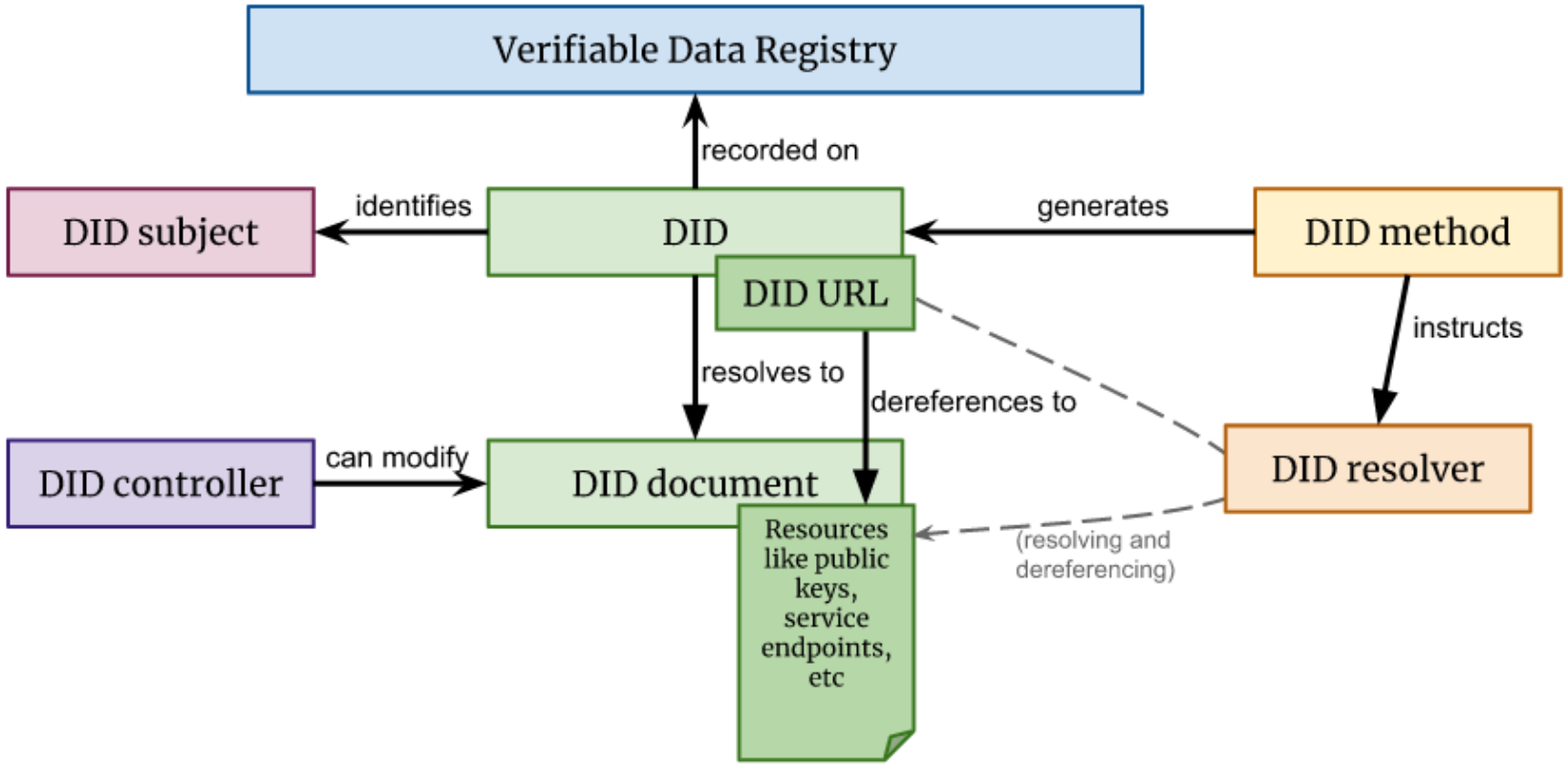


Centralized and isolated identifier problems

- The ID and the certification pertaining to it as well as the privacy information are not controlled by the certification owner.
- Centralized authorities may cause single point failure in identifier and certification management
- Silo-like application paradigm lacks interoperability and portability.

Decentralized identifier (DID) is a new type of identifier that enables verifiable, decentralized digital identity

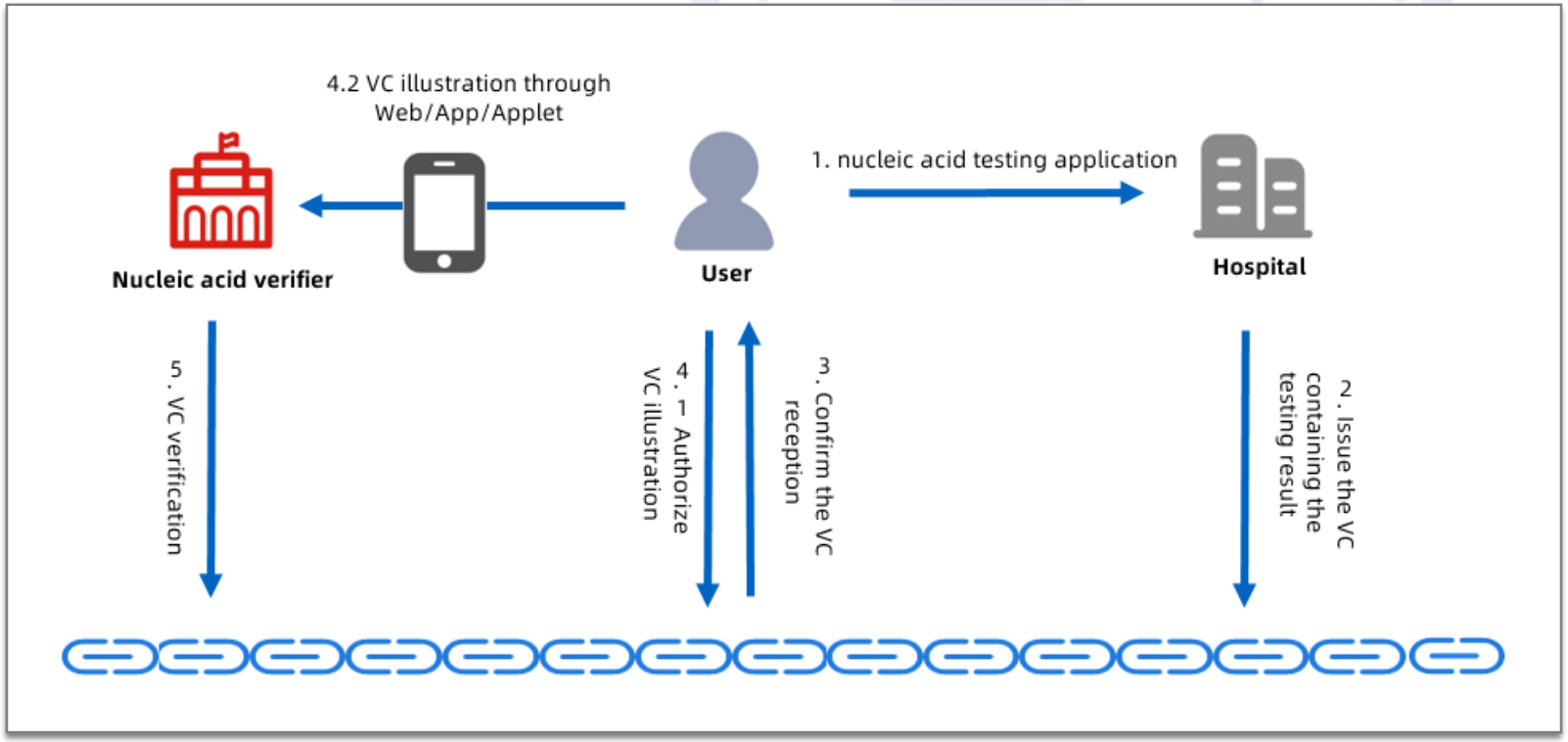
- A DID refers to any subject, e.g., a person, organization, thing, data model, abstract entity, etc

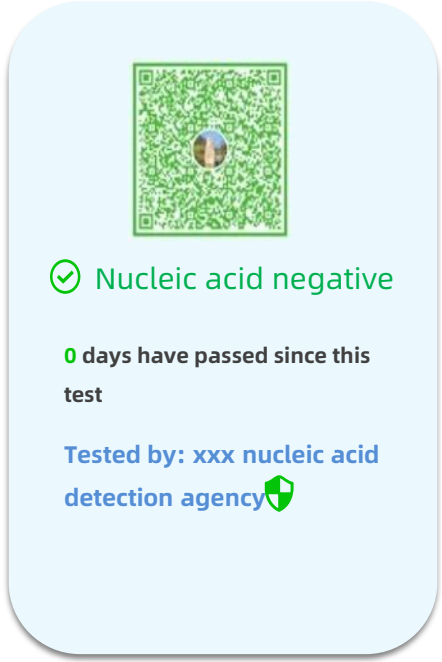


DID application in the COVID-19 nucleic acid test certification

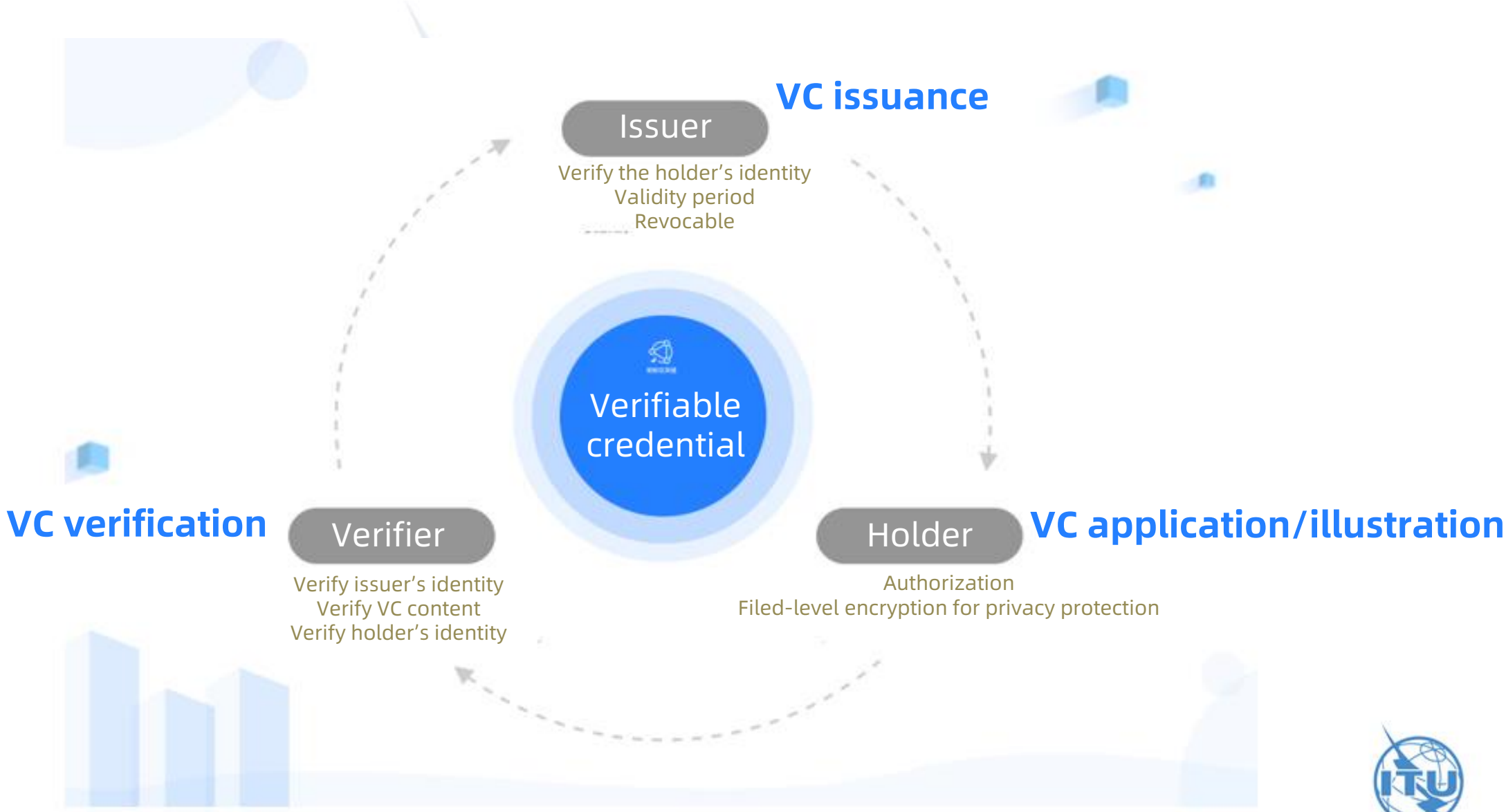
The testing result is one attribute under the DID holder:

- The utilization of attribute should be authorized by the DID holder
- Operation of attribute is archived on the blockchain





The basic model of DID



DID registration on the blockchain

DID subject

Private key owner

= did:mychain:0cfc0d755fd39926a97e8...

DID Management

DID creation | DID verification | DID updating

DID document

A set of properties
describe the DID subject

Property	Required?	Value constraints
id	yes	A string that conforms to the rules in § 3.1 DID Syntax.
alsoKnownAs	no	A set of strings that conform to the rules of [RFC3986] for URIs.
controller	no	A string or a set of strings that conform to the rules in § 3.1 DID Syntax.
verificationMethod	no	A set of Verification Method maps that conform to the rules in § Verification Method properties.
authentication	no	A set of either Verification Method maps that conform to the rules in § Verification Method properties) or strings that conform to the rules in § 3.2 DID URL Syntax.
assertionMethod	no	
keyAgreement	no	
capabilityInvocation	no	
capabilityDelegation	no	
service	no	A set of Service Endpoint maps that conform to the rules in § Service properties.

VC operation on the blockchain

A verifiable credential can represent all of the same information that a physical credential represents.

- VC issuer/holder shall register DID
- VC verifier may not have DID

Third party can issue new VC to user

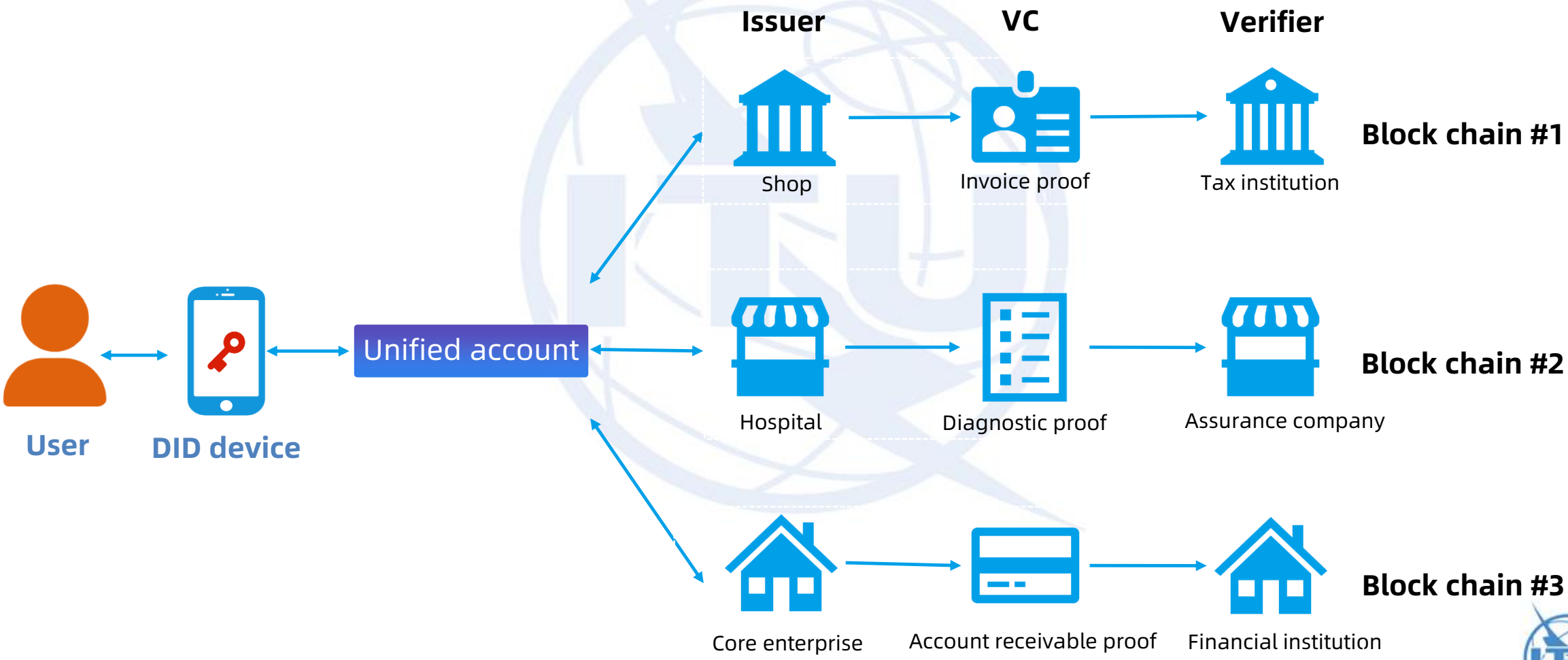
User can authorize other party to verify its VCs

VC Management

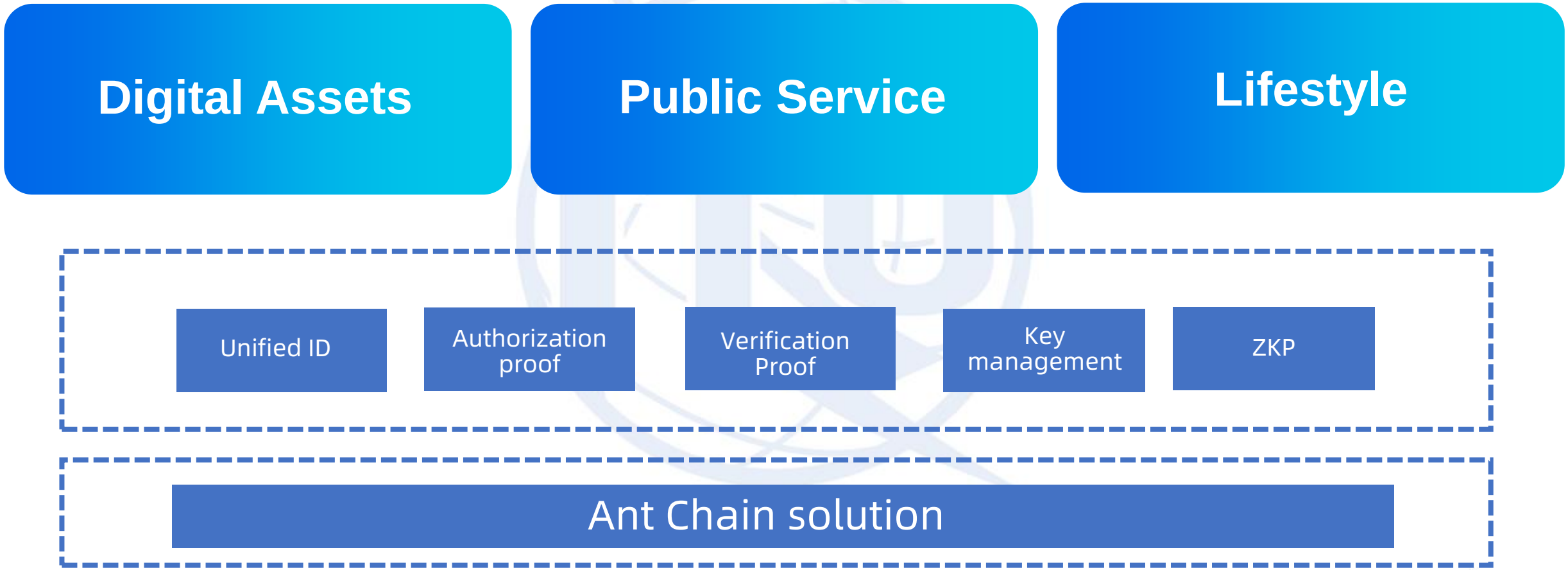
An example of Verifiable Certification


```
{
    "proof": {
        "type": "ecdsa",
        "verificationMethod": "did:mychain:0002:d3dcec27ccd014f69bd858042c172294ab00e53297f1e974803495143597837 7#keys-1",
        "signatureValue": "KZ5QXStw4r+leTPoI9GTk7niuPjMg3whu/CnahdxXCALV9mgZnlxqnb8rKDN5D0PVR29ILDy1hWZ\r\ntNwp++JSjAA=\r\n"
    },
    "content": {
        "issuanceDate": 1616566382052,
        "subject": "did:mychain:0002:9fea1497ba2dc3de8c0dfe4967be88ba9f648c03d3da806764098295bfc94279",
        "expire": -1,
        "claim": {
            "result": "negative",
            "itemName": "Nucleic acid detection",
            "orgName": "Hospital xx",
            "timestamp": 1615564800000
        },
        "id": "vc:mychain:0002:36d84299911e3077cdbc870b4ceec0403f3be326bb5b25e1c558f6a9d88fc4ba",
        "type": [
            "VerifiableCredential",
            "FETCH_DATA"
        ],
        "version": "0.7.0",
        "issuer": "did:mychain:0002:d3dcec27ccd014f69bd858042c172294ab00e53297f1e9748034951435978377",
        "status": {
            "id": "vc:mychain:0002:36d84299911e3077cdbc870b4ceec0403f3be326bb5b25e1c558f6a9d88fc4ba",
            "type": "BlockChainStatusList"
        }
    }
}
```

DID service


Issuer
VC
Verifier
Shop
Invoice proof
Tax institution
Block chain #1
User
DID device
Unified account
Hospital
Diagnostic proof
Assurance company
Block chain #2
Core enterprise
Account receivable proof
Financial institution
Block chain #3

DID system and its capabilities



Thank you!