Final demo

106070033 蘇子軒

Goal

Design a selective disclosure work flow which is able to :

1. issuer only sign once
2. selective disclosure to others
3. selective disclosures are limit to the specific user

Idea

the Certificate contains two part :

- Certificate : to prove the certificate content in Verify
- Verify : the content claim of certificate

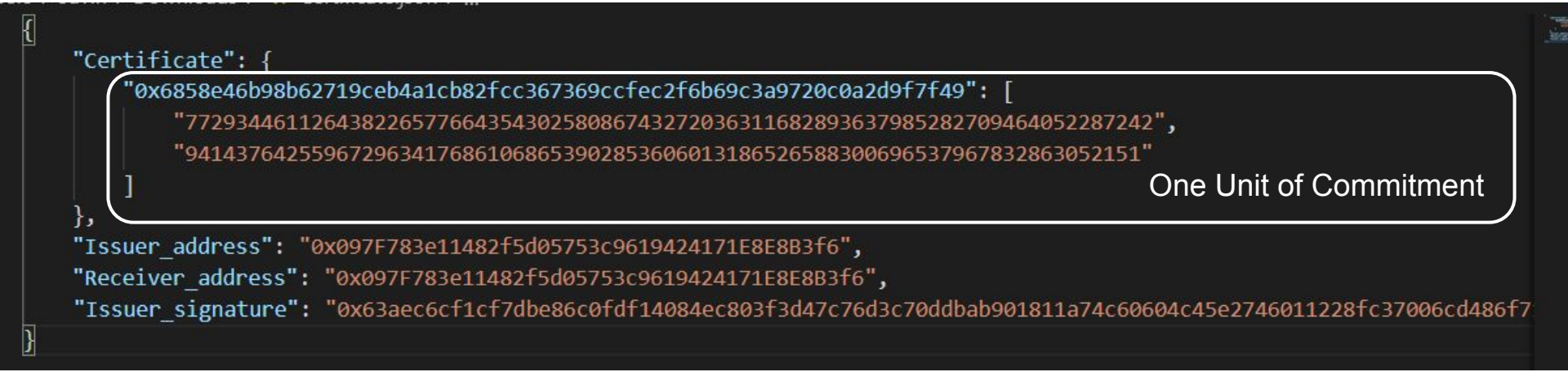
Verify - the content that owner claim


```
{
    "IPFSHash": "QmfPYiPqAHf3FfgQvxSAtcwKh8wLihEW9SC6NHpVJDfuBR",
    "VerifyList": [
        {
            "key": "title",
            "value": "XXX diploma",
            "random": "0xea7f48d56330fa6dbfecab8144389de4e872e91f8fa14cd7883820256d"
        },
        {
            "key": "issue date",
            "value": "2021/6/30",
            "random": "0x16ebe81603011cb209629a802f2f9639e4ba5213fe955b6bf105a02d77"
        },
```


<- Link to Certificate

One Unit of Data

Certificate - Data to prove the content we just claim

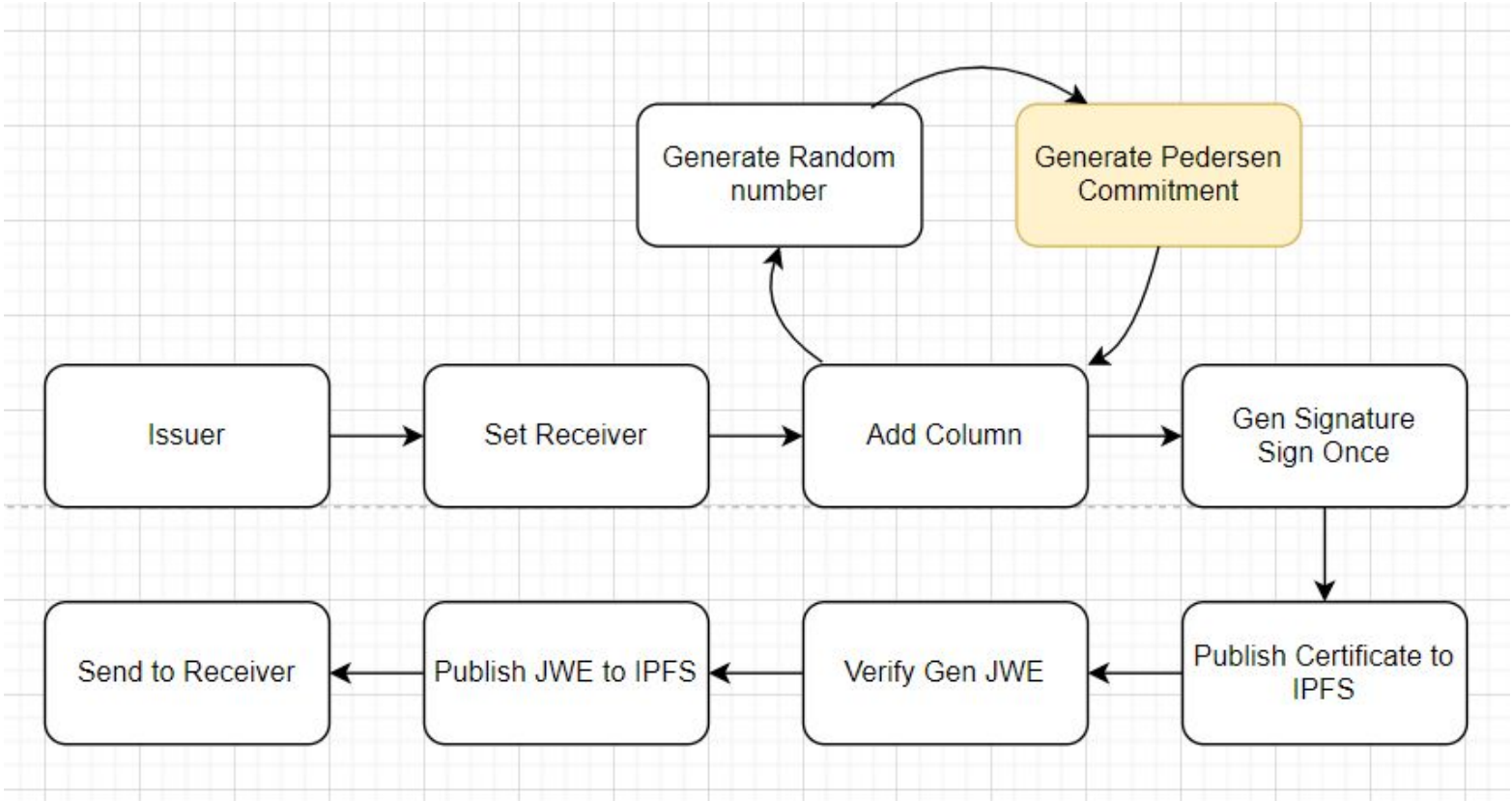


- Commitment = $(g^{v_i} h^{r_i})$
- Pedersen commitmenet is collision resistence
- The Signature will prove the Certificate contents are made by issuer

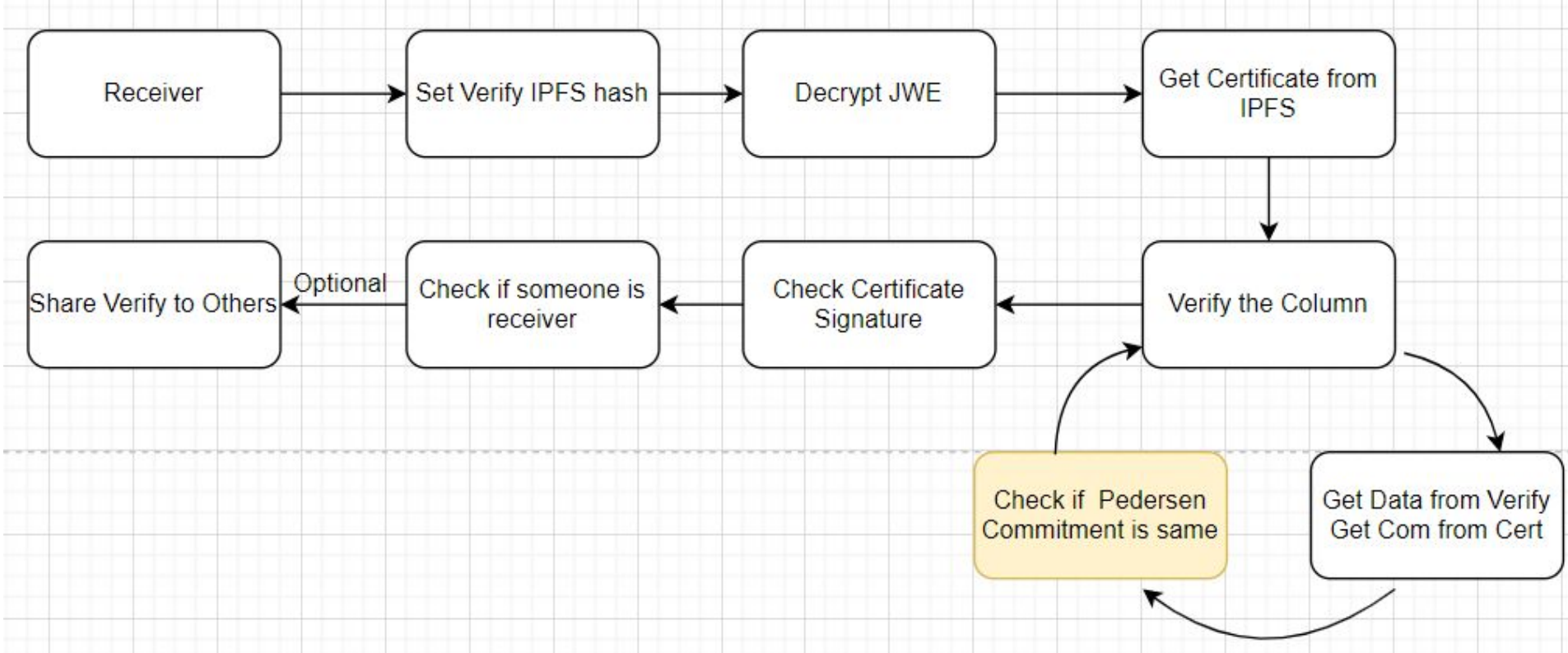
Verify points

1. Check if the Certificate signature is signed by issuer
2. Check if each unit of data is correspond to the Commitment
3. Check the owner of Verify file is same as Certificate receiver

Issue Certificate Work flow(Demo)



Verify Certificate Workflow(Demo)



JWE(Json Web Encryption)

- JWT : symmetric encryption of Verify
- decodeMessage : asymmetric encryption of JWT’s key using receiver’s PK


```
{
    "jwt": {
        "protected": "eyJhbGciOiJkaXIiLCJlbmMiOiJYQzIwUCJ9",
        "iv": "LOXx-Epa3gqkEiMv4ojVFuJkWNTASsqb",
        "ciphertext": "zCZbQ1_oxnIRnQ2CWCGpU2JANRfqw22orZ2ARf8VLXpioe3qrPzPtmbPxBfUhWEWGfHGg-Yrr4DQF
        "tag": "NHFpz8TWN1Aq7smOMiNZwA"
    },
    "decodeMessage": {
        "iv": "6fec99220a098f6ccf5ff67515cad2da",
        "ephemPublicKey": "04868723d77dfeea6f5467932a692fd4f0371acbdde16b071a5f22dfb3f13bacb7f37c534
        "ciphertext": "e0b9138bae6a18fabaf1086b6f6f4d394244ce7d521357a665785e6a8e2c2afa55c64aab0b55a
        "mac": "eb3dba551b4777928394d773f83bf1e65c24b6323ff5935d5f828885a5e0a729"
    }
}
```

Conclusion

Complete :

- a Certificate workflow with verifiable and sharing property
- the sharing of certificate is limit to specific user

Issue :

- What should be the Key of the Certificate if don’t want to reveal the content Key
- Do not achieve minimum data disclosure as ZKP does

QA