GNOMON: DECENTRALIZED IDENTIFIERS FOR SECURING 5G IOT DEVICE REGISTRATION AND SOFTWARE UPDATE

Rafael Ansay, James Kempf, Oleg Berzin, Chen Xi, Imam Sheikh

Equinix
PUBLIC KEY INFRASTRUCTURE (PKI): DEVICE REGISTRATION

- PKI is the de-facto standard for securing IoT Device connectivity to Cloud

2020

IoT Device uses client certificate to authenticate itself to an IoT Service

Device Credential

Devices with certificates signed by device manufacturers CA register to Cloud IoT Service
PUBLIC KEY INFRASTRUCTURE (PKI): SOFTWARE UPDATE

- PKI is the de-facto standard for securing IoT Device software update

IoT Device uses software publisher certificate to verify the signature on the software distribution

Software Publishers with a software publisher certificate signed by a Certificate Authority
PROBLEMS WITH CERTIFICATES FOR IOT

- Certificates expire
  - If they are not renewed in a timely fashion, the device may become unusable

- False positive revocation
  - The CA may put the certificate on the revocation list due to a misinterpretation of attack data

- Scalability
  - PKI was not designed for billions of devices

- Deployment complexity
  - Deploying a CA is too complex for consumers and many businesses
Decentralized PKI: Decentralized Identifiers

- Decentralized Identifiers
  - A permanent (persistent identifier) – never needs to change
  - Resolvable – look it up to get metadata
  - Cryptographically verifiable – prove ownership using crypto
  - Decentralized – no centralized registration authority is required

DID: did:example:123456789abcdefghijk

Built on Blockchain!
DIDS AND DID DOCUMENTS

- **DID document**
  - Provides cryptographic keying and cryptosystem information allowing the DID to be verified.
  - Links to additional services also provided.
    - Example: location of Identity Hub.

- **DID documents are stored in Identity Hubs.**

- **Universal resolver resolves DIDs to DID documents.**

```json
{
    "@context": "https://w3id.org/did/v1",
    "id": "did:example:123456789abcdefg4",,
    "publicKey": [{
        "id": "did:example:123456789abcdefg4#keys-1",
        "type": "RsaSigningKey2018",
        "owner": "did:example:123456789abcdefg4",
        "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\n"
    }],
    "authentication": [
        {"type": "RsaSignatureAuthentication2018",
        "publicKey": "did:example:123456789abcdefg4#keys-1"
        }],
    "service": [{"type": "IdentityHub",
        "serviceEndpoint": "https://id-hub.example.com/gnomon/8377464"
    }]
}
```
DID METHODS: MICROSOFT ION

- DIDs are formed and managed according to methods
- ION (Identity Overlay Network) forms a "Layer 2" blockchain network
  - Runs on top of the Bitcoin and IPFS
- Can scale up to 10k transactions per sec
- Open source
Verifiable credentials allow cryptographically attestable statements to be made about identities established using DIDs.

Software publishers publish a VC to the Identity Hub for new distributions under the software image DID.

IoT devices running that image are informed about the updates.

They download the update and verify the signature against the signature in the VC.

A certificate for software distributions!
SOFTWARE DISTRIBUTION REGISTRATION AND SOFTWARE UPDATE FLOW
GNOMON OPEN SOURCE GIT REPO

- **Open source code:** [https://github.com/cidd04/ionic/tree/master/ionic-iot](https://github.com/cidd04/ionic/tree/master/ionic-iot)

- **Created the Ionic SDK - A small and efficient library for digital identities on top of the ION Network** [https://github.com/cidd04/ionic/tree/master/ionic-lib](https://github.com/cidd04/ionic/tree/master/ionic-lib)

- **Screen shot of Gnomon in operation**

```bash
root@593033b399a0:/decentralized-identifiers/ionic-iot/lib# ./ionic.sh upgrade-software
Software Upgrade start.
Authentication Successful. This device is authorized to access the Hub
Latest Version is 2.0.0
Current Version is 1.0.0
Software Update is available
Downloading latest software from: https://file-examples.com/wp-content/uploads/2017/02/zip_SMB.zip ...
Download Successful.
Verifying signature...
Image Signature: 335b281804b34184aa10a9edf164664d6523b45a8e43e71991d4a8620f59276b6419ce8495bcc57776204e8eb770de01e3f25152c53e1409a87024152bb7e9e
Public Key Hex: 032b655152a85fb043c61b5202a02f17f039f018146f7e64b596c498cb1d849
Type: Ed25519KoblitzSignature2016
Verifying successful.
Software is OK and is ready for installation
root@593033b399a0:/decentralized-identifiers/ionic-iot/lib# 
```
CONCLUSION

- Decentralized Identifiers hold great promise for addressing the security issues with IoT
- Gnomon addresses trust and scalability issues for software update with decentralized identifiers and verifiable credentials
- Gnomon solves certificate expiration and certificate revocation issues thru DIDs and Verifiable Credentials
- Strong alternative to current PKI
ACKNOWLEDGEMENTS

Slide 3 - zip PNG Designed By IYIKON from Pngtree.com