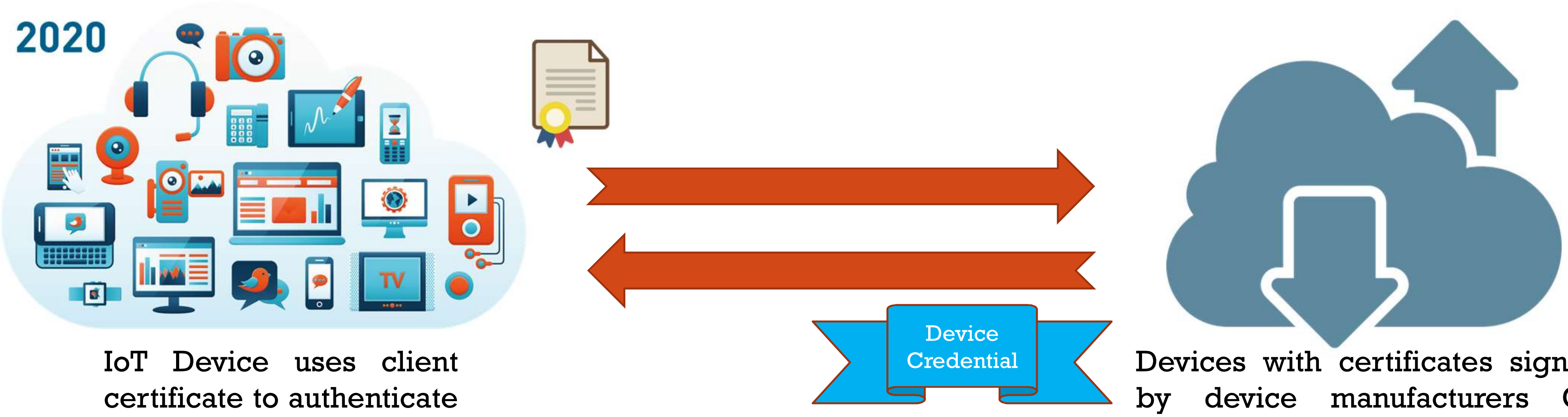
GNOMON: DECENTRALIZED IDENTIFIERS FOR SECURING 5G IOT DEVICE REGISTRATION AND SOFTWARE UPDATE

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



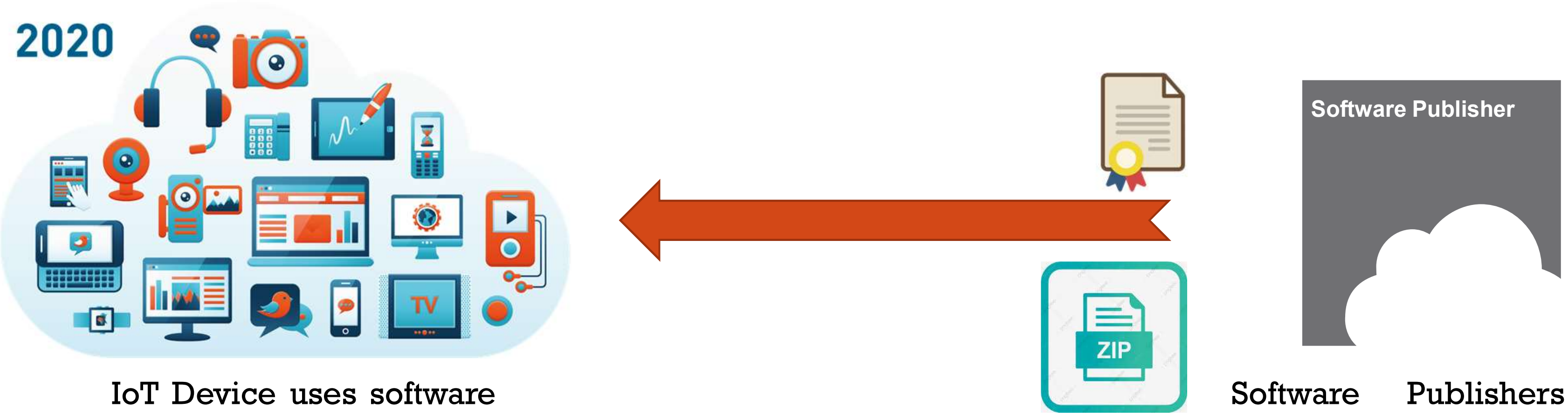
Device Credential

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

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



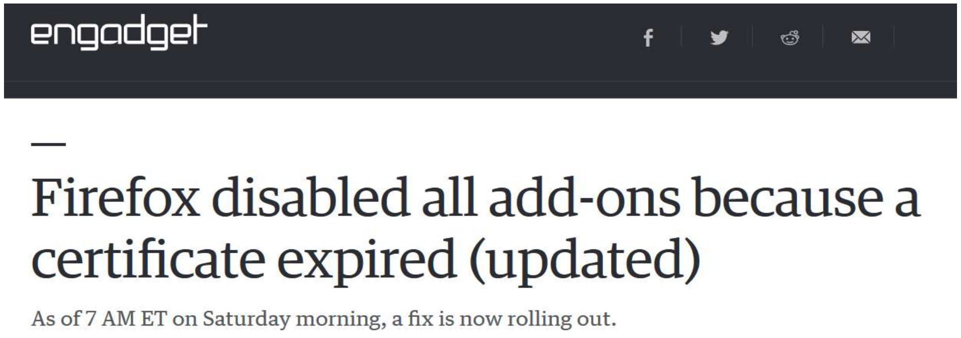
IoT Device uses software publisher certificate to verify the signature on the software distribution

Signed Software Distribution

Software Publishers with a software publisher certificate signed by a Certificate Authority

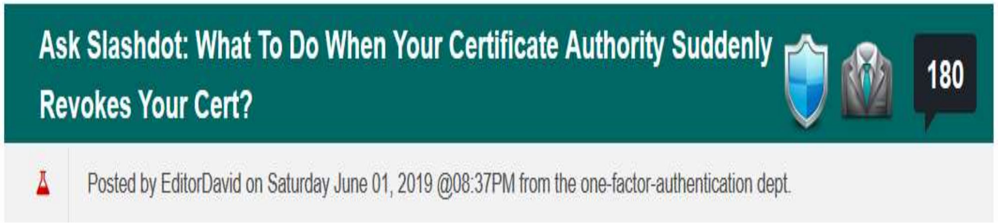
PROBLEMS WITH CERTIFICATES FOR IOT

- 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



Firefox disabled all add-ons because a certificate expired (updated)

As of 7 AM ET on Saturday morning, a fix is now rolling out.



Ask Slashdot: What To Do When Your Certificate Authority Suddenly Revokes Your Cert?

Posted by EditorDavid on Saturday June 01, 2019 @08:37PM from the one-factor-authentication dept.

DECENTRALIZED PKI: DECENTRALIZED IDENTIFIERS

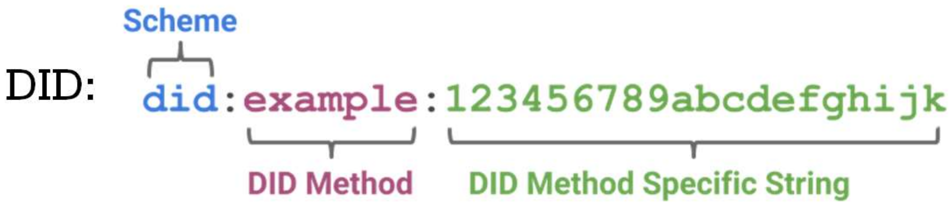
- Decentralized Identifiers

  - **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

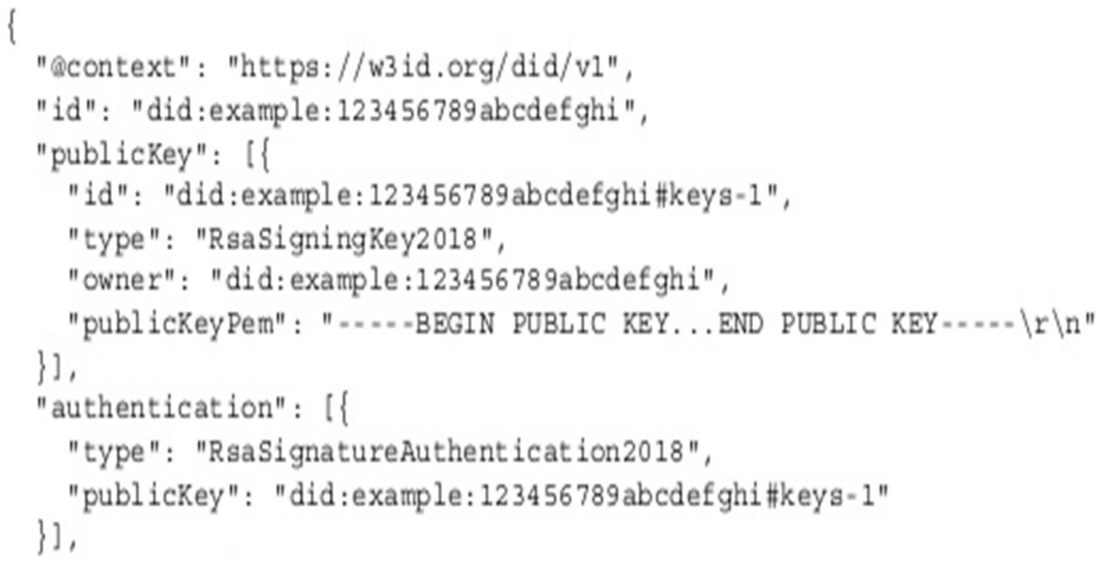


DID: did:example:123456789abcdefghijk

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.

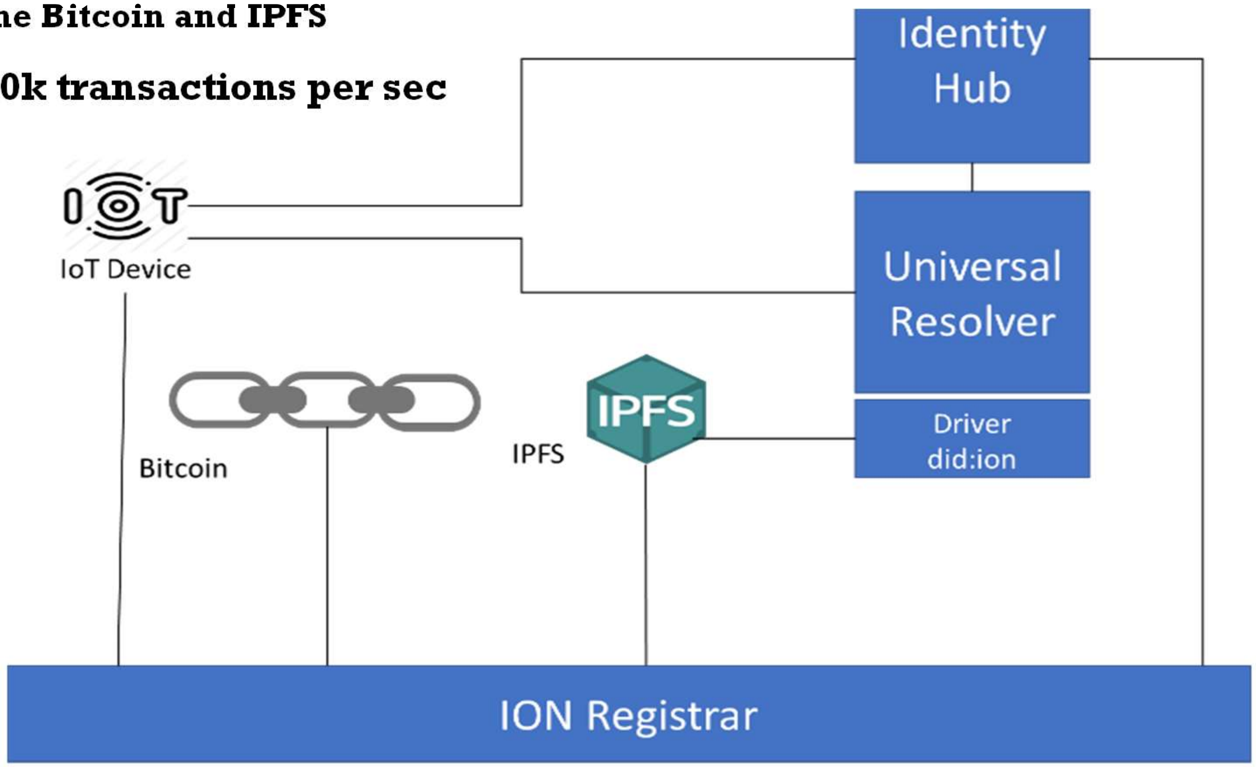


```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaSigningKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "authentication": [{
    "type": "RsaSignatureAuthentication2018",
    "publicKey": "did:example:123456789abcdefghi#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



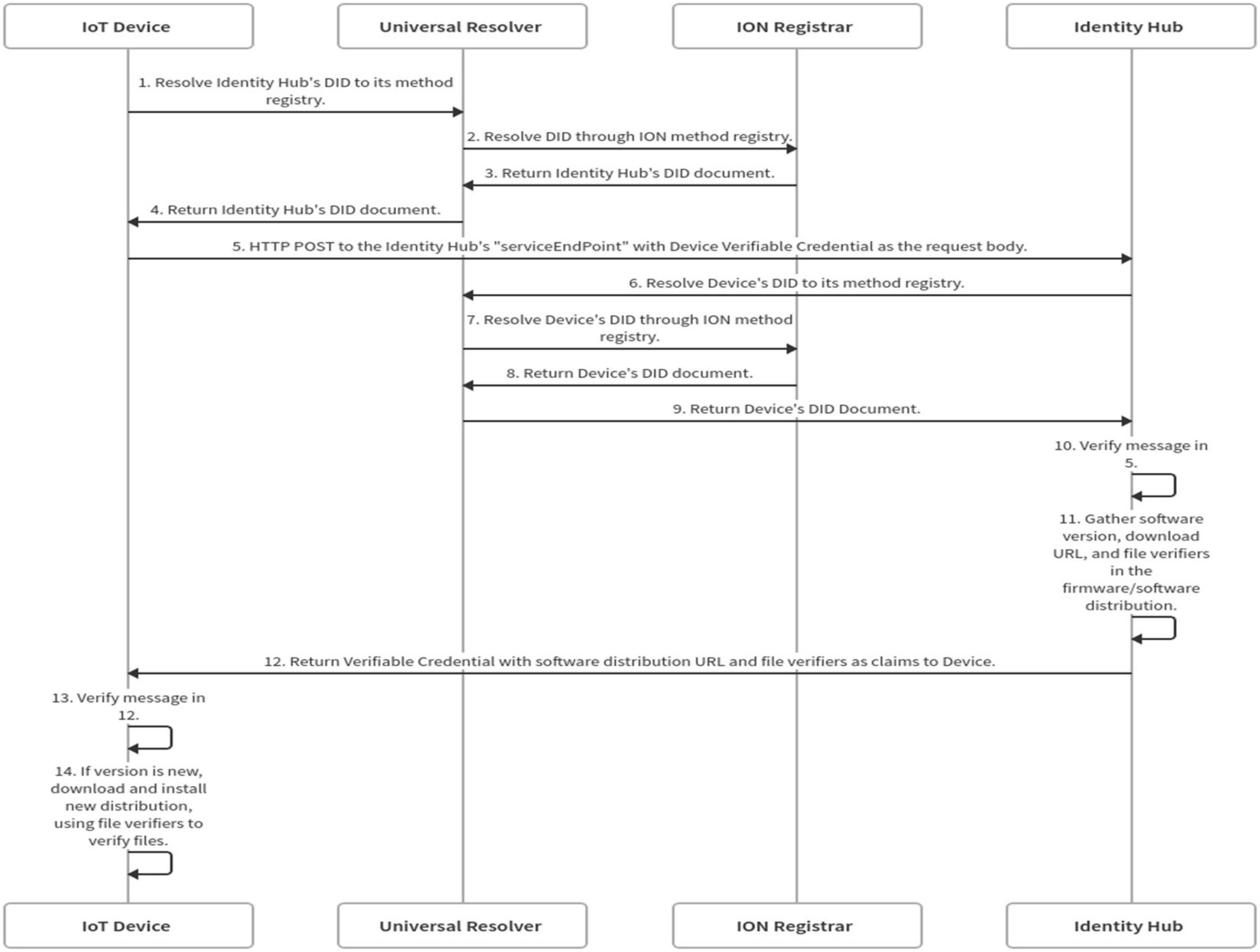
VERIFIABLE CREDENTIALS FOR SOFTWARE UPDATE

- **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.**

```
"credentialSubject": {
  "version": "2.0.0"
  "imageUrl":
    "https://examples.com/
      files/update2.0.0.img",
  "imageSignature": '335…e9e"
  "type":
     "EcdsaKoblitzSignature2016",
  "publicKeyHex": "032…849"
}
```

A certificate for software distributions!

SOFTWARE DISTRIBUTION REGISTRATION AND SOFTWARE UPDATE FLOW



IoT Device

Universal Resolver

ION Registrar

Identity Hub

1. Resolve Identity Hub's DID to its method registry.

2. Resolve DID through ION method registry.

3. Return Identity Hub's DID document.

4. Return Identity Hub's DID document.

5. HTTP POST to the Identity Hub's "serviceEndPoint" with Device Verifiable Credential as the request body.

6. Resolve Device's DID to its method registry.

7. Resolve Device's DID through ION method registry.

8. Return Device's DID document.

9. Return Device's DID Document.

10. Verify message in 5.

11. Gather software version, download URL, and file verifiers in the firmware/software distribution.

12. Return Verifiable Credential with software distribution URL and file verifiers as claims to Device.

13. Verify message in 12.

14. If version is new, download and install new distribution, using file verifiers to verify files.

IoT Device

Universal Resolver

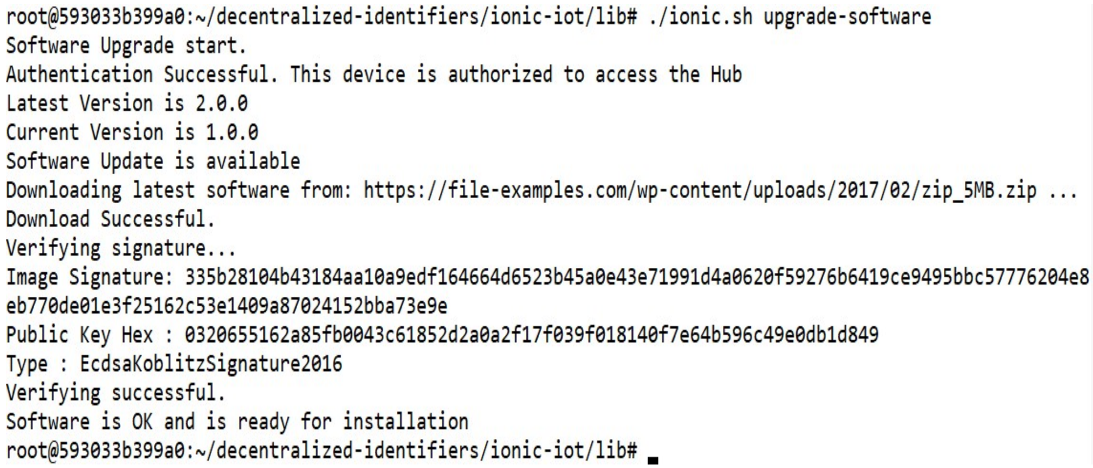
ION Registrar

Identity Hub

POWERED BY swimlanes.io

GNOMON OPEN SOURCE GIT REPO

- **Open source code: 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**
- **Screen shot of Gnomon in operation**



```
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_5MB.zip ...
Download Successful.
Verifying signature...
Image Signature: 335b28104b43184aa10a9edf164664d6523b45a0e43e71991d4a0620f59276b6419ce9495bbc57776204e8
eb770de01e3f25162c53e1409a87024152bba73e9e
Public Key Hex : 0320655162a85fb0043c61852d2a0a2f17f039f018140f7e64b596c49e0db1d849
Type : EcdsaKoblitzSignature2016
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