

Web-of-Things Framework Security

<https://github.com/w3c/web-of-things-framework>

Web-of-Things Framework at Github

- Web-of-Things Framework is a project started by W3C
- <https://github.com/w3c/web-of-things-framework>
- Provides software developers with a ready to use Internet of things system
- Experimental code and iterative development

Reach out to the industry and experts

- To make sure the security implementation does make sense, it uses standards and terms of quality it is up to standards
- Get guidelines, peer review and perhaps development input or any type of help from this expert group to make sure we are on the right track at the Web-of-Things Framework

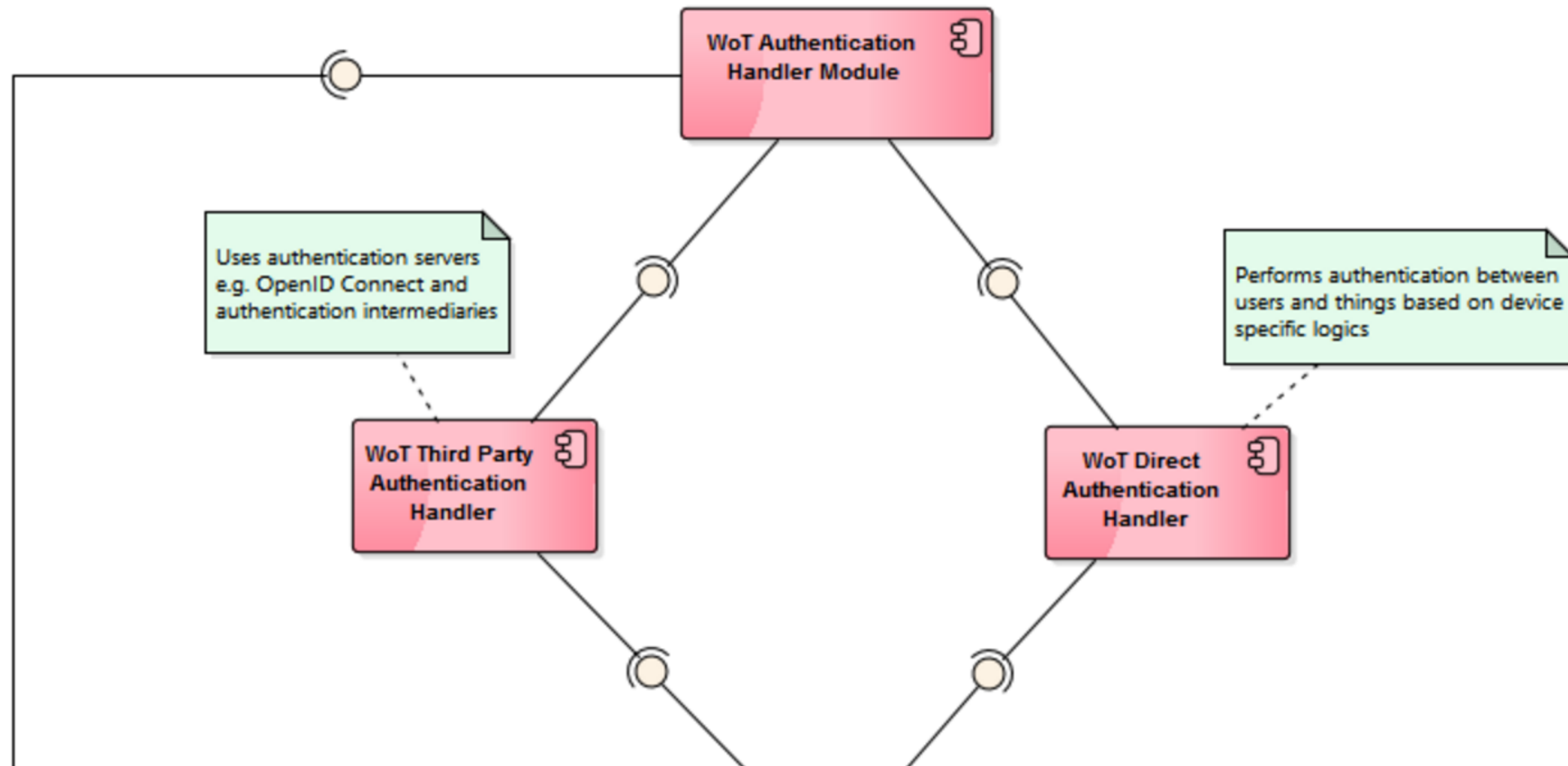
Architecture

- Encapsulates low level machine to machine and human to machine communication as well as security implementation details in the framework
- JSON-LD
- The thing description language (TDL) declares the metadata, events, properties and actions.
- Loosely coupled architecture and event driven design
- Thing module to handle devices, devices' events, properties and actions
- Transport modules: REST HTTP, Web socket, CoAP and P2P

Security

- Document started at <https://github.com/w3c/web-of-things-framework/blob/master/security.md>
- Authentication
- Access control
- Data integrity
- Device provisioning and secure upgrade
- Managing cryptography keys (ARM Trust Zone)

wot_security_component



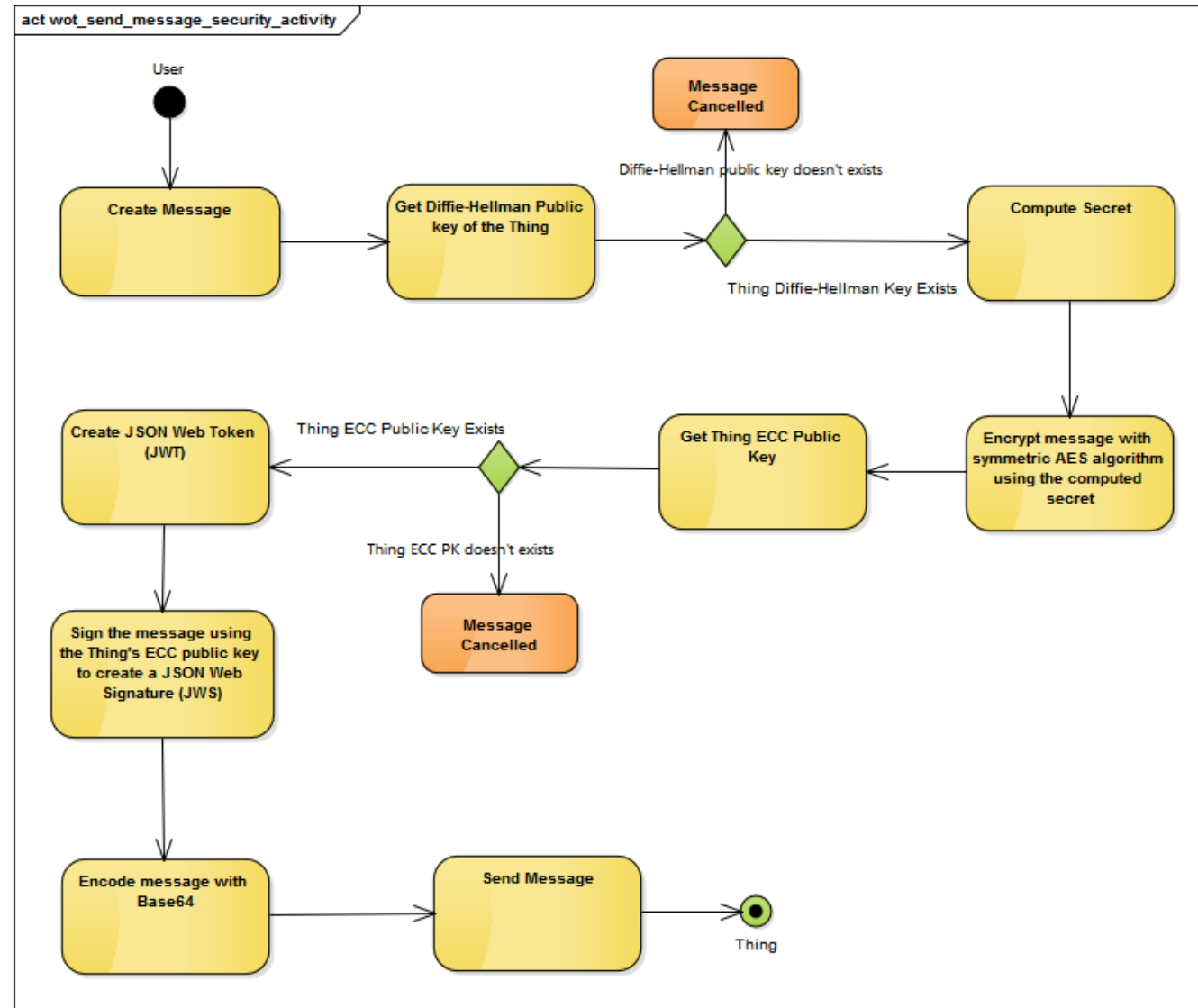
Framework specific authentication

- WoT Direct Authentication handler to implement WoT specific authentication mechanism i.e. not using third party authentication servers
- Use ECC
- Things and human users use public/private key (PPK) infrastructure and PPK cryptography functions to secure messages
- Each actors of the system must generate a public/private key pair. (Typically keys generated prior to configuring the device and will be burned into the devices' firmware).
- The Thing/user publishes the public key to other users of the system.
- The data integrity and authenticity of the messages is guaranteed with PPK signatures
- All messages between users are secured with AES 128 and AES 256 symmetric encryption/decryption.
- The system uses Diffie Hellman key exchange algorithms to facilitate the exchange and security of session keys.

Uses standards

- The Web of Things security uses existing open standards.
- The open standard security token format JSON Web Token (JWT)
- The encrypted content open standard JSON Web Encryption (JWE)
- The JSON Web Algorithms (JWA) open standard specification that registers cryptographic algorithms and identifiers
- The JSON Web Signature (JWS) open standard that represents content secured with digital signatures or Message Authentication Codes (MACs) using JSON-based data structures will be utilized in Web of Things security.
- Currently the JWT, JWS and JWE modules are implemented

Message handling sample



Questions to the group

- What about RSA on low power IoT devices, should be that in scope?
- What about Telehash?
- What about quantum cryptography?
- Contact: tibor@zovolt.com