Security WG Meeting, 5/22/19

Attendees: . Others may have joined after the meeting started and attendance was captured.

Agenda

Old Business

- Edinburgh Update
    - Moving service access to Vault to a Dot release. Issues in getting it done for this release.
    - Plan of work
        - c.1. Moving the secret service client library from edgexfoundry-holding are to edgexfoundry organization in GitHub.
            - With DevOps, get CI/CD setup
        - c.2. Apply the secret service client to coredata service for POC.
        - c.3. Retry logic update within the coredata service to adopt the new secret client.
        - c.4. Add security command line option within coredata service and update the retry logic.
        - c.5. Integration testing with secret service.
        - c.6. Apply the approach to other microservices (command, metadata, notifications, logging, export client, etc.)
        -
        - s.1. Update secret store and API-gateway structure to be consistent with EdgeX core projects.
        - s.2. Add unit testing cases for secret service.
        - s.3. Update docker compose file for developer script
        - s.4. Add testing cases and docker compose file in black box testing
    - Schedule
        - Dot release at the end of July/first part of August
- Fuji work (as a result of F2F meetings in Seoul)
    - In
        - Generation of PKI
            - Distribution of per service Vault secrets
        - HW secure storage abstraction layer (design only)
            - How to protect the Vault Master Key
        - Ensuring the services running are those expected (and authorized)
        - Renew/refresh threat assessment
        - Need document defining what security is/does and can/will do
    - Out
        - Service to service security
            - Implementation of service-to-service communications
        - Securely providing service updates
        - How to securely provision new devices/sensor
        - Device identification and authentication/authorization
        - Hyperledger/blockchain/digital ledger integration

        - Protect data at rest
            - In DB like Mongo
            - In log files
        - Privacy concerns (HIP-A, GDRP, …)

New Business

- any