Core Working Group Meeting Notes (15-Aug-2019)

Attendees:

Old Business

- Security-proxy-setup (formerly security-api-gateway)
  - Initial PR #1627 has been merged
  - Series of follow up issues from PR comments have been created, working through that.
- Go-mod-secrets
  - Anthony B. from Dell has been working on this per decisions in last week's Core WG
    - Add TLS Transport (for comms with Vault)
    - Removal of Set/Delete capabilities

New Business

- Integrating Security Services w/Core Services
  - Granularity of feature enablement versus global
  - Proposal to work toward Fuji without constraints based on Edinburgh
    - Differences will be documented in release notes
  - How to inform services of enabled features?
    - Environment variable
      - Example: DISABLE_USE_SECRET_STORE (or USE_SECRET_STORE=true?)
      - *DISABLE_USE_SECRET_STORE will be used, secret store integration will always be "ON" unless this var is present. We don't really care about the value, it's the presence that matters but we should still set a "true" value*
      - Can currently be used to override configuration within config-seed
        - Example variable format – edgex-core-data_Clients_Logging_Host
        - Proposed name based on existing convention
          - edgex-core-data_Security_Secret_Store=true
    - Configuration
      - *Discussed the possibility of a global configuration applicable to all services in the platform (edgex/security in Consul for example)*
        - *In this case, there would be a global setting for each bullet below.*

- o *Edgex_security_secret_store=true/false ***
    - ▪ *Utilize this even in the case where Consul is not running*
  - o *In each individual service*
    - ▪ *Location of Vault token could be different*
    - ▪ *Remote versus FS versus BLOB in the TOML*
- Proposed new [Security] section in the TOML
- Sub-items align to granular features within the realm of Security
  - o Secret store – enabled, yes or no
    - ▪ *Details related to Vault token location (File system)*
    - ▪ *Or even the content of the token in config*
  - o Kong
    - ▪ *Services themselves have no knowledge of this currently (for Fuji)*
  - o TLS
    - ▪ *Services themselves have no knowledge of this currently (for Fuji)*
  - o Authentication / Authorization
    - ▪ *Services themselves have no knowledge of this currently (for Fuji)*
  - *Within each sub-items, there could also be additional sections (to be fleshed out)*
- ▪ Cmd line
  - *We didn't discuss this at all so we're not considering using these at all in this scenario*
- ▪ Questions
  - Do we support all three?
  - Order of precedence?
  - What if they're in conflict?
- Any new business?