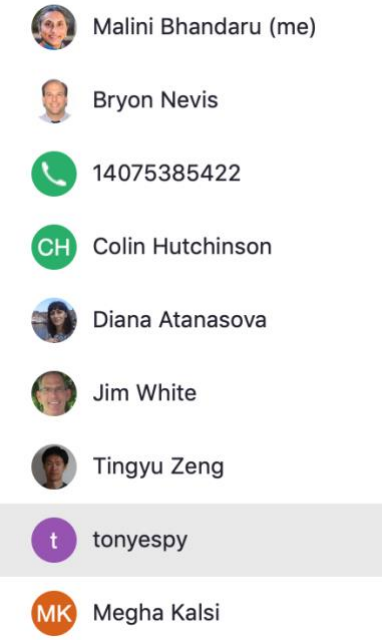
EdgeX Security WG Meeting 04/15/2020



- Agenda
- Inconsistent configuration settings across the various microservices - Tony & Bryon
- Security Vulnerabilities: Snyk Reports - & Community Bridge
- Hardware Root of Trust abstraction -- Bryon & Jim White
- shared with ARM - response awaited
- Device Service - secure communication cross hosts - Bryon
- Future of SNI (Service Naming Indicator) - Tingyu
- Follow-up items
    - Is Redis Secure? -- Good progress by Andre and reviews by Bryon
    - EdgeX-UI: hardcoded passwords - No update
    - Hanoi security feature https://docs.google.com/document/d/1FS2C_r1xmAMj9AePtRCvUklYRdOKL_TjrO-CX466MZU/edit?usp=sharing

SIR

No new high issues. Linux Community Bridge is reporting out on issues. These do not reflect our latest and greates. James Gregg has helped the COmmunity Bridge effort.

Configuration inconsistencies

Tony -- perfect storm -- after config seed removed

Cert paths inconsistent, CA versus caas prefix. So the SecretService vs. SecretStore difference was explained by @bnevis-i, thanks.

Regarding the config keys used for the root CA file path, @tingyuz said we couldn't fix this because it would break compatibility:

> Some use CaFilePath (security-secretstore-setup), some use CACertPath (security-proxy-setup),

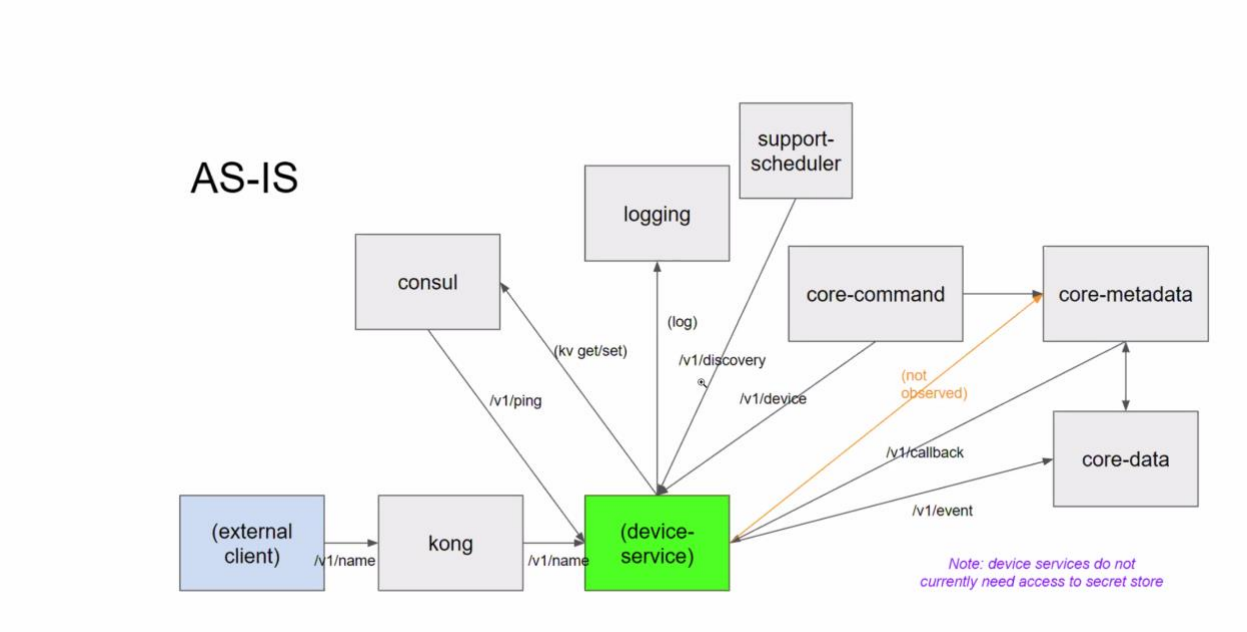
I questioned the statement that this would break compatibility because we made some other changes to config keys as part of Geneva. In fact see the following commit 4ecacc7 where all of the keys under SecretService were changed from lowercase to CamelCase.

And finally, do we still need to copies of the rootCA certificate with different names per:

> I've always wondered why we have two identical root certificates, one named **ca.pem** and one named **EdgeXFoundryCA.pem** that get created?

Other aspects: Docker configuration files and non-docker
Clean-up task 1: Make security proxy and .. use the same path
(copy from the issue, third paragraph), root CA file path
Clean-up task 2: get rid of the copy of the certificate, called EdgeX …
Lower case to camel case?
The value of the key, lowercase/upper case
Add a comment to not confuse people going forward.

Securing Device Service communication



Service Naming Indicator (SNI) - Tingyu

https://github.com/edgexfoundry/edgex-go/issues/1539

Questions: What was the origin of this feature. Security feature, possibly David Feriera?
Jim White does not recall the motivation and most customers say security is a requirement but might not have details such as SNI.

Bryon: config file for proxy setup has ability to support SNI based requests, it has been supported by configuration.toml. But, when config seed was removed, it brought this feature back into focus and the question of how to support it.
Bryon thinks what has been implemented is half baked.

Tony had in the past mentioned to Tingyu leave whats there, no harm.
But it might be time to “deprecate”. Tingyu to follow up with Tony.

Kong Conference - Colin

Colin informs that there is a free Kong conference https://konghq.com/events/destination-decentralization/
Colin will update on Security channel if it will be available recorded.