ATM Software

XFS4IoT SP-Dev Workgroup

5th November 2024

Confidential

XFS4IoT SP-Dev Workgroup agenda

- Recap from previous meeting
- SP-Dev framework update
- TLS encryption and demo
- What’s next?
- Next meeting

Recap from previous meeting

Recap from previous meetings

- Post-break recap
  - Framework updates
  - Demos
  - Guest speakers
- SBS presentation
  - DK interface specification & certification overview
  - Changes and status of DK for XFS4IoT

Confidential. This document must not be copied or distributed without KAL’s written permission

ATM Software

SP-Dev Framework v2.4

Updates in SP-Dev Framework v2.4

- Corrected KeyManagement capabilities LoadCertificateSigner options to match XFS4IoT 2023-2 Specification

- Supported validating partial counts in CashDispenser.Dispense

- Corrected issue with VendorMode Inactive state on StatusChangedEvent

- Added Auxiliaries UPS status Good

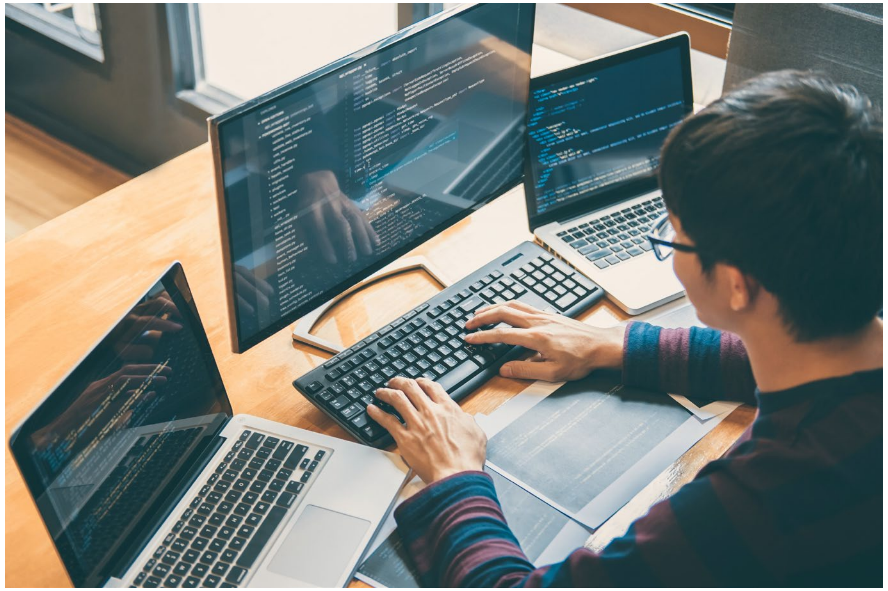
Updates in SP-Dev Framework v2.4

- Updated GetCashStorageConfiguration and GetCheckStorageConfiguration to allow the service to return null when storage is not detected

- Supported returning Chip ATR response on CardReader.ChipPower command
  - Added in XFS4IoT specification 2023-2

- Improved Denominate and Dispense commands performance with large amounts

Updates in SP-Dev Framework v2.4



- Added support for CheckUnit lights added in XFS4IoT 2023-2
- Added support for target position Reject for CashManangement.CalibrateCashUnit and CashDispenser.TestCashUnits
- Relaxed parameter checks for CardReader.Reset command
  - — Ignore application provided storage id when media is ejected, or no action is performed

Updates in SP-Dev Framework v2.4

- Corrected RetractArea handling for CashManagement.Retract command
- Updated KeyManagement command capabilities to include ExportRSADeviceSignedItem
- Corrected Camera status reporting to handle multiple camera from the same service correctly
- Updated Keyboard DataEntry, PinEntry and SecureKeyEntry commands to return KeyNotSupported error code

Updates in SP-Dev Framework v2.4

- Updated message header to include below fields
  - —Status for Acknowledgement messages
  - —CompletionCode for Completion messages
  - —ErrorDescription for Completion messages

Command header

2021-1 command header:

```
"header":
{
   "type": "command",
   "name": "Common.Status",
   "requestId": 12345,
}
```

2023-2 command header:

```
 "header":
{
   "type": "command",
   "name": "Common.Status",
   "version": “2.0",
   "requestId": 12345,
   "timeout": 1000
}
```

Completion header

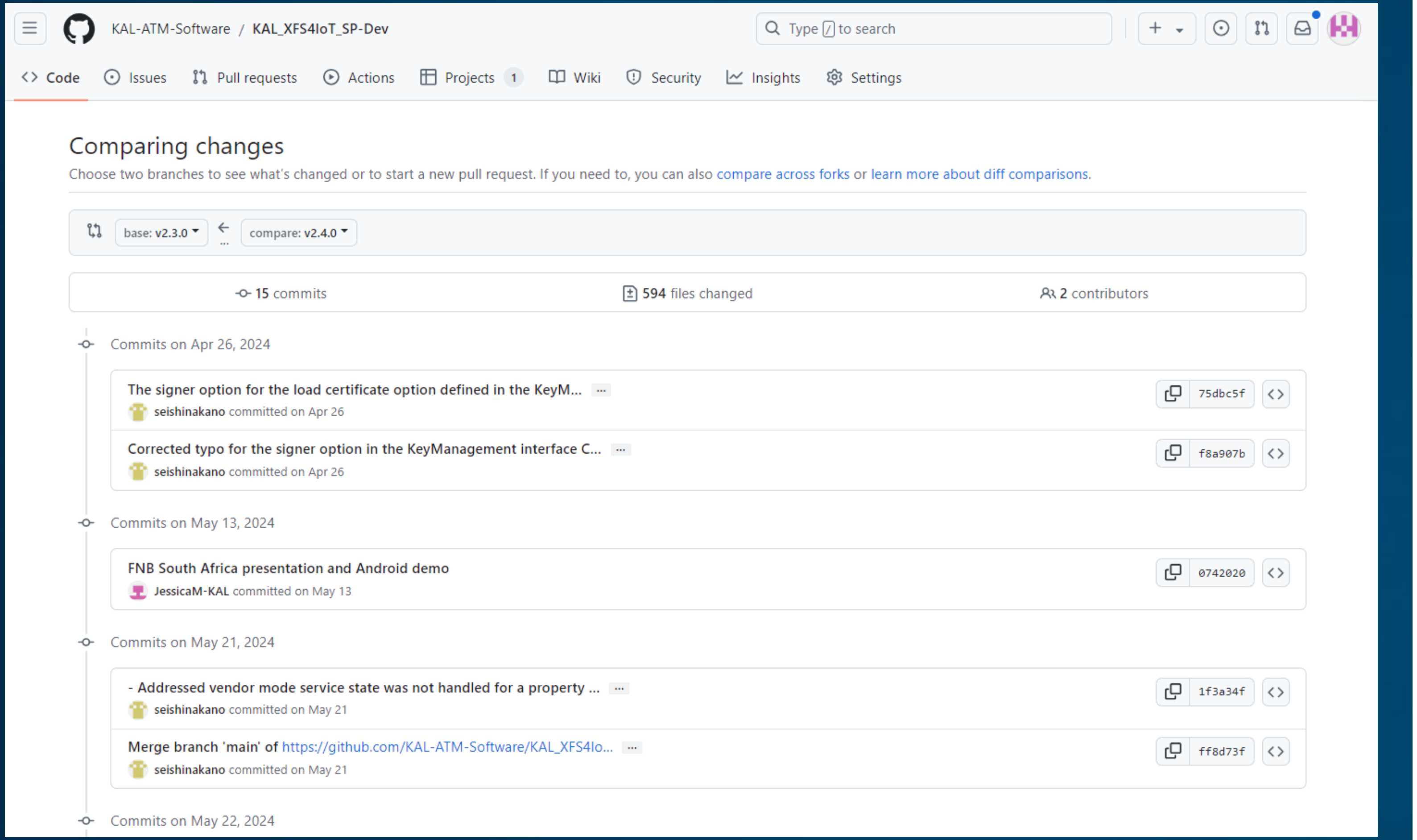
2021-1 completion header:

```
"header":
{
   "type": "completion",
   "name": "Common.Status",
   "requestId": 12345,
}
```

2023-2 completion header:

```
 "header":
{
   "type": "completion",
   "name": "Common.Status",
   "version": “2.0",
   "requestId": 12345,
   "completionCode": "fraudAttempt"
   "errorDescription": "Error text"
}
```

Comparing SP-Dev Framework versions



Comparing changes

Choose two branches to see what's changed or to start a new pull request. If you need to, you can also compare across forks or learn more about diff comparisons.

base: v2.3.0 ← compare: v2.4.0

15 commits | 594 files changed | 2 contributors

Commits on Apr 26, 2024

- The signer option for the load certificate option defined in the KeyM... — seishinakano committed on Apr 26 — 75dbc5f
- Corrected typo for the signer option in the KeyManagement interface C... — seishinakano committed on Apr 26 — f8a907b

Commits on May 13, 2024

- FNB South Africa presentation and Android demo — JessicaM-KAL committed on May 13 — 0742020

Commits on May 21, 2024

- - Addressed vendor mode service state was not handled for a property ... — seishinakano committed on May 21 — 1f3a34f
- Merge branch 'main' of https://github.com/KAL-ATM-Software/KAL_XFS4Io... — seishinakano committed on May 21 — ff8d73f

Commits on May 22, 2024

https://github.com/KAL-ATM-Software/KAL_XFS4IoT_SP-Dev/compare/v2.3.0...v2.4.0

- Changes on GitHub
- Compare between releases
- Shows all commits between package versions

Transport Layer Security (TLS)

What is Transport Layer Security (TLS)?

Network encryption at a low level

Ensures:

- Confidentiality - no one can steal data like PAN
- Integrity - No one can change messages, like dispense amounts
- Availability - solution must be practical, easy to implement, and work in relevant environments

Why is it import to XFS4IoT?

Critical assets vulnerable to attackers - Cash, customer data, PIN, PAN etc.

More vulnerable system - network connection compared to XFS3 local binary interface.

XFS4IoT does permit alternatives - physical security. i.e. connection is local to machine. Same security as XFS3.

How does TLS/Handshake work?

- Client and Server agree algorithms to use. The “Cipher Suite”
- Client and Server exchange random values, public information and certificates
- Client checks the Server certificate against CA
- (Server may check Client certificate, if mTLS is being used)
- Client and Server now share enough information to securely calculate a shared "Master Secret". Typically, with Diffie-Hellman
- This is used to derive all working keys, typically for AES

Issues and improvements

- Currently works on Windows and Linux, but not yet on Android

- The device is the TLS server and needs a certificate
- The connection goes from the client/Data center to the server/hardware
  - For both, it would be better if the connection went from the hardware to the Data Center. XFS Committee is considering this

Demo: TLS on Windows

ATM Software

What's next?

Demos, POCs and guest speakers

- Framework updates and roadmap
- More guest speakers
- More demos

Next call

Zoom

- First Tuesday of each month at 1300 UK time for 30 mins

Next call: 3rd December 2024
1300 UK, 0800 US EST, 2200 Tokyo time

Calls are 30 mins long

We will continue to use Zoom

(Interpretation in Japanese, Chinese and Spanish is available using Zoom's interpretation feature)