ATM Software

XFS4IoT SP-Dev Workgroup

7 September 2021

Scope of the CEN XFS Committee

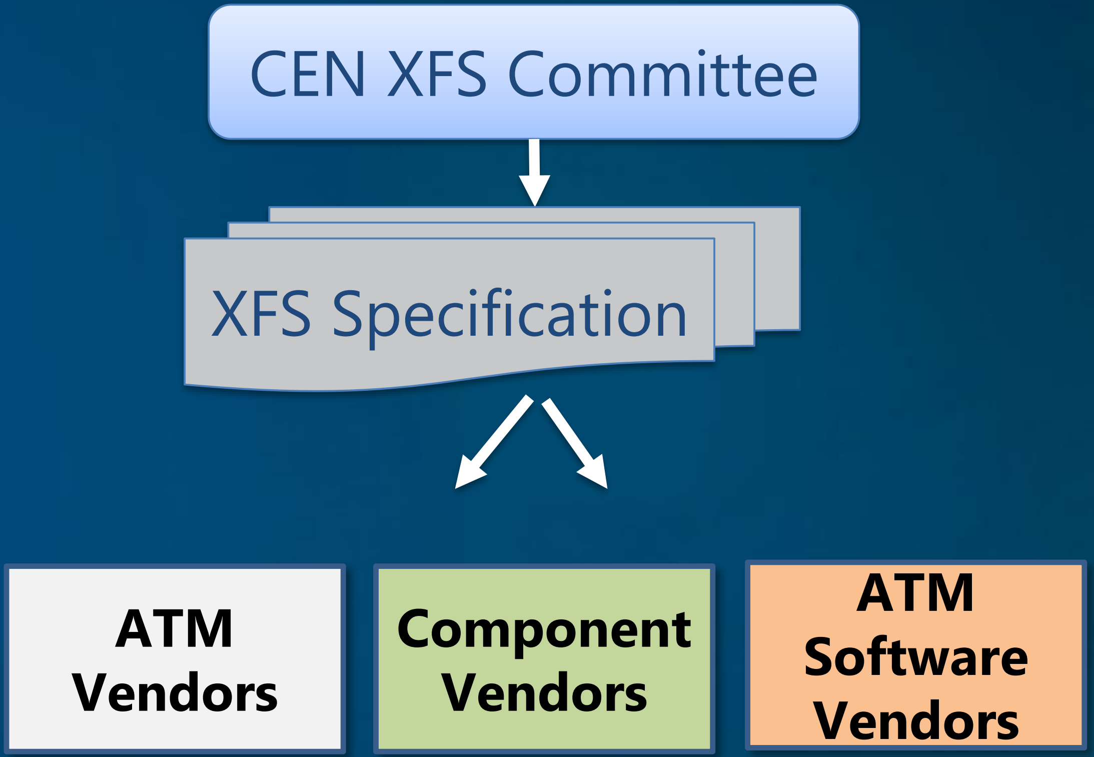
There have been several questions about the CEN committee

The CEN Committee:

- defines the XFS specification
- publishes the XFS specification

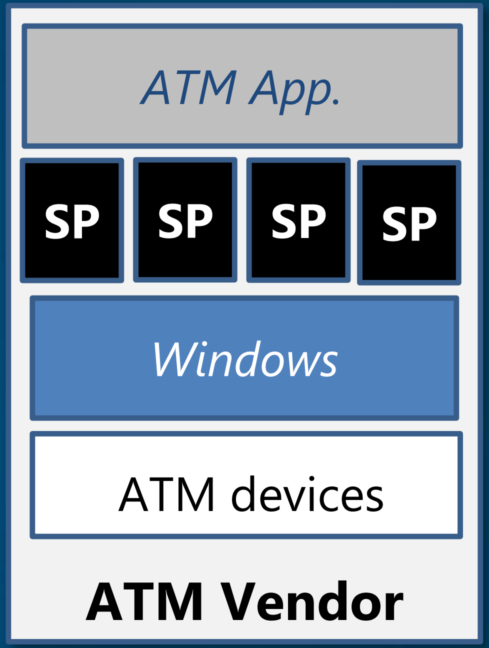
The CEN Committee does not:

- develop or test SPs
- publish implementation or testing specifications
- certify the XFS implementation from the vendors



KAL XFS4IoT SP-Dev Workgroup

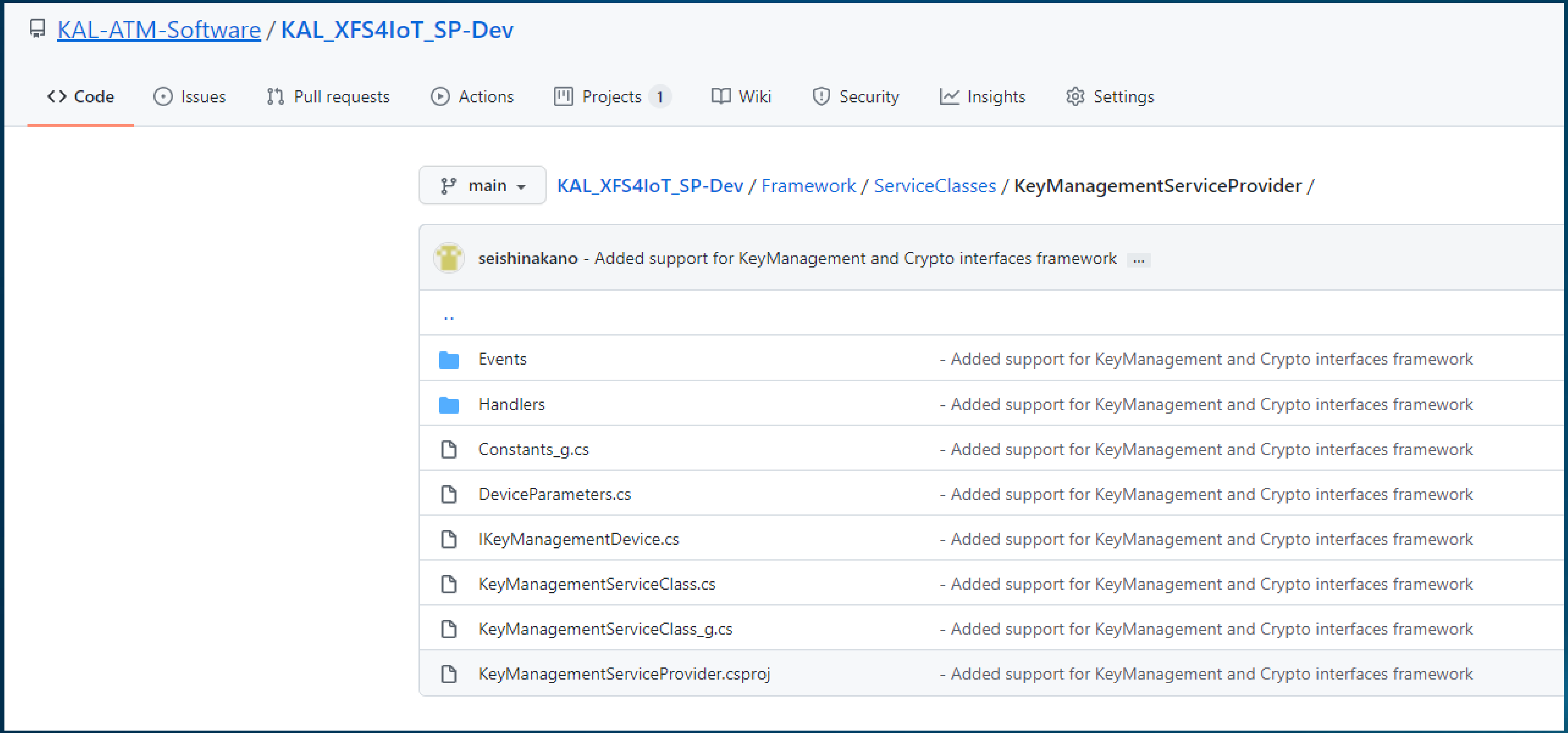
- SP-DEV workgroup helps create SPs
- Vendors can use the framework to create new SPs
- Vendors are responsible for development and testing of XFS for your system



Key Management and Crypto classes release

Key Management & Crypto support

— Key Management and Crypto classes now available



KAL-ATM-Software / KAL_XFS4IoT_SP-Dev

KAL_XFS4IoT_SP-Dev / Framework / ServiceClasses / KeyManagementServiceProvider /

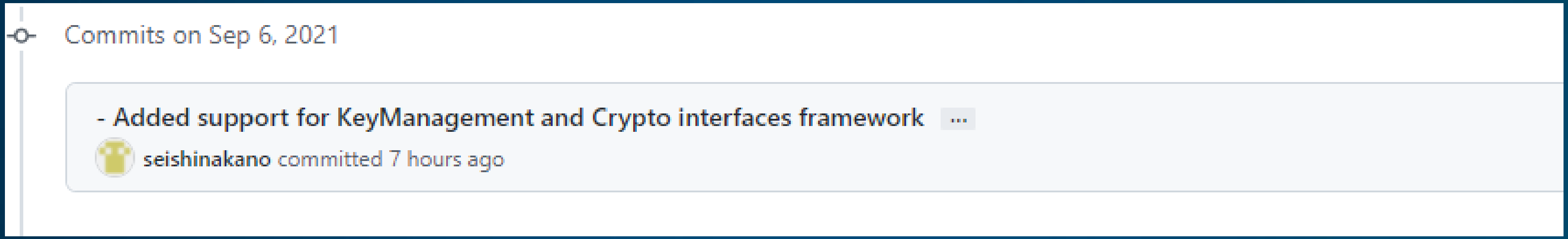
seishinakano - Added support for KeyManagement and Crypto interfaces framework ...

..

Events	- Added support for KeyManagement and Crypto interfaces framework
Handlers	- Added support for KeyManagement and Crypto interfaces framework
Constants_g.cs	- Added support for KeyManagement and Crypto interfaces framework
DeviceParameters.cs	- Added support for KeyManagement and Crypto interfaces framework
IKeyManagementDevice.cs	- Added support for KeyManagement and Crypto interfaces framework
KeyManagementServiceClass.cs	- Added support for KeyManagement and Crypto interfaces framework
KeyManagementServiceClass_g.cs	- Added support for KeyManagement and Crypto interfaces framework
KeyManagementServiceProvider.csproj	- Added support for KeyManagement and Crypto interfaces framework

Key Management & Crypto support

— Details of the changes in the following Commit



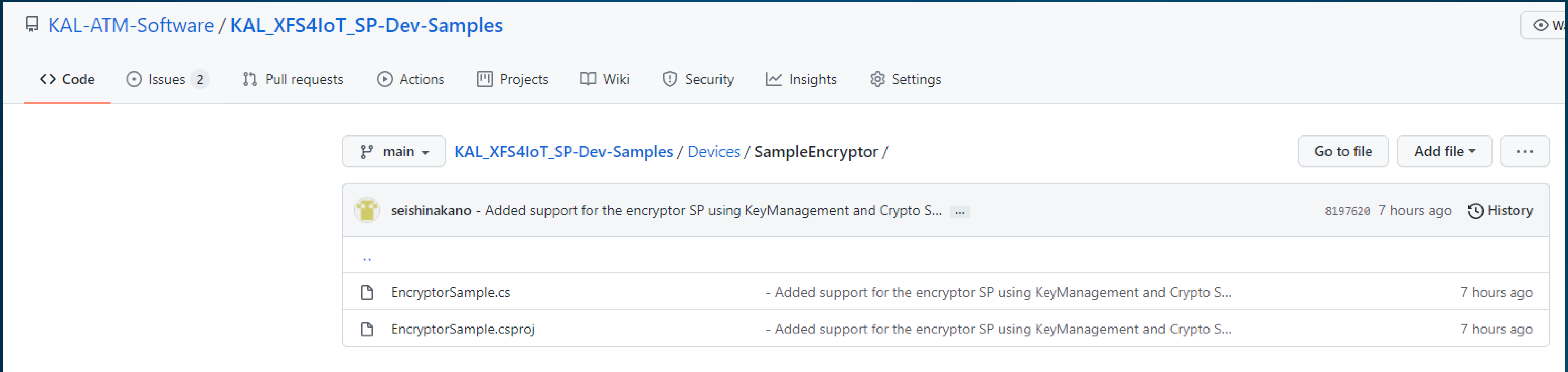
Commits on Sep 6, 2021

- Added support for KeyManagement and Crypto interfaces framework ...

seishinakano committed 7 hours ago

Key Management & Crypto support

— Encryptor sample also available



KAL-ATM-Software / KAL_XFS4IoT_SP-Dev-Samples

KAL_XFS4IoT_SP-Dev-Samples / Devices / SampleEncryptor /

seishinakano - Added support for the encryptor SP using KeyManagement and Crypto S... 8197620 7 hours ago

..

EncryptorSample.cs - Added support for the encryptor SP using KeyManagement and Crypto S... 7 hours ago

EncryptorSample.csproj - Added support for the encryptor SP using KeyManagement and Crypto S... 7 hours ago

Key Management & Crypto support

— Data encryption

— Data decryption

— MAC algorithms support including HMAC as defined in TR31 protocol

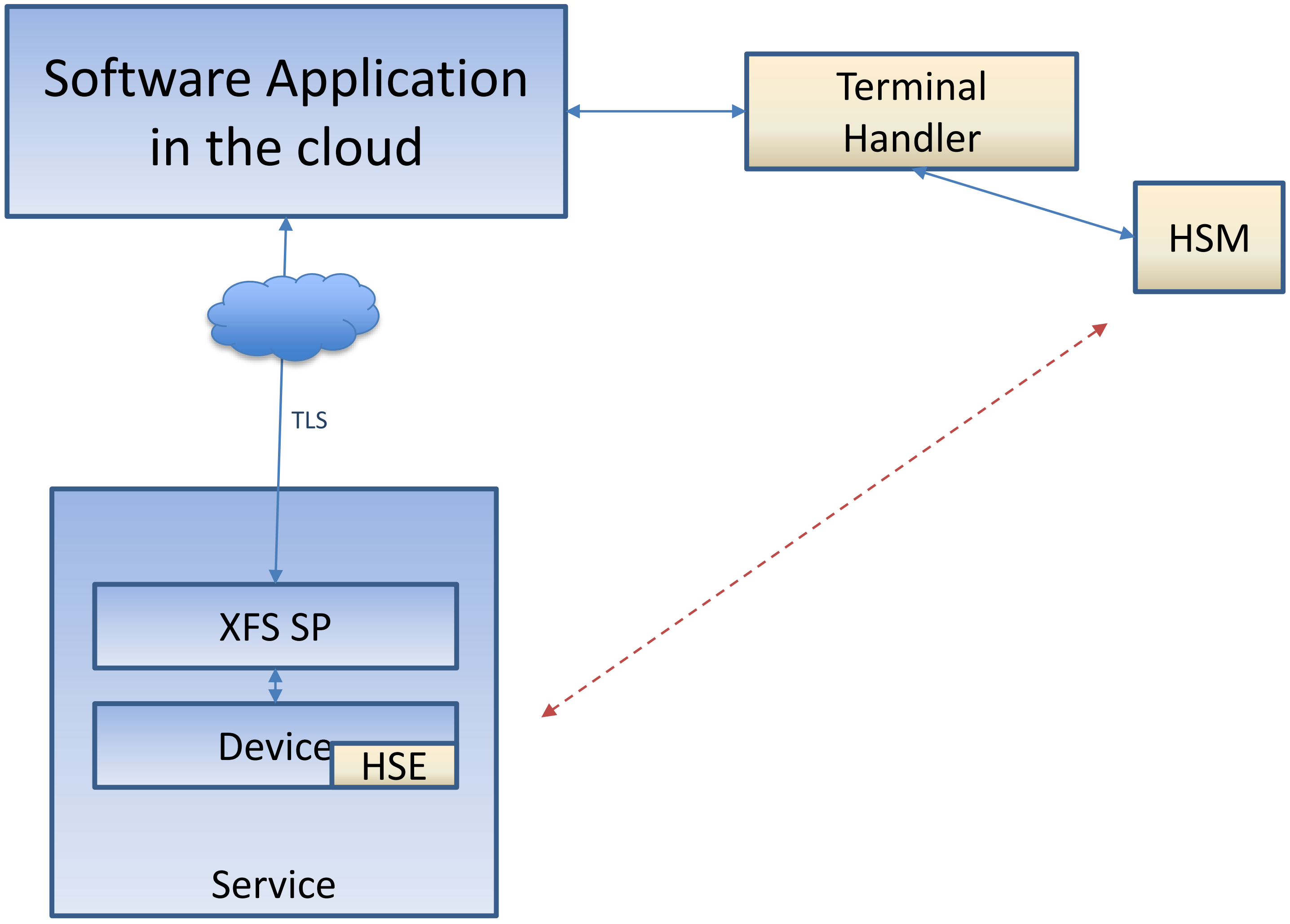
- Generate MAC
- Verify MAC

Key Management & Crypto support

- Remote Key Loading with TR34 supported
- Other types of RKL are also fully supported (signature-based, E-RKL …)
- Key Exchange with TR31 supported
- Enabling E2E security feature
- Any device can support Key Management – just requires an HSE

E2E security on generic device

- Crypto capability inside device provided by the HSE



Demo with real EPP

Demo with real EPP

Demo video available on YouTube *here*.

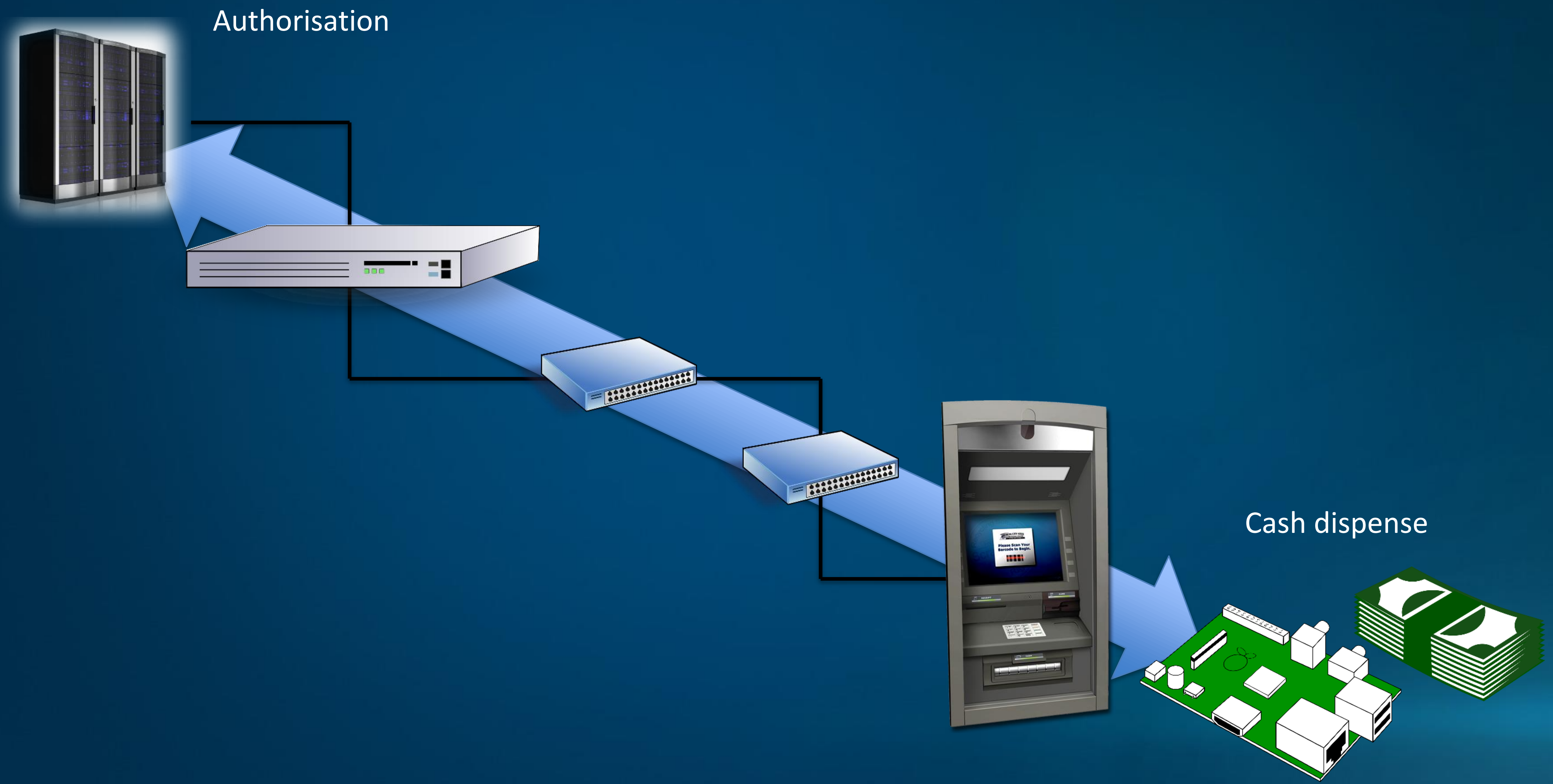
All previous demo videos can be found on the KAL ATM Software YouTube channel:

https://www.youtube.com/user/ATMsoftware/videos

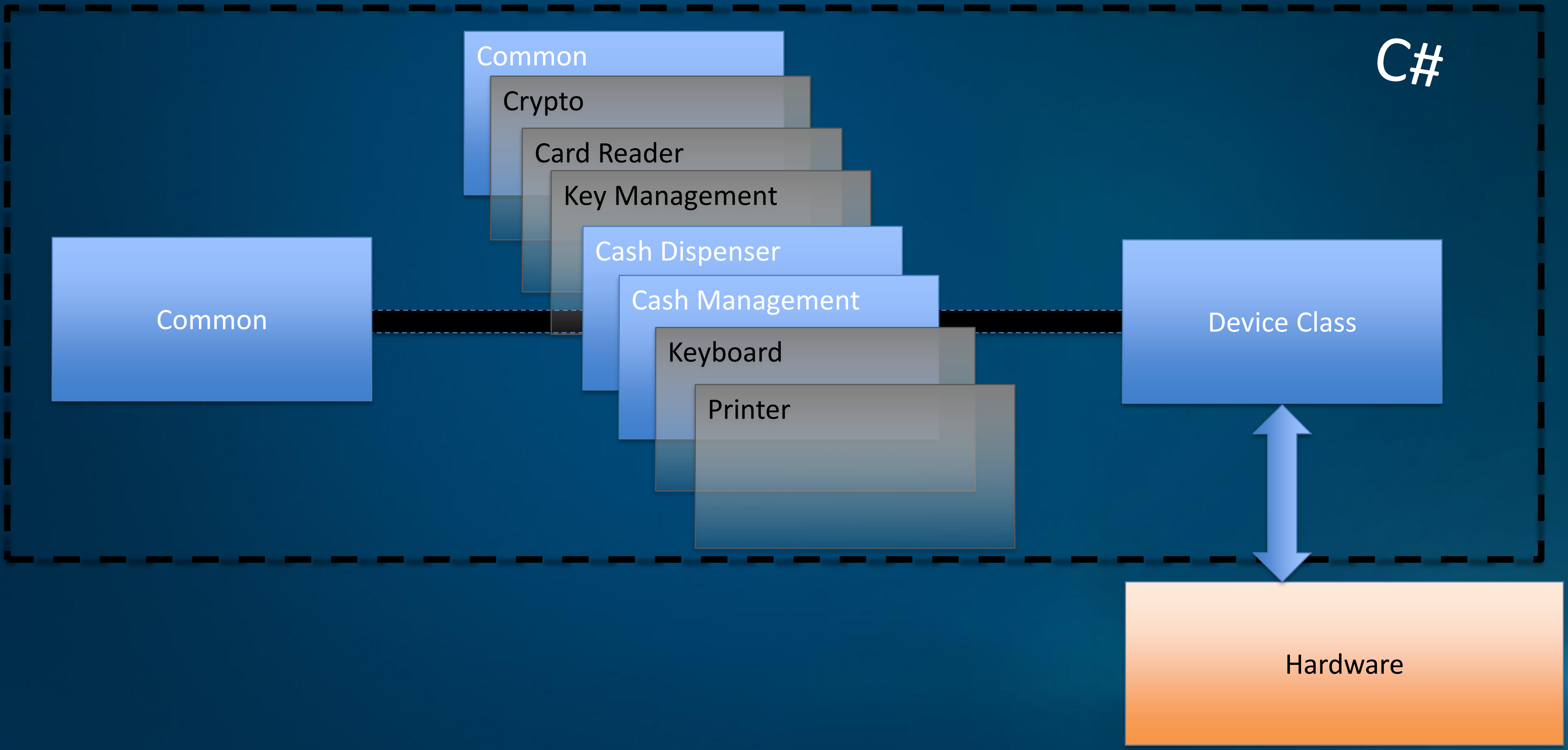
KAL
ATM Software

E2E security roadmap

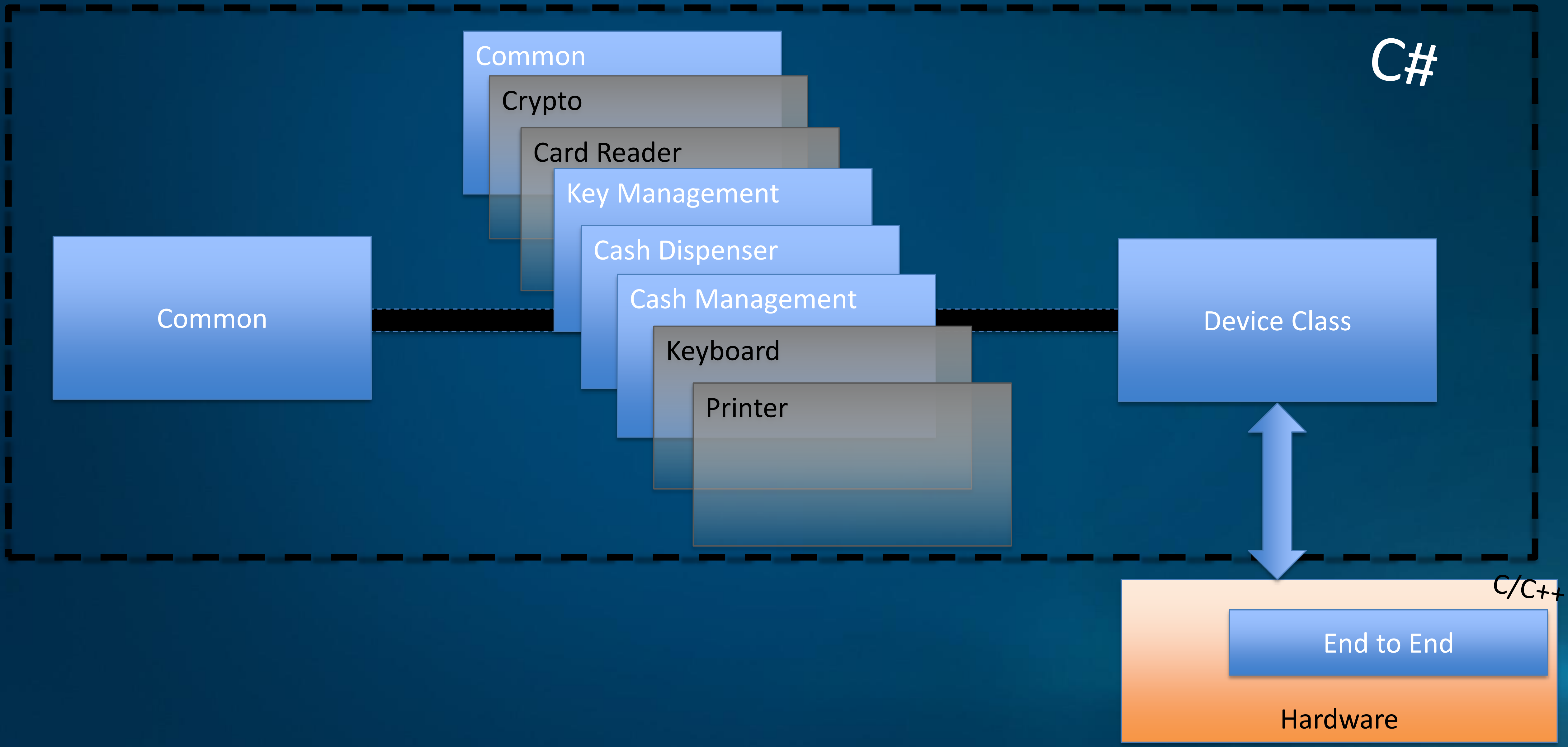
Review of E2E security



Framework today



Framework with End to End security

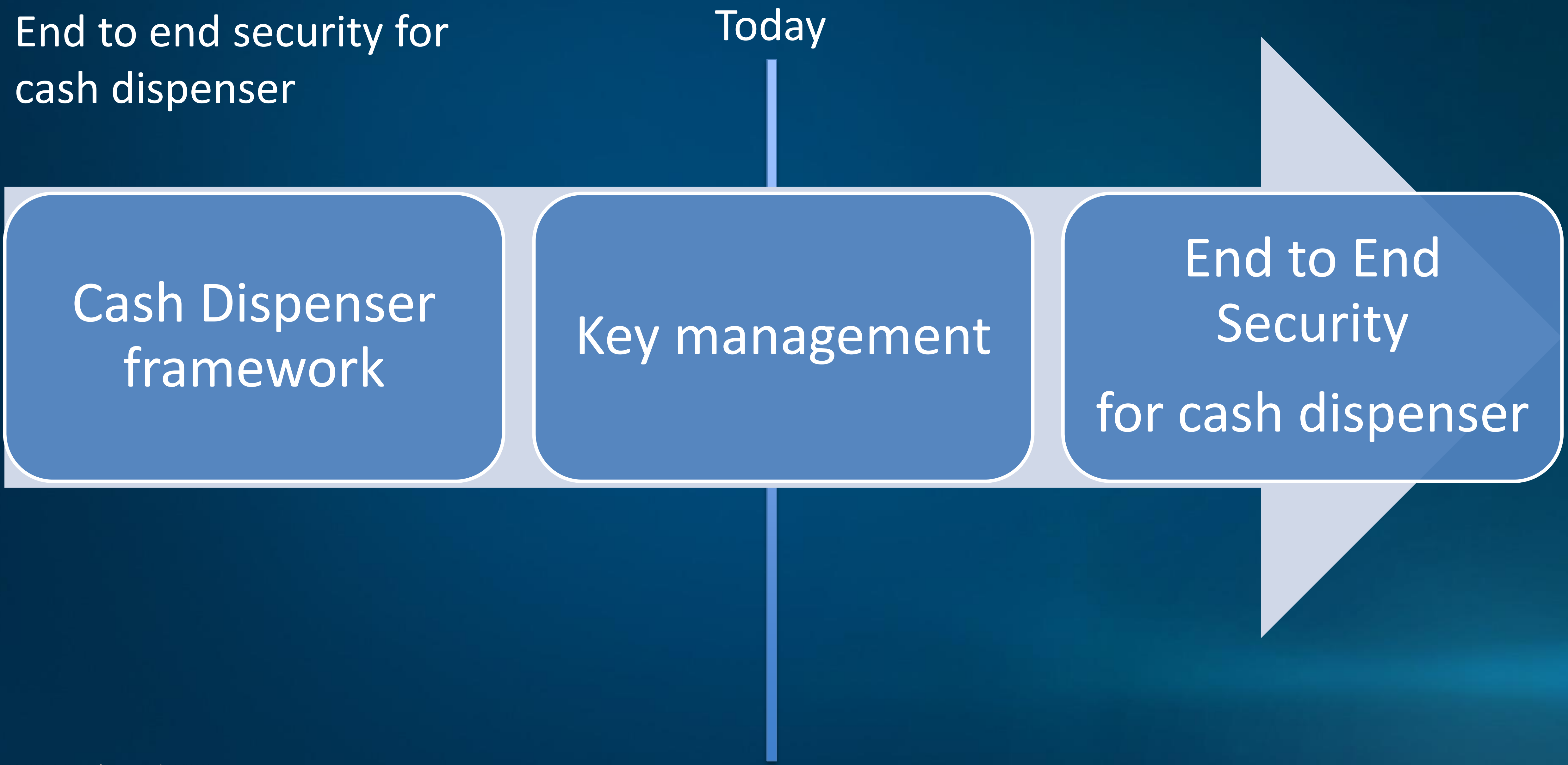


Key management

- Only key management – no need for Crypto or Keyboard support
- TR34 for remote key loading – load ‘Master’ key
- TR31 for key loading
- Two keys: XFSAuthenticateHost and XFSAuthenticateDevice

Roadmap

End to end security for cash dispenser



Today

Cash Dispenser framework

Key management

End to End Security

for cash dispenser

Framework – status review September 2021

Framework status so far

- 4 devices supported
  - — Card Reader
  - — Cash Dispenser
  - — Text Terminal
  - — EPP
- C# sample code for SP customization released for all devices
- C++ sample code also released
- Demos with real devices (videos on YouTube)

Framework status so far

- All framework code is available to:
  - — Implement XFS4 SPs
  - — Review
  - — Write test tools
  - — Test with our sample

Framework status

- Framework code updated regularly
  - If CEN specification is updated
  - Feedback from workgroup member
  - New generic features being added (i.e. command cancellation)

Star or *Watch* the repo to get notified of all updates to the framework

Card reader framework

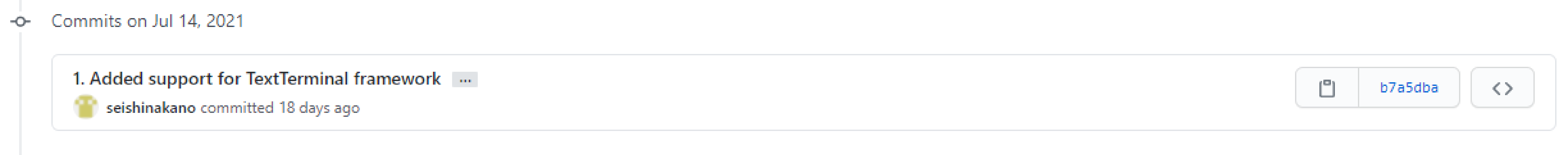
- Released May 2021
- All commands, responses and events are supported
- Being updated on a regular basis

Cash dispenser framework

- Released July 2021
- All Dispenser commands are supported
- New End-to-End security feature is **not** yet included

Text Terminal (TTU) framework

- Released July 2021
- Only forms are not *yet* supported
- Details of the changes can be seen in the commit



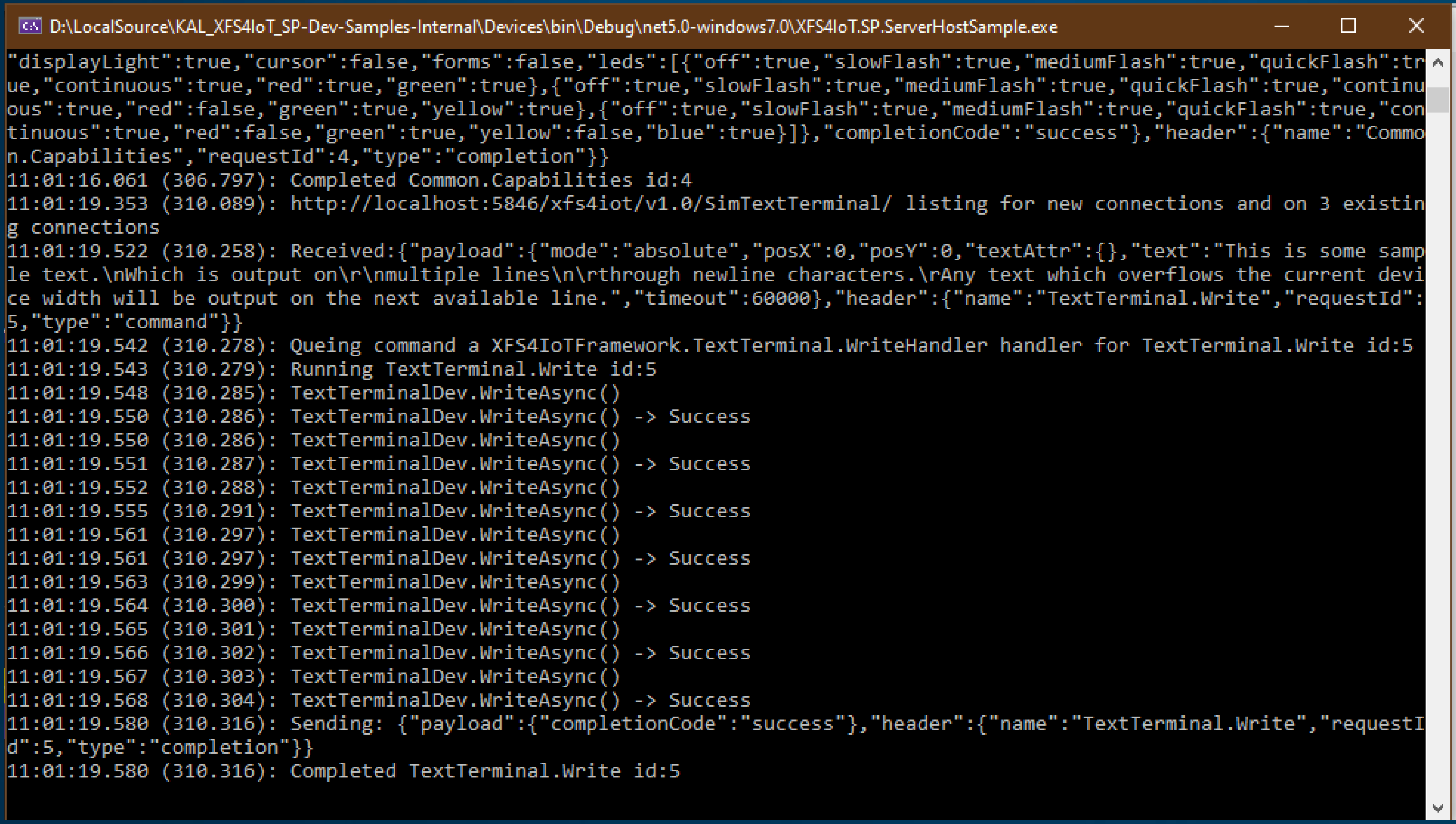
Commits on Jul 14, 2021

1. Added support for TextTerminal framework …

seishinakano committed 18 days ago

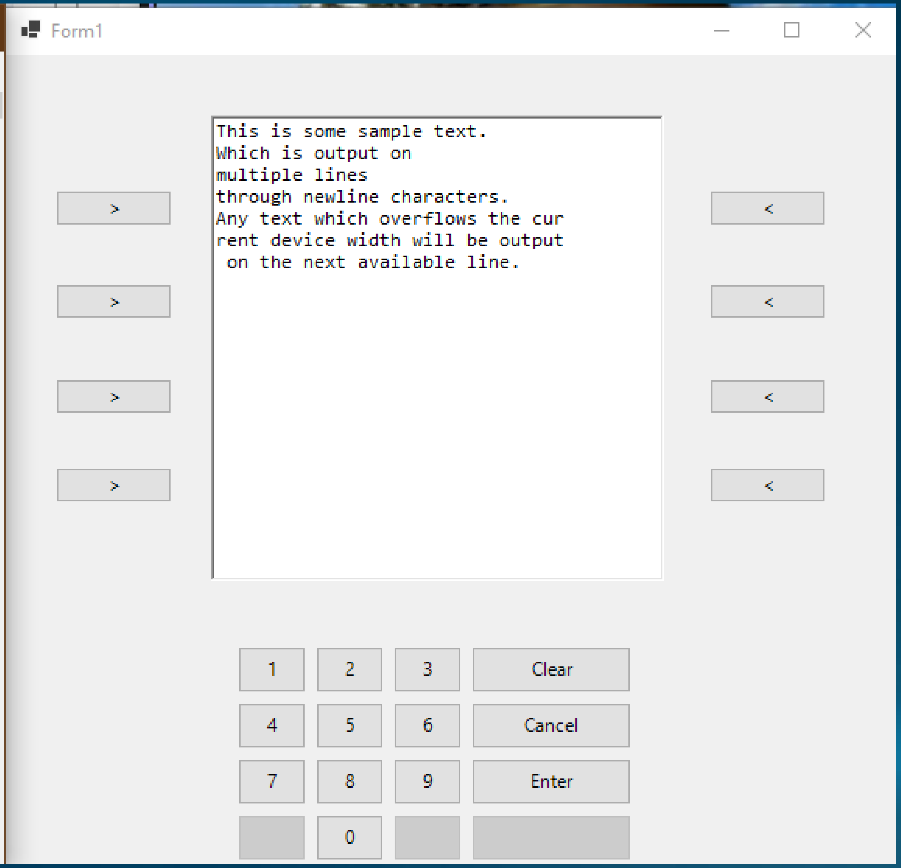
Text Terminal framework

- Sample code available in C#
- Includes simple UI for the sample device



D:\LocalSource\KAL_XFS4IoT_SP-Dev-Samples-Internal\Devices\bin\Debug\net5.0-windows7.0\XFS4IoT.SP.ServerHostSample.exe

```
"displayLight":true,"cursor":false,"forms":false,"leds":[{"off":true,"slowFlash":true,"mediumFlash":true,"quickFlash":tr
ue,"continuous":true,"red":true,"green":true},{"off":true,"slowFlash":true,"mediumFlash":true,"quickFlash":true,"continu
ous":true,"red":false,"green":true,"yellow":true},{"off":true,"slowFlash":true,"mediumFlash":true,"quickFlash":true,"con
tinuous":true,"red":false,"green":true,"yellow":false,"blue":true}]},"completionCode":"success"},"header":{"name":"Commo
n.Capabilities","requestId":4,"type":"completion"}}
11:01:16.061 (306.797): Completed Common.Capabilities id:4
11:01:19.353 (310.089): http://localhost:5846/xfs4iot/v1.0/SimTextTerminal/ listing for new connections and on 3 existin
g connections
11:01:19.522 (310.258): Received:{"payload":{"mode":"absolute","posX":0,"posY":0,"textAttr":{},"text":"This is some samp
le text.\nWhich is output on\r\nmultiple lines\n\rthrough newline characters.\rAny text which overflows the current devi
ce width will be output on the next available line.","timeout":60000},"header":{"name":"TextTerminal.Write","requestId":
5,"type":"command"}}
11:01:19.542 (310.278): Queing command a XFS4IoTFramework.TextTerminal.WriteHandler handler for TextTerminal.Write id:5
11:01:19.543 (310.279): Running TextTerminal.Write id:5
11:01:19.548 (310.285): TextTerminalDev.WriteAsync()
11:01:19.550 (310.286): TextTerminalDev.WriteAsync() -> Success
11:01:19.550 (310.286): TextTerminalDev.WriteAsync()
11:01:19.551 (310.287): TextTerminalDev.WriteAsync() -> Success
11:01:19.552 (310.288): TextTerminalDev.WriteAsync()
11:01:19.555 (310.291): TextTerminalDev.WriteAsync() -> Success
11:01:19.561 (310.297): TextTerminalDev.WriteAsync()
11:01:19.561 (310.297): TextTerminalDev.WriteAsync() -> Success
11:01:19.563 (310.299): TextTerminalDev.WriteAsync()
11:01:19.564 (310.300): TextTerminalDev.WriteAsync() -> Success
11:01:19.565 (310.301): TextTerminalDev.WriteAsync()
11:01:19.566 (310.302): TextTerminalDev.WriteAsync() -> Success
11:01:19.567 (310.303): TextTerminalDev.WriteAsync()
11:01:19.568 (310.304): TextTerminalDev.WriteAsync() -> Success
11:01:19.580 (310.316): Sending: {"payload":{"completionCode":"success"},"header":{"name":"TextTerminal.Write","requestI
d":5,"type":"completion"}}
11:01:19.580 (310.316): Completed TextTerminal.Write id:5
```



```
This is some sample text.
Which is output on
multiple lines
through newline characters.
Any text which overflows the cur
rent device width will be output
 on the next available line.
```

Next meeting and announcements

What’s next?

- Other Pinpad-related classes (Keyboard & Pinpad)
- Cash dispenser E2E security feature support
- E2E security demo on small devices
- Guest speaker

Next call

MS Teams

- First Tuesday of each month at 1300 UK time

Next call: 5th October 2021, 1300 UK, 0800 US EST, 2100 Tokyo time

(Note: **Australia** changes clocks on the 3rd October. It will be 2300 Sydney time on the 5th Oct – 1hr later than normal. UK, EU clocks will change before the November meeting).