

The ARM logo is displayed in a white, lowercase, sans-serif font. The background of the slide features a dark blue, abstract pattern of circuit traces and nodes, with a grid of small white plus signs overlaid on it.

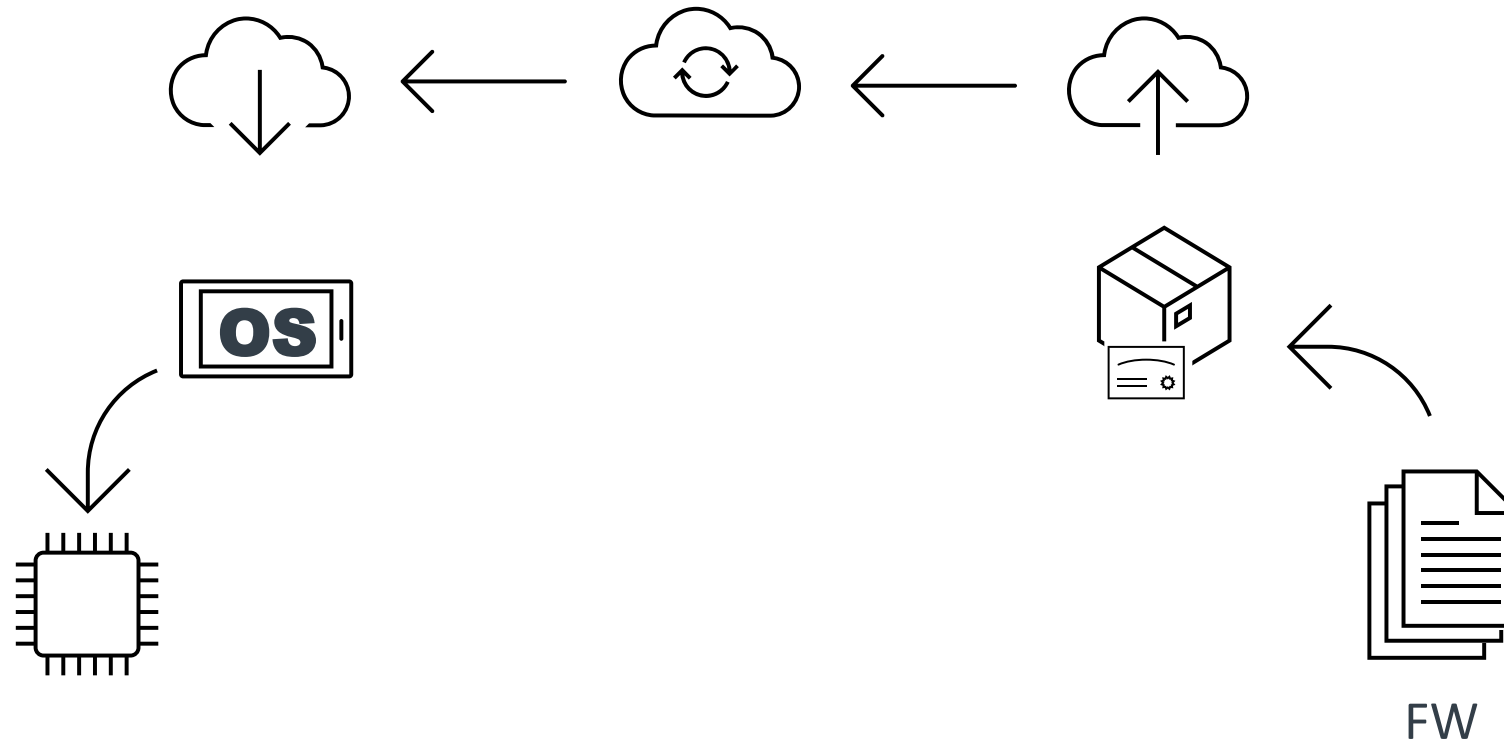
arm

Standard FW update on A-class Arm devices

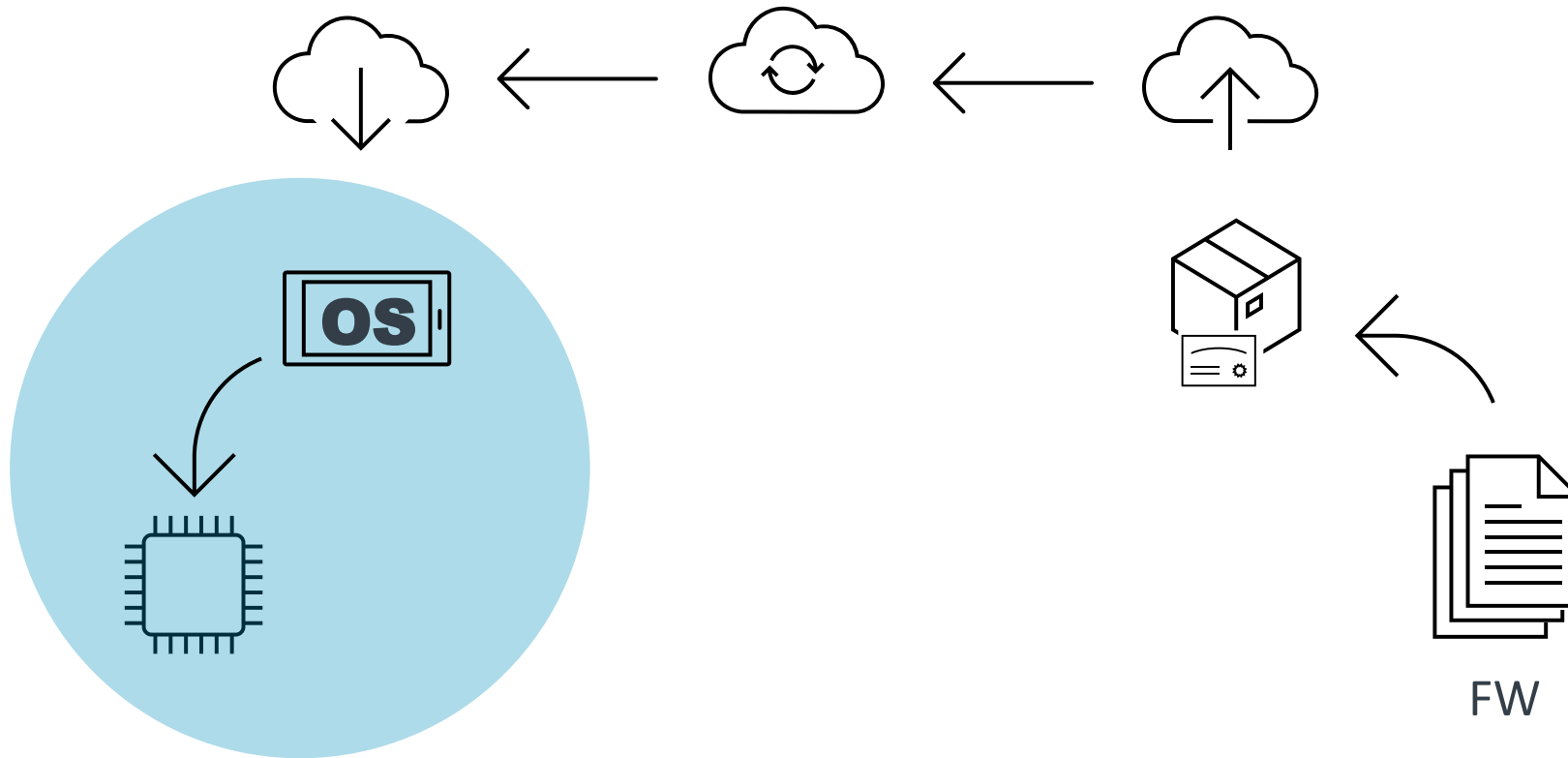
Linaro Virtual Connect 2021

Jose Marinho
24th March 2021

FW delivery hinges on many technologies



FW delivery hinges on many technologies



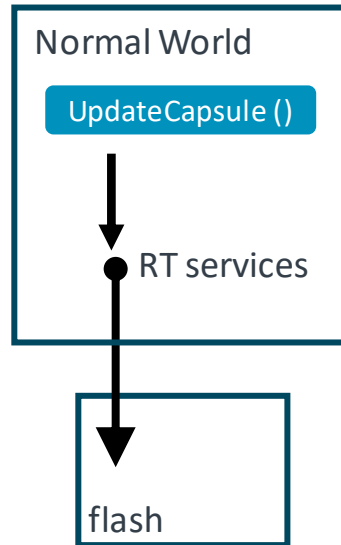
Terminology clarification

- UEFI → industry standard [1]
 - Defines an API
- UEFI implementation: EDK2, U-boot, etc ...
 - Implementations of the standard UEFI API
- In this presentation: the term UEFI implementation refers to both U-boot and EDK2.

[1] [https://uefi.org/sites/default/files/resources/UEFI Spec 2.8B May 2020.pdf](https://uefi.org/sites/default/files/resources/UEFI%20Spec%202.8B%20May%202020.pdf)

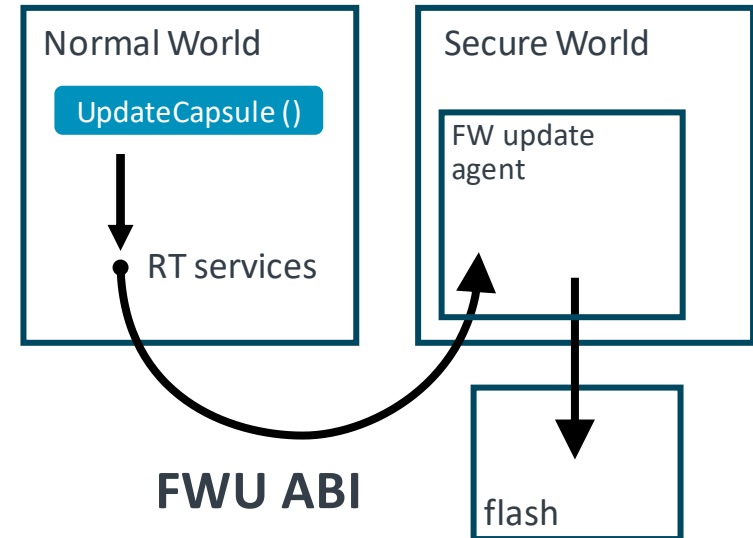
Support diverse platform designs

1



- Lower cost
- More resets
- Open to DoS attacks

2 Primary scenario

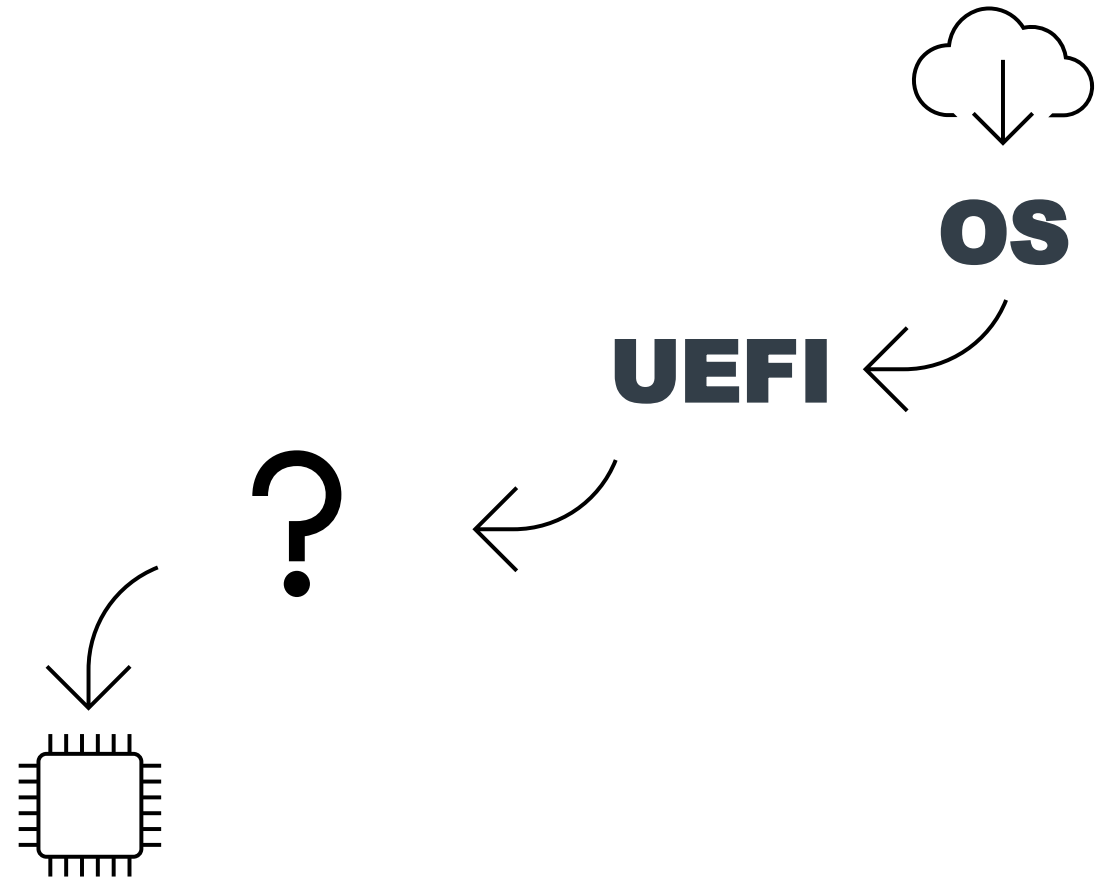


- Emerging trend
- Dedicated flash for Secure World
- Single reset update
- Reduced system downtime

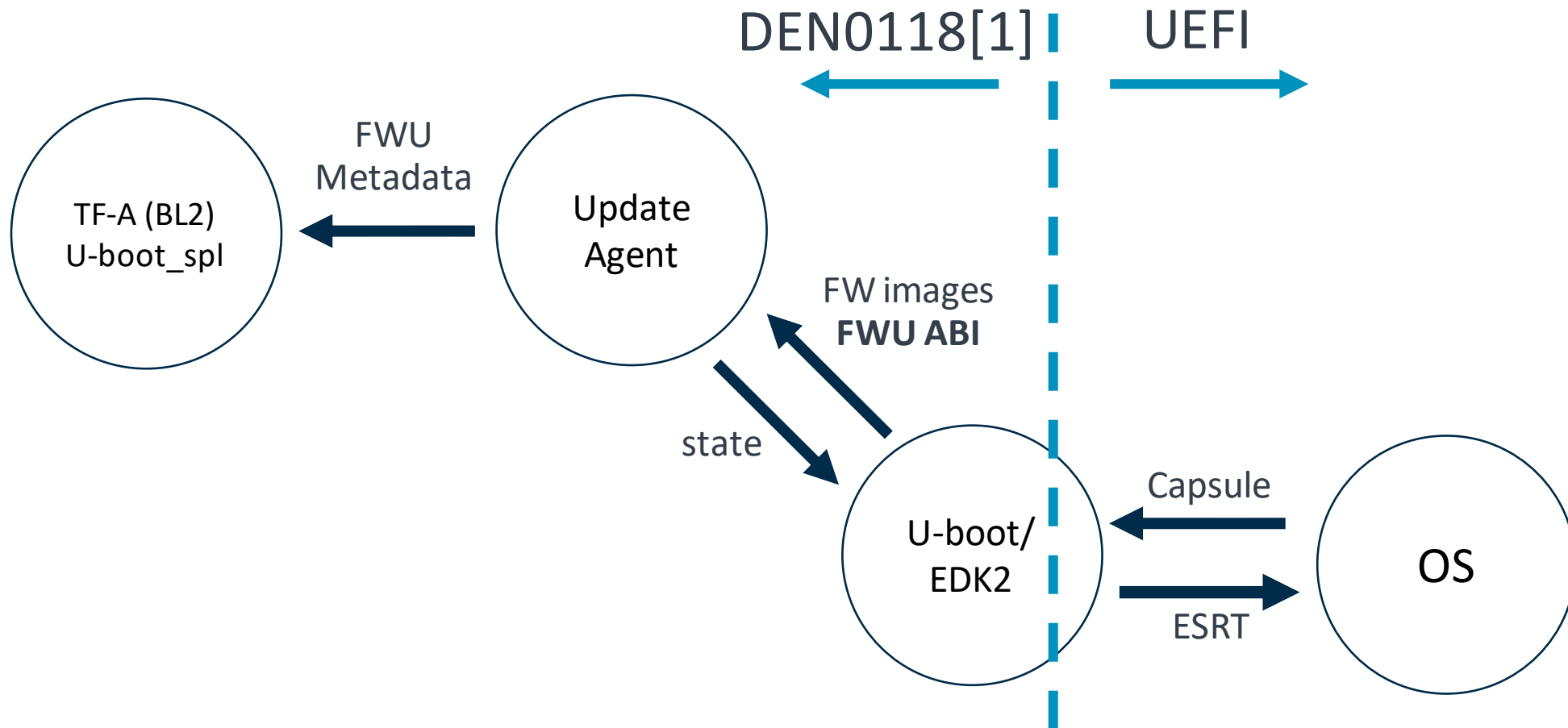
Opportunities for standardization

FW update? There's a standard for that!

- (UEFI) UpdateCapsule well established.
- What's missing?
 - Solutions for Interoperability.
 1. FW image communication to Secure World.
 - State info exchange with platform boot code.
 2. Standard A/B bank support

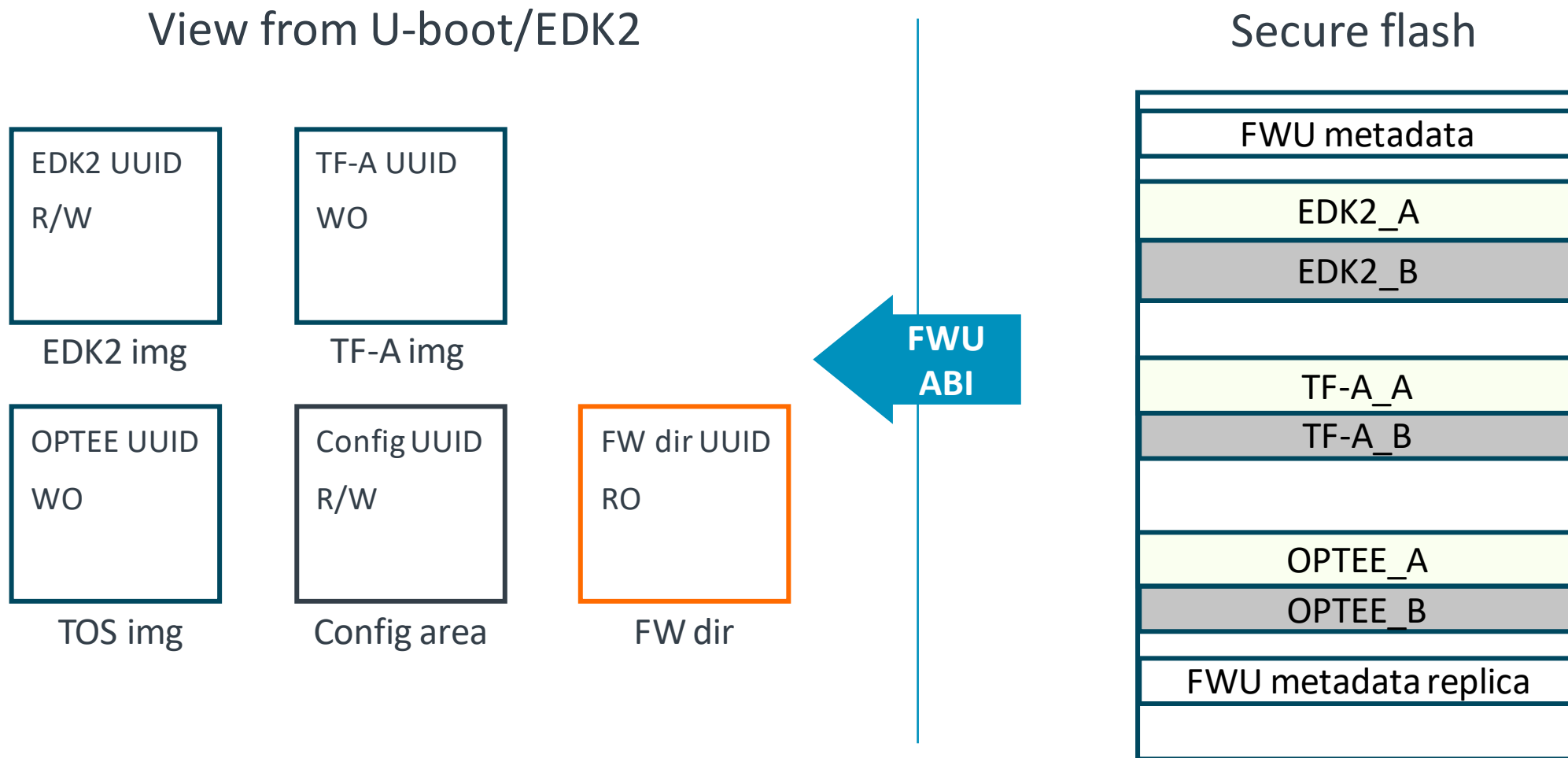


Interfaces between agents are standardized



[1] https://developer.arm.com/-/media/Files/pdf/PlatformSecurityArchitecture/Architect/FWU-PSA-A_DEN0118_1.0ALP2.pdf

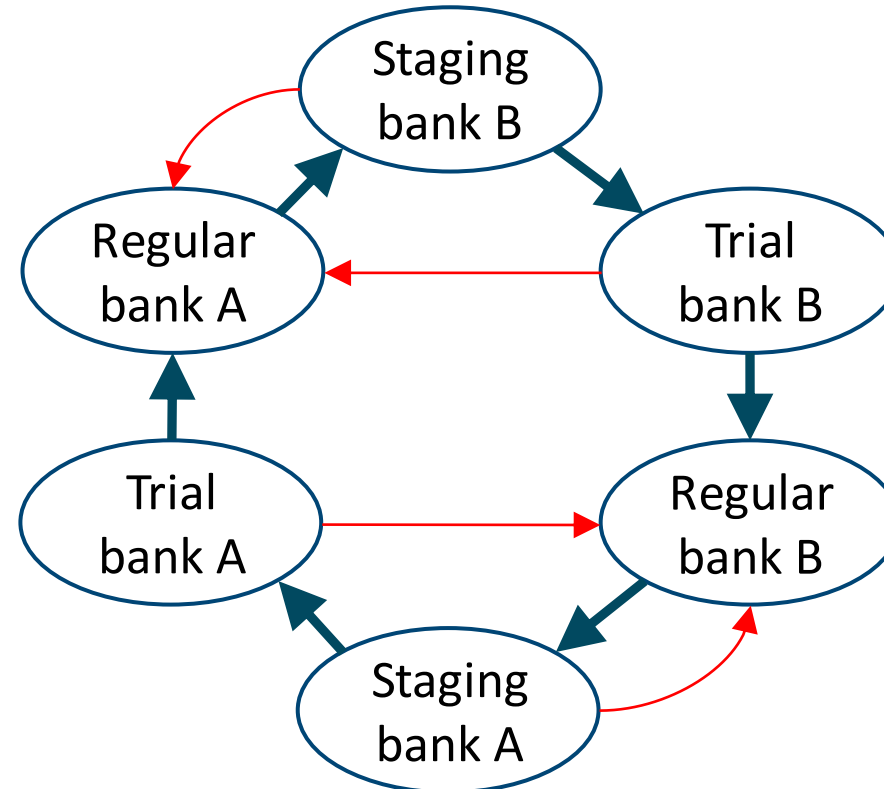
Udata Agent exposes a file abstraction



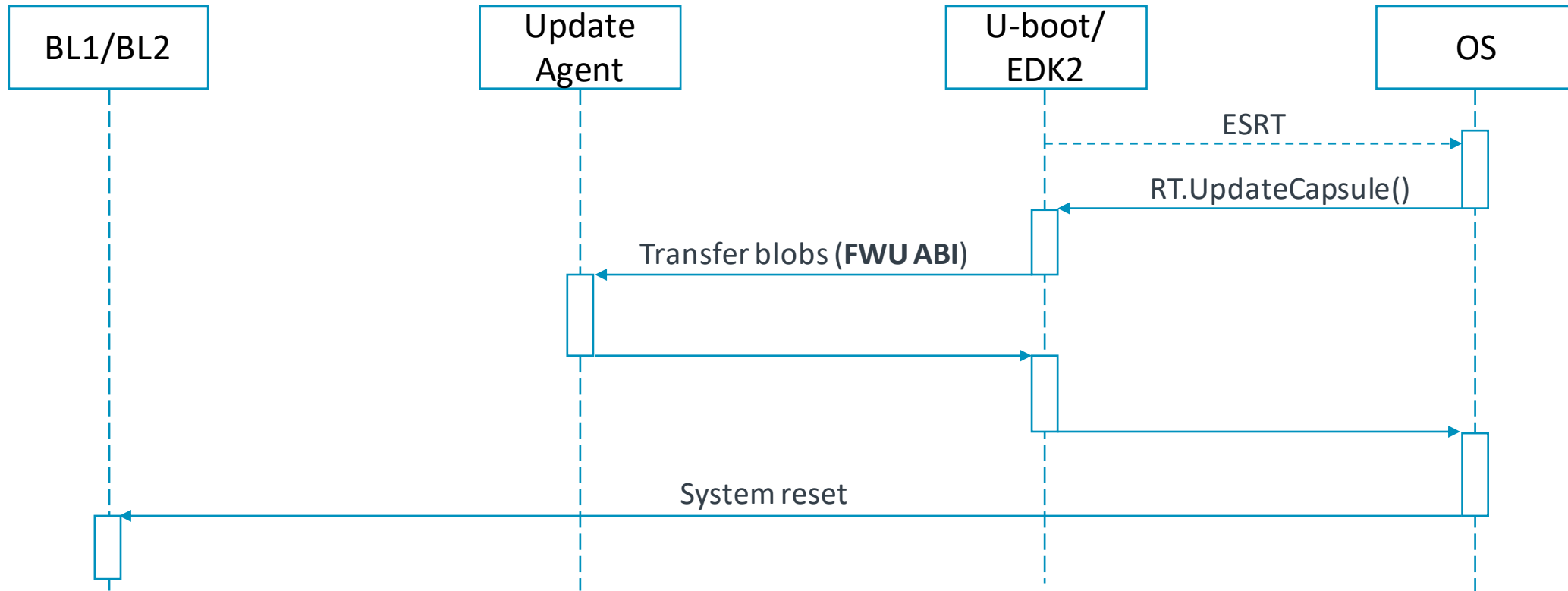
A-class standard ABI – transfers blobs and navigates FSM

A-class FWU ABI:

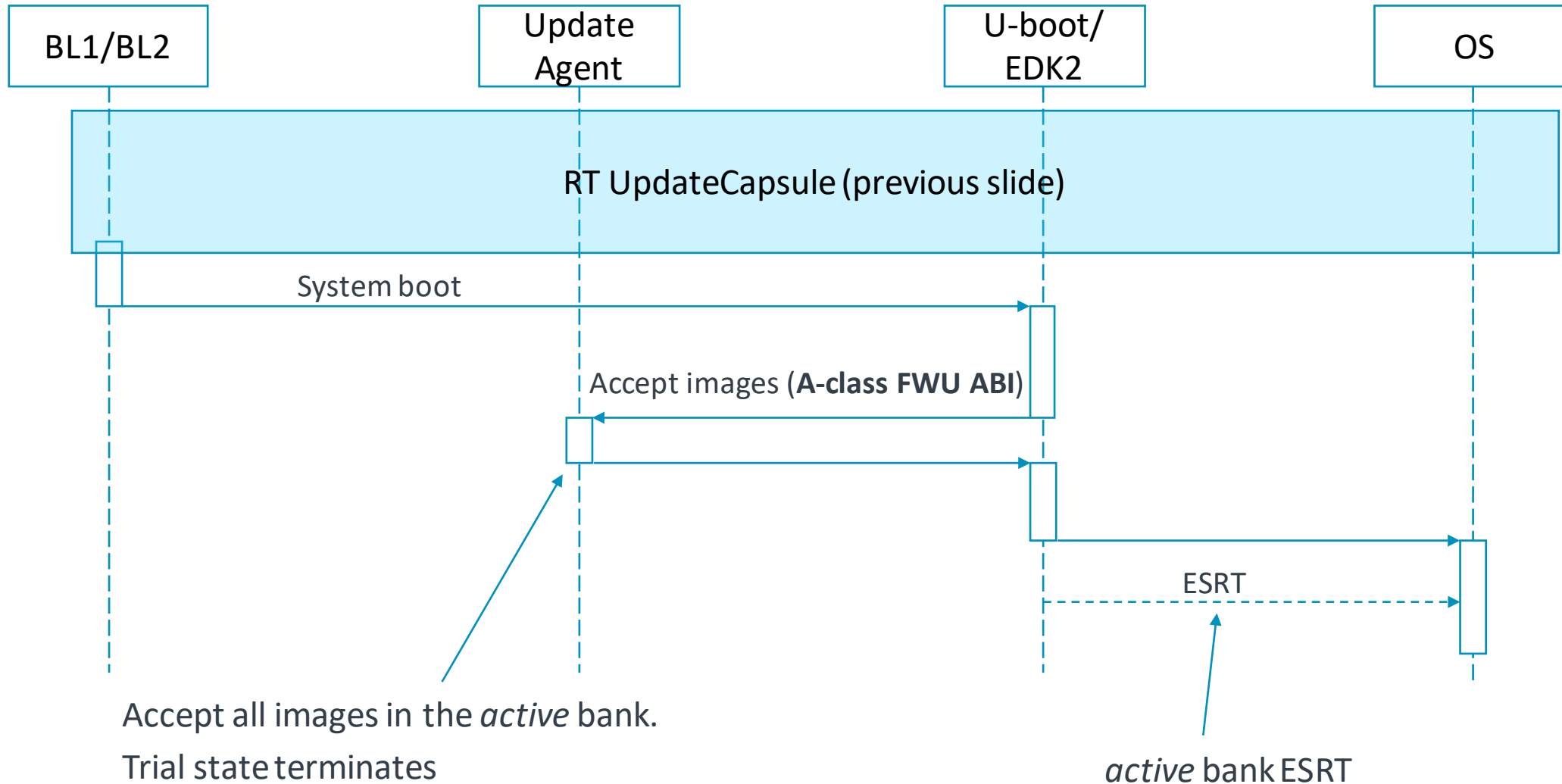
- fwu_discover
- fwu_begin_staging
- fwu_end_staging
- fwu_cancel_staging
- fwu_open
- fwu_write_stream
- fwu_read_stream
- fwu_close
- fwu_accept_image
- fwu_set_active



UEFI Runtime capsule update



UEFI Trial boot

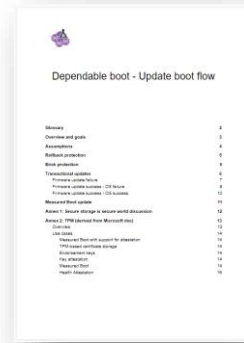


Project status

QEMU prototype [2]

1. StandaloneMM (EDK2)
2. OP-TEE
3. U-boot
4. TF-A

Ongoing upstreaming to U-boot



UEFI design
Document
(under development)



Firmware update
protocol Alpha [1]

[1] https://developer.arm.com/-/media/Files/pdf/PlatformSecurityArchitecture/Architect/FWU-PSA-A_DEN0118_1.0ALP2.pdf

[2] https://github.com/jmarinho/u-boot-manifest-m_fwu_proto.xml

Feedback welcome!



- Specification (Alpha version): https://developer.arm.com/-/media/Files/pdf/PlatformSecurityArchitecture/Architect/FWU-PSA-A_DEN0118_1.0ALP2.pdf
- jose.marinho (at) arm.com

arm

Thank You

Danke

Gracias

谢谢

ありがとう

Asante

Merci

감사합니다

धन्यवाद

Kiitos

شكراً

ধন্যবাদ

תודה

arm

The Arm trademarks featured in this presentation are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. All other marks featured may be trademarks of their respective owners.

www.arm.com/company/policies/trademarks