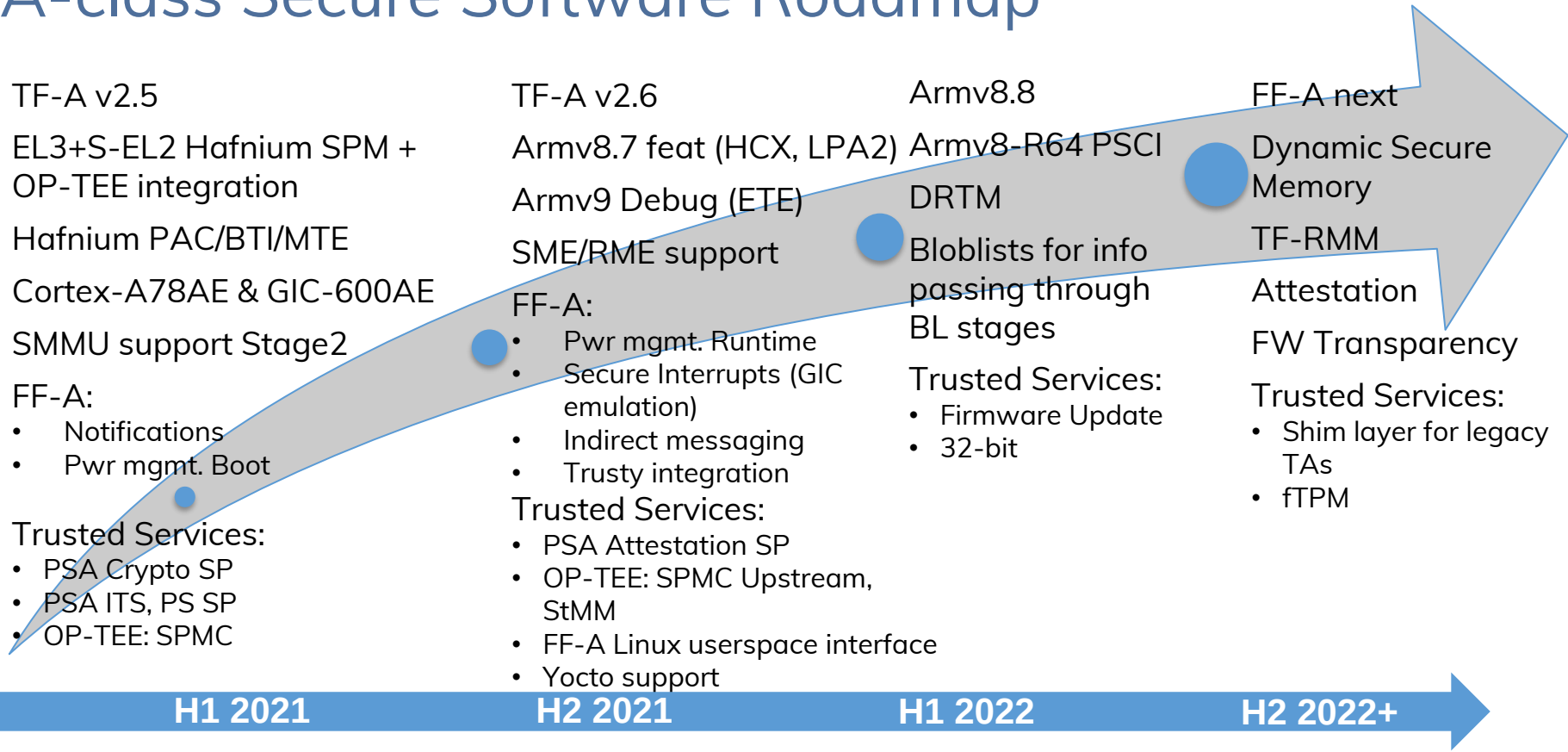
A-class Secure Software Roadmap



TF-A v2.5

EL3+S-EL2 Hafnium SPM + OP-TEE integration

Hafnium PAC/BTI/MTE

Cortex-A78AE & GIC-600AE

SMMU support Stage2

FF-A:
- Notifications
- Pwr mgmt. Boot

Trusted Services:
- PSA Crypto SP
- PSA ITS, PS SP
- OP-TEE: SPMC

TF-A v2.6

Armv8.7 feat (HCX, LPA2)

Armv9 Debug (ETE)

SME/RME support

FF-A:
- Pwr mgmt. Runtime
- Secure Interrupts (GIC emulation)
- Indirect messaging
- Trusty integration

Trusted Services:
- PSA Attestation SP
- OP-TEE: SPMC Upstream, StMM
- FF-A Linux userspace interface
- Yocto support

Armv8.8

Armv8-R64 PSCI

DRTM

Bloblists for info passing through BL stages

Trusted Services:
- Firmware Update
- 32-bit

FF-A next

Dynamic Secure Memory

TF-RMM

Attestation

FW Transparency

Trusted Services:
- Shim layer for legacy TAs
- fTPM

H1 2021 **H2 2021** **H1 2022** **H2 2022+**

FF-A spec (SPCI) v1.0 specification EAC - https://developer.arm.com/docs/den0077/a