RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

Ultrablue

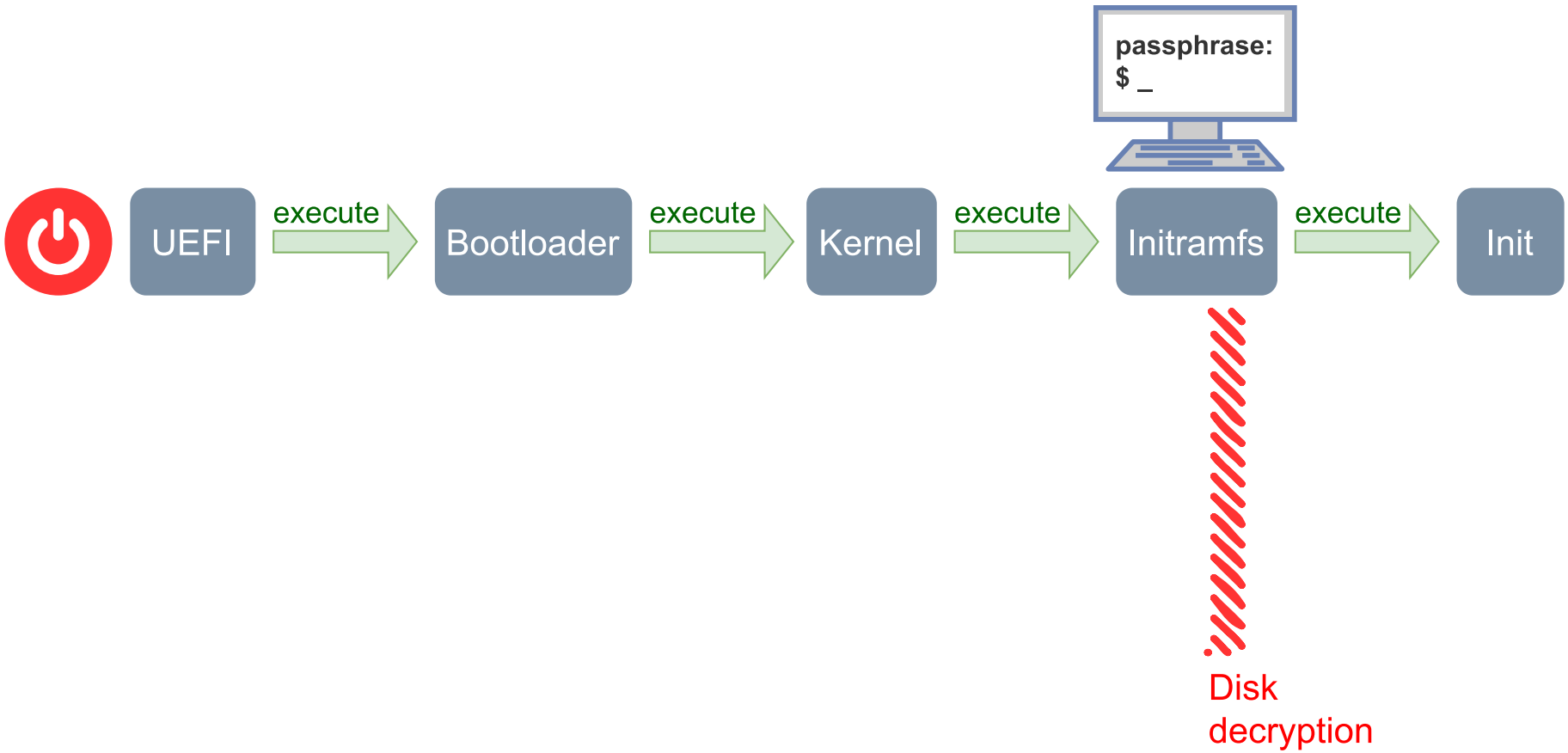
Remote attestation over Bluetooth

Loïc Buckwell, Gabriel Kerneis, Nicolas Bouchinet

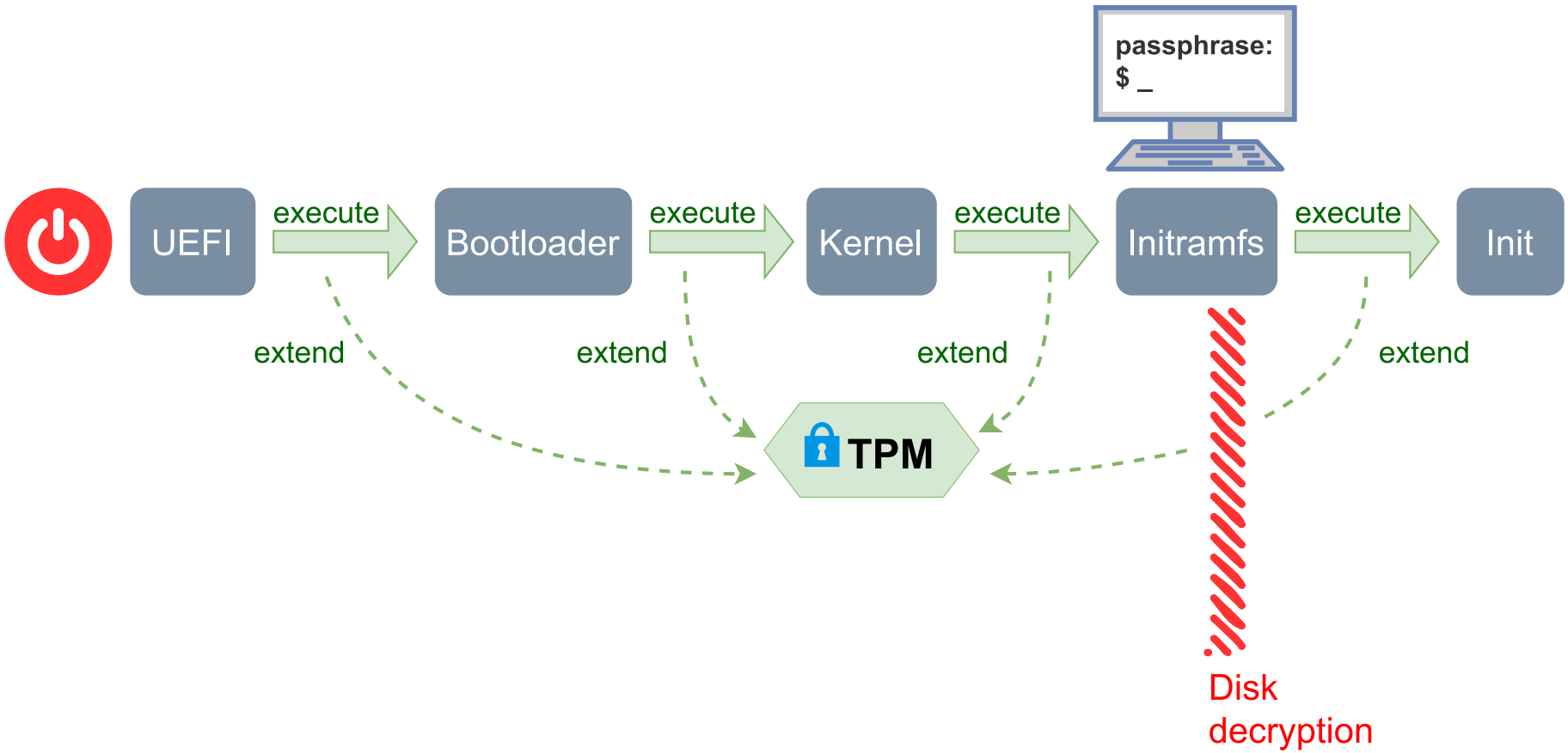
French National Cyber Security Agency

September 21, 2022 – OSFC 2022

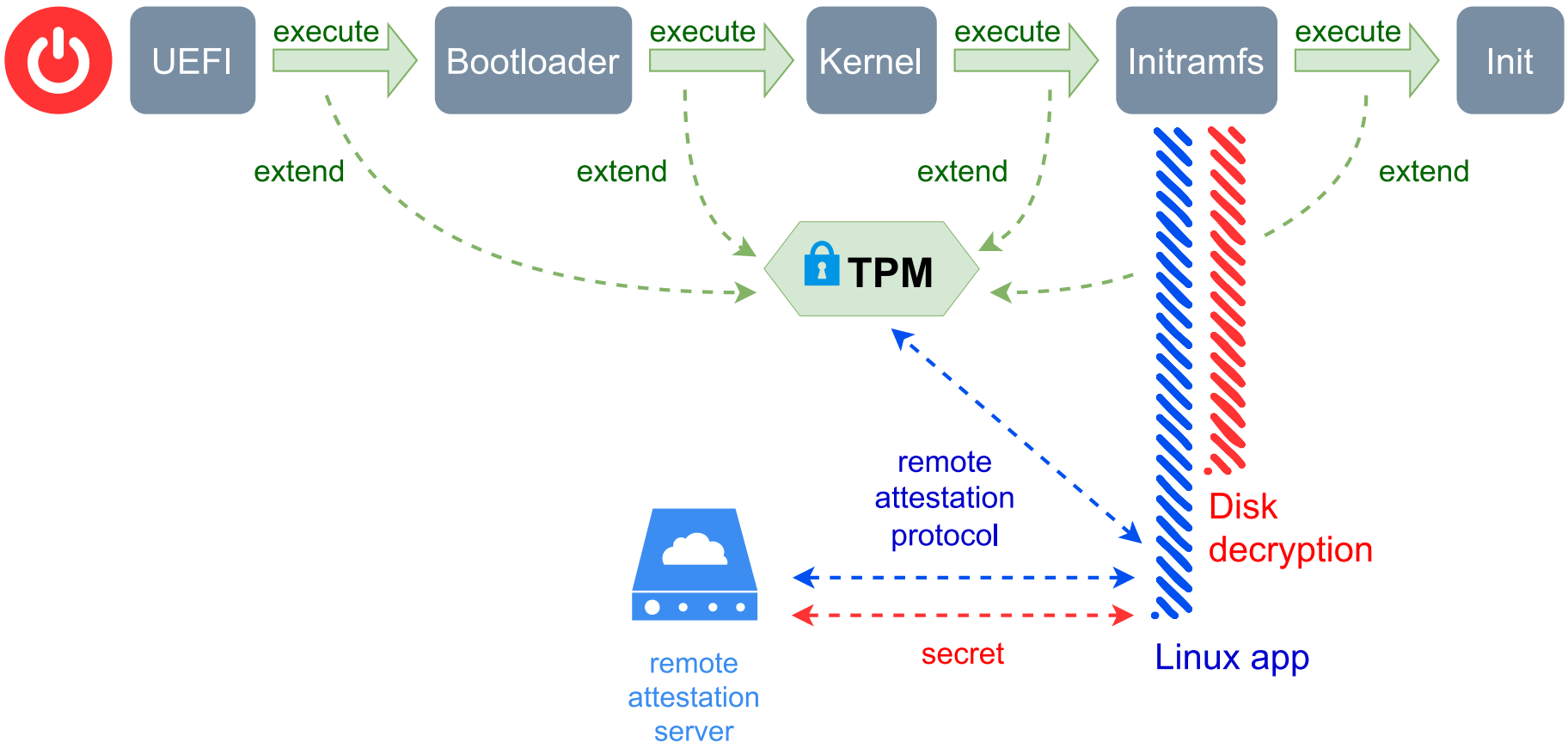
Bootchain


passphrase:
$ _
UEFI
execute
Bootloader
execute
Kernel
execute
Initramfs
execute
Init
Disk
decryption

Bootchain with TPM



Bootchain with TPM and remote attestation



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Ultrablue – User-friendly lightweight TPM remote attestation over Bluetooth

Your phone does remote attestation

Ultrablue Stack

GO

Bluetooth SMART

GO

Bluetooth SMART

Kotlin

GO

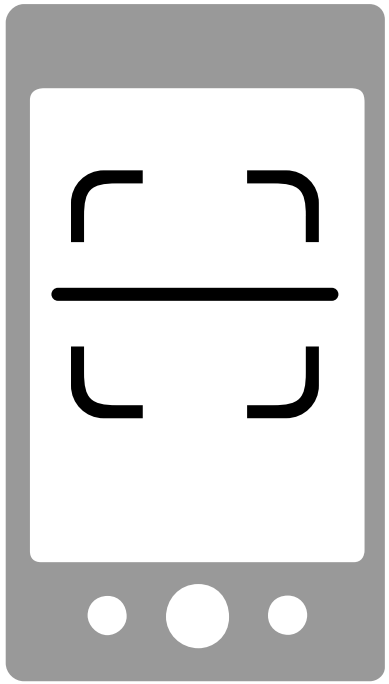
Bluetooth SMART

Swift

server
(laptop)

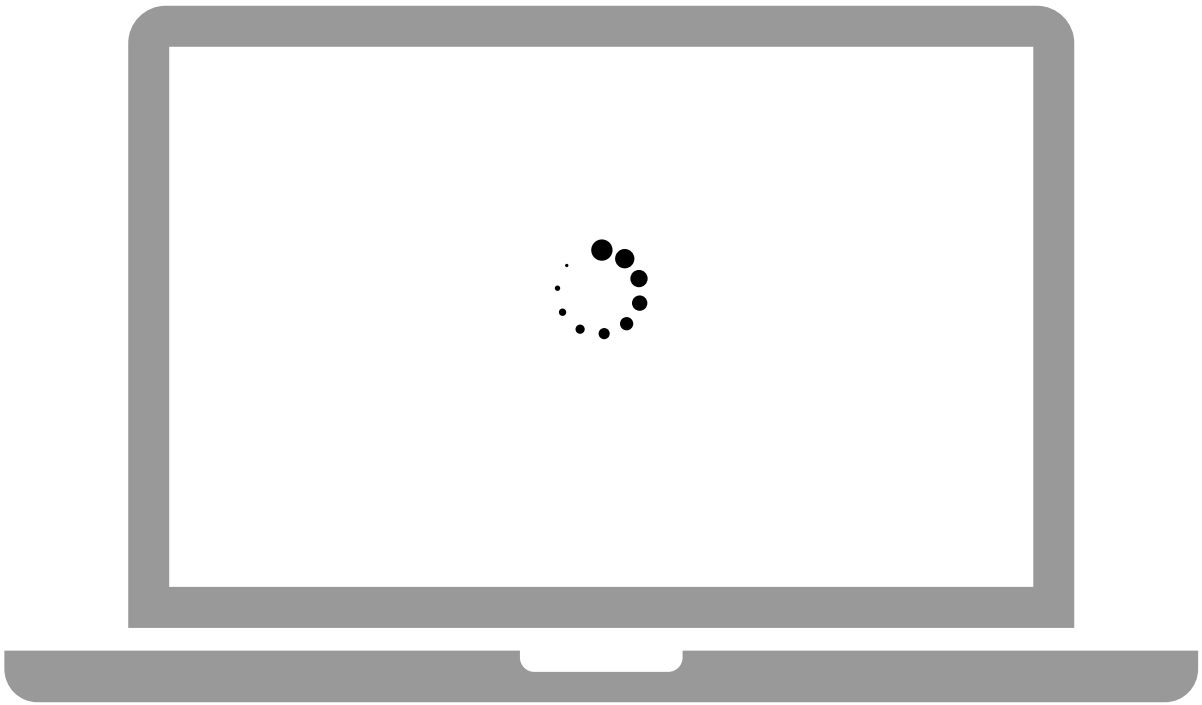
clients
(smartphone)

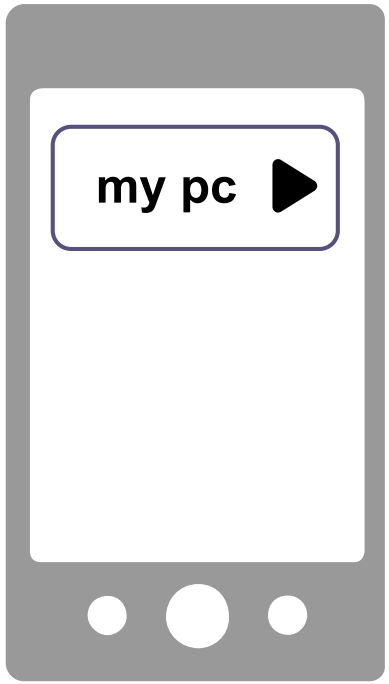
Ultrablue Workflow - Enrollment



- Use a QR code to share channel encryption key
- Get the reference state
- Boot state trusted on first use

Ultrablue Workflow - Attestation

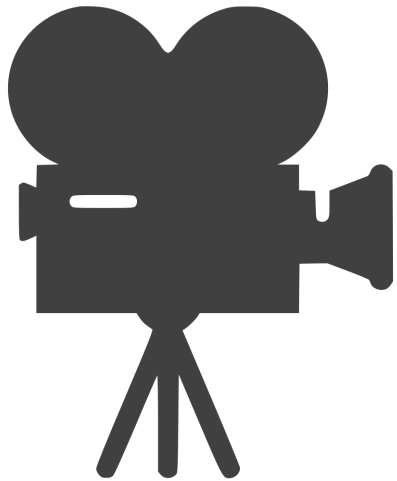




- Get new boot state
- Inspect changes easily
- Control attestation result

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Ultrablue Demo



RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

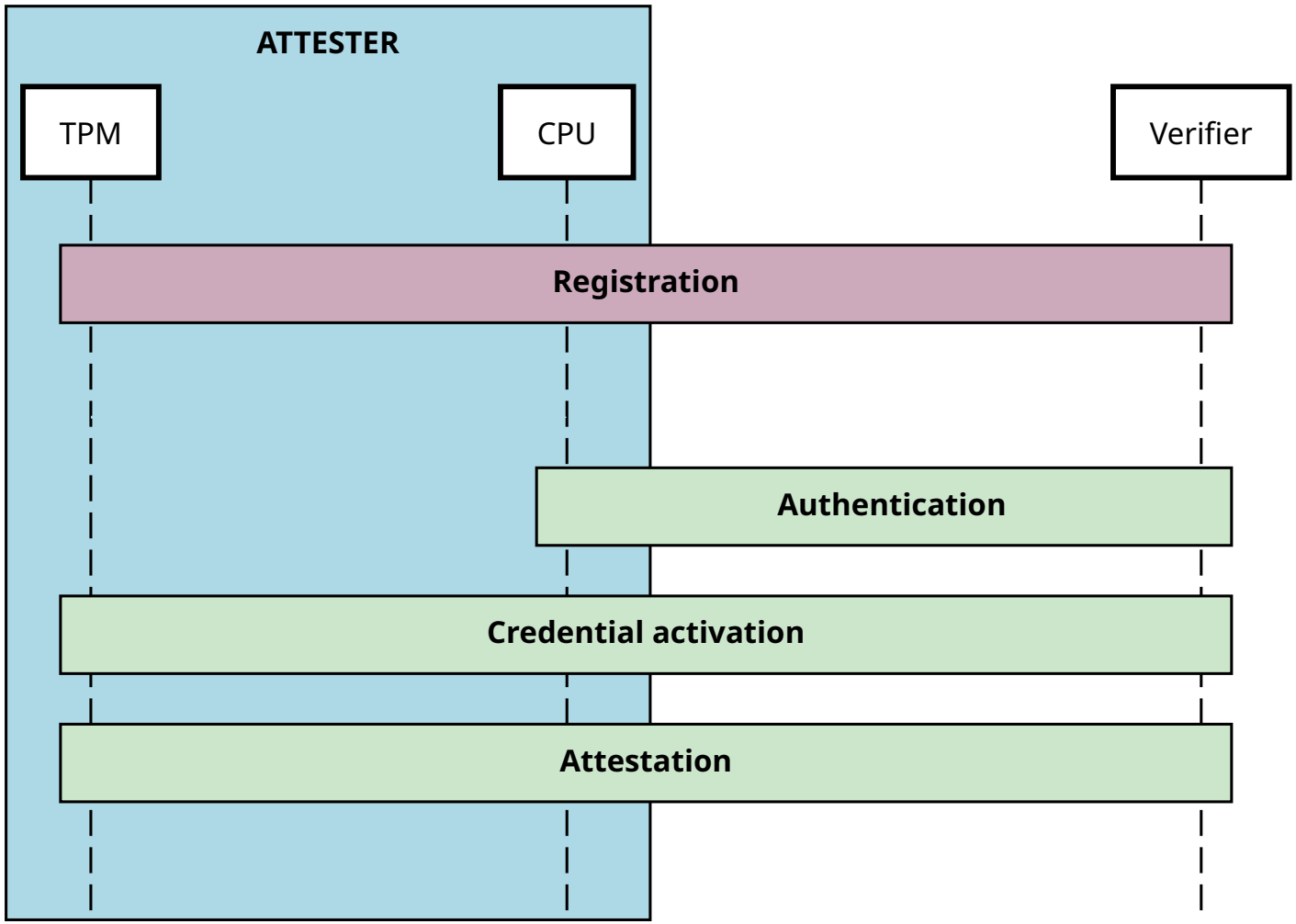
Ultrablue is versatile

- Embeddable in initramfs, or runnable at a later stage
- Usable as a second factor for disk decryption
  (via PCR extension and LUKS TPM slot)
- Sample scripts to build a test VM demonstrating those features
- We welcome use-cases, suggestions and contributions!

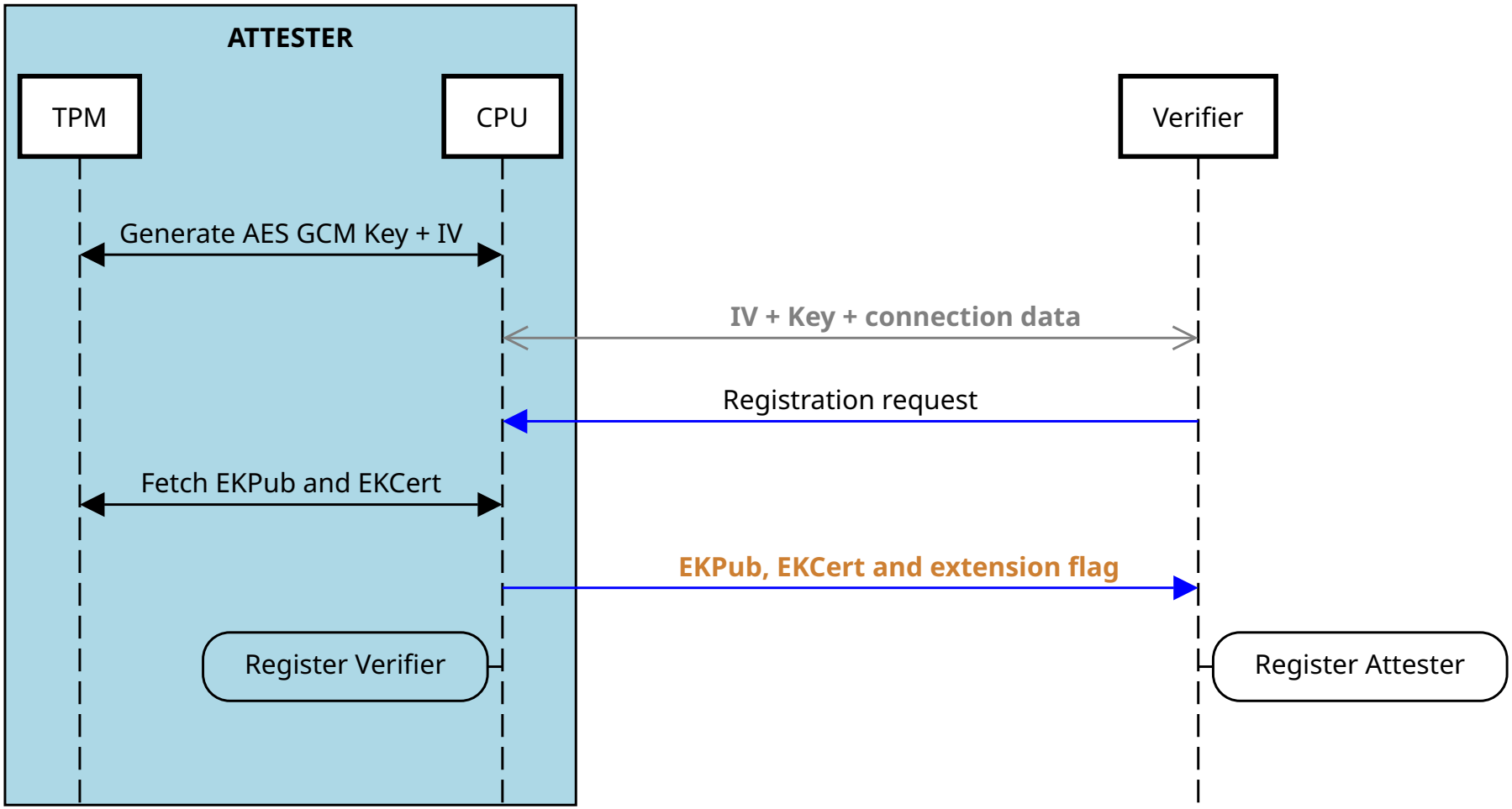
RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Ultrablue protocol

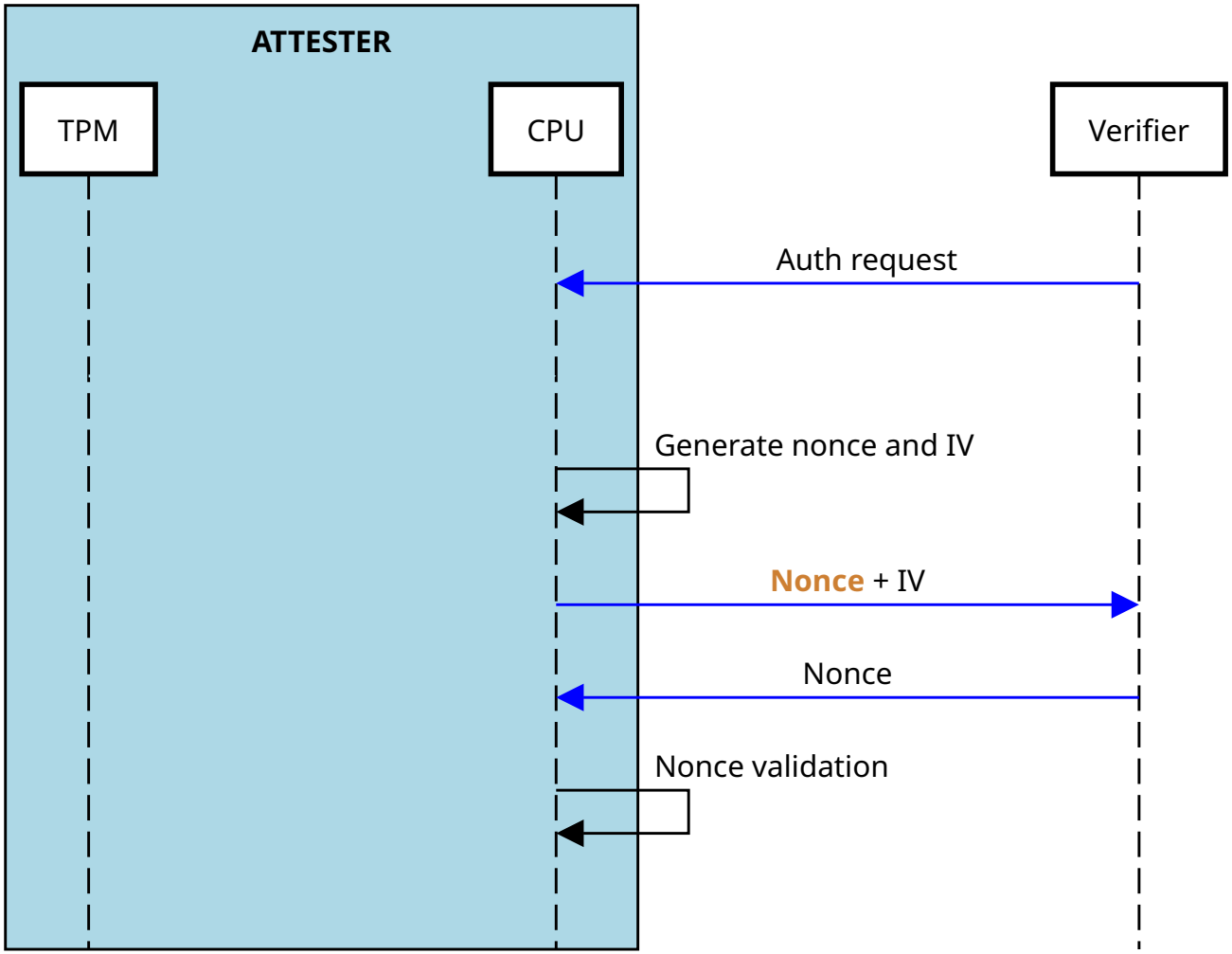
Protocol overview



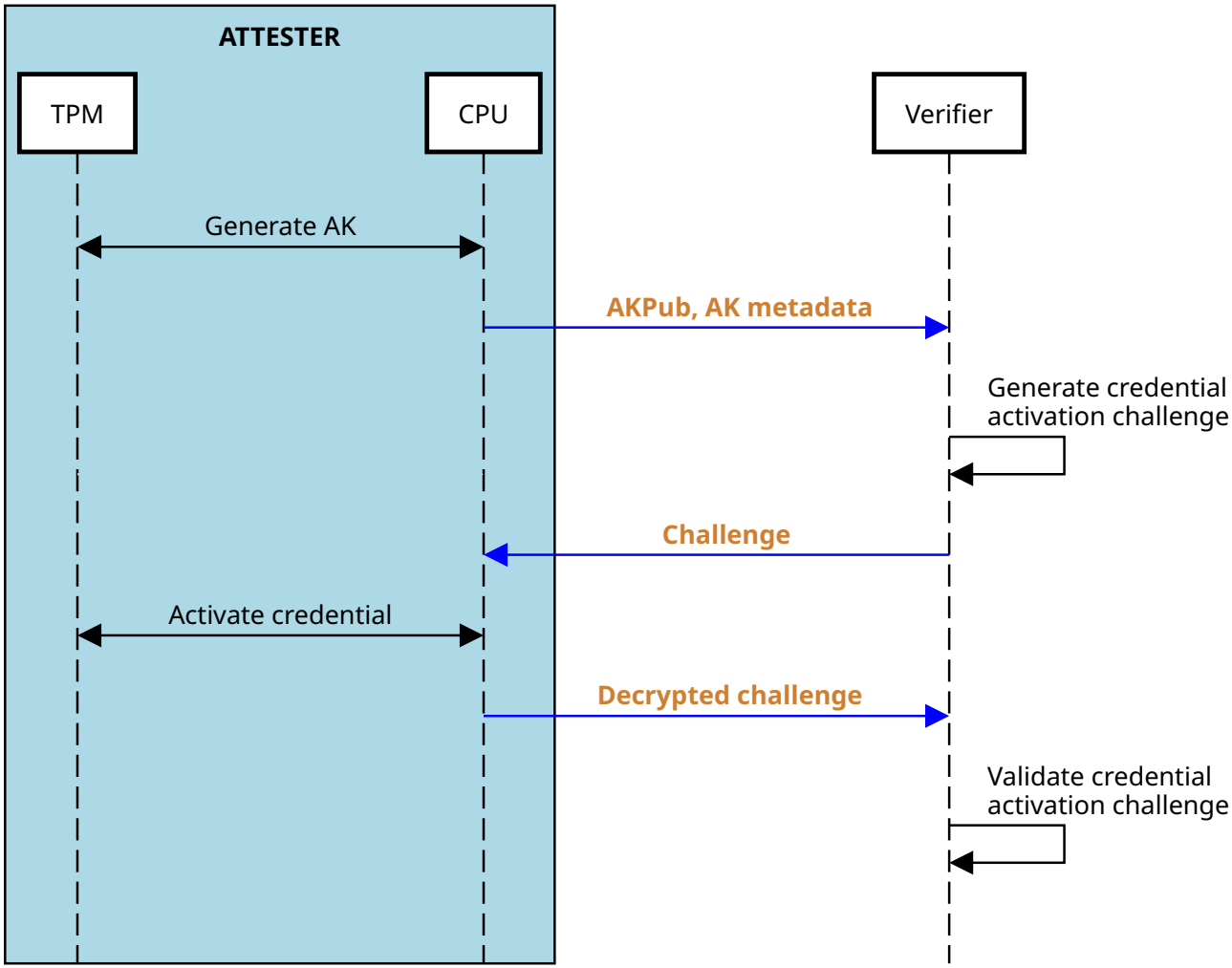
Registration – Store device and TPM identity



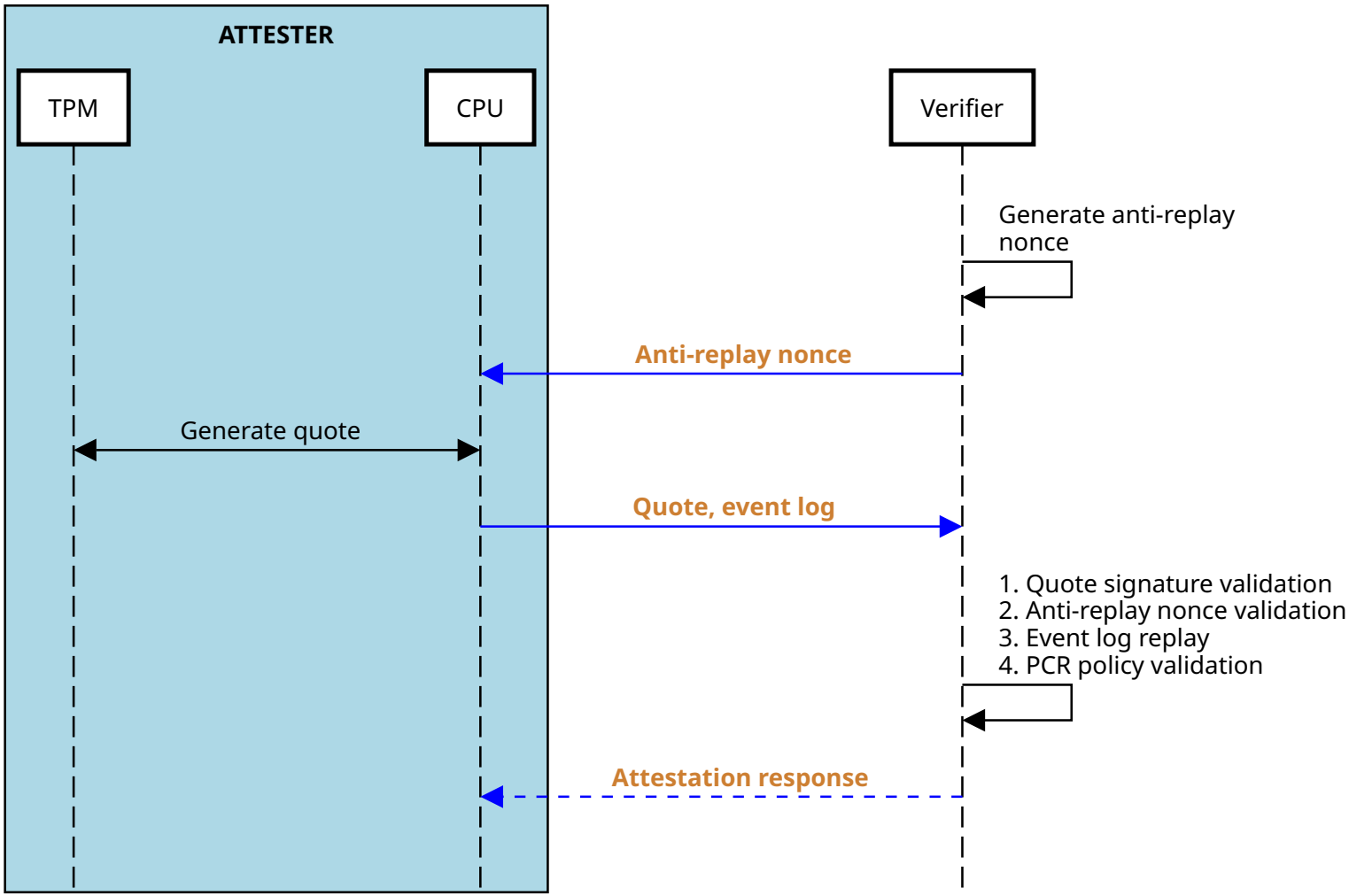
Authentication – Mitigate DoS attacks



Credential activation – Fetch Attestation Key



Attestation – Validate boot state



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

What's next?

- Get more users and contributors
- UI improvements on Android
- Clean up and publish encryption code
- Integrate with external projects to ease setup

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

https://github.com/ANSSI-FR/ultrablue