RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

Ultrablue

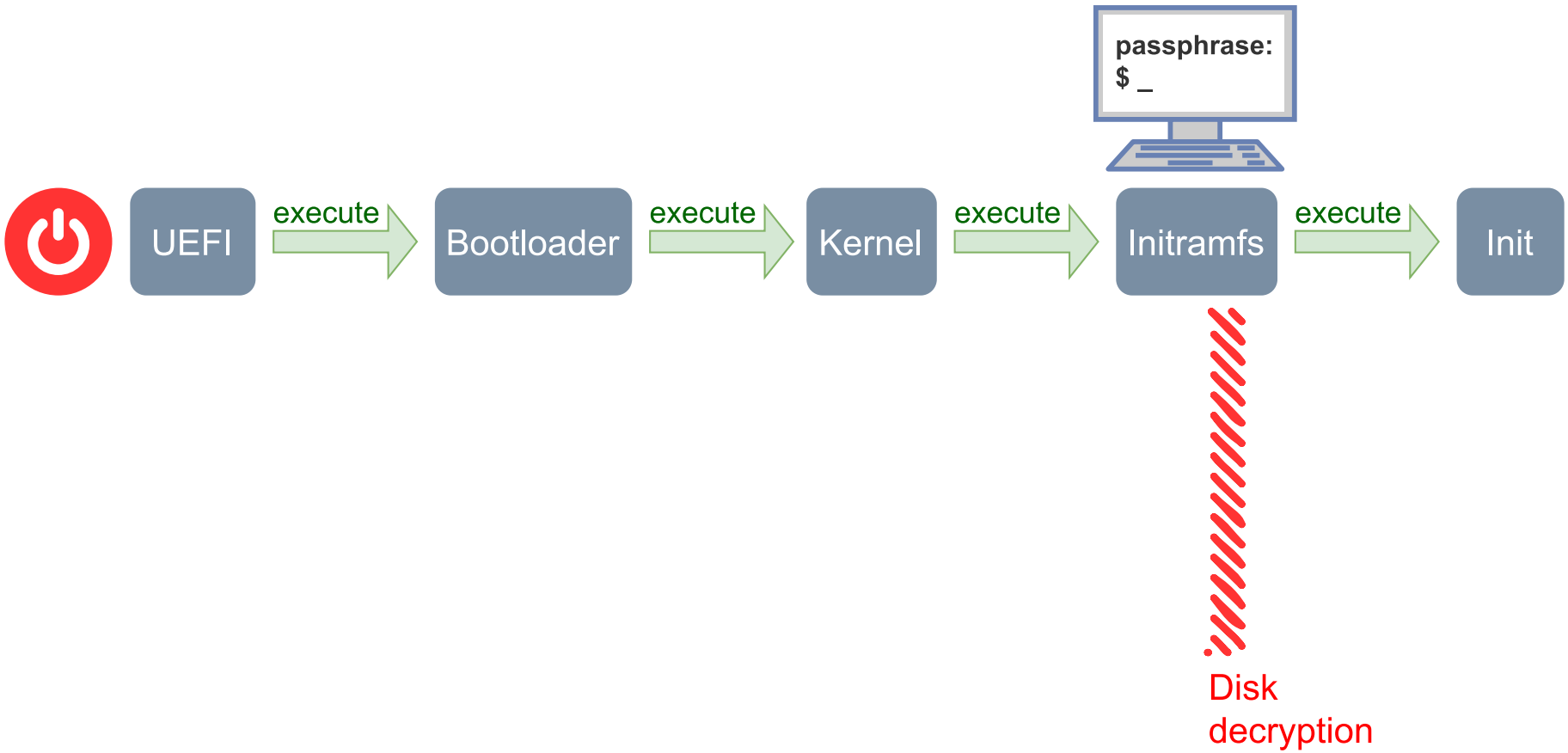
Remote attestation over Bluetooth

Gabriel Kerneis, Loïc Buckwell, Nicolas Bouchinet

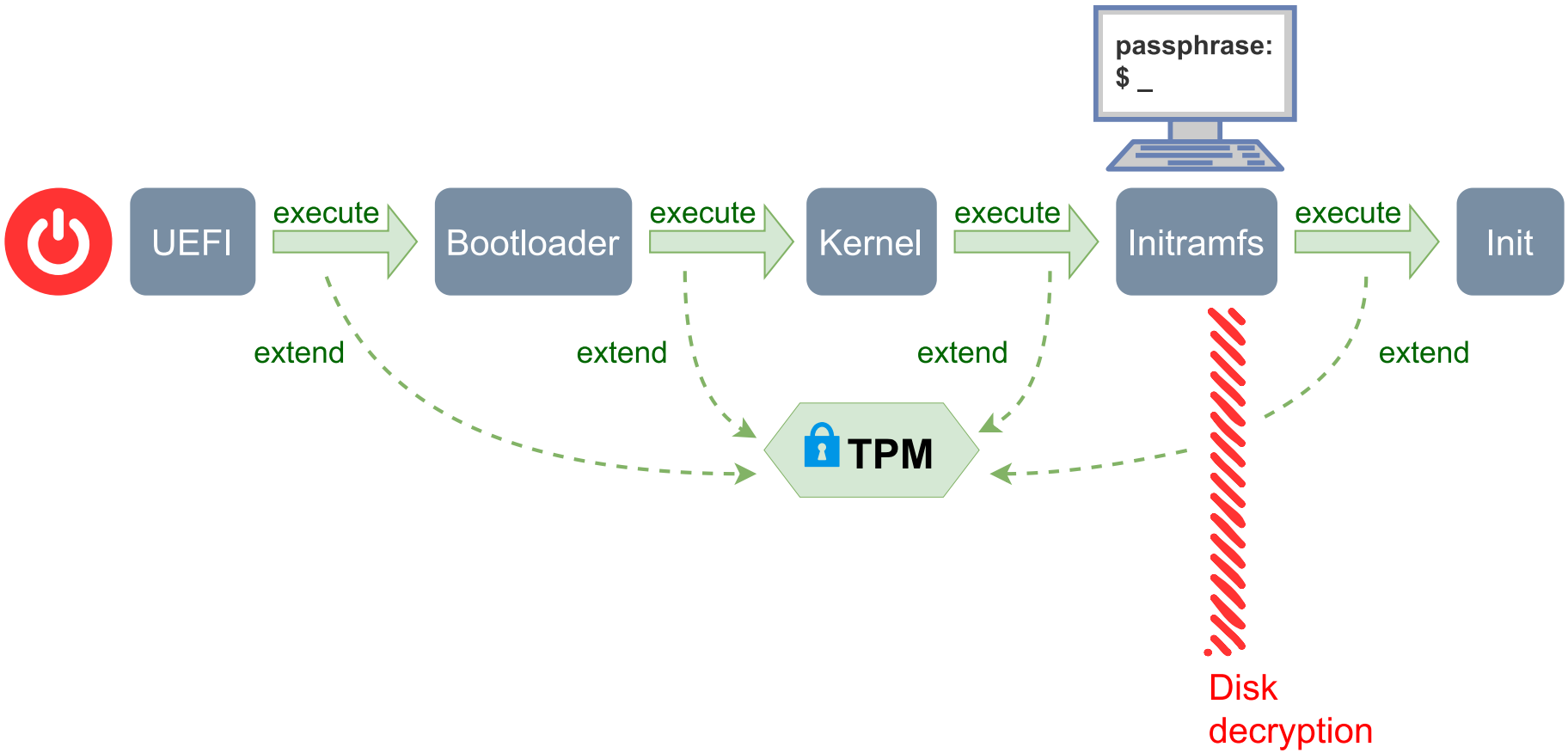
French National Cyber Security Agency

February 4 – FOSDEM 2023

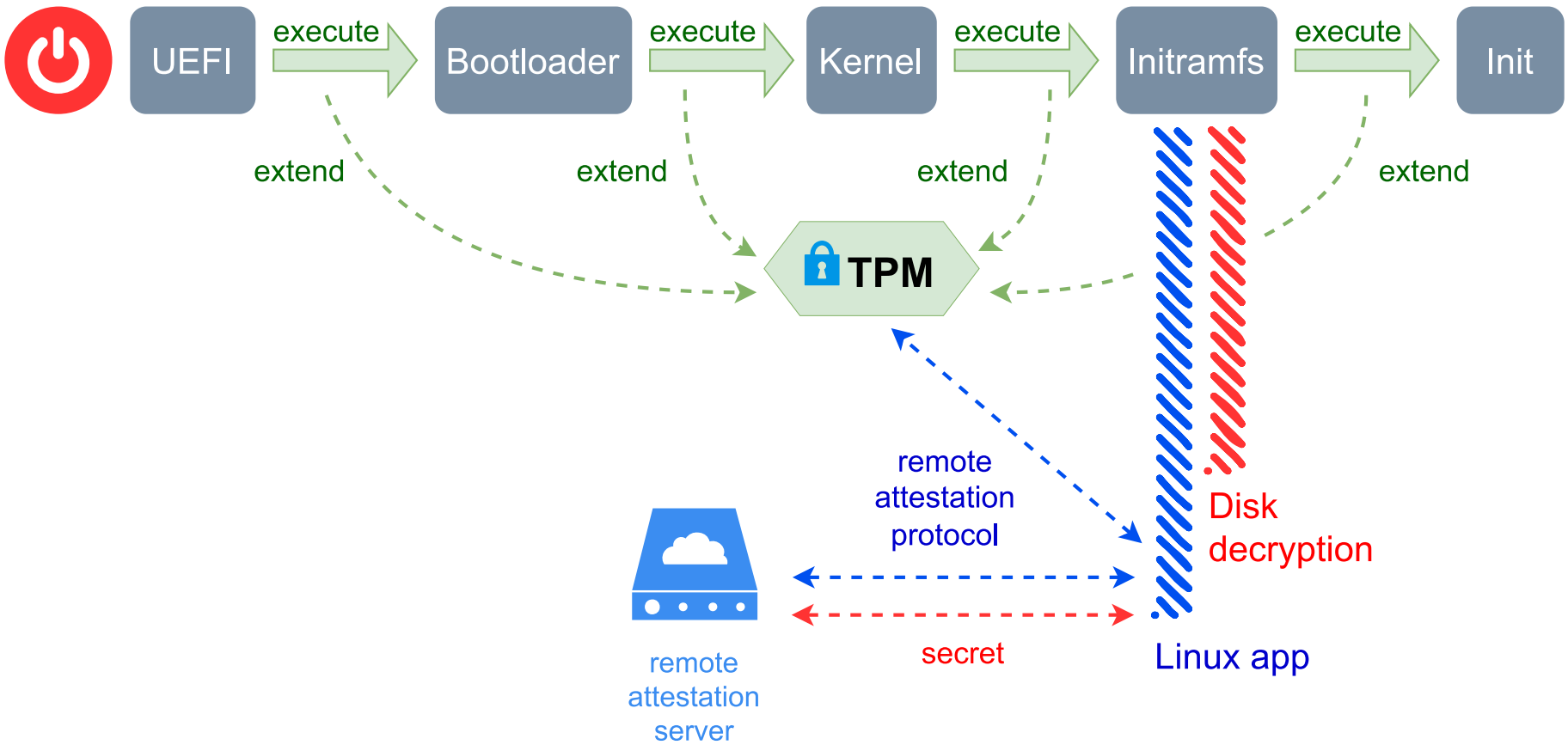
Bootchain


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

Ultrablue Stack



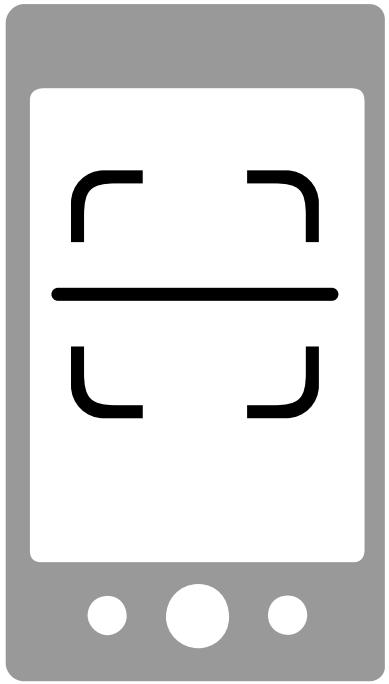





server
(laptop)

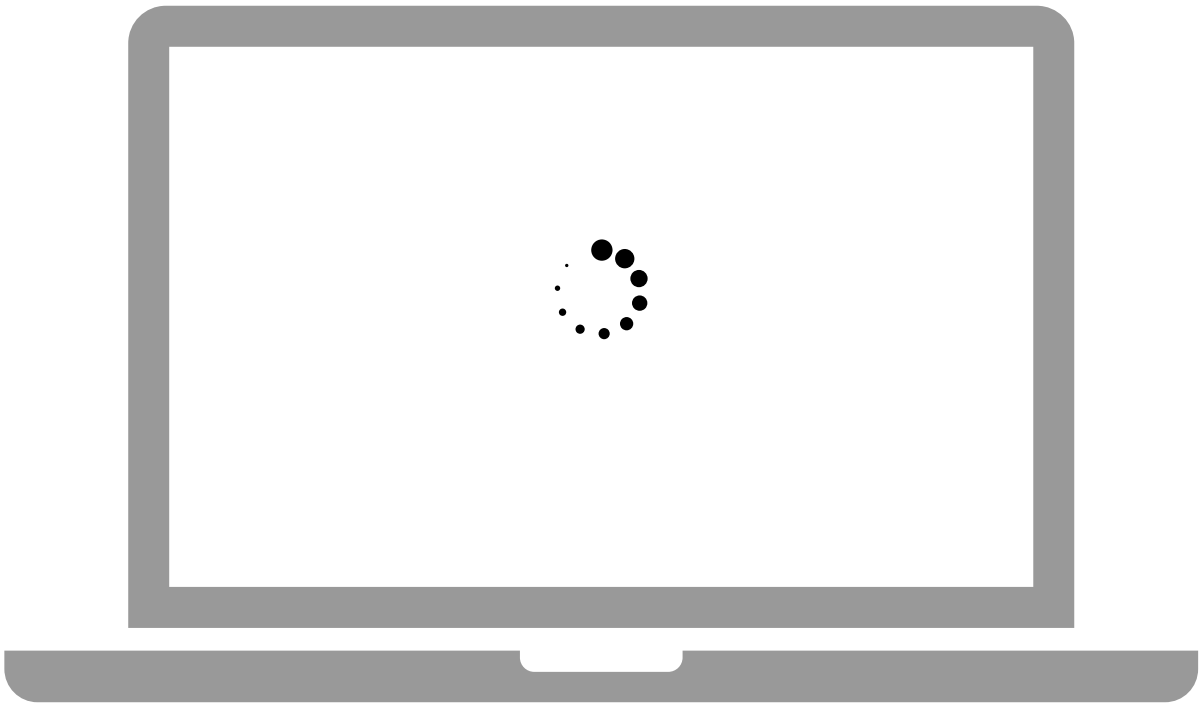
clients
(smartphone)

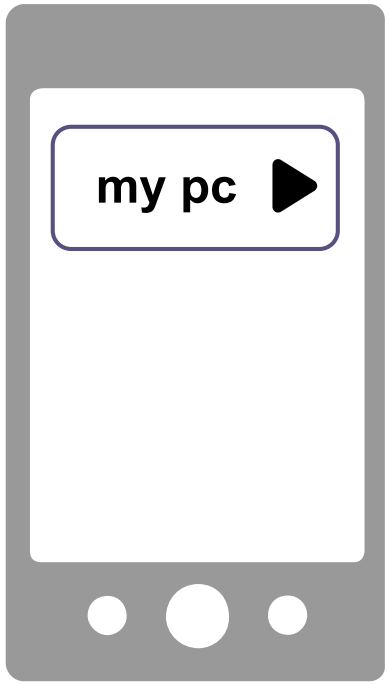
Ultrablue Workflow - Enrollment



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

Ultrablue Workflow - Attestation

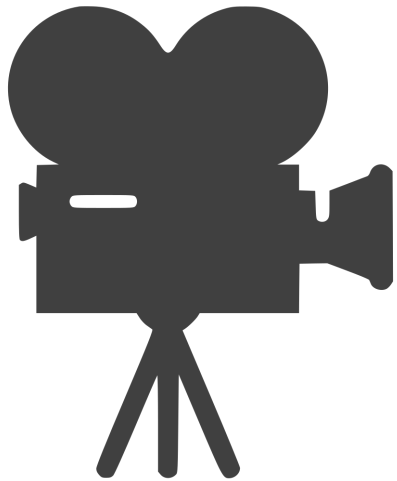




- Get new boot state
- Inspect changes easily
- Control attestation result

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Ultrablue Demo



RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

Ultrablue is versatile

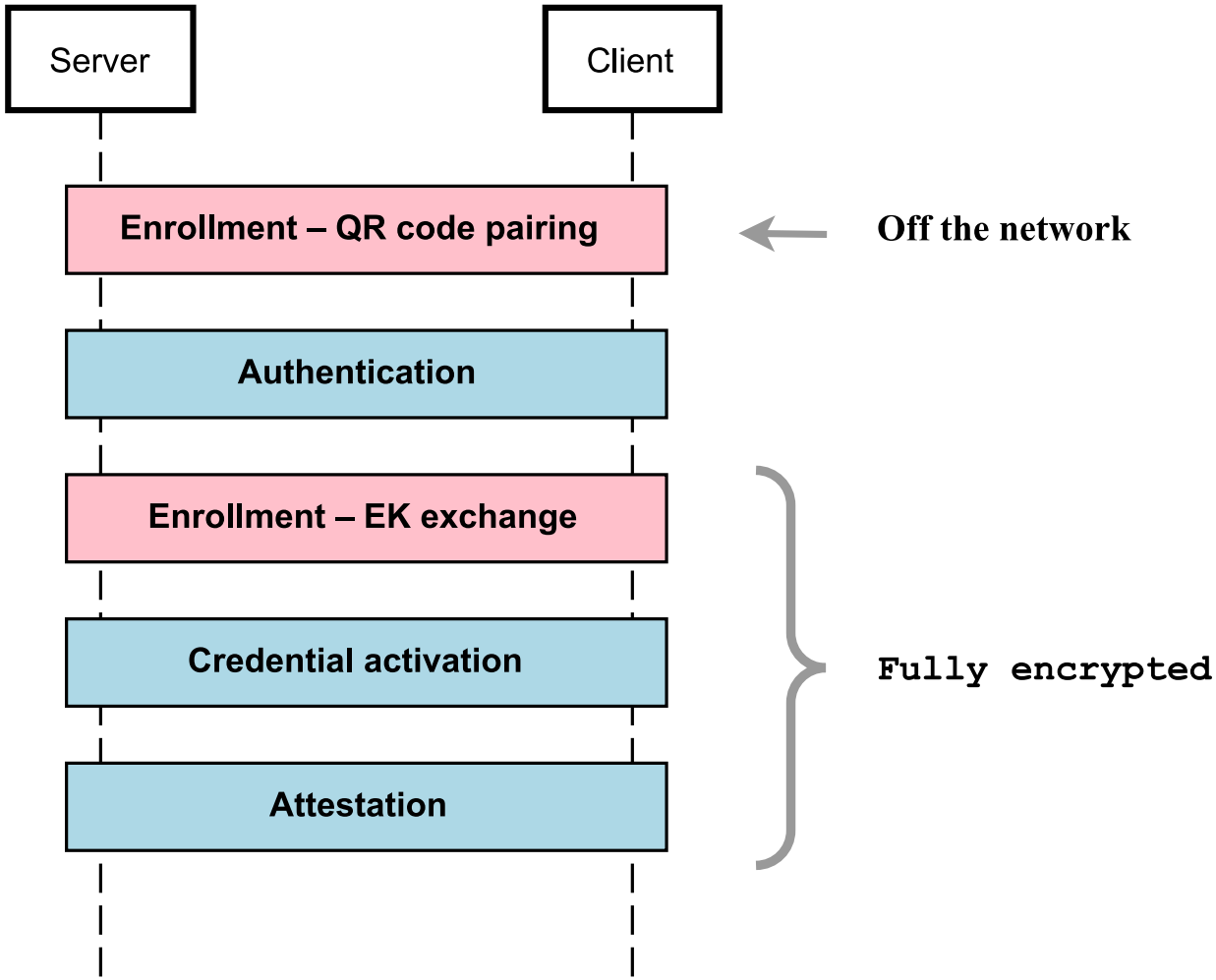
- Embeddable in initramfs, or runnable at a later stage
- Usable as a second factor for disk decryption
  (via PCR extension and LUKS TPM slot)
- Sample `mkosi` scripts to build a test VM demonstrating those features
- We welcome use-cases, suggestions and contributions!

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

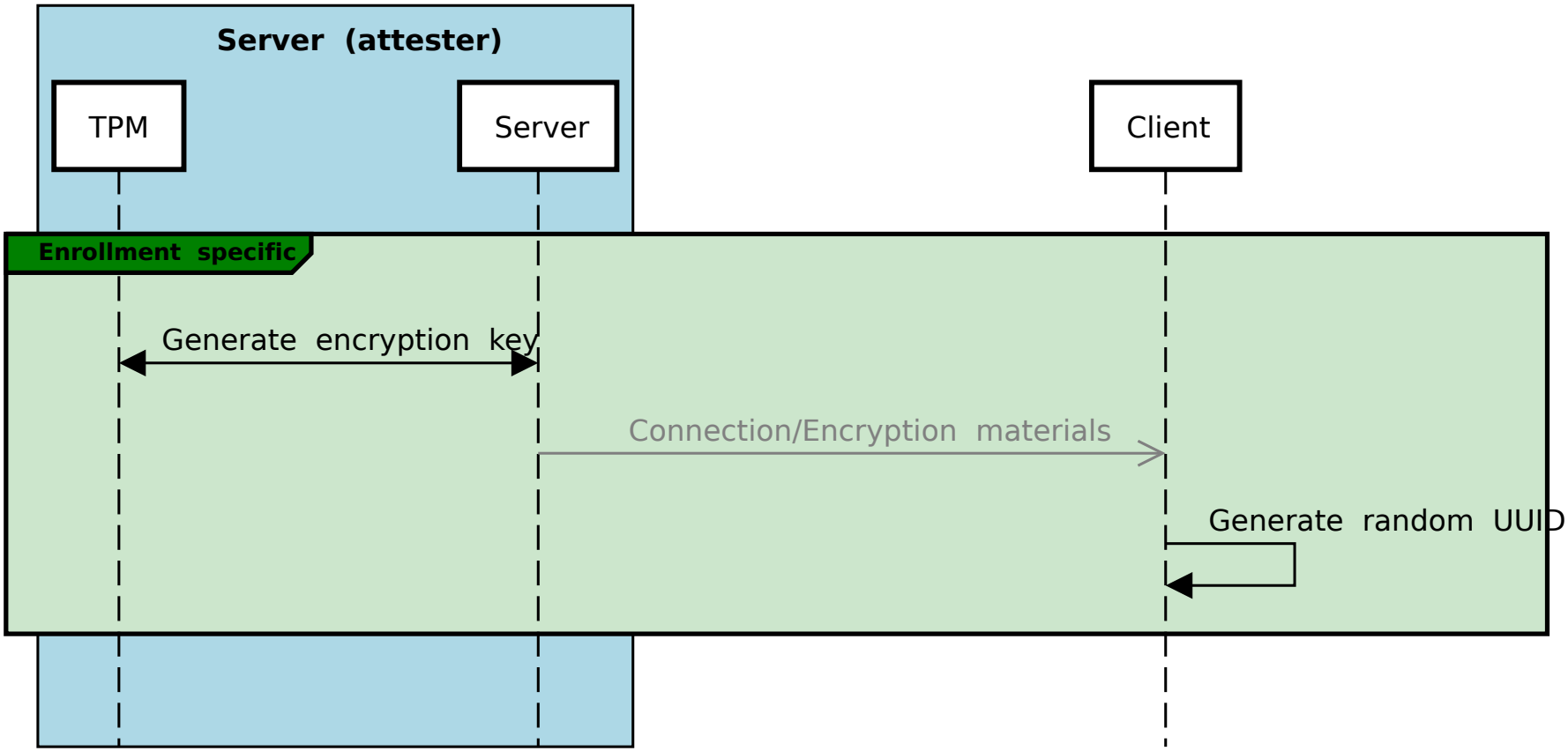
Ultrablue protocol

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

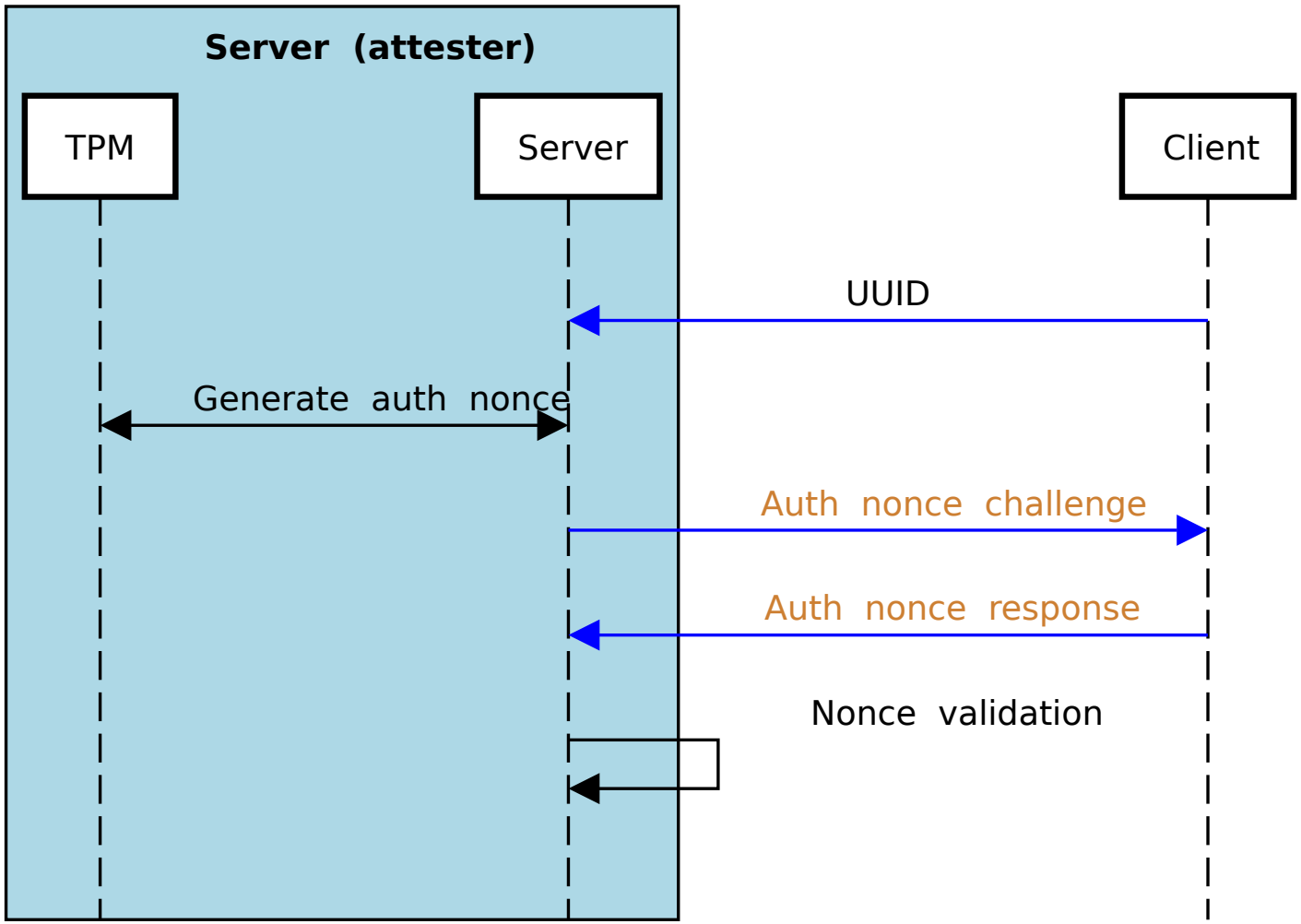
Protocol overview



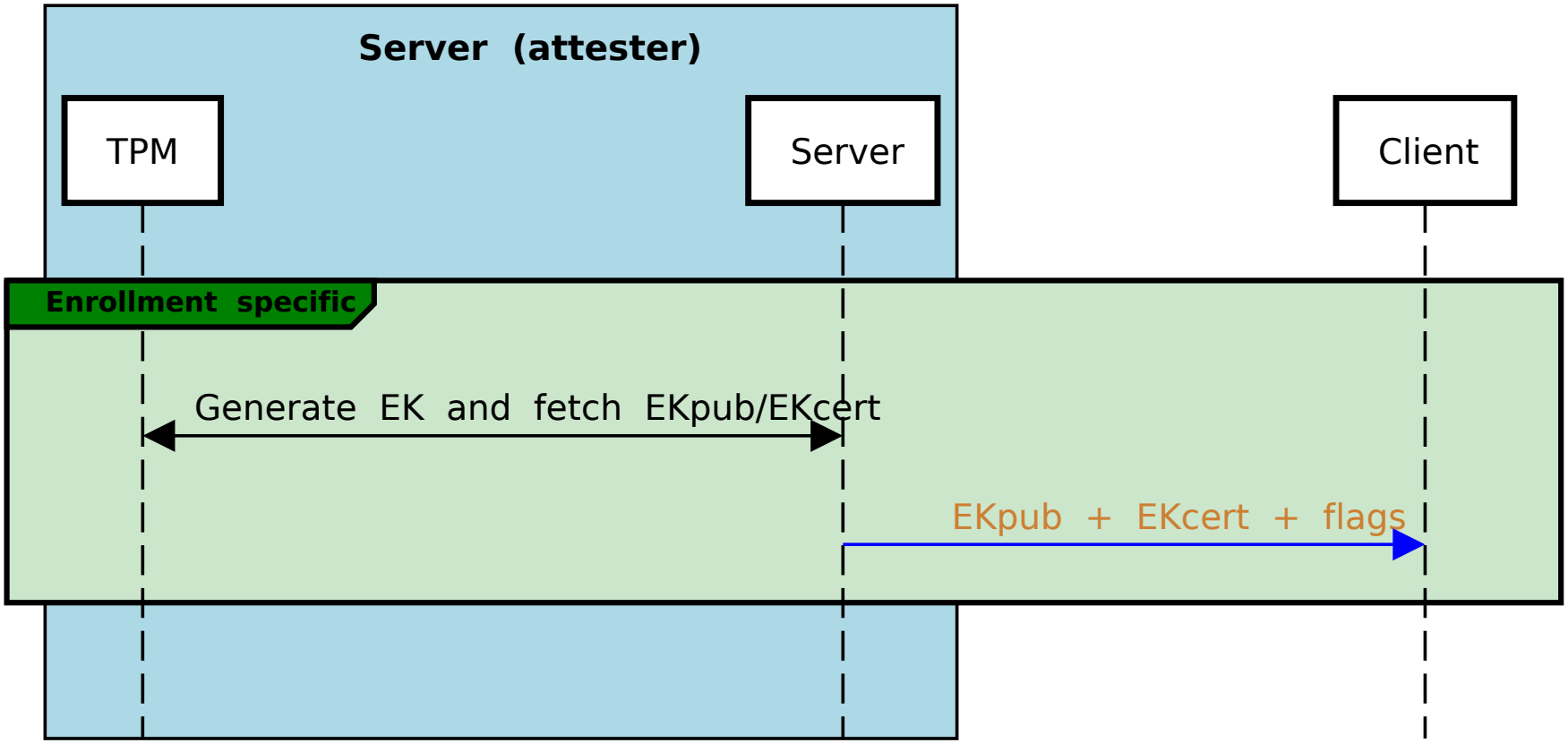
Enrollment – QR Code and UUID generation



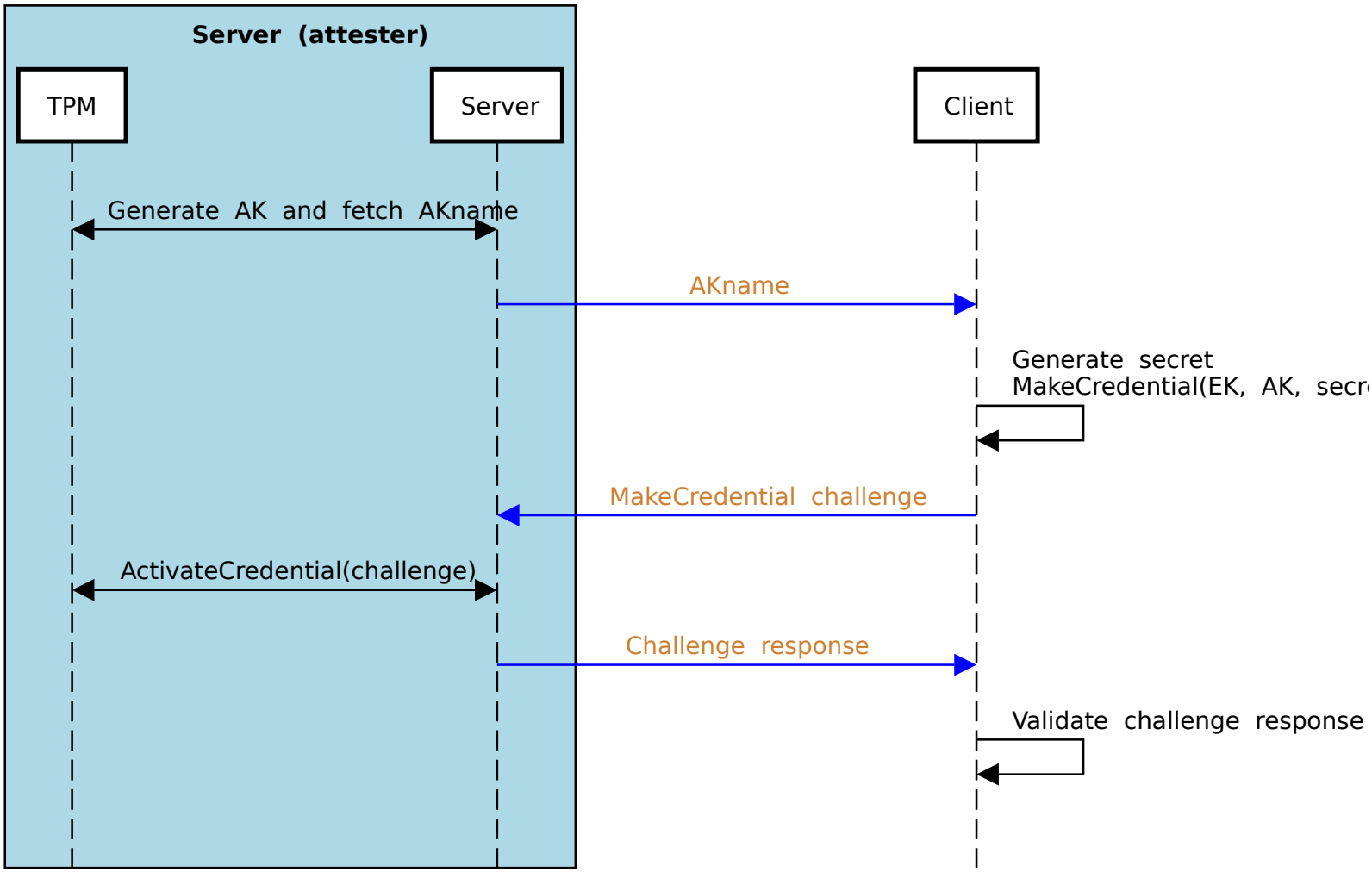
Authentication – Mitigate DoS attacks



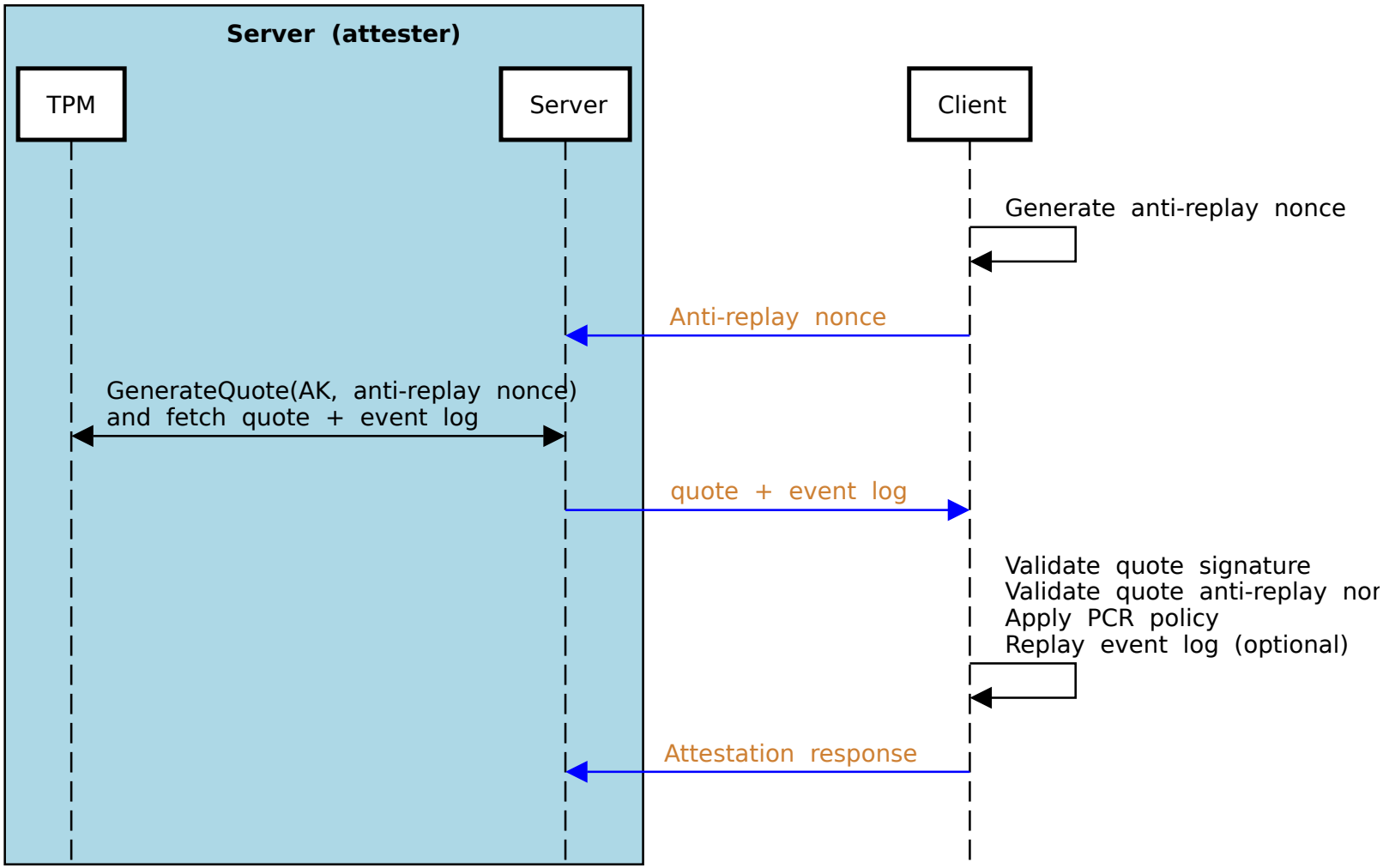
Enrollment – Endorsement key exchange



Credential activation – Generate an Attestation Key



Attestation – Validate boot state



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

What's next?

- Integrate with external projects to ease setup
- Get more users and contributors
- Test our FOSDEM release!
  github.com/ANSSI-FR/ultrablue/releases

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

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