Global Platform®

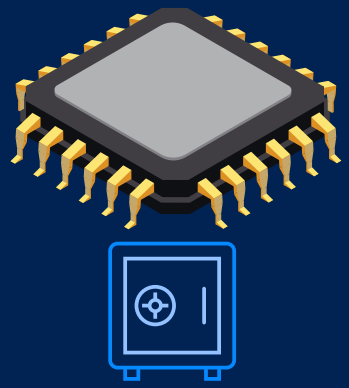
Setting the Scene for Panel on Key Management Standardisation Opportunities

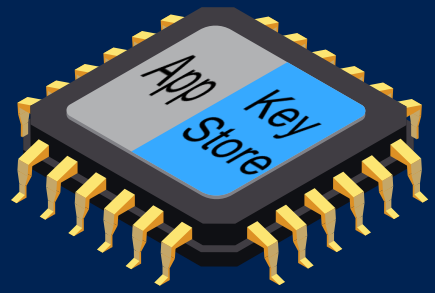
Automotive KeyStore Evolution:

MicroController
(often AutoSAR)
using a HW Element

Microcontroller
With isolated software
for key management
(MicroTEE)

Microprocessor with TEE
- Many apps / guests





Hardware KeyStore API

Software KeyStore API

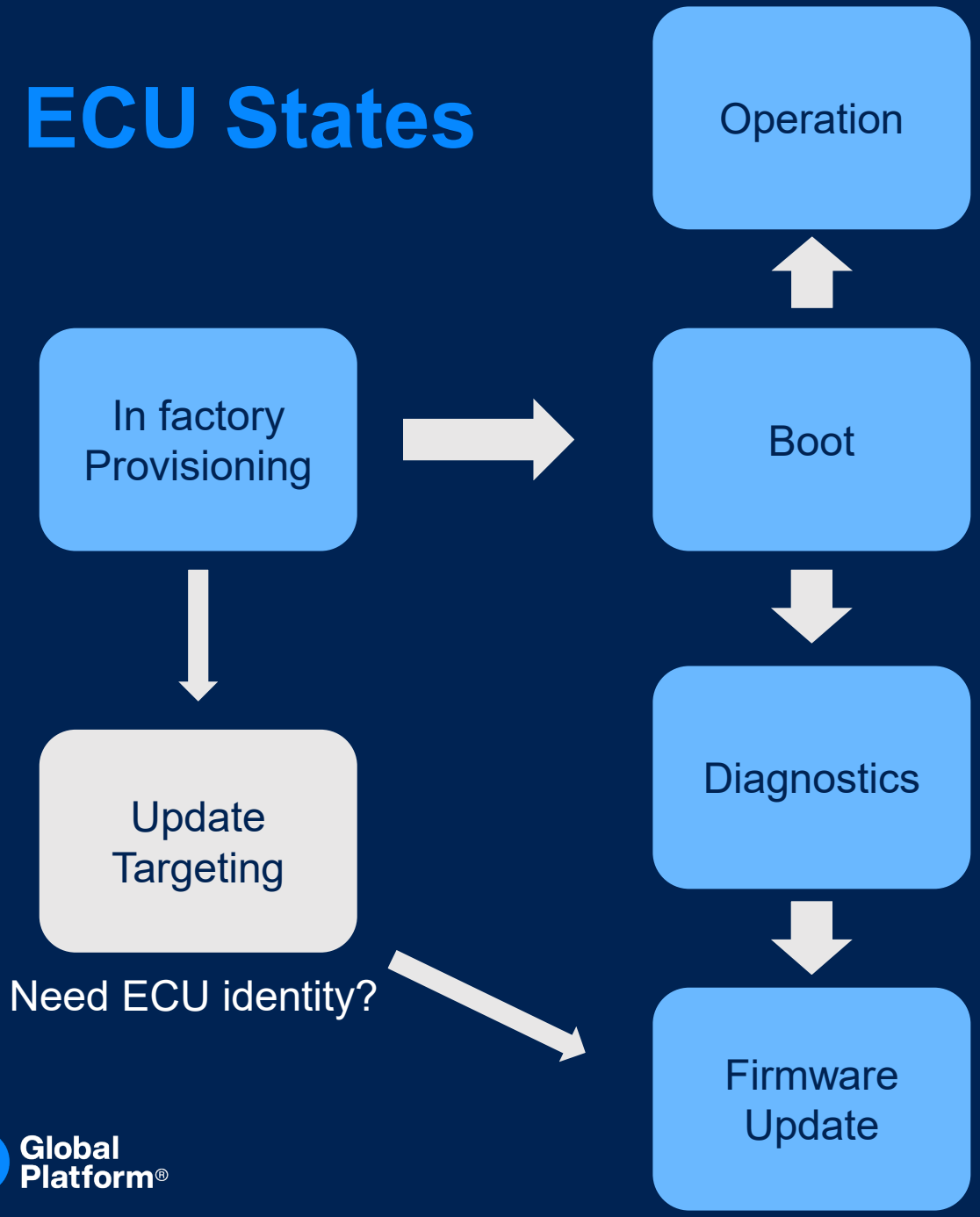
Software KeyStore API

Global Platform®

How much to standardize?

Global Platform®

ECU States



Need keys for core operations (e.g. comms)
e.g. ECUs on CAN need same CAN MAC key

Need to validate image is correct
HMAC(Image + ECU Key) → MAC

Need to “unlock” diagnostics
(Limited trust)

Need to validate new image
PKI? PQC?

Global Platform®

Securing the digital future

→globalplatform.org