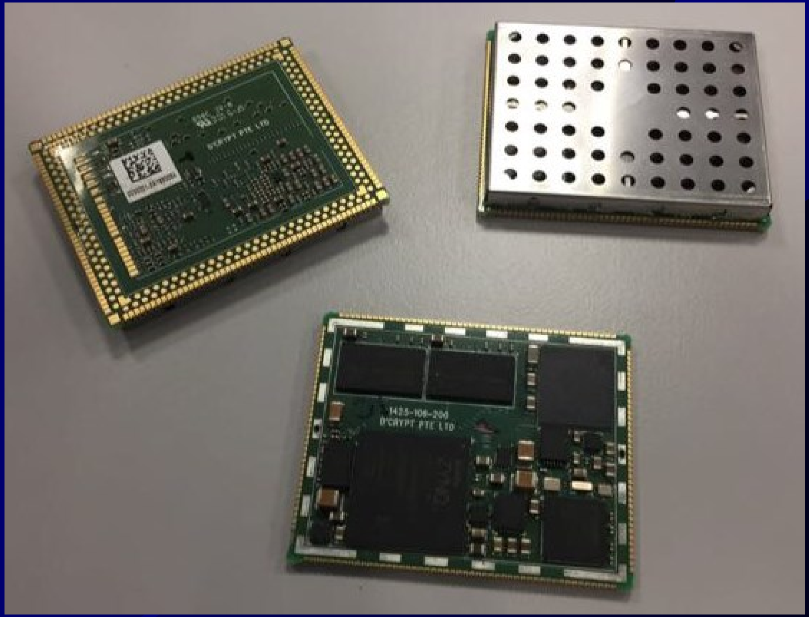
V2X ECDSA in TSM

The material presented in this document is Confidential and Proprietary to
D’CRYPT PTE LTD and must not be reproduced in whole or in part or disclosed
to any third party without the prior written consent of the Company.

TSM

Trusted Security Module

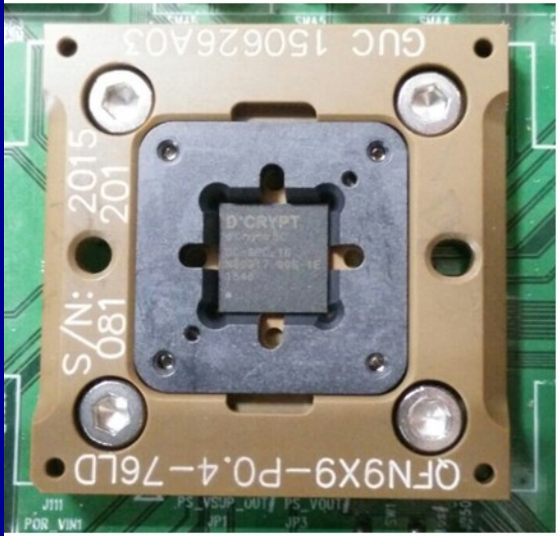
- Consist of a SoC-FPGA and eHSM (*d'Cryptor SC*)
  - SoC-FPGA handles application processing and connectivity
  - *d'Cryptor SC* handles cryptographic processing.



The material presented in this document is Confidential and Proprietary to
D'CRYPT PTE LTD and must not be reproduced in whole or in part or disclosed
to any third party without the prior written consent of the Company.

d’Cryptor SC

Single Chip Level-4 Cryptographic Core for TSM

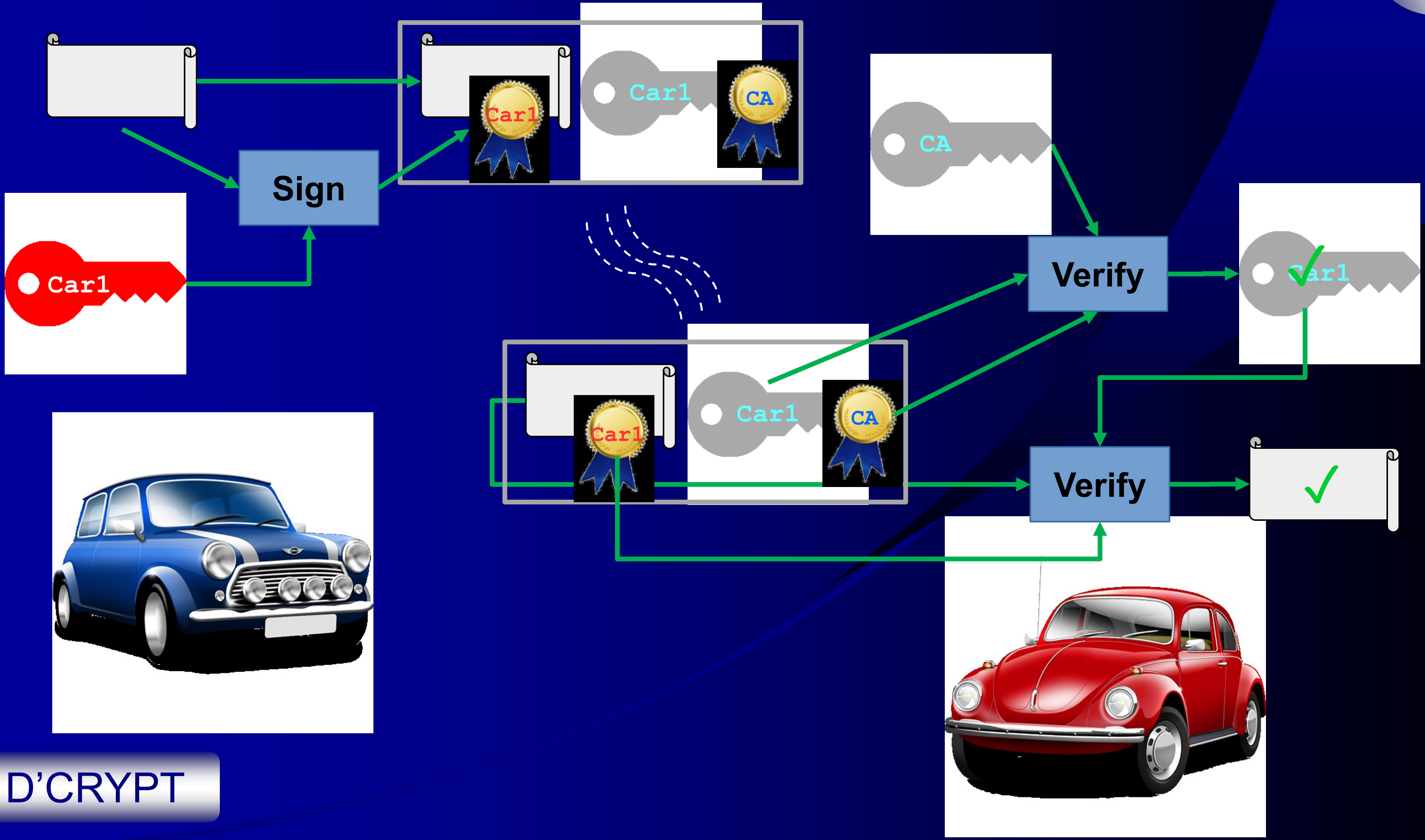


d’Cryptor SC in a test-socket

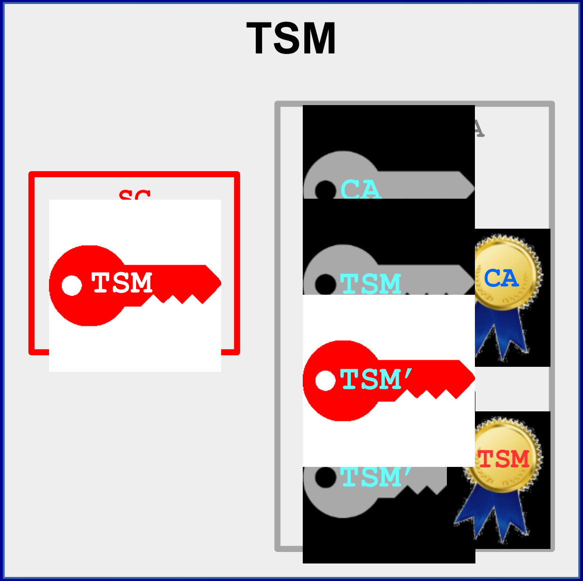
9×9mm QFN package

The material presented in this document is Confidential and Proprietary to
D’CRYPT PTE LTD and must not be reproduced in whole or in part or disclosed
to any third party without the prior written consent of the Company.

V2V Message Authentication

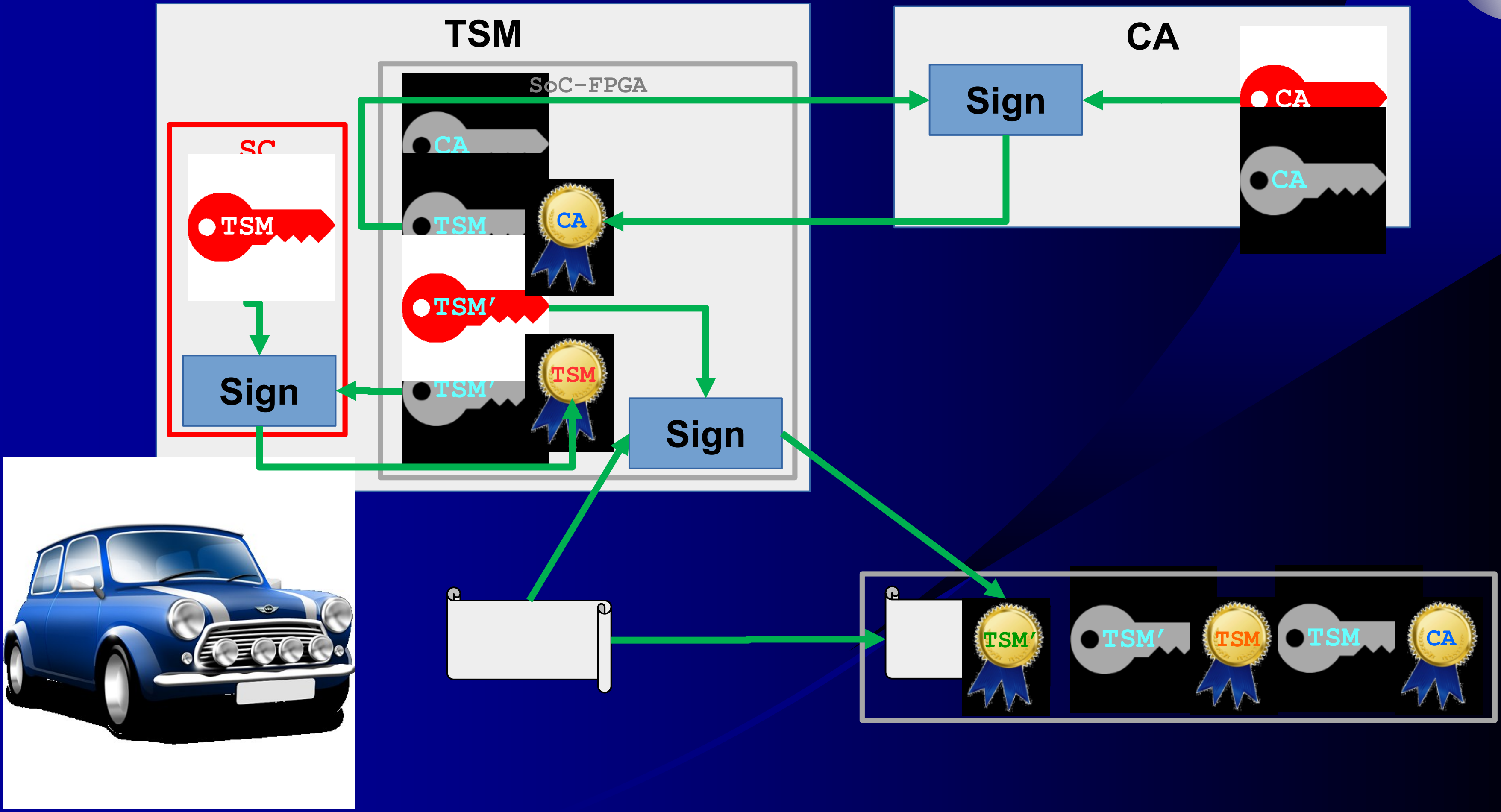


V2X ECDSA Requirement

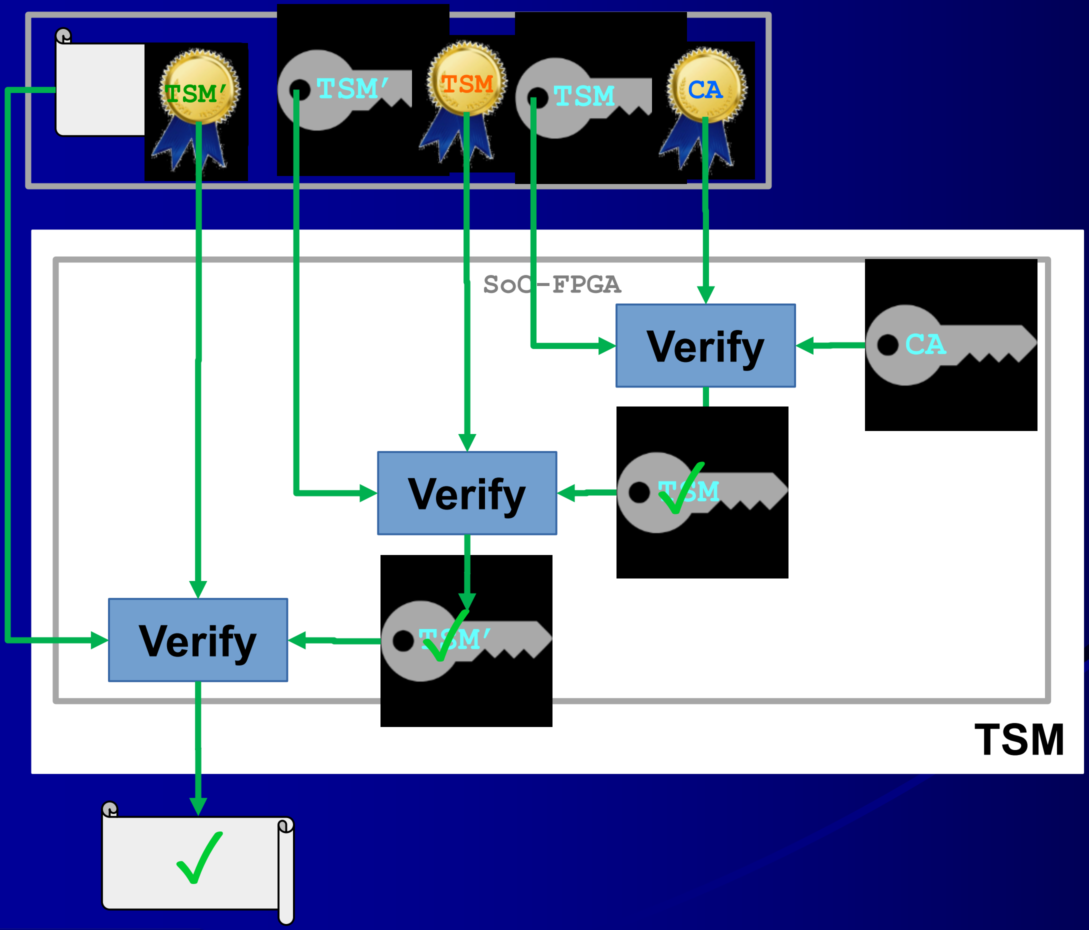


- 20 TX/sec → 20 signs/sec
- 200 RX/sec → 400 verifies/sec
- SC is not able to process at such high rate.
- ECDSA signing and verification move into FPGA fabric using ephemeral key-pair.
  - Additional key-pair brings verification to 600 verifies/sec

Signing with Ephemeral Key



Verifying with Ephemeral Key



D’CRYPT