

Certificate

Statement on CC EAL5+ Certification of ATC4096- MP312

1 ATC4096-MP312 component description

Hardware The LEGIC advant crypto transponder chip ATC4096-MP312 is based on the MF3Dx2 (NXP DESFire EV2), a Common Criteria (EAL5+) certified product.

This contactless smart card chip is compliant to the ISO 14443 A specification and is supporting 3DES and AES algorithms for authentication and data encryption. It also supports an ISO 7816 compliant file system.

Security Level Configuration The ATC4096-MP312 complies with the settings defined within the evaluation certificate and uses the MF3Dx2 in the following security level configuration:

- Mutual authentication with 112 bit 3DES key / algorithm
- Data encryption with 112 bit 3DES or 168 bit AES key / algorithm
- Message integrity with secure MAC

2 References

Certificate The certificate granted by the German Federal Office for Information Security and the corresponding evaluation documents are available on <https://www.bsi.bund.de>.

- Product descriptions**
- Data sheet - ANSSI-CC-2016/32 MIFARE DESFire EV2 - 26.05.2016
 - Data sheet - MF3D(H)x2, Rev 3.1 - 17. May 2018, document number: 364231 *
 - Product Description - Crypto Transponder Chip ATC2096-MP312, document number: LA-23-540a - 05.2019 **

* Available through NXP Semiconductors

** Available on the LEGIC Extranet