Certificate

Statement on CC EAL4+ Certification of ATC4096-MP311

1 ATC4096-MP311 component description

Hardware The LEGIC advant crypto transponder chip ATC4096-MP311 is based on the MF3ICD81 (NXP DESFire EV1), a Common Criteria (EAL4+) 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-MP311 complies with the settings defined within the evaluation certificate and uses the MF3ICD81 in the following security level configuration:

- Mutual authentication with 112 bit 3DES key / algorithm
- Data encryption with 112 bit 3DES or 128/256 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 – MF3ICD81 MIFARE DESFire EV1, Rev. 3.6 – 9. Feb. 2011, document number: 134036 *
- Data sheet – MF3ICD81 Guidance, Delivery and Operation Manual, Rev. 3.9 – 26. May 2011, document number: 146939 *
- Product Description – Crypto Transponder Chip ATC2096-MP311, document number: LA-23-530g – 11.2011 **

*   Available trough NXP Semiconductors
** Available on the LEGIC Secure Extranet