Hardware with Security Boxes Evaluations

Applus+ Laboratories provides evaluation services of security boxes for most of their industry applications. Our services include both, accredited evaluations for certification schemes and independent evaluations.

Security boxes are hardware products responsible to capture, protect and transfer data in secure way. Their security functionalities rely mainly in the box that protect the hardware against physical attacks.
Security boxes can also incorporate additional countermeasures such as the use of protections in hardware, processors and secure boots, keys and software countermeasures, and, for further protection, the product can be safeguard in a secure physical environment such us a bunkers or a protected room.

Wide ranges of IT products used in multiple industries are in fact security boxes

- Smart Terminals for payment, health, access control, transport, amongst others.
- HSM for payment, health, digital signature (eg. eIDAS) , intelligent networks, amongst others
- Smart meters for water, gas and electricity utilities
- Tachograph components: vehicle units, motion sensors, external GNSS facility
- Security connectors for healthcare: E-Health-Konnektor
- Drones
- Other applications

SECURITY AND FUNCTIONAL EVALUATIONS

Due to the type of markets they operate and sensitivity of the data stored and transferred, most secure boxes, and their components that manage security functionalities, must be evaluated following a certification scheme, either sectorial or

generalist.
Even when there is no mandatory certification for a specific industry application, independent security evaluation are a key element to enhance end-client trust in the security of the product.
Applus+ Laboratories has an engineer team experienced in security and functional evaluations on security boxes, hardware, software and communication protocols.

Security Evaluations for a Certification Scheme Applus+ is a security lab accredited to evaluate hardware with security boxes for various certification schemes with international recognition. Depending of the sector, the device must be evaluated for one or more certification schemes, which may include a security and/or a functional evaluation.

- Common Criteria**:** CC is a Certification scheme based on seven Evaluation Assurance Levels (EAL), applicable to all types of security boxes and recognized in most countries as the benchmark certification for IT security. Applus+ Laboratories is accredited to conduct evaluations of security boxes up to EAL 7, as it is recognized by SOGIS for the Security Boxes technical domain.
- Common.SECC: This Certification is exclusive for the payment terminals aimed at the German and UK markets. The evaluation uses the Common Criteria methodology and its protection profiles but the certificate is issued by the Common. SECC. Applus+ meets the two conditions to evaluate security boxes under for Common.SECC, to be an accredited lab for the Hardware with Security Boxes technical domain and be an active member of the working group JTEMS.
- Payment Schemes: Most payment schemes require a functional evaluation for terminals. Applus+ Laboratories is accredited to conduct functional testing form the following payment schemes: EMVCo, Visa, Amex and Discover.

Independent security evaluations for security boxes: In those cases where the certification is not mandatory, the vendor can opt to pre-evaluate or evaluate the security and functionality of the product with Applus+ in order to offer assurances to the final client. Our independent evaluations are tailored to each type of component and use case, and can be adapted to the client needs.

Note: Because Applus+ Laboratories is accredited as a third party laboratory by several evaluation and certification schemes, and in order to guarantee its impartiality, Applus+ engineers are never involved in actual product development or solutions implementation.