



Evaluation Laboratory



Evaluating the Security of your Products and Solutions

When developing a new security-sensitive solution in the area of banking, mobile telephony, Pay TV or transportation, a key is to adopt the right methodology to ensure that security objectives are met.

Gaining assurance – before deployment – that the product is robust enough to face state-of-the-art attacks is also of significant value.

Trusted Labs helps you reach these goals by offering evaluation services around a three-step approach: architecture review, design review, testing.

Why call on Trusted Labs?

- The expertise at Trusted Labs' evaluation laboratory is built upon industry-leading standards and technologies such as MasterCard CAST, PCI PED, Java Card™, GlobalPlatform, OMTP, mobile payment security, and mobile Java security.
- Beyond merely helping our customers conform to standard security requirements with a pass/fail report, Trusted Labs aims to guide developers and designers to improve their product.
- Trusted Labs wants to ensure that developers and designers understand the security issues and the background behind standard security requirements, so they are themselves able to design the security mechanisms that fit their product. The aim is to help customers increase their skills in security. Trusted Labs' whole methodology is built around this principle.
- Trusted Labs has years of experience in building evaluation schemes, with associated process and security technical requirements.
- Trusted Labs also benefits from its TL SAT tool featuring a unique technology for the static analysis of Java applications.

Who benefits from these services?

- Operators, wishing to build certification requirements and assess the security of their suppliers' products.
- Developers of security software or hardware solutions wishing either to pass a standard certification, or to benefit from a third-party security analysis with security recommendations and report that can be provided to their customers.

Description of the service offering

- Security evaluation process design (Certification process definition, implementation guidelines definition), for mobile operators, pay TV operators, banking operators.
- Security training: Java Card™ (security & performance), GlobalPlatform, PCI PED, STIP, MasterCard CAST.
- Security architecture review: based on documentation review and interviews with designers in order to assess the security of a product at an early stage of the design.
- Source code security review: automated or not, with recommendations for improvements.
- Software testing: robustness testing and software attacks complementing source code review.
- Physical testing.

References

- SFR: security audit of mobile applications.
- MasterCard CAST: Java Card™ evaluations of numerous platforms and applications.
- MasterCard CAST: evaluation of mobile payment solutions.
- EMVco, VISA, Mastercard: writing security guidelines for payment applications.
- Texas Instruments, Viaccess: security evaluations of hardware architectures.