Smart ticketing, *enabled by* ITSO

## ITSO SAM certification to the security assurance “Common Criteria” (CC) evaluation standard EAL4+, Protection Profile 9911

*Certificate (2005/38) issued by DCSSI, 24th November 2005*

The CC standard is a multipart framework that is used as the basis for the evaluation of security properties of IT products and systems in market sectors such as the Military, Aerospace and Finance industries worldwide.

Within each of these industries there are specific product “protection profiles” that are internationally recognized as applicable to particular products. For Smartcard based products, the relevant Protection Profile for the ITSO SAM is designated PP9911, which includes the silicon, the underlying Operating System, and the Application.

In completing the certification process using the appropriate Protection Profile, you are gaining approval by an independent and recognized authority that your entire product is as secure as you need or claim it to be.

The Common Criteria standard (currently at v2.2) harmonizes several older security assurance standards, namely ITSEC (The European Information Technology Security Evaluation Criteria), CTCPEC (Canadian Criteria) and US Federal Criteria (FC) into one Common Criteria for Information Technology Security Evaluation (CC) and for stating security requirements in a standardized way. Increasingly it is replacing national and regional criteria with a worldwide set accepted by the International Standards Organization in ISO15408.

By establishing such a common criteria base, the results of an IT security evaluation are meaningful to the widest audience as CC enables comparability between the results of independent security evaluations. It does so by providing a common set of security requirements and assurance measures.

The evaluation process establishes a level of confidence that the product meets these security requirements and as such helps consumers to determine that the IT product or system is secure enough for its intended application. The CC addresses protection of information from unauthorized disclosure, modification, or loss of use although it may also be applicable to aspects of IT security outside of these three.

The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The CC concentrates on threats to that information arising from human activities, whether malicious or otherwise, but may apply to some non-human threats as well.

CC security evaluations are performed by independent, Evaluation Facilities (CLEF) licensed by an appropriate Certification Body (CB). For the ITSO SAM, the evaluation was carried out by CEACI (Thalès Microelectronics – CNES [Centre National D’Etudes Spatiales] ), at the THALES Microelectronics evaluation center based in Toulouse and the Certification Body is the DCSSI (Direction Centrale de la Securite des Systemes d’Information), a French Government organization that reports to the National Defense General Secretary. Both organisations have long experience in this field and among many other projects were responsible for the successful CC certification of the Atmel secure microcontroller platform upon which the ITSO SAM is based.

CC has a range of Evaluation Assurance Levels from 1 to 7 where, simplistically, the higher the number, the more rigorous (and consequentially more expensive) the evaluation process required to gain certification. For example, EAL1 the lowest level is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. EAL7, the highest level, is applicable to the development of security implementations for applications in extremely high-risk situations and/or where the high value of the assets justifies the significantly higher costs involved in performing the evaluation. Practical application of EAL7 is currently limited to a small number of highly specialist implementations due to the nature, formality and cost of the evaluation process. In other words you may produce the most highly secure product available but it may be so expensive to produce that it does not make commercial sense to bring it to market.

EAL4, which is the assurance level chosen for the ITSO SAM, permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices. EAL4 is one of the most popular Evaluation Levels within the smartcard industry and has been used for the certification of many banking smartcard products such as EMV.

It was considered that, as ITSO is already a fully accounted environment, there would be no significant extra level of comfort and therefore return on investment to attempt higher than EAL4 for the ITSO SAM.

In addition to the EA level there is also a Strength of Function requirement, which is either Standard or High. This relates to the tests that will be performed to try to crack the security of the product. The ITSO SAM Strength of Function is chosen to be High.

To achieve a CC certification is a highly detailed process where the product, including all its design documentation, is reviewed and tested by the CLEF to ensure that it meets the security assurance level being sought. Such an undertaking can typically last 1 to 2 years.

The deliverables which are provided to the CLEF evaluators range from high-level documentation describing a summary of the security functionality, to detailed trace logs of each line of source code cross-correlated to its functional requirement. There are a significant number of such deliverables required for the process, all of which are independently verified by the CLEF. The CLEF must have the ability to independently rebuild, compile, execute and retest the implementation as well as verifying all of the claims made regarding the product's security.

The process for the evaluation is continual in that each deliverable is provided to the evaluator during the design, development and test cycles. Then final testing (such as penetration testing for the specialized power monitoring attacks DPA, SPA, DFA) is carried out on the product. Once all deliverables have been provided and all tests carried out by the CLEF, a detailed report with a package of all material is prepared and sent to the Certification Body who review it and if appropriate, award the certificate to the product.

The ITSO SAM completed the Common Criteria evaluation process with CEACI during 2005. This included the detailed design and source code for the implementation. The certificate (2005/38) was issued by DCSSI on 24th November 2005.