

itsone news

Issue 1 January 2006

Common Criteria Certification

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 Sécurité des Systèmes 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

consequently 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.

Continued on the next page

5th MOVING ON CONFERENCE
7 - 9 March 2006, Glasgow

ITSO Workshop Speakers announced:

John Verity
ITSO

International Standards
What is happening and where does ITSO sit?

Shashi Gedia
Phillips
Desfire

What is it and what does it bring to the game?

Francis Sykes
CNA
Calypso

What is it and what does it bring to the game?

Conn Crawford
NSCWP
Smart Connect

What does this software package do?

David Hytch
Logica

Back offices

The role they play in ITSO

Jonathan Young

The Scottish Executive

Transport on the Entitlement Card

Live any minute now with 1.2M cards! -
The experience so far

Andreas Schauer
Giesecke & Devrient
A look into the future

Continued from page 1

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 is 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.

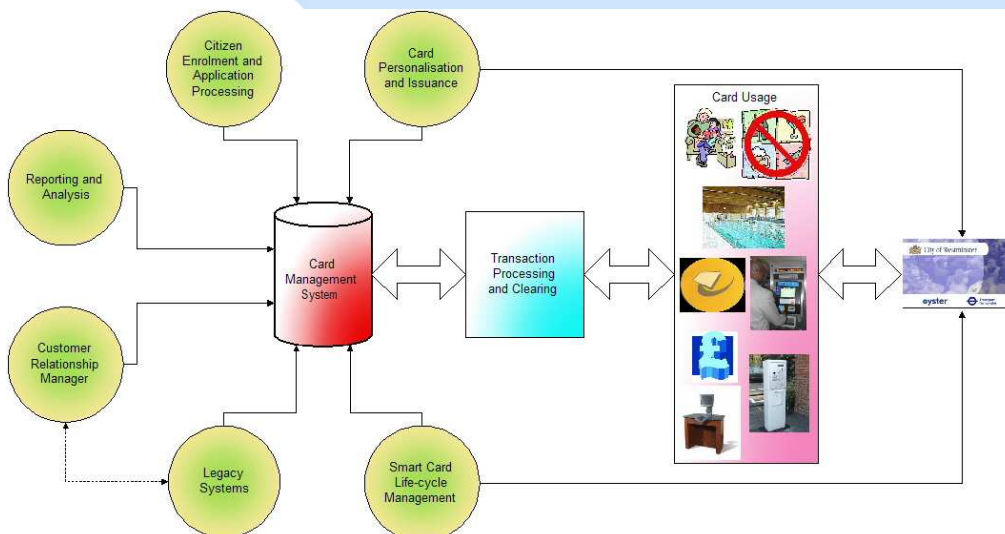
John Verity
Head of Compliance, ITSO Limited

Smart Connect Components of the Smart Connect software package

In the last issue of the newsletter we made reference to the software from the NSCWP going through certification. A number of you have asked what this software does. The components of the Smart Connect software package for local authorities are as follows:

- Web-based enrolment system, designed to be flexible enough to incorporate any existing paper-based application form
- Enrolment system facilitating the rationalisation of a number of application forms (allowing a citizen to apply for a number of services without completing multiple forms)
- Image capture capability (including the citizen's photograph and signature)
- Sophisticated eligibility checking and recording facilities (allowing citizens to present their proof of entitlement only once and enabling a scanned copy of any documentary proof to be stored in the card management database)
- Microsoft SQL Server 2000 Cardholder database
- Card management system including routines for data import / export, hotlisting and re-issuing cards
- Card print and personalisation software allowing local authorities to produce cards without the assistance of an external print bureau, if desired
- On-card java applets
- Card data viewing software allowing citizens to view the data that is stored on their smart card
- Card data maintenance software allowing local authorities to update the data stored on a citizen's card and at the same time ensure the integrity of the data in the back-end database
- Web-based user interface allowing citizens to log-on using their smart card and view the details stored about them on-line

Overview of components



For further details contact: national.smartcard@bracknell-forest.gov.uk
Or: Richard Tyndall 07880-787-007 ; Steven Gale 07976-341-690

Intelligent Transport Systems for the United Kingdom

A new site relating to transport has been launched recently: www.itsinpractice.com

ITSinpractice is a peer-reviewed on-line journal published by Traffic Engineering and Control (TEC) in association with ITS United Kingdom. ITSinpractice provides practitioners in the ITS community with the opportunity to publish serious, in-depth papers on recent research and projects and the practical issues relating to the procurement and deployment of intelligent transport systems. Papers are uploaded to the site on a regular basis.

www.itsinpractice.com available to members of ITS (UK) and subscribers to Traffic Engineering and Control.

Subscribers to ITSinpractice will be able to access current volumes of the journal plus all past papers, which will be stored in a searchable archive.

Debelle Carol, Editor,
Traffic Engineering and Control magazine

Issue 7 (December 2005) of ITSO Newsletter contained a mistake: the name of company Burall Ltd was spelled incorrectly. ITSO apologises for oversight.

SMARTER LIVING THROUGH TRANSPORT SMARTCARDS

Smartcard technology is transforming travel across London, with Scotland about to follow suit. The benefits realised by this technology are not limited to transport, but could radically alter many aspects of modern living by providing seamless and rapid financial transactions for all forms of retail.

The Centre for Transport Policy is holding a one day conference on **Tuesday 16th February 2006** at the CBI Conference Centre in London to look closely at the way the Smartcard electronic revolution is unfolding.

Some of the key areas to be discussed are:

- the growth of London's Oystercard
- how the public sector has decided to lead the way in Scotland
- what are the barriers preventing Smartcards taking off in the rest of England?
- is there a business case for private operators?
- realising the wider potential for spheres outside transport

Further information is available on our website www.rgu.ac.uk/abs/events/page.cfm?page=29823

Alternatively please do not hesitate to contact:

The Conference Section
The Centre for Transport Policy
The Robert Gordon University
Schoolhill
Aberdeen
AB10 1FR

Tel: 01224 263134
Fax: 01224 263129

Website: www.abs.ac.uk/cftp

ITS WORLD CONGRESS. LONDON 2006

ITS World Congresses have been held annually since 1994 with the host country rotating tri-annually between Europe, the Americas and Asia Pacific. They are the only truly international meetings addressing policy and deployment experience for Intelligent Transport Systems and combine a technical programme of conference papers with a substantial Exhibition. Over the four days of the main event the Congresses typically bring together around 5000 suppliers, clients, users, researchers and academics from across the world to share emerging knowledge and best practice. In addition, many organisations stage meetings immediately before or immediately after the Congresses to exploit the fact that in most subjects 90% or so of the World's experts will be gathered together.

Having this year's ITS World Congress here in the UK is a major opportunity for everyone involved in developing and delivering ITS at the industrial, service and policy levels. That is why the UK Government is supporting the event, with the Department for Transport chairing the national steering group and working very close with our UK and international colleagues. DfT also chairs the International Programme Committee and the Congress Board of Directors. The Department of Trade and Industry, Transport for London and ITS UK are the other key national partners; but we have an inclusive process where the wider ITS community can and does get involved.

There is considerable momentum and excitement around the London Congress – the exhibition is set to be the biggest so far, and there has been a very high number of technical papers (we crossed the 1000 line and they are still coming in) and other session ideas submitted. Demonstrations and technical visits are an important part of the overall Congress and we hope to have a strong UK presence there, with plans and ideas now starting to take off in earnest.

Bringing the Congress to the UK gives an ideal and cost-effective opportunity to showcase UK ITS deployment and enable UK practitioners to gain from international experience. It enables us to showcase how we are deploying leading-edge ITS initiatives to support delivery of Government objectives, particularly in terms of improved road safety and efficiency and provision of seamless transport services where travellers can make more informed choices.

It is very unlikely that this event will return to the UK for many years.

ITSO hopes to run an "ITSO VILLAGE" at the Congress and all ITSO Supplier Members and Registered Suppliers are invited to join in. Contact stoddyp@aol.com for more information.

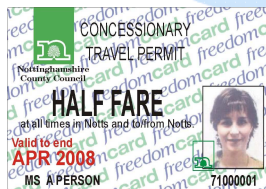
Eric Sampson, Department for Transport

Peter Stoddart, ITSO Ltd

Nottinghamshire County Council awards ACT the HOPS contract for the 'freedom card' ITSO migration project

Following a lengthy OJEU Negotiated Procurement process Nottinghamshire County Council announced that ACT (Applied Card Technologies Ltd) have been awarded the contract to provide a managed service for the Council's ITSO HOPS/AMS (Host Operator Processor System/Asset Management System).

Eager to forge ahead with the delivery, a swift start was made on the contract acceptance date of 28th December 2005; such is the



commitment of both ACT and NCC to implement one of the first ITSO schemes in the UK.

The migration of the existing inter-operable 'freedom card' scheme to the ITSO specification will allow even greater

flexibility of use and further opportunities for expansion to other transport modes, integrated ticketing, seamless travel and additional applications, encompassing over 110,000 card holders.

ITSO is fast becoming the recognised industry standard for all transport operators, in line with the Department for Transport and the need for integrated travel across the UK. 2006 is set to see the move from development into operation for a number of schemes and the progression towards further interoperability.

Information for this edition of ITSO Newsletter has been sourced from:

- www.itso.org.uk
- www.itsinpractice.com
- Nottinghamshire County Council January 2006 Press Release
- The Centre for Transport Policy, The Robert Gordon University (Aberdeen) December 2005 Press Release



ITSO Limited
Room 122, Centro House
16 Summer Lane
Birmingham B19 3SD

T: 0121 233 2598
F: 0121 233 0994

ITSO Ltd.
Registered in England and Wales
No. 4115311
© 2006