

## GESTe: A consortium fully supporting the CC adoption for payment terminals security evaluation in the SEPA

Carolina Lavatelli, Trusted Labs, Member of GESTe Consortium  
Nathalie Feyt, Thales CEACI, Member of GESTe Consortium

11<sup>th</sup> ICCC, 2010, September 21-23, Antalya,  
Turkey

# Contents

- Payment terminal context
  - International recognition of terminals security evaluations
  - Necessary refinement of Common Criteria evaluation methodology
- Presentation of GESTe consortium
  - A project including key stakeholders representatives
  - Complementary skills
  - Innovation
- Contribution for CC adoption in payment terminal industry
  - Evaluation methodology
  - JIL-Application of Attack Potential Methods to terminals
- Perspectives

# Payment terminals security evaluation today

- The security certification of payment terminals is made by domestic or international schemes using different methodologies:
  - Domestic schemes like ZKA and Currence have developed their proprietary security requirements,
  - UK Cards uses the standardized Common Criteria methodology (based on a dedicated CC Protection Profile), and
  - the international PCI SSC has its own PCI-PED certification program.
- This situation leads to high terminal certification costs combined with a time consuming multi-certification process for the industry.
- The SEPA – Single Euro Payment Area - initiative gives the opportunity for the standardisation of terminals security evaluations in Europe.
- JTEMS (JIL Terminal Evaluation Methodology Subgroup) created to support the application of CC to the evaluation of payment terminals.

# Towards CC adoption

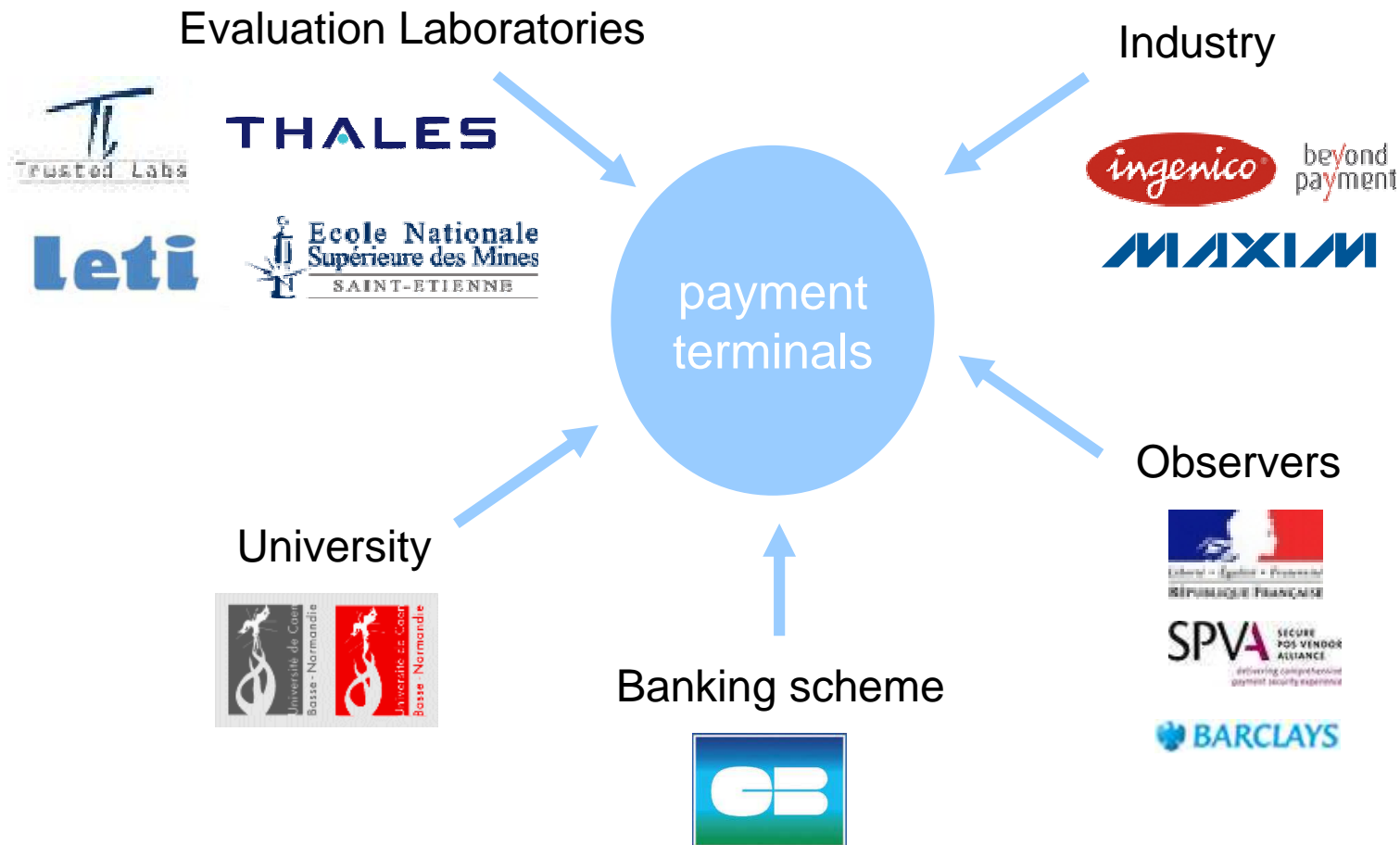
- The payment terminal industry has three specificities, which impact the CC implementation for terminal security evaluations:
  - The TOE (POI) is intrinsically « composed », since terminals can be monochip or multichip with different applications and peripherals, each holding part of the security functionality. Moreover, these components do not offer the same resistance level to attacks.
  - Short time-to-market, i.e few months, and numerous regular upgrades, with an impact on the duration and cost of evaluation.
  - Compliance with international PCI standards required for recognition and reuse of evaluation tasks.
- JTEMS Protection Profile for POI was built to address these issues

# GESTe consortium

- The GESTe consortium has been set-up to support the implementation of SEPA requirements to establish a common security certification framework for payment terminals in Europe based on Common Criteria methodology.
- French Innovative R&D project
  - Labels from TES and SCS “Competitiveness clusters”
  - 2 years project: From March 2009 to March 2011

GESTe stands for « Gestion de l’Evaluation de la Sécurité des Terminaux »  
(in English, « Management of the Security Evaluation of Terminals »)

# GESTe stakeholders



Ingenico (Head of the project), CEA LETI, CESTI-CEACI THALES, Ecole Nationale Supérieure des Mines de St Etienne (CMP), Groupement des Cartes Bancaires « CB », Maxim, Trusted Labs, Université de Caen (lab PRINT CRDP). 6

# GESTe activities

- POI evaluation methodology
- Design of HW, SW and combined attack methods
- Design and test of innovative solutions
- Legal aspects of the SEPA certification framework
- Communication

# GESTe contributions on CC

- Active participation to JTEMS
- Based on PP POI, which defines a dedicated EAL POI
- Definition of the POI evaluation methodology
- Definition of POI attack methods

# EAL POI

- The POI assurance level defined in the PP is an EAL2+ package
- With refined ADV\_ARC, AGD\_OPE, ALC\_CMC, ALC\_DEL, ALC\_DVS
- With extended AVA\_POI that focuses on each POI component at the right attack potential
- Adapted to POI characteristics and as well as to effort and time-to-market constraints.

# CEM applied to POI

- All requirements and guidance in one document, for developers and evaluators
- Generic CEM evaluation work units interpreted to meet the POI assurance level and the TSF decomposition in parts
- New evaluation work units for AVA\_POI based on AVA\_VAN.2

# Extract of work units of POI CEM (refined SAR and TSF parts)

- **ADV\_ARC.1-2:** security domains must cover the isolation of payment application
- **ALC\_DVS.2-1:** The development environment stands for the design, manufacturing, assembling and maintenance environments of TOE components, including the final assembly and the Initial Key Loading facilities.
- **ALC\_DVS.2-1:** If the manufacturer is in charge of initial-key-loading himself he must verify the authenticity of the security enforcing components for himself. Otherwise, the manufacturer must provide means to the initial-key-loading facility to assure the verification of the authenticity of the security enforcing components.
- **ADV\_TDS.1-2:** The TSF subsystems shall be described in sufficient details such that they can be linked to one of the following groups: CoreTSF, CoreTSFKeys, PED MiddleTSF, Middle TSF, MSR (as an option).

# Planning of the CEM for POI

- New release by December 2010, ready for starting pilot evaluations
- Conformant to certified version of PP POI (currently under evaluation by CEACI Thales)
- Document available to JTEMS members, comments are welcome !

# Attack methods

- New challenges, in software, combined hardware and software attacks,
- But also in the context of fraud on terminals which is different from standard smartcard one, in particular on the attack potential debate.

# Attack methods

- Classical attacks coming from actual evaluations are included
- New categories of attacks have been proposed in this JTEMS document
- GESTe consortium is working essentially on
  - Distance attacks
  - Perturbation attacks
  - Physical Spoofing attacks
  - Logical attacks (at POI interfaces)

# Attack methods

- First attempts to use the rating proposed in JIL attack potential reveal problems that have to be solved in JTEMS:
  - Multiple composition of attack quotation
  - Many proposed attacks methods are not final attacks which grant access to sensitive assets of the POI
  - Define attacks methods on POI components (like chipsets, or PinPad keyboards for example)
  - Reuse between different evaluations schemes

# Attack methods

- JTEMS has to adapt and refine to terminals evaluation the JIL attack potential document.
- OSEC pilot evaluations based on the new PP POI shall demonstrate the feasibility of the approach and shall allow improving the quotation guidelines.
- The challenge will be to offer reusability at least of intrusion tests between schemes, PCI and CC.

# Perspectives

- We foresee to develop constructive dialog between the actors of the payment ecosystem (developers, payment schemes, banks) that we expect will lead to the adoption of CC evaluation in SEPA countries.
- The approach, regarding both the structure of the consortium and the insertion in CC organizations, seems promising for future use of CC in security evaluation in markets that have been out of the scope so far: avionics, ground transportation, space, ...

# Thank you !

Carolina Lavatelli, [carolina.lavatelli@trusted-labs.com](mailto:carolina.lavatelli@trusted-labs.com)

Nathalie Feyt, [nathalie.feyt@thalesgroup.com](mailto:nathalie.feyt@thalesgroup.com)