

# Dedicated EAL: the payment terminal experience

**Carolina Lavatelli  
Claire Loiseaux**

**Trusted Labs**

ICCC 2009

September 22<sup>nd</sup> – 24<sup>th</sup>

Tromsø, Norway



**Trusted Labs**

# Contents



- Context of payment terminals in Europe
  - Evaluation methodology that enjoys international recognition
  - Satisfactory ratio effort/assurance
- Point of Interaction (POI) in the CC framework
  - Why it is a bit more complicated than usual
  - Protection profile and POI-dedicated EAL
  - A way of evaluating complex products



- The situation of payment terminals evaluation in Europe
  - Each country states its own security levels and requirements
  - E.g. schemes: ZKA (Germany), APACS (UK), PCI+ (Netherlands)
  - Obstacle for mutual recognition of evaluations
- European Payments Council (EPC) in its Single Euro Payments Area (SEPA) Cards Framework (SCF)
  - Definition of a common process for the certification of terminals, cards, and network interfaces
  - Any terminal certified for SEPA transactions by a certification body in one SEPA country can be deployed in any SEPA country for acceptance of SEPA cards across all SCF compliant schemes
- Common Approval Scheme (CAS) initiative of European card schemes
  - Agreement on common security requirements and evaluation methodology for use in SEPA
  - Compliant with Payment Card Industry (PCI) security requirements
  - Reduced number of security evaluations to be performed by manufacturers and reduced the costs of security certification



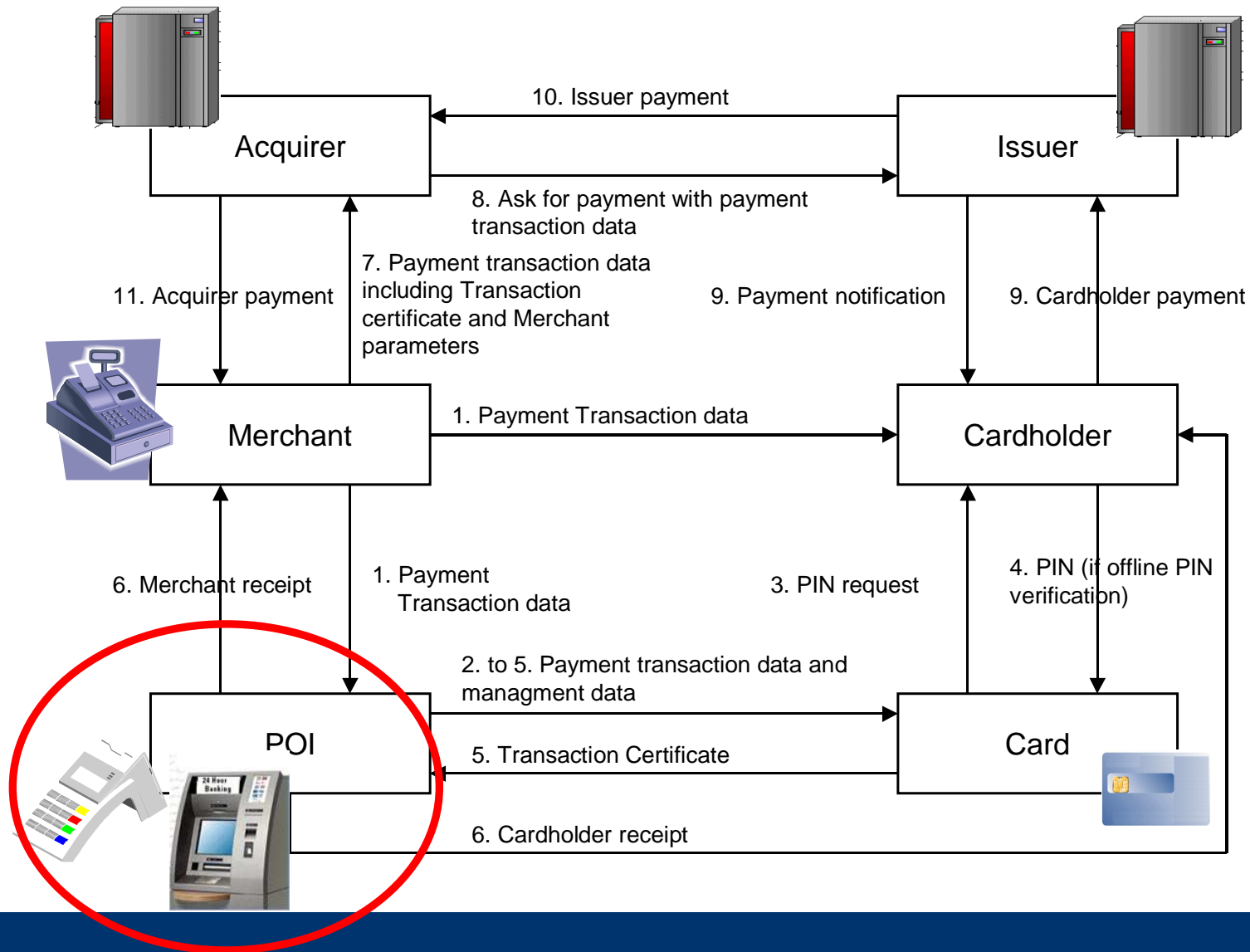
# Why CC ?



- CAS promoted the investigation of CC methodology for terminals
  - Feasibility studies since 2006
  - Protection profile started in 2007
  - Creation of JIL Terminal Evaluation Methodology Subgroup (JTEMS) in 2008
  
- Why CC evaluation of terminals ?
  - Pertinence of CC confidence model (evidence-based, reproducible results, decentralized certification)
  - Strong experience of european ITSEF in the card-side of the payment
  - Sharing of PCI PED evaluation experience through PCI labs



# Point of Interaction (POI) at work

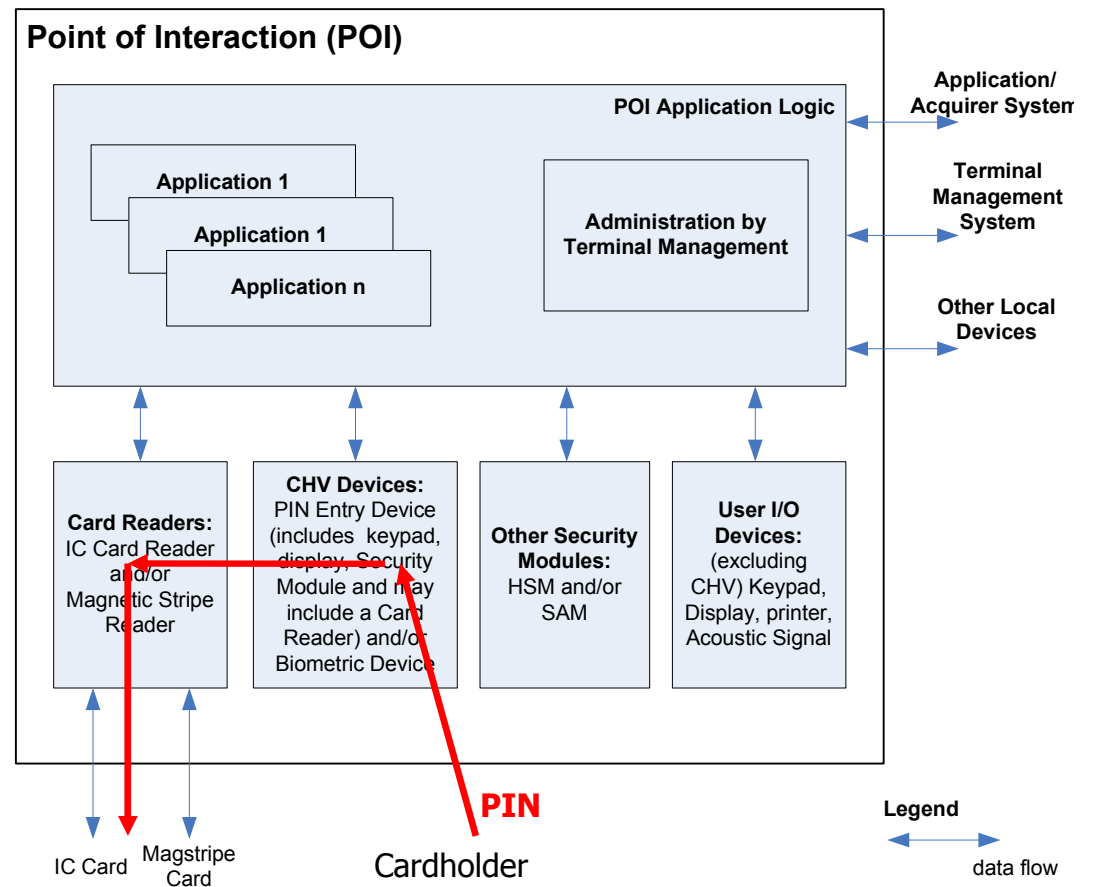


# What's the POI



- Payment terminal with IC card based online and offline transaction capabilities

- Numerous components:
  - Card Readers
  - Keypad, display
  - Encryption module
  - Peripherals
  - Payment applications
  - Communication SW
  - ...
- Assets flow between components
  - more or less robust:
    - Cardholder PIN
    - Amount
    - Scripts
    - ...



# What are the issues for a POI PP ?



- Many different architectures (TOE types)
  - Integrated (PED and Card Reader)
  - Distributed
- Components with heterogeneous robustness levels
  - Encryption module
  - Keypad, Display
  - Card Reader
  - Embedded SW (may be COTS)
- Assets protection requirements depends on the deployment environment (Europe, world)
  - Plaintext PIN-based transactions not the focus in Europe
- No predefined EAL offers sufficient assurance and is still economically viable and adapted to market constraints
  - E.g. EAL2 (low robustness), EAL4 (costly conformity check), etc ..



# How to solve the puzzle



- POI PP embeds all architectures (configurations) and security levels
  - Based on PCI and CAS requirements
  - Applications outside the scope of evaluation (differ from country to country)
  - The TSF is structured in security levels
  - Each PP configuration maps security features to the security levels
  - POI-dedicated EAL with refined vulnerability analysis
- Joint work with SRC Security Research & Consulting GmbH
  - First PP POI ideas presented at ICCS 2007 (Rome)



# POI TSF structured in three levels



## Examples of security features (to map to a security level)

- PIN Entry
- Encipherment of PIN for offline or online encrypted authentication
- Encipherment of PIN for offline plaintext  
PIN authentication
- Decipherment of PIN by the IC Card Reader  
and transmission to the IC in plaintext
- Periodic authentication of PIN processing software
- Administration (e.g. downloading, update) of  
PIN processing software and keys
- Processing of POI management and transaction data
- Magstripe Card Reader protection
- Tamper-evidence/resistance (PED, IC Card Reader, Magstripe Reader)
- Shielding

High security level

Moderate security level

Basic security level



# Examples of mappings



- PIN Entry
  - « Moderate level » in all POI/PP configurations
- Encipherment of PIN for offline or online encrypted authentication
  - « High level » in all POI/PP configurations
- Plaintext PIN processing
  - « Moderate level » in configurations with world-wide constraints
  - « Basic level » in configurations where plaintext PIN authentication fraud is reduced



# EAL dedicated to POI



- EAL2+ package
- Requirements on development (ADV), guidance (AGD), testing (ATE) and life cycle (ALC) from EAL2
- **ALC\_DVS.1 added to EAL2 essentially for Initial Key Loading Facility**
- **Definition of extended vulnerability analysis requirement AVA\_POI**
- **AVA\_POI is a refinement of AVA\_VAN.2**
- AVA\_POI focuses on each POI component at the right attack potential
- POI EAL stays within the limits of the international recognition
- Conformity checks remain affordable both from developer and evaluator viewpoints



# Overview of POI EAL



	SAR	POI
EAL2	ADV_ARC.1	REFINED
	ADV_FSP.2	STANDARD
	ADV_TDS.1	STANDARD
	AGD_OPE.1	REFINED
	AGD_PRE.1	STANDARD
	ALC_CMC.2	REFINED
	ALC_CMS.2	STANDARD
	ALC_DEL.1	REFINED
	ATE_COV.1	STANDARD
	ATE_FUN.1	STANDARD
	ATE_IND.2	STANDARD
	AVA_VAN.2	STANDARD
		ALC_DVS.1
EXTENDED	<b>AVA_POI.1 / POI-Basic</b>	<b>Basic TSF POI components</b>
	<b>AVA_POI.2 / POI-Moderate</b>	<b>Moderate TSF POI components</b>
	<b>AVA_POI.3 / POI-High</b>	<b>High TSF POI components</b>



# What changes with AVA\_POI



- Applies to part of TSF instead of full TOE
- Limited dependencies (from AVA\_VAN.2) for all attack potentials
- Introduction of the notion of « availability » of implementation
  - No evaluation task on implementation itself
  - Used to improve vulnerability analysis
- Attack potential scale adapted to POI
  - POI-Basic, POI-Moderate, POI-High
  - Defined in supporting document (compliant with PCI PED)



# POI PP status



- Version 1.7 released for comments to JTEMS members last June
  - CC conformity check
  - PCI PED conformity check
- Updated version for evaluation expected end of October
- ANSSI shall sponsor PP evaluation
  
- JTEMS also works on supporting evaluation documents
  - Instantiation of CEM
  - Attack methods paper
  
- French R&D project GESTe (Groupe d'Evaluation de la Sécurité des Terminaux électroniques) supports JTEMS
  - Ingenico (leader), Innova Card/Maxim, Trusted Labs, Groupement des Cartes Bancaires, CEA LETI, CESTI-CEACI Thalès, ENSM SE, PRINT-CRDP Université de Caen
  - March 2009 – March 2011



# Perspectives



- The POI experience is a step towards the use of CC in domains where the principle « one-product / one-EAL » does not hold
- Introducing flexibility at the SAR level would allow the security evaluation of complex products with components of heterogeneous security levels (e.g. including COTS)
- Real payment terminal evaluations conformant to POI PP shall provide feedback on on the approach and the ways it can be reproduced.

