

JTEMS - a technical community for the evaluation of payment terminals

Sandro Amendola, SRC
Ingo Hahlen, BSI
11th ICCC, Turkey

Outline of the presentation

JTEMS

- **Example for a technical CC-community apart from smart card world**
- **Understand JTEMS as new technical community**
 - ▶ **Reasons for founding JTEMS (Background)**
 - ▶ **Starting the technical community**
 - ▶ **Goals and Terms of Reference (ToR)**
 - ▶ **Collaboration within the group**
 - ▶ **Co-existence with existing standards and evaluation processes**
 - ▶ **Current and future work items**
 - ▶ **Summary**

Background Information (I)

JTEMS

- **Existence of several payment systems within Europe:**
 - ▶ Use of proprietary technology and interfaces
 - ▶ Different evaluations for approval of devices
 - ▶ Cost intensive certifications within Europe as consequence
- **New legal framework (NLF) for Single European Payment Area (SEPA) for Cards:**
 - ▶ Elimination of differences in technology and standards used by payment systems
 - ▶ Implementation of interoperable system until 2010
 - ▶ Mutual agreements to underpin interoperability

Background Information (II)

JTEMS

- Payment systems founded Common Approval Scheme (CAS) initiative to implement NLF
- Items of CAS work:
 - ▶ Scope of security relevant features for cards and payment terminals - CAS requirements - that must be evaluated
 - ▶ Commitment to evaluation methodology for payment terminals - CC
- CAS initiated foundation of JTEMS as consortium of labs, certification bodies (CBs), developers and payment system representatives to:
 - ▶ Discuss technical aspects with experts in this field
 - ▶ Produce CC-supporting documents to interpret the CC according to the requirements of this special technical domain
 - ▶ Provide assurance that results of one evaluation can be used in approval processes of different payment schemes.
- Orientation on the smart card working groups ISCI WG1 and JHAS

Starting the work

JTEMS

- **Kickoff Meeting:**
 - ▶ Organised by ZKA (approval body for German payment system (ec))
 - ▶ Brought CBs and labs together
 - ▶ Introduced Protection Profile (POI PP) expressing the harmonized CAS requirements in CC language
- **Result:**
 - ▶ Common understanding of goals and principles developed
 - ▶ Work packages identified
 - ▶ CBs (a. o. FR, GE, NL, UK), labs (a. o. T-Systems, Thales, Trusted Labs, SRC, TÜV-IT, brightsight), payment systems (a. o. UK Card Association, ZKA, PIN, Cartes Bancaire, VISA, MasterCard, American Express) volunteered to start working

Goals and ToR

JTEMS

- **Terms of Reference (ToR) for JTEMS:**
 - ▶ **Maintain POI PP to express requirements in CC language**
 - ▶ **Adapt and interpret CC for this technical domain**
 - ▶ **Standardize and harmonize rating of POI security**
 - ▶ **Associate labs, CBs, payment systems and vendors supporting the goals of JTEMS**
 - ▶ **Respect confidentiality of discussions and results**
- **Re-use of knowledge gained by participating in JTEMS is allowed and considered a reward for contribution**

Summary of starting conditions

JTEMS

- **Motivation:**
 - ▶ Payment systems require security evaluations
 - ▶ Success of voluntary initiative important for mutual recognition
- **Stakeholders:**
 - ▶ Stakeholders involved from the beginning
- **Forming the community:**
 - ▶ ZKA, UK Card Association and Cartes Bancaire sponsor PP development and work of chairperson holding the group together
- **Common understanding of participants:**
 - ▶ CC evaluation as basis for mutual acceptance by payment systems
 - ▶ Purpose: Optimize CC for specific technical area
 - ▶ Confidential forum with open minded participants
 - ▶ Focus on technical work with CAS handling more political issues

JTEMS

Collaboration – the beginning

- **First steps were long winded:**
 - ▶ Controversies about POI PP with different VAN-levels in one PP
 - ▶ CAS requirements not fixed
 - ▶ Compliance of POI PP to PCI requirements not clear
 - ▶ Regulation for exchange of confidential information
 - ▶ Work on JTEMS additional to day-to-day business
 - ▶ Vendors were sceptical about the whole procedure
- **1,5 years to attain major improvements:**
 - ▶ Consensus for POI PP and preparation for certification
 - ▶ Successful involvement of vendors

JTEMS

Collaboration - Improvements

- **Improved funding**

- ▶ Initiative (GeSTE) combining labs of the French CC scheme, French vendors, academic resources, etc., founded and supported by public money

- **New cooperations outside of JTEMS:**

- ▶ Vendors agreed on a better coordination founding the Secure POS (Point Of Sale) Vendor Alliance (SPVA)
- ▶ Payment systems founded steering committee (OSeC) for coordination of activities relating to CC-based evaluations of banking terminals

Expectations of group members

JTEMS

- **Payment systems**
 - ▶ Cooperate closely towards a pilot evaluation
 - ▶ Produce results that are helpful for their approval process
 - ▶ Maintain or improve system security
- **Governmental CC schemes**
 - ▶ Re-use results of the JTEMS activities for other areas of the CC
 - ▶ Propagate the CC standard instead of a new proprietary scheme
- **Evaluation labs**
 - ▶ Gain access to the new market of CC evaluations for banking terminals
 - ▶ Assure fair conditions with respect to evaluation efforts
 - ▶ Improve the efficiency of the evaluation process
- **Vendors**
 - ▶ Facilitate the approval of payments systems for their products
 - ▶ Better understand and influence a key process

JTEMS

Summary of improvements

- **Activity:**
 - ▶ More activities of some participants (e.g. GesTE) motivated the whole group
- **Mutual Trust:**
 - ▶ Payment systems gained confidence in multiple recognition of evaluation results
 - ▶ European and global payment systems trust CBs to oversee evaluation
 - ▶ Participants bring in their experiences – problems with intellectual properties openly discussed
- **Benefits:**
 - ▶ Vendors appreciate the influence on the evaluation methodology and other activities
 - ▶ CBs test new concepts for improvement of CC in this technical domain
 - ▶ Labs recognize the benefit in improving standards and develop a mutual understanding about state-of-the-art attacks

JTEMS

Co-existence with current practice

- **Security evaluations conducted since many years**
 - ▶ Secure banking terminals are very important for payment systems
 - ▶ European payment systems established different evaluation methodologies
 - ▶ Global payment systems have established Payment Card Industry (PCI) standard
- **CC approach is in the area of conflict of European and global payment systems**
 - ▶ Merge to CC-approach heavily changes current practice
 - ▶ CC-approach must satisfy the expectations

JTEMS

European payment systems

- Define the security level from payment systems' perspective
- Their approval processes rely on output of evaluation processes and additional risk related information must be provided by the CC process in future
- Huge experiences with current security evaluations
- Key factors for evaluation (time, costs, resources) are well known and accepted by the market
- Regulations are under complete governance of the corresponding system including fast responses to new attacks
- Accreditation of labs is established

JTEMS

Global payment systems

- Europe is not their most important market for banking terminals
- Must take environment of all parts of the world in account (e.g. no Chip-and-PIN support in the US)
- Face more distributed attacks (e.g. for spoofing card data in Europe and withdrawal of money in Asia)
- Labs accredited worldwide but most evaluations conducted in Europe
- Basis for approval of some European payment schemes
- Approval of global payment systems is crucial for all vendors

CC approach and PCI standards

JTEMS

- **CC approach most valuable if CC certificate also usable for approval of global payment schemes**
- **PCI requirements included in POI PP – checked by PCI lab**
- **PCI assurance requirements reflected in new assurance family for vulnerability assessment**
- **Creation of additional documents relating to PCI instructions for evaluators**
- **Intensive discussion about attack methods involving PCI representatives**

JTEMS

Challenges with PCI standard

- **Accreditation of labs**
 - ▶ Establish confidence of PCI in skills of labs accredited in a national CC scheme
 - ▶ Allow access to PCI internal documentation required to produce PCI reports
 - ▶ Define requirements of PCI concerning the output of the CC process for PCI approval process
- **Co-existence of both standards**
 - ▶ Reflection of changes in PCI requirements and methodology in the CC approach

Open work items

JTEMS

- **Complete CC-evaluation of POI PP**
- **Conduct pilot evaluation**
- **Continue work on documents interpreting the CC with respect to banking terminals**
- **Find practical approach for site visit requirements**
- **Continue discussion with PCI about recognition of certificates**
- **Define requirements for output of CC process to be used for payment system approval process**

Evaluation of POI PP

JTEMS

- **PP will be evaluated in the French CC-scheme**
- **Certificate expected by the end of this year**
- **Certified PP will be publicly available on the websites of ANSSI**

Pilot evaluation

JTEMS

- **Preparations:**
 - ▶ Documents regarding evaluator guidance are mature enough
 - ▶ POI PP reached stable state
 - ▶ Many European payment systems intent to accept positive evaluation results as basis for approval process
 - ▶ OSeC installed steering committee to closely monitor the evaluation process
- **Participants**
 - ▶ Consortium consisting of CB, lab, vendor asked for participation
 - ▶ Arrangement of Product version, time schedules and commercial aspects as precondition for participation

Site visit requirements

JTEMS

- **Challenges:**
 - ▶ **Tight budget restrictions**
 - ▶ **Distributed development**
 - ▶ **Suppliers producing parts for different vendors (e.g. keypads)**
 - ▶ **Activities constantly changing between the sites**
- **Most important sites must be identified**
- **Commensurate compromise between visiting all sites and restrictions in time and money must be identified**
- **Site Certification may be a useful approach**

Summary – Challenges

JTEMS

- **Improve value of certificate:**
 - ▶ Confirm existing estimation of key factors (time, cost)
 - ▶ Convince payment systems that quality of CC-approach is comparable to current evaluations
 - ▶ Emphasize value of CC-certification for vendors
 - ▶ Improve mutual recognition with PCI
- **Overcome Delay:**
 - ▶ Invest more money to support technical work (e.g. specification of attacks)
 - ▶ Assign more time to members for working on JTEMS topics
- **Crucial next steps:**
 - ▶ Conduct Pilot evaluation
 - ▶ Optimize all processes for goals of SEPA

JTEMS

Summary – Positive Factors

- **Promising starting conditions:**
 - ▶ External pressure
 - ▶ Technical work items
 - ▶ Sponsorship for crucial positions and deliverables
 - ▶ Stakeholder representatives with technical background
- **Established collaboration:**
 - ▶ Open discussions without issues with intellectual property
 - ▶ Trust in each other has been established
 - ▶ Relationship to other communities (OSeC/CAS, JIWG, SPVA) clarified and accepted
 - ▶ Esteem of each participant
- **Increased importance of CC:**
 - ▶ Establishment of a new technical area
 - ▶ Optimization usable for other technical areas
 - ▶ Innovative cooperation with payment systems

JTEMS

Thank you!
Any question?

JTEMS

