Common Criteria in Austria - Overview and Experiences

Herbert Leitold

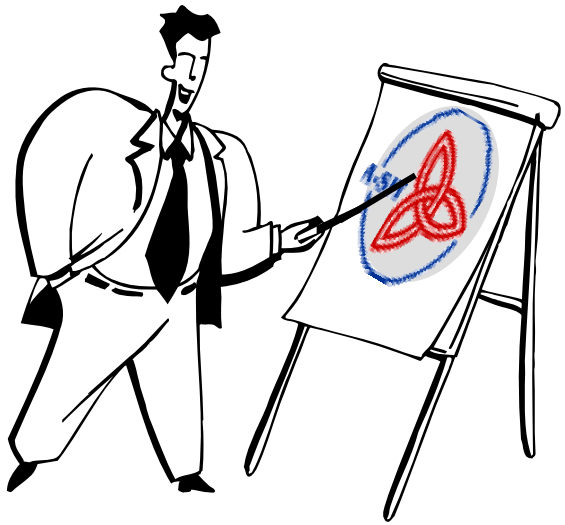
Secure Information Technology Center – Austria A-SIT

Prof. Reinhard Posch

Federal Chancellery,

Federal Chief Information Officer

Table of contents



- Introduction
- CC Drivers in Austria
  - National Signature law / projects
  - EU Signature Directive
- Experiences / Conclusions

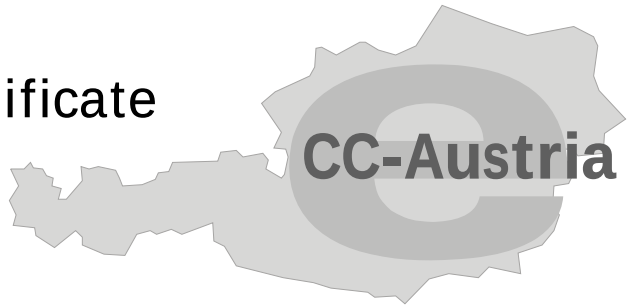
About A-SIT / Myself

- A-SIT's link to Common Criteria
  - Public-funded association
    - Independent advisory on IT security aspects
  - Confirmation body under Signature Law
    - Assesses the conformity of signature-creation devices (e.g. smartcards) against security requirements in the law
- My personal link to Common Criteria
  - Contributed to EESSI Protection Profiles
    - Secure signature-creation devices: SSCD-PP
    - CA cryptographic modules: CMCSO-PP, CMCKG-PP

Herbert.Leitold@a-sit.at

Austria and CC in a nutshell

- Austria's road to CC
  - Proposal to Federal ICT Board in 2001
  - Joined the CCRA in 2002
- Status in CCRA
  - Certificate consuming participant
  - Currently no plans to become a certificate authorising participant
- Major drivers
  - 01/2000 : Signature Law enacted
  - 11/2000 : Cabinet Council decided Citizen Card(s)
  - 1999-2003: EESSI – launched 1999, SSCD-PP completed in 2001, certified in 2002, EU reference number in 2003



Herbert.Leitold@a-sit.at

CC Drivers in Austria

- Legal Environment
  - Signature Law and Bylaws
  - Citizen Card Projects
  - CC-Influence on Legislation
- EU Initiatives
- Expectations / Observations

Certification requirement

Austrian Signature Law (2000)

§ 18(1) Technical components which allow the forgery of signed data to be reliably recognized and reliably prevent unauthorized use of signature creation data procedures shall be used […].
[…]
(5) The technical components and procedures for generating secure signatures must be constantly and adequately verified using state-of-the-art technology. Compliance with security requirements must be certified by a confirmation body (§ 19).

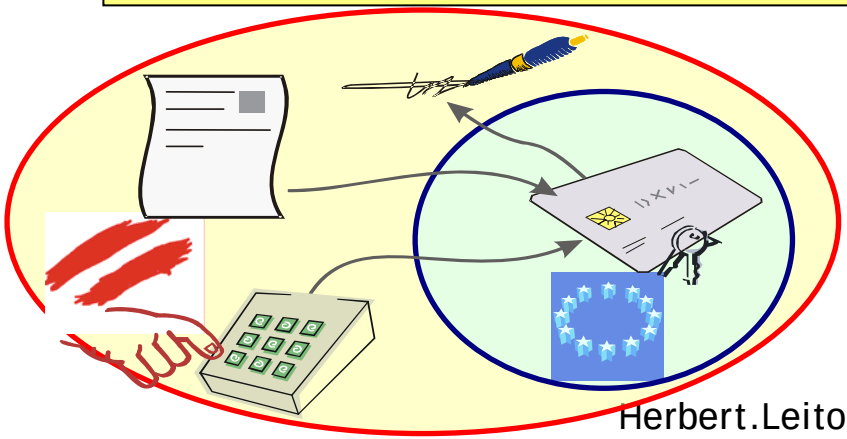
Herbert.Leitold@a-sit.at

More specifically …

1st Austrian Signature Order (2000)

§ 9. (1) Suitable protection profiles from the Common Criteria (ISO 15408) [...] recognised by a confirmation body shall be used to test […]

(2) Technical components and procedures may also be tested […] using ITSEC and, where applicable, in accordance with FIPS 140-1 or BS 7799. If ITSEC is used, assurance level E 3 with security mechanisms with "high" minimum strength [*… for the SSCD …*]; assurance level E 2 with security measures with "high“ minimum strength must be applied for other technical components and procedures.

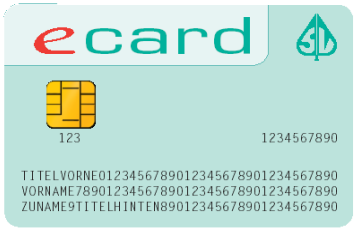


“other components” e.g. referred to card readers or to viewers to display the data to be signed.

Herbert.Leitold@a-sit.at

Austrian Citizen Card Initiatives for E-Government

Bank cards:
Each bank (ATM) card issued since March 2005 is also an SSCD (prepared, citizen is free to activate the citizen card function)



Health insurance card:
Rollout to each citizen started May 2005, to be completed in November 2005, currently issuing 70.000 cards/day (prepared, citizen free to activate)

National ID card with chip:
under discussion (not yet available)

further initiatives:

- Mobile phones (avail as citizen card)
- CSPs issuing qualified certificates (avail.)
- Austrian computer society card (discontinued)
- future technologies (PDAs, cell phones, WIM)??

Herbert.Leitold@a-sit.at

EU as CC-driver

EU Signature Directive
"Reference numbers"

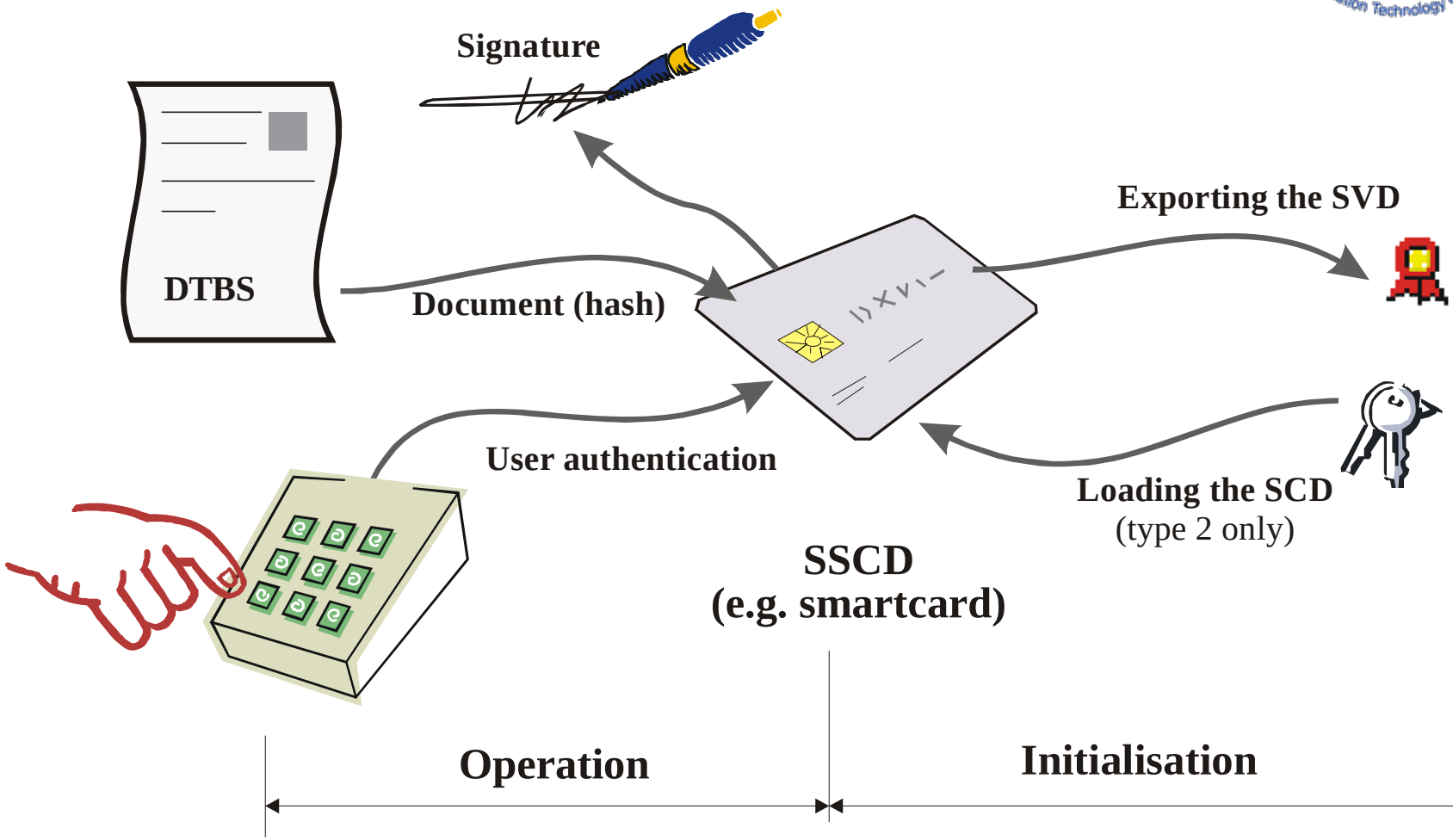
§ 5. (5) The Commission may […] establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities.
Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), [*CA's HSMs*] and Annex III [*i.e.SSCD*] when an electronic signature product meets those standards.

EESSI developed Protection Profiles that finally became reference numbers

- 3 SSCD-PPs (BSI-PP-0004-2002 / -0005 / -0006)
- 2 CMCSO-PPs (DCSSI PP/0308 & PP/0309)

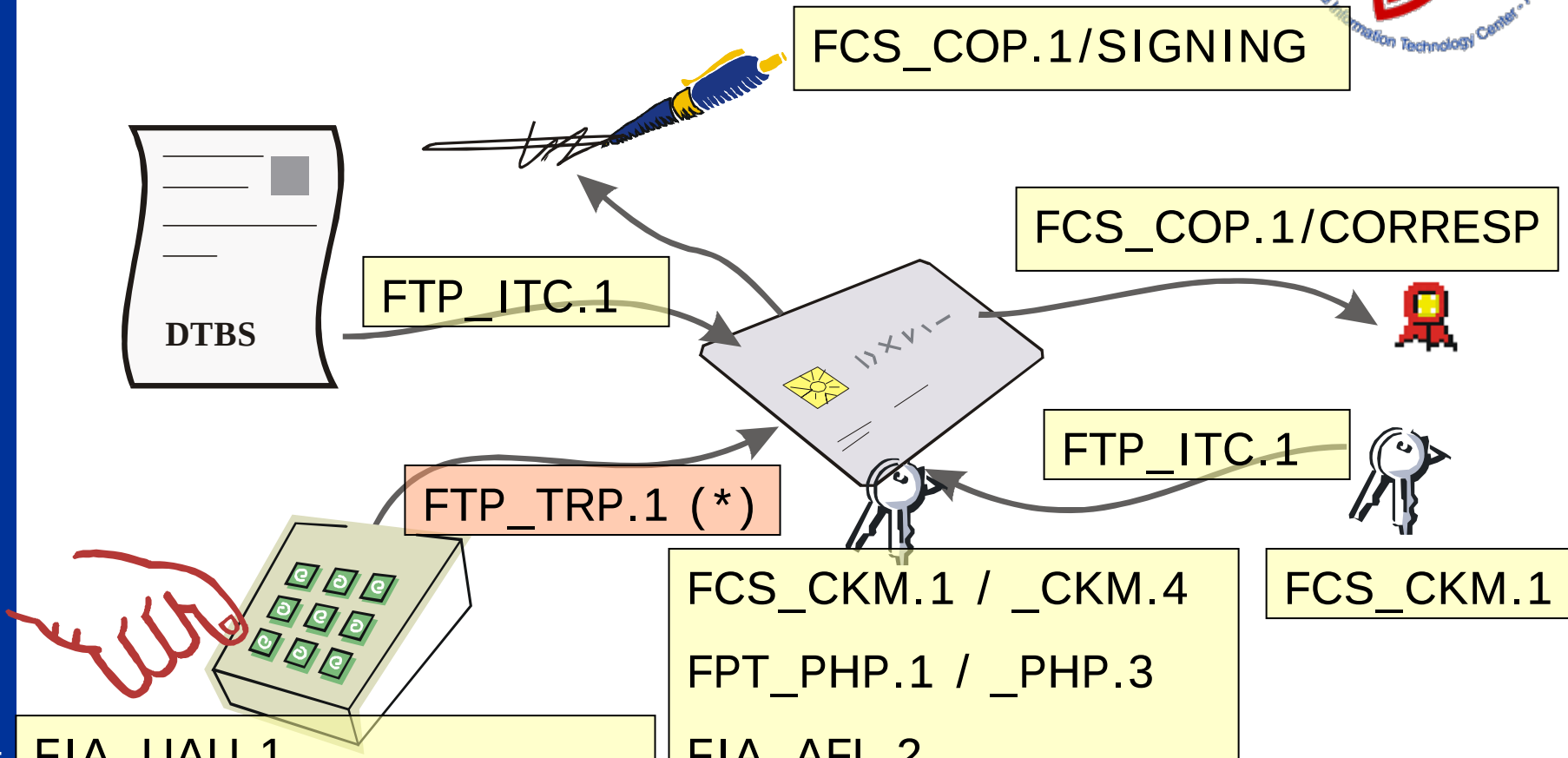
Herbert.Leitold@a-sit.at

SSCD-PP - An Overview



Herbert.Leitold@a-sit.at

SFRs (at least a few of them..)



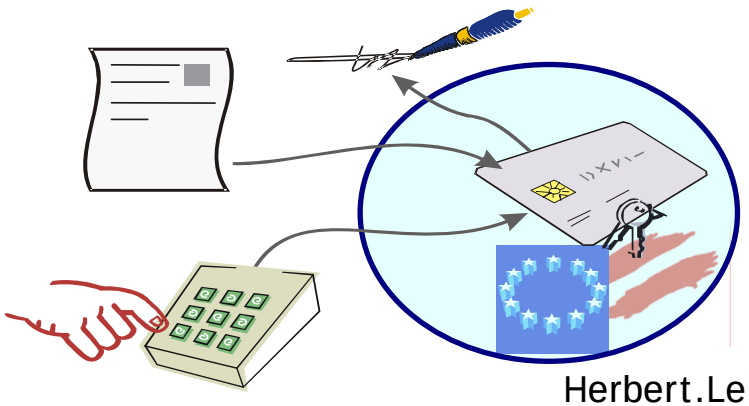
Herbert.Leitold@a-sit.at

Amended bylaws ...

2nd Austrian Signature Order (01/2005)

§ 9. (1) When testing technical components for creating secure electronic signatures security targets shall be applied, that are recognised suitable by a confirmation body. In particular Common Criteria Protection Profiles […] or ITSEC can be used.

(2) For the testing under (1) reference numbers are to be observed, which […] under article 3 (5) of Signature Directive 1999/93/EC […].



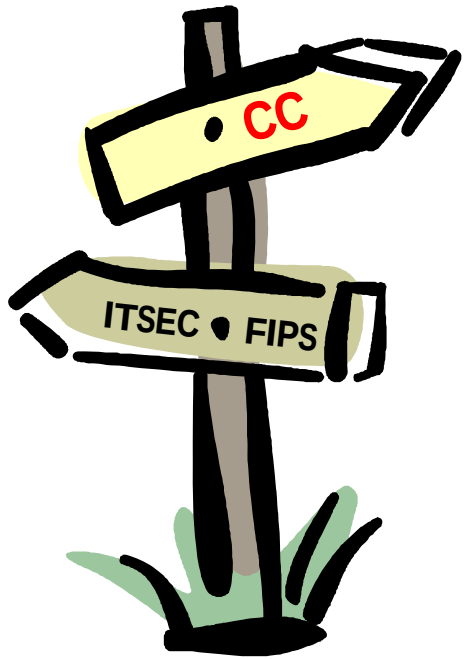
Most further provisions in excess of SSCD-PP have been removed from the Signature Order, e.g. no longer a legal certification requirement for card readers or viewers.

"SSCD-PP does the job"

Herbert.Leitold@a-sit.at

Expectations have been …

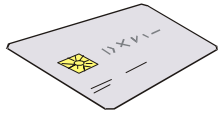
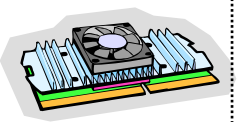
- In theory
  - Protection Profiles suffice to express security needs stated in laws in a technology-neutral way
  - CCRA gives international recognition for vendors which is a value
  - EU reference numbers should ease A-SIT's job, as a CC certificate is sufficient
  - etc.
- In practice
  - Laws are amended from time to time
  - PPs may no longer fit domestic approaches
  - Vendors don't take up immediately "just for the sake of applying CC"
  - etc.



Herbert.Leitold@a-sit.at

Criteria applied so far for confirmations acc. to Austrian Signature Law / Orders

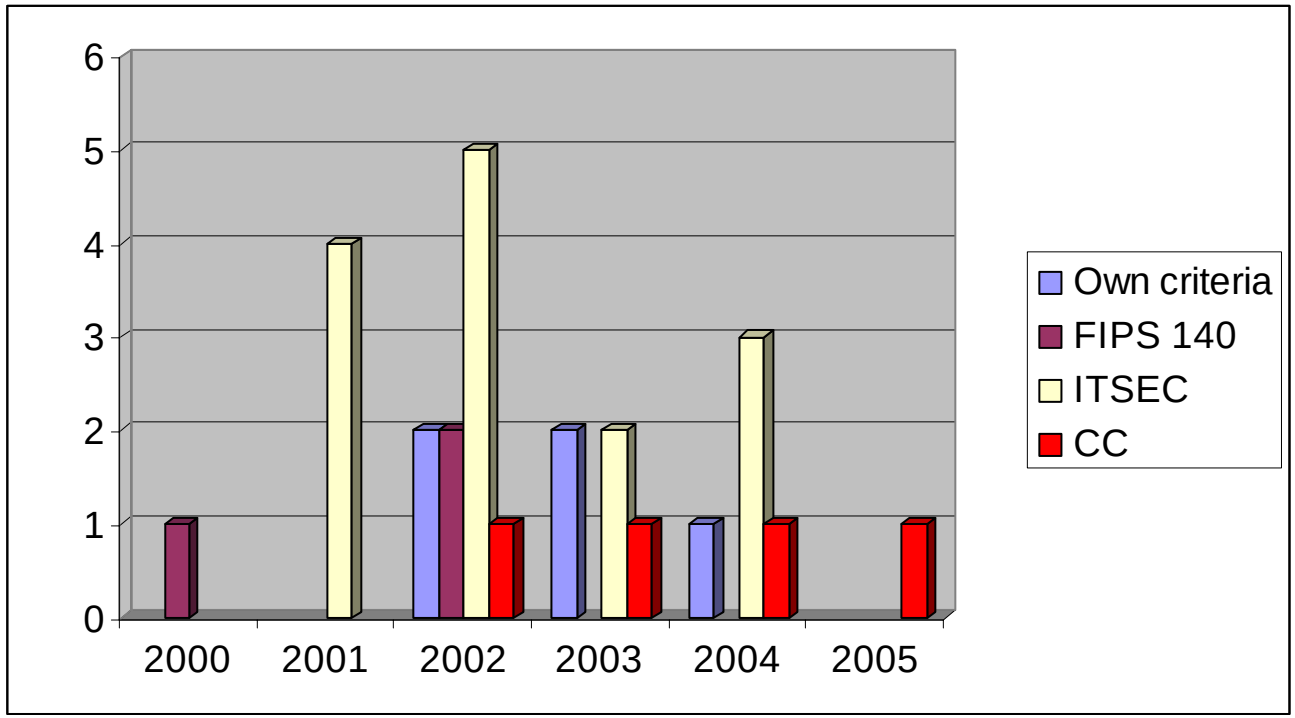
A-SIT confirmations are usually based on certificates issued e.g. in Germany
(not counting re-confirmations or alternative configurations of same device)

Type	#	„own“	FIPS-140	ITSEC	CC	CC-EESSI
SSCD 	9			7 x E4	*2* x EAL4+	(1) *2nd configur.*
Card reader 	7			7 x E2		
Software (viewer) 	6	5			1 x EAL3+	
HSMs (CAs) 	3		1 x level 4 2 x level 3		(*1 x re-confirmation also EAL4+*)	
Total	25	5	3	14	4	(1) *2nd config. not used*

Herbert.Leitold@a-sit.at

Criteria vs. time

- A-SIT confirmations since 2000 were based on:
  (not counting re-confirmations or configurations of same device)



Herbert.Leitold@a-sit.at

Experiences / Conclusions

(out of Austrian signature & citizen card environment)

- HSM market somehow FIPS-140 dominated
- Reference number not the only vendor-driver
  - Austrian (German, French, …) confirmation against EU Directive suffices
- "Global" CCRA not the only driver for vendors
  - Value of certification against EU Directive beyond EU?
- Trusted path was "show stopper" for applying SSCD-PP for major Citizen Card roll-outs
  - Legal requirement for certified readers gone
  - Vendors "copied" all of SSCD-PP, but did not enforce FTP_TRP
  - One SSCD-PP configuration of bank card exists, but that isn't widely used in the field
- These observations certainly do not put CC or Austrian's decision to join CCRA into question

Herbert.Leitold@a-sit.at

Thank you for your attention

Secure Information Technology Center – Austria

Herbert.Leitold@a-sit. at

http://www.a-sit.at