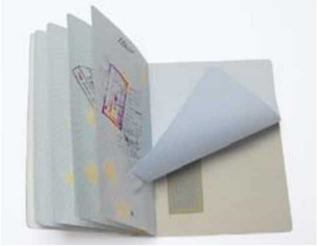
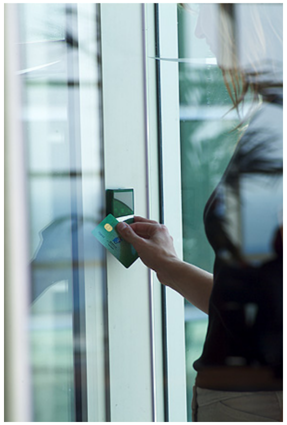
Build a CC assurance package dedicated to your risk assessment

Francois GUERIN
Security Program Manager
francois.guerin@gemalto.com

Gemplus & Axalto merge into Gemalto

- €1.7 billion in combined pro-forma 2005 revenue
- 11,000 employees,1500 R&D engineers
- 21 production sites, 32 personalization and 9 R&D centers

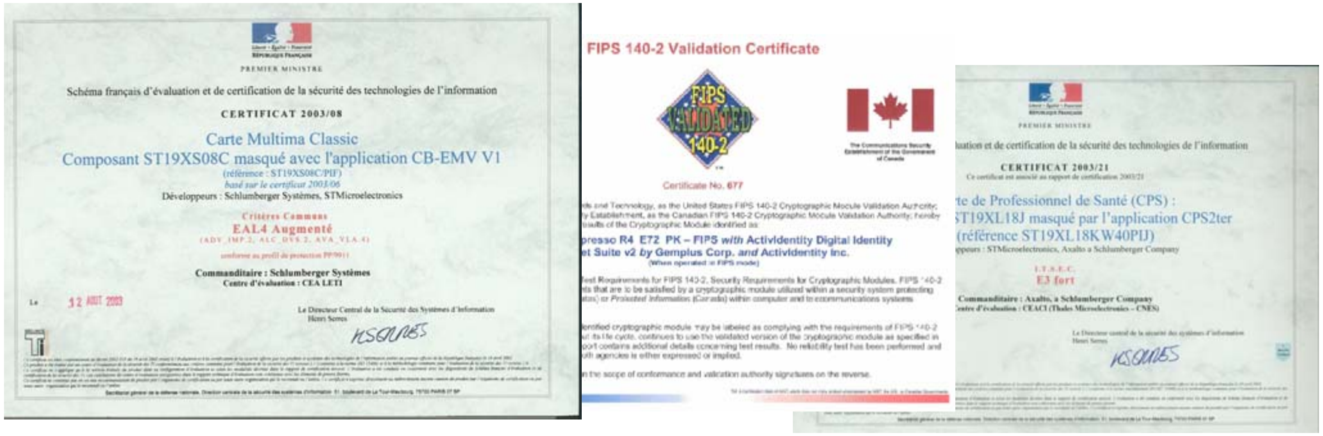




Gemalto delivers secure personal devices, platforms and services, enabling its clients to offer trusted and convenient digital services to billions of individuals

Gemalto experience in security evaluations

- Mastering Standard schemes for smart cards
  - More than 25 CC certificates (From EAL1+ to EAL5+)
  - More than 10 FIPS 140-X and FIPS 201 certificates
  - More than 20 ITSEC certificates
  - 7 sites certified ISO 27001 (some in progress)



PREMIER MINISTRE

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT 2003/08

Carte Multima Classic
Composant ST19XS08C masqué avec l'application CB-EMV V1
(référence : ST19XS08C/PIF)
basé sur le certificat 2003/06
Développeurs : Schlumberger Systèmes, STMicroelectronics

Critères Communs
EAL4 Augmenté
(ADV_IMP.2, ALC_DVS.2, AVA_VLA.4)
conforme au profil de protection PP/9911

Commanditaire : Schlumberger Systèmes
Centre d'évaluation : CEA LETI

Le 12 AOUT 2003

Le Directeur Central de la Sécurité des Systèmes d'Information
Henri Serres

[illegible]

FIPS 140-2 Validation Certificate

The Communications Security Establishment of the Government of Canada

Certificate No. 677

...ds and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority;
...y Establishment, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby
...sults of the Cryptographic Module identified as:

...presso R4 E72 PK – FIPS with ActivIdentity Digital Identity
...et Suite v2 by Gemplus Corp. and ActivIdentity Inc.
(When operated in FIPS mode)

...Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2
...nts that are to be satisfied by a cryptographic module utilized within a security system protecting
...ata) or Protected Information (Canada) within computer and telecommunications systems.

...entified cryptographic module may be labeled as complying with the requirements of FIPS 140-2
...ut its life cycle, continues to use the validated version of the cryptographic module as specified in
...port contains additional details concerning test results. No reliability test has been performed and
...oth agencies is either expressed or implied.

...n the scope of conformance and validation authority signatures on the reverse.

PREMIER MINISTRE

...luation et de certification de la sécurité des technologies de l'information

CERTIFICAT 2003/21
Ce certificat est associé au rapport de certification 2003/21

...te de Professionnel de Santé (CPS) :
...ST19XL18J masqué par l'application CPS2ter
(référence ST19XL18KW40PIJ)
...ppeurs : STMicroelectronics, Axalto a Schlumberger Company

I.T.S.E.C.
E3 fort

Commanditaire : Axalto, a Schlumberger Company
Centre d'évaluation : CEACI (Thales Microelectronics – CNES)

Le Directeur central de la sécurité des systèmes d'information
Henri Serres

[illegible]

- Leader to provide products in private schemes in markets:

  (Banking, MobileCom, PayTV, ID, Transportation, Health, IT,…)

> We spend near 10 M€ per year for product and site evaluations

Setting the problem

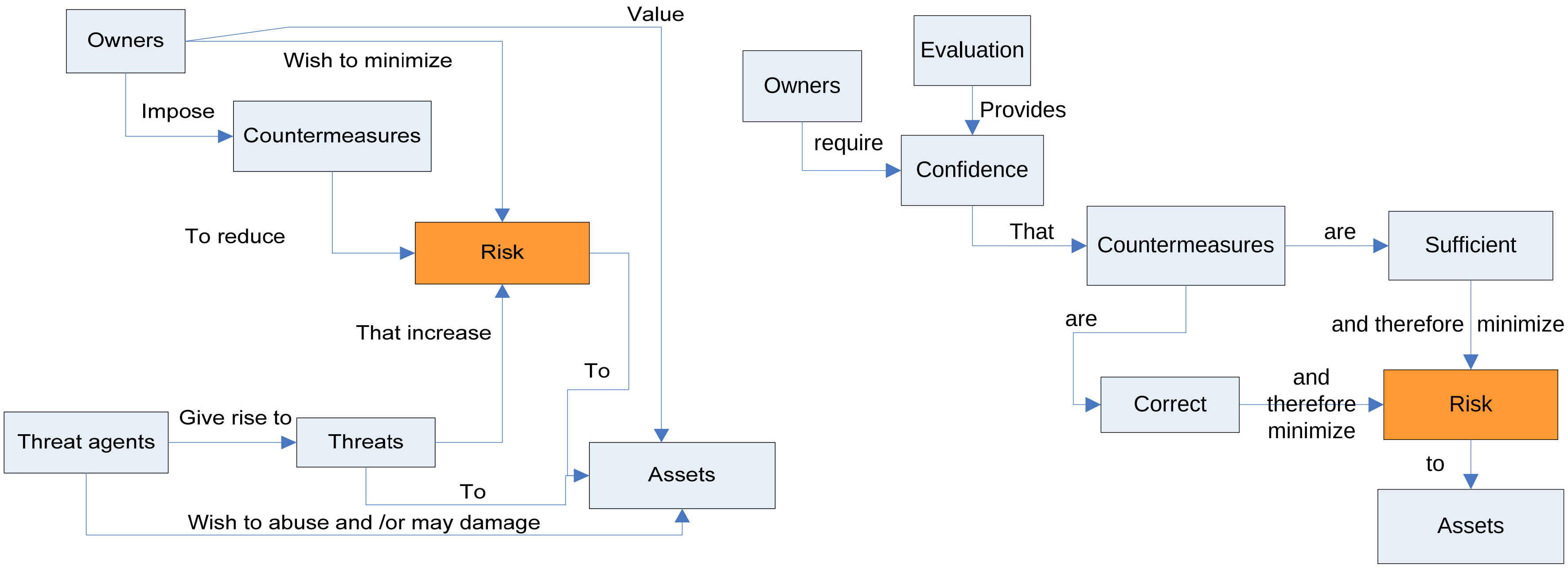
- The EAL4+ level has been chosen in the past as a defacto standard package for smart card evaluation by some sponsors.

- For many customers, it is not now the appropriate answer.

- These customers choose to build a private scheme rather than using an appropriate CC package.

- This presentation would like to say CC may be the solution
  - with the assurance package consistent with our risk assessment.
  - with a security evaluation really connected to risk assessment.

CC security concepts



Risk is one of the major CC concepts but not really used in evaluation

Common questions for customer ?

- How to obtain customer confidence on product ?

- What is the security level expected for such product under evaluation?
- What is the risk acceptable level for such product ?
- What is the actual level of fraud?

- What are the requested correctness and robustness evidences ?

=> I don’t know …

so I request the highest achievable assurance level (EAL4+, EAL5+)

But such evaluation is long and costly, no more relevant with shorter time to market.

Evaluation, risk assessment and acceptance

- The evaluation demonstrates that a correct TOE in combination with a correct operational environment will counter the threats by meeting security objectives for the TOE and the environment.

- The certificate provided by the CB validates the results of the evaluation performed by the evaluator based on the ST.

- The sponsor takes the decision to accept of exposing the assets to the threats by deploying the TOE.

- The sponsor assumes the risks to deploy using evaluation as entry point.

Risk Acceptance : Balance risks vs Benefits

Risks :

Money

Image

Durability of company

Employee & Customer security

Benefits :

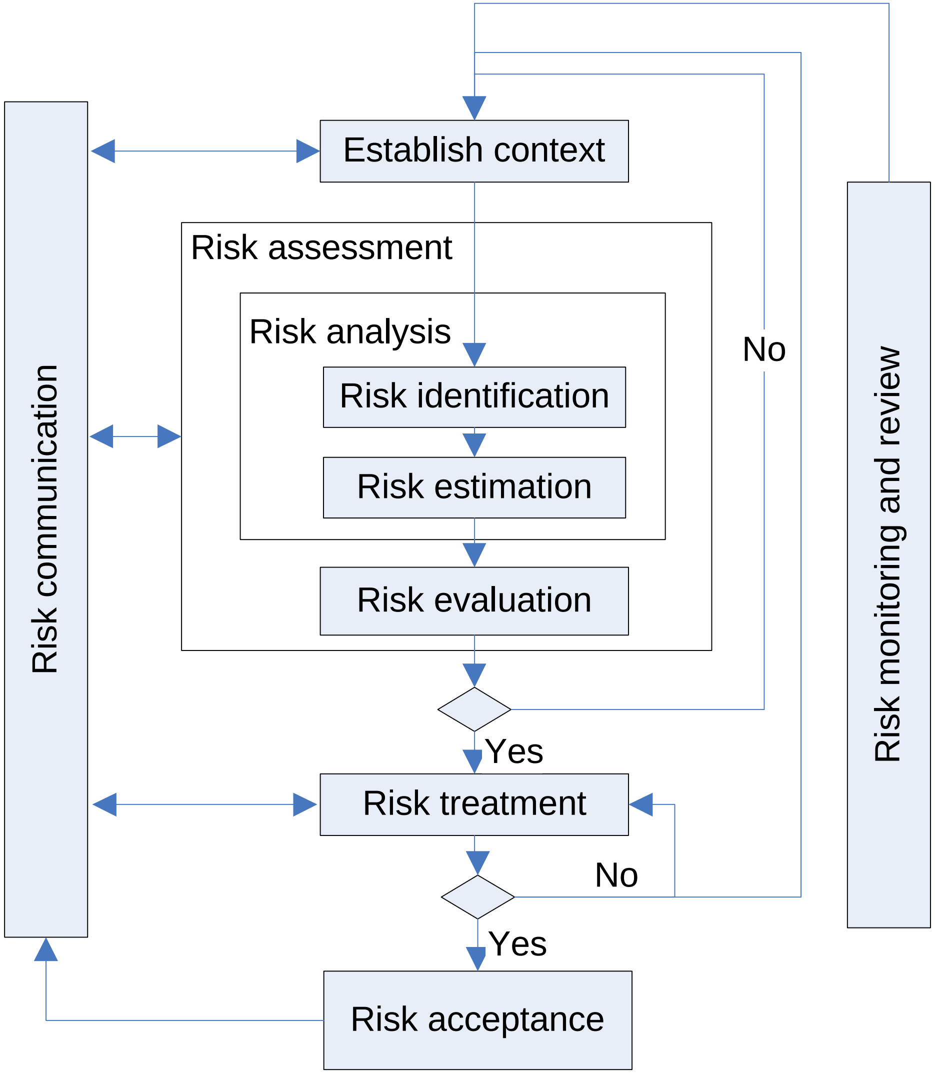
Money

Market share

Competitors

Business opportunity

Risk Management Process (CC & ISO 27005)



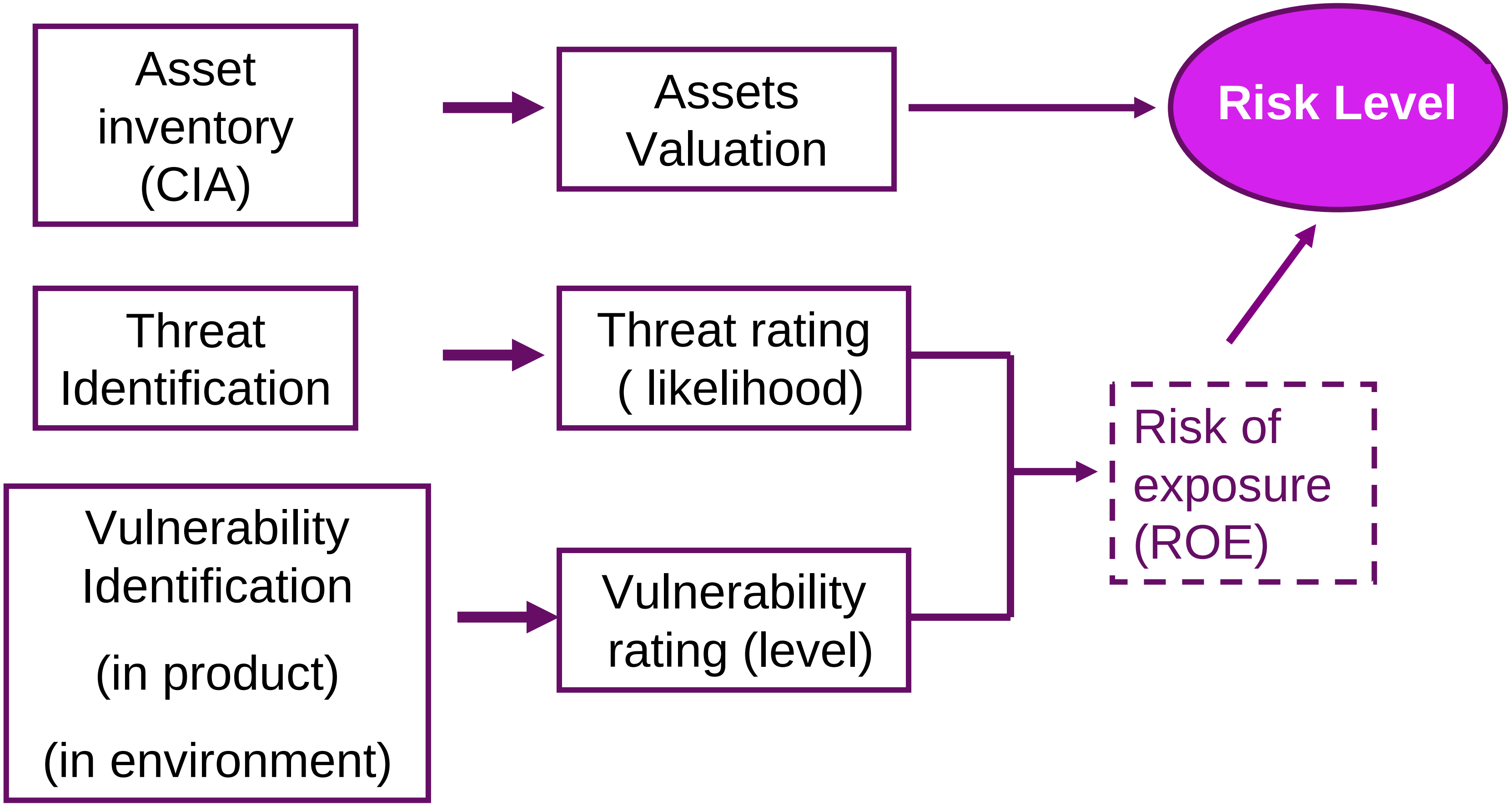
ST

Attack potential defintion

JIL attack quotation table

JIL attack paths reference

Risk Assessment : Risk Level & parameters



Asset Valuation

- Impact that loss of CIA may have on business

- **Confidentiality**: Access is restricted to authorized personnel only
- **Integrity**: Information is accurate and complete
- **Availability**: Information is accessible when required

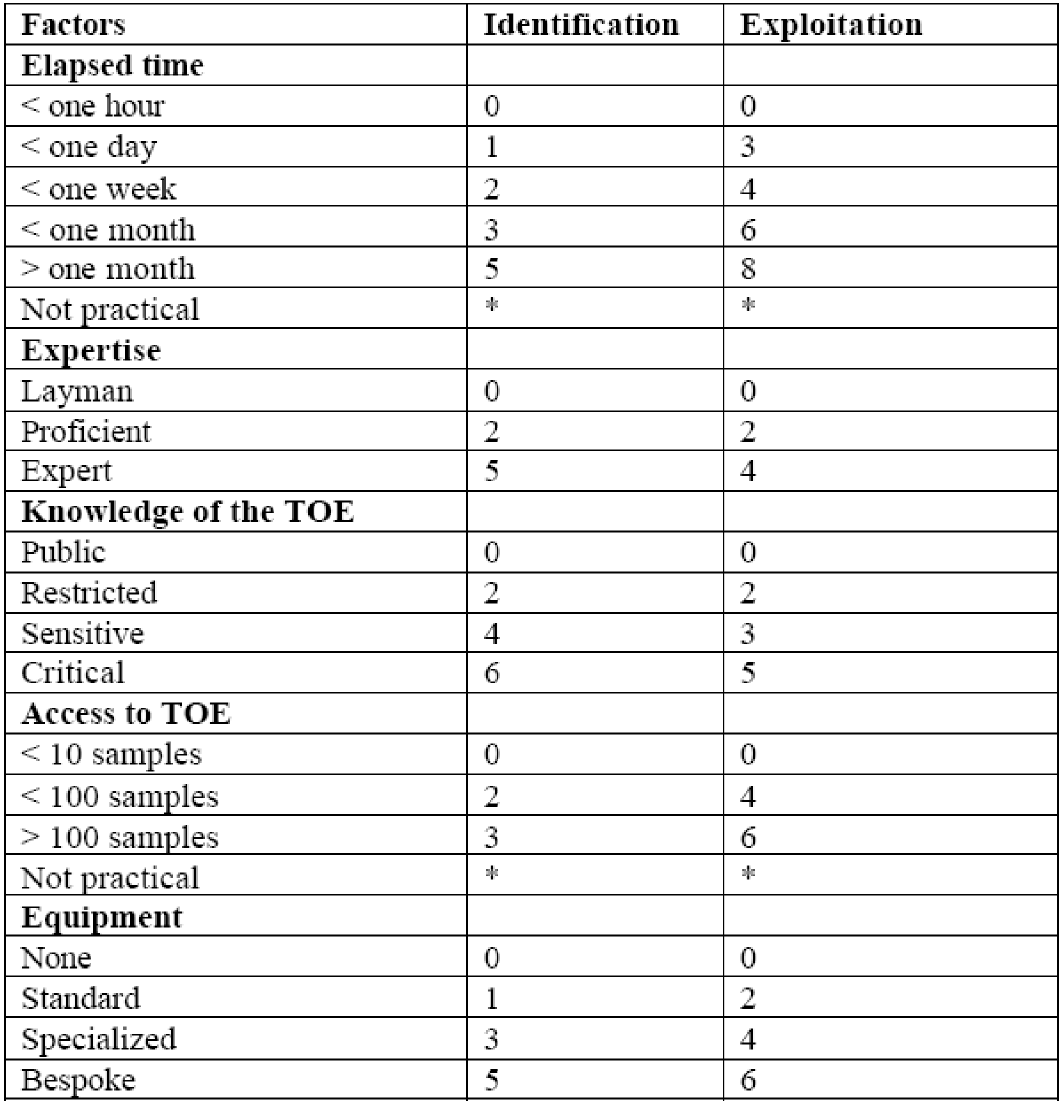
Loss of :	Impact on Business			
	Low	Medium	High	Very high
Confidentiality	1	2	3	4
Integrity	1	2	3	4
Availability	1	2	2	4

Threat definition & way of attack

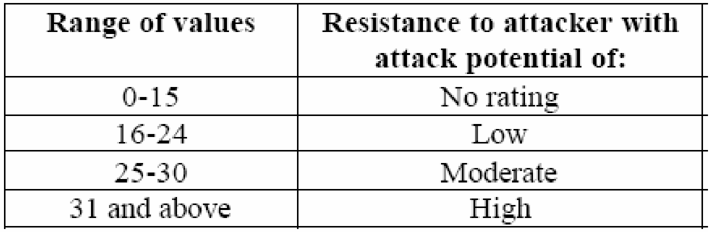
- Threat = Asset (Data & services)
  Threat agent ⇔ Motivation, opportunity
  Way of attack ⇔ Vulnerability

Threat agent / way of attack	Spoofing (mystification,lying)	Tampering (modification)	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Administrators	X	X	X	X		
Competitor	X	X	X	X	X	X
Hacker	X	X	X	X	X	X
Terrorist	X	X	X	X	X	X
Students	X	X		X		X
Authorized user		X	X	X		X
Unauthorized user	X	X	X	X		X

Smartcard attack quotation table from JIL



Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Access to TOE		
< 10 samples	0	0
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized	3	4
Bespoke	5	6



Range of values	Resistance to attacker with attack potential of:
0-15	No rating
16-24	Low
25-30	Moderate
31 and above	High

With CC V2.3

risk of exposure rated [0,5] using Threats, vulnerabilities and attack quotation

Risk Level = ROE * Asset Valuation

Asset Valuation	Risk Of Exposure					
	0	**1**	**2**	**3**	**4**	**5**
1=Low	0	1	2	3	4	5
2=Medium	0	2	4	6	8	10
3=High	0	3	6	9	12	15
4=Very High	0	4	8	12	16	20

Risk level acceptance = management decision

Risk Level	Option for the treatment of risk
0	Risk is very low. No action to be taken.
1 → 2	No additional control to be put in place. Check efficiency of already implemented controls.
3 → 7	Check efficiency of controls already in place. New controls are to be implemented wherever possible.
8 → 12	High level of risk. Requires new controls and permanent monitoring.
13 →16	High level of risk. Immediate actions are decided for the implementation new controls.
17 →20	Risk is intolerable: either the vulnerability can be lowered by an immediate action or the asset can be modified to make it less strategic for the company business, or the risk has to be transferred

What activities for customer confidence ?

- Confidence in Product Security may be obtained through:
  - Risk Management
  - Shared Evaluation Methodology
  - Checks on Product security
  - Checks on Process (Dev, Manufacturing, Perso,Installation, Admin, usage)
  - Checks on Environment (Dev, Manu, Perso, IT)
  - Checks on delivery (roles, procedures, Logical & Physical)

- Confidence increases with the scope of evaluation
  - (balance for confidence increase and cost & delay)

EAL packages with Common Criteria V3.1

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	4	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

For each package, a mix of Product, Process and Environment evaluation

CC assurance classes & risk coverage

	APE	ASE	ADV	AGD	ALC	ATE	AVA
Assurance on Product resistance	X	X	X				X
Assurance on Product correctness	X	X	X	X	X	X	
Assurance on Product Devt Process	X	X	X		X	X	X
Assurance on Product Manufacturing Process	X	X			X		
Assurance on Product Personalization Process	X	X			X		
Assurance on Final Delivery	X	X			X		
Assurance on Guidance for operation	X	X		X			
Assurance on Environment Development	X	X			X		
Assurance on Environment Manufacturing	X	X			X		
Assurance on Environment Personalization	X	X			X		

We should split in different packages according to customer priorities

Risk on environment & CC family coverage

Objective : to be sure that product under construction and associated assets are protected before operational stage

	APE & ASE	ALC_DVS
Assurance on Environment Development	X	X
Assurance on Environment Manufacturing	X	X
Assurance on Environment Personalization	X	X

A BSI proposal is done to cover reusable site evaluation (environment and process).

Risk on product dev assurance & CC coverage (1)

	APE& ASE	ADV_SPM	ADV_FSP	ADV_TDS	ADV_ARC	ADV_IMP	ADV_INT	ALC_CMS	ALC_CMC	AGD_PRE	AGD_OPE
Product Assurance Design evidence	X	X	X	X	X	X	X	X			
Assurance on Product Devt Process	X	X	X	X	X	X	X	X	X		
Assurance on Product Manufacturing Process	X							X	X	X	
Assurance on Product Personalization Process	X							X	X	X	
Assurance on Final Delivery	X							X	X		
Assurance on Guidance for operation	X								X	X	X

Objective : Demonstrate product correctness with:

- check of product deliverable correctness
- check of application of a defined process

Risk on product dev assurance & CC coverage (2)

	ATE_FUN	ATE_COV	ATE_DPT	ATE_IND	ALC_LCD	ALC_TAT	ALC_DEL	ALC_FLR	ALC_DVS
Product Assurance testing evidence	X	X	X	X					
Assurance on Product Devt Process	X	X	X		X	X		X	X
Assurance on Product Manufacturing Process					X	X		X	X
Assurance on Product Personalization Process					X	X		X	X
Assurance on Final Delivery							X		
Assurance on Guidance for operation									

Objective : Demonstrate product correctness with:

- check of product deliverable correctness
- check of application of a defined process

Risk on product resistance & CC coverage

	APE &ASE	ADV_FSP	ADV_ARC	ADV_IMP	AVA_VAN
Product vulnerability search	X	X	X	X	X
Product resistance study					X

Objective : Demonstrate product robustness with:

- search of product vulnerabilities
- performing penetration testing

Example of CC package for medium robustness

Objectives	Focused on major customer issues : Service availability, major asset CIA objectives, No theft of valued services
Risk Management	Context shared (threat, attacker profile, asset, objectives) & SF & vulnerabilities, ready for computation
Evaluation Methodology	Described and shared
Product scope	ST including context (asset valuation, hacker profile, security objectives, and SF)
Product Correctness	No effort
Product Robustness	ADV_FSP.2, ADV_ARC.1, ADV_IMP.1, to only search vulnerabilities AVA_VAN.3 (releasing TDS.3, AGD_X dependencies) and penetration testing with Potential enhanced Basic
Process	No checks
Environment	No checks
Duration	1 + 2 months (EAL4+ # 8 + 4 months)
Cost	< 70 K€ (EAL4+ # 200K€)

Example of a mixed package focused on Product

Objectives	Focused on major customer issues : Service availability, major asset CIA objectives, No theft of valued services
Risk Management	Context shared (threat, attacker profile, asset, objectives) & SF & vulnerabilities, ready for computation
Evaluation Methodology	Described and shared
Product scope	Complete ST (asset valuation, hacker profile, security objectives, SFR and SF)
Product Correctness	ALC_CMC, ALC_CMS, ATE_FUN, ATE_IND
Product Robustness	ADV_FSP.2, ADV_ARC.1, ADV_IMP.1, with evaluator training on product design to help in vulnerability search AVA_VAN. 3 (releasing TDS.3, AGD_X dependencies) and penetration testing with High Potential
Process	No checks
Environment	No checks
Duration	2 + 3 months
Cost	< 100 K€

Answers

CC is a flexible toolbox if you release dependencies.

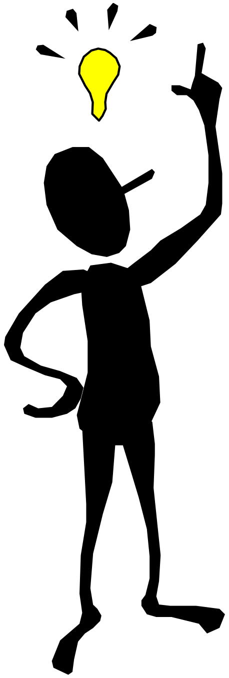
It is possible to define CC packages :

- adapted to a specific customer security objectives,
- consistent with a well defined risk assessment.

The most critical point is the shared risk assessment and the ranking of priorities to set the most effective evaluation scheme with selection of items within:

Product correctness and robustness, process, environment.

Questions



Thank you for your attention