



CC x FIPS140 + ICSA / PCI = ?!#@??

How the CC intersects and compares with other security evaluation programs and what this means for the rest of us.

10th ICCC, September 2009

2 Introductions

■ Lachlan Turner

- Vancouver, Canada
- 8 yrs of IT security experience
- Former CCIMB member.... ‘The CC is like the mafia, once you’re in, you can’t get out!’
- www.linkedin.com/in/lachlanturner



■ DOMUS IT Security Lab

- Ottawa, Canada
- 15 yrs of evaluation experience
- Evaluation is core business
 - CC
 - FIPS
 - PCI ...and more
- www.domusitsl.com



Agenda

1. The 'Security Assurance Landscape'

- The CC isn't alone...
- What other evaluation programs are out there?

2. Analysis

- How do the different programs intersect?
- How do they compare?

3. Conclusions

- What does this mean for vendors?
- What does this mean for the CC?

4 Security Assurance Landscape

- The CC is not alone
- Many evaluation programs exist (30+)
- Let's take a look at them.... briefly!
- **Disclaimer:** This list is not exhaustive but is indicative of the 'security assurance landscape' today.

Technology Groups								
Crypto Security	Mobile Security	Anti-Malware	Content Security	Network Security	IC / SC Security	Auditing Tools	Identity Mgmt	Payment Tech's
Common Criteria – International								PCI PED
CESG Claims Tested Mark* (CCTM) – UK								APACS
First Level Security Certification * (CSPN) – France								INTERAC
BITS Product Certification – US Financial Services								PCI+
In-House Evaluation (Military / Intelligence)								APCA
ICSA Labs					EMVCo	SCAP	FIPS 201	EPCI
FIPS 140		ProtectStar			CAST	-	-	ZKA
-	-	NSS Labs			VHAR	-	-	EP2
-	-	Checkmark			-	-	-	PTS
-	-	PCSL	-	-	-	-	-	CETREL
-	-	CheckViz	-	-	-	-	-	Telekurs
-	-	AVTest	-	-	-	-	-	ETSL
-	-	AVCompare	-	-	-	-	-	PBS
-	-	-	-	-	-	-	-	NETS

Evaluation Programs



Security Assurance Landscape

Crypto Security	Mobile Security	Anti-Malware	Content Security	Network Security	IC / SC Security	Auditing Tools	Identity Mgmt	Payment Tech's
Common Criteria - International								PCI PED
CESG Claims Tested Mark* (CCTM) - UK								APACS
First Level Security Certification * (CSPN) - France								INTERAC
BITS Product Certification - US Financial Services								PCI +
In-House Evaluation (Military / Intelligence)								APCA
ICSA Labs					EMVCo	SCAP	FIPS 201	EPCI
FIPS 140	ProtectStar				CAST	-	-	ZKA
-	-	NSS Labs			VHAR	-	-	EP2
-	-	Checkmark			-	-	-	PTS
-	-	PCSL	-	-	-	-	-	CETREL
-	-	CheckVir	-	-	-	-	-	Telekurs
-	-	AVTest	-	-	-	-	-	ETSL
-	-	AVCompare	-	-	-	-	-	PBS
-	-	-	-	-	-	-	-	NETS

6 Cryptography

Crypto Security	Mobile Security	Anti-Malware	Content Security	Network Security	IC / SC Security	Auditing Tools	Identity Mgmt	Payment Tech's
Common Criteria - International (specification / supporting functionality)								PCI PED
CESG Claims Tested Mark* (CCTM) - UK								APACS
First Level Security Certification * (CSPN) - France								INTERAC
BITS Product Certification - US Financial Services								PCI +
In-House Evaluation (Military / Intelligence)								APCA
ICSA Labs					EMVCo	SCAP	FIPS 201	EPCI
FIPS 140	ProtectStar				CAST	-	-	ZKA
-	-	NSS Labs			VHAR	-	-	EP2
-	-	Checkmark			-	-	-	PTS
-	-	PCSL	-	-	-	-	-	CETREL
-	-	CheckVir	-	-	-	-	-	Telekurs
-	-	AVTest	-	-	-	-	-	ETSL
-	-	AVCompare	-	-	-	-	-	PBS
-	-	-	-	-	-	-	-	NETS

7 Mobile Security

Crypto Security	Mobile Security	Anti-Malware	Content Security	Network Security	IC / SC Security	Auditing Tools	Identity Mgmt	Payment Tech's
Common Criteria - International								PCI PED
CESG Claims Tested Mark* (CCTM) - UK								APACS
First Level Security Certification * (CSPN) - France								INTERAC
BITS Product Certification - US Financial Services								PCI +
In-House Evaluation (Military / Intelligence)								APCA
ICSA Labs					EMVCo	SCAP	FIPS 201	EPCI
FIPS 140	ProtectStar				CAST	-	-	ZKA
-	-	NSS Labs			VHAR	-	-	EP2
-	-	Checkmark			-	-	-	PTS
-	-	PCSL	-	-	-	-	-	CETREL
-	-	CheckVir	-	-	-	-	-	Telekurs
-	-	AVTest	-	-	-	-	-	ETSL
-	-	AVCompare	-	-	-	-	-	PBS
-	-	-	-	-	-	-	-	NETS

8 Anti-Malware

Crypto Security	Mobile Security	Anti-Malware	Content Security	Network Security	IC / SC Security	Auditing Tools	Identity Mgmt	Payment Tech's
Common Criteria - International								PCI PED
CESG Claims Tested Mark* (CCTM) - UK								APACS
First Level Security Certification * (CSPN) - France								INTERAC
BITS Product Certification - US Financial Services								PCI +
In-House Evaluation (Military / Intelligence)								APCA
ICSA Labs					EMVCo	SCAP	FIPS 201	EPCI
FIPS 140	ProtectStar				CAST	-	-	ZKA
-	-	NSS Labs			VHAR	-	-	EP2
-	-	Checkmark			-	-	-	PTS
-	-	PCSL	-	-	-	-	-	CETREL
-	-	CheckVir	-	-	-	-	-	Telekurs
-	-	AVTest	-	-	-	-	-	ETSL
-	-	AVCompare	-	-	-	-	-	PBS
-	-	-	-	-	-	-	-	NETS

Content Security

Crypto Security	Mobile Security	Anti-Malware	Content Security	Network Security	IC / SC Security	Auditing Tools	Identity Mgmt	Payment Tech's
Common Criteria - International								PCI PED
CESG Claims Tested Mark* (CCTM) - UK								APACS
First Level Security Certification * (CSPN) - France								INTERAC
BITS Product Certification - US Financial Services								PCI +
In-House Evaluation (Military / Intelligence)								APCA
ICSA Labs					EMVCo	SCAP	FIPS 201	EPCI
FIPS 140	ProtectStar				CAST	-	-	ZKA
-	-	NSS Labs			VHAR	-	-	EP2
-	-	Checkmark			-	-	-	PTS
-	-	PCSL	-	-	-	-	-	CETREL
-	-	CheckVir	-	-	-	-	-	Telekurs
-	-	AVTest	-	-	-	-	-	ETSL
-	-	AVCompare	-	-	-	-	-	PBS
-	-	-	-	-	-	-	-	NETS

10 Network Security

Crypto Security	Mobile Security	Anti-Malware	Content Security	Network Security	IC / SC Security	Auditing Tools	Identity Mgmt	Payment Tech's
Common Criteria - International								PCI PED
CESG Claims Tested Mark* (CCTM) - UK								APACS
First Level Security Certification * (CSPN) - France								INTERAC
BITS Product Certification - US Financial Services								PCI +
In-House Evaluation (Military / Intelligence)								APCA
ICSA Labs					EMVCo	SCAP	FIPS 201	EPCI
FIPS 140	ProtectStar				CAST	-	-	ZKA
-	-	NSS Labs			VHAR	-	-	EP2
-	-	Checkmark			-	-	-	PTS
-	-	PCSL	-	-	-	-	-	CETREL
-	-	CheckVir	-	-	-	-	-	Telekurs
-	-	AVTest	-	-	-	-	-	ETSL
-	-	AVCompare	-	-	-	-	-	PBS
-	-	-	-	-	-	-	-	NETS

Crypto Security	Mobile Security	Anti-Malware	Content Security	Network Security	IC / SC Security	Auditing Tools	Identity Mgmt	Payment Tech's
Common Criteria - International								PCI PED
CESG Claims Tested Mark* (CCTM) - UK								APACS
First Level Security Certification * (CSPN) - France								INTERAC
BITS Product Certification - US Financial Services								PCI +
In-House Evaluation (Military / Intelligence)								APCA
ICSA Labs					EMVCo	SCAP	FIPS 201	EPCI
FIPS 140	ProtectStar				CAST	-	-	ZKA
-	-	NSS Labs			VHAR	-	-	EP2
-	-	Checkmark			-	-	-	PTS
-	-	PCSL	-	-	-	-	-	CETREL
-	-	CheckVir	-	-	-	-	-	Telekurs
-	-	AVTest	-	-	-	-	-	ETSL
-	-	AVCompare	-	-	-	-	-	PBS
-	-	-	-	-	-	-	-	NETS

12 Security Audit Tools

Crypto Security	Mobile Security	Anti-Malware	Content Security	Network Security	IC / SC Security	Auditing Tools	Identity Mgmt	Payment Tech's
Common Criteria - International								PCI PED
CESG Claims Tested Mark* (CCTM) - UK								APACS
First Level Security Certification * (CSPN) - France								INTERAC
BITS Product Certification - US Financial Services								PCI +
In-House Evaluation (Military / Intelligence)								APCA
ICSA Labs					EMVCo	SCAP	FIPS 201	EPCI
FIPS 140	ProtectStar				CAST	-	-	ZKA
-	-	NSS Labs			VHAR	-	-	EP2
-	-	Checkmark			-	-	-	PTS
-	-	PCSL	-	-	-	-	-	CETREL
-	-	CheckVir	-	-	-	-	-	Telekurs
-	-	AVTest	-	-	-	-	-	ETSL
-	-	AVCompare	-	-	-	-	-	PBS
-	-	-	-	-	-	-	-	NETS

13 Identity Management

Crypto Security	Mobile Security	Anti-Malware	Content Security	Network Security	IC / SC Security	Auditing Tools	Identity Mgmt	Payment Tech's
Common Criteria - International								PCI PED
CESG Claims Tested Mark* (CCTM) - UK								APACS
First Level Security Certification * (CSPN) - France								INTERAC
BITS Product Certification - US Financial Services								PCI +
In-House Evaluation (Military / Intelligence)								APCA
ICSA Labs					EMVCo	SCAP	FIPS 201	EPCI
FIPS 140	ProtectStar				CAST	-	-	ZKA
-	-	NSS Labs			VHAR	-	-	EP2
-	-	Checkmark			-	-	-	PTS
-	-	PCSL	-	-	-	-	-	CETREL
-	-	CheckVir	-	-	-	-	-	Telekurs
-	-	AVTest	-	-	-	-	-	ETSL
-	-	AVCompare	-	-	-	-	-	PBS
-	-	-	-	-	-	-	-	NETS

Payment Technologies

Crypto Security	Mobile Security	Anti-Malware	Content Security	Network Security	IC / SC Security	Auditing Tools	Identity Mgmt	Payment Tech's
Common Criteria - International (can also be applicable)								PCI PED
CESG Claims Tested Mark* (CCTM) - UK								APACS
First Level Security Certification * (CSPN) - France								INTERAC
BITS Product Certification - US Financial Services (possibly applicable)								PCI +
In-House Evaluation (Military / Intelligence)								APCA
ICSA Labs					EMVCo	SCAP	FIPS 201	EPCI
FIPS 140	ProtectStar				CAST	-	-	ZKA
-	-	NSS Labs			VHAR	-	-	EP2
-	-	Checkmark			-	-	-	PTS
-	-	PCSL	-	-	-	-	-	CETREL
-	-	CheckVir	-	-	-	-	-	Telekurs
-	-	AVTest	-	-	-	-	-	ETSL
-	-	AVCompare	-	-	-	-	-	PBS
-	-	-	-	-	-	-	-	NETS

Overwhelmed?

- Vendors can have lot of hoops to jump through...
 - Can vendors leverage evidence across programs?
 - Do the programs compliment each other?
 - Are they faster, more effective, better, or just different to CC?



Where are we?

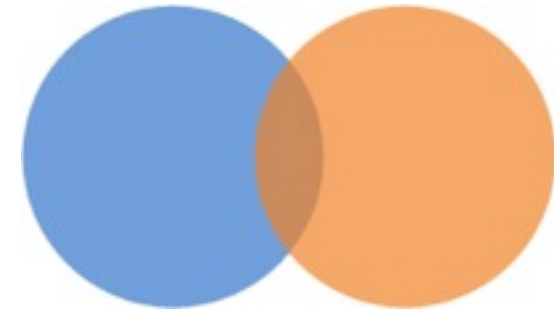
1. The 'Security Assurance Landscape' ✓
2. Analysis
 - How do the different programs intersect with CC?
 - How do they compare to the CC?
3. Conclusions



17 CC Relationships to...

- **FIPS 140-2** (Cryptographic Module Validation)
- **FIPS 201** (US Identity Management)
- **APACS** (UK Payments Association)
- **PCI PED** (Payment Card Industry)
- **BITS** (US Financial Services)

CC and FIPS 140

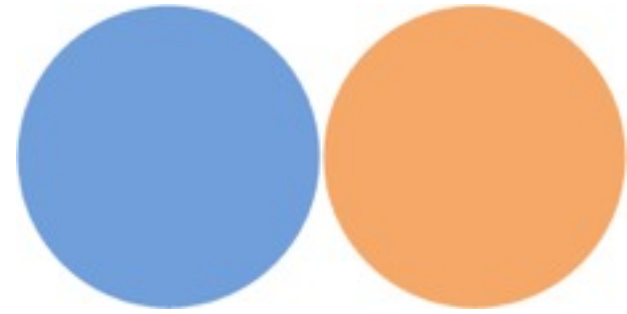


- FIPS 140
 - Cryptographic module validation
 - US/Canada centric (but widely recognized)

- CC doesn't cover evaluation of crypto
- CC does cover specification of crypto
- FIPS140-2 Levels 2, 3 & 4 require CC evaluation of the operational environment
- Some CC schemes require FIPS140-2 validation of crypto components of the CC TOE

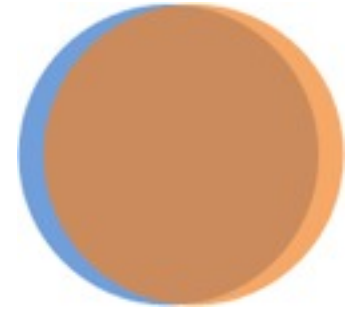
- Can be an overlap of input evidence
 - E.g. self protection

CC and FIPS 201



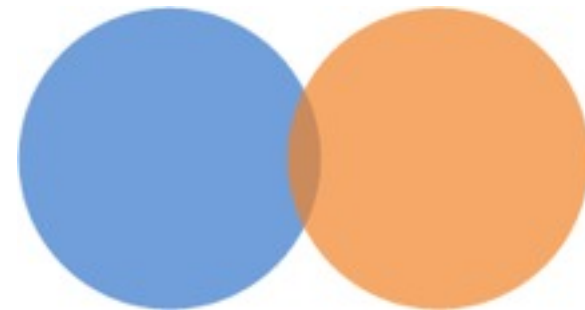
- FIPS 201 (NPIVP)
 - US Personal Identity Verification (PIV) framework
 - Incorporates PIV card application and middleware **conformance testing** to NIST SP 800-73
- No intersection between CC and FIPS 201 but...
- NVLAP labs perform the conformance testing (who also do CC)
- PIV card applications must run on FIPS 140-2 validated platform
- May be input evidence overlap

CC and APACS



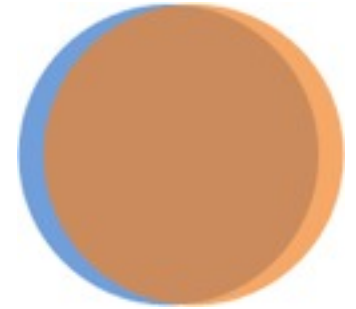
- APACS
 - UK Payment Administration
 - PIN Entry Device security evaluation
- APACS use a Protection Profile to specify PED requirements
- Evaluations performed by 'CCRA' labs
- APACS perform the role of Certification Body
- Input evidence is the same

CC and PCI PED



- PCI PED
 - Payment Card Industry
 - PIN Entry Device (PED) security evaluation
- Prescriptive requirements set related to PED security
- Looks more like FIPS 140 than CC
- Some evidence overlap (e.g. 1 device undergoing both APACS and PCI PED evaluations would be able to leverage evidence across both)

CC and BITS



- BITS
 - US Financial Services Round Table
 - Security evaluation of IT products for use within the US financial services industry
- BITS specify a suite of CC packages
- Vendors conform with CC packages and undergo a standard CC evaluation
- BITS confirm and apply the 'BITS Tested Mark'
- Input evidence the same – some additional reporting.

Where are we?

1. The 'Security Assurance Landscape' ✓
2. Analysis
 - How do the different programs intersect with ✓CC?
 - How do they compare to the CC?
3. Conclusions



Comparison of the CC with...

- FIPS 140-2
- ICSA Labs



25 How to compare?

Functional Scope	What functionality is within scope of the program?
Assurance Claims	How is assurance claimed?
Assurance Domains	What does the consumer have assurance in?
Assurance Life-cycle	How long does the assurance last?
Assurance Methodology	How is assurance gained?
Time/Effort	How much effort is required (reflected by time)?
Measure of Effectiveness	How is effectiveness measured?
Program Governance	How is the program organized?

26 Functional Scope

CC	FIPS140-2	ICSA Labs
All security functionality (except crypto)	Cryptographic Modules	<ul style="list-style-type: none">• Anti-spam• Anti-spyware• Anti-virus• Firewalls• IPSec• Network Intrusion

27 Assurance Claims

CC	FIPS140-2	ICSA Labs
<ul style="list-style-type: none">• EALs 1 - 7• Custom Packages• Extensible	Security Levels 1- 4	1 Level 'ICSA Labs Certified'

28 Assurance Domains

CC	FIPS140-2	ICSA Labs
<ul style="list-style-type: none">• Design• Development• Implementation• Guidance• Delivery	<ul style="list-style-type: none">• Design• Configuration Mgmt• Implementation• Delivery	<ul style="list-style-type: none">• Implementation

29 Assurance Lifecycle

CC	FIPS140-2	ICSA Labs
<ul style="list-style-type: none">• Point in time• Specific version• Assurance continuity a separate, optional process	<ul style="list-style-type: none">• Point in time• Specific version	<ul style="list-style-type: none">• Ongoing• Incorporates new versions• Periodic re-test• Vendor must address discovered vulnerabilities

Assurance Methodology

CC	FIPS140-2	ICSA Labs
<ul style="list-style-type: none">• Claims based• Top down• Design / documentation focus• Heavy certification	<ul style="list-style-type: none">• Requirements based• Design review• Testing focus• Heavy certification oversight	<ul style="list-style-type: none">• Requirements based• Black box testing• No certification oversight

Time / Effort

CC	FIPS140-2	ICSA Labs
<ul style="list-style-type: none">8 - 24 months	<ul style="list-style-type: none">6 - 8 months	<ul style="list-style-type: none">Months..(don't have numbers but assume a month or

Measure of Effectiveness

CC	FIPS140-2	ICSA Labs
<ul style="list-style-type: none">• None	<ul style="list-style-type: none">• Metrics recorded by certification body	<ul style="list-style-type: none">• Metrics recorded by lab

- Metrics are typically based on non-compliances

33 Program Governance

CC	FIPS140-2	ICSA Labs
<ul style="list-style-type: none">• Many labs• Many accreditation bodies• Many certification bodies• CCRA governance body	<ul style="list-style-type: none">• Many labs• One certification body (US, Canada)• One accreditation body• Small governance	<ul style="list-style-type: none">• One lab• Input from industry bodies (criteria development)

34 Analysis Summary

- There are many assurance programs, differentiated by:
 - Functional scope
 - Assurance scope and depth
 - Audience
- Other evaluation programs with shorter timeframes differ from the CC:
 - Requirements based (CC is claims based)
 - Limited scope
 - Less depth of assurance (development practices)
 - Less formal recognition
 - Less parties involved in governance
 - Not extensible
- There is no coordinated effort to measure the CC's effectiveness.

Where are we?

1. The 'Security Assurance Landscape' ✓
2. Analysis ✓
3. Conclusions
 - What does this mean for vendors?
 - What does this mean for the CC?



Vendors

- Take a strategic approach to evaluation
 - No one size fits all
 - Ensure optimal selection of evaluation programs, scope and assurance level
 - Leverage resources / evidence across programs
 - Ongoing certification strategy – design & development

- Look for evaluation partners that can provide support across multiple evaluation programs
 - E.g. PIN Entry Device vendors – significant efficiencies to be gained by leveraging effort across programs
 - E.g. CC and FIPS 140 – both in one lab, can be parallel

Common Criteria Directions



- **Measuring effectiveness?**
 - Can we measure the effectiveness of the CC program?
 - Can we implement informed continuous improvement?

- **Depth of assurance (development practices)?**
 - Can we (officially) separate development assurance (ALC), from design and implementation assurance (ASE, ADV, AGD, AVA)?
 - E.g. Vendor can have development practices evaluated and certified separately from a TOE evaluation.

Common Criteria Directions

- **Claims based (move to requirements based)?**
 - Can we foster international collaboration on an agreed set of PPs and supporting guidance?
 - E.g. similar to European efforts with ICs / Smartcards

- **Governance**
 - Can we introduce innovations to streamline governance over the CC?
 - E.g. metrics based decision support tools

Where are we?

1. The 'Security Assurance Landscape'
2. Analysis
3. Conclusions



Questions?

