



Why isn't there reuse of certification requirements?

Scott Shorter, Cisco Systems

Eve Pierre, SAIC

Outline

- History
- Early Days
- CCRA and Mutual Recognition
- Benefit of Mutual Recognition
- CC Schemes Drifting Apart
- Area of Divergence
- Why Certification Reuse is Desirable
- CC and Crypto – Reuse Scenarios
- Summary

History

- 1983 TCSEC (Orange Book)
- 1990 ITSEC (introduced Security Targets)
- 1993 CTCPEC (hybrid approach)
- 1996-2000 CCRA and Mutual Recognition
- 1996 CC V1.0 published
- 1999 CC V2.1 published
- 2005 CC V2.3 published
- 2000-2006 Vendors free to evaluate
- 2006 CC V3.1 Release 1 Published
- 2009 CC V3.1 Release 3 published
- 2007-2010 CC Schemes drifting in policy and approach

Early days

- 1983 TCSEC (Orange Book)
 - Fixed set of functional requirements
- 1990 ITSEC (introduced Security Targets)
 - Vendor could select appropriate functionality
- Each country had its own set of requirements and they perform their evaluation based on their own needs.
- Vendors had to evaluate the same product in different countries, with different methodologies.

Early days

- The Common Criteria emerged as the convergence of requirements and methodologies from several countries
- 1993 – 1996 - Concerted international efforts to put together the set of common requirements
- 1996 – 2000 – Trial evaluations performed by all parties involved

CCRA and Mutual Recognition

- Common Criteria Recognition Arrangement signed in October of 1998 by United States, Canada, France, Germany, the Netherlands and the United Kingdom
- Ratified in 2000 by current membership
- Mutual recognition permits international reuse of CC certifications

Benefits of Mutual Recognition

- Industry has a fixed set of resources to apply to a problem, vendors can either focus resources on making products better and evaluating their security once, or divert the effort into spending time doing incompatible, non-reusable certifications in different regions or countries
 - Some vendors cannot afford a single certification, let alone multiple certifications in different countries
- Governments can come together globally to determine the best certification approach and help the vendors scale better to meet the increasing demand

CC Schemes Drifting Apart?

- Different schemes have developed differing requirements
- The collective effect of years of policy interpretation has led to differences in the CC process between countries.
- PP can stipulate country specific certification requirements
- How to obtain mutual recognition of certifications other than CC?

Areas of Divergence

- How Development Life Cycle is evaluated
- Schemes Policies
- Protection Profiles
- Cryptographic Requirements

Areas of Divergence

- How Development Life Cycle is evaluated
 - Mandatory Site Visit
 - Audit of development environment
 - Audit of CM System
- Schemes Policies
 - Limits on duration of evaluation
 - Requirements for getting into evaluation
 - Advertised features must be included in the TOE
 - LOI
 - Validated ST
- Protection Profiles
 - Not all certificate producing Schemes develop PPs
 - Extended requirements in PPs

Areas of Divergence

- Cryptographic requirements

The greatest area of divergence among schemes

Originally, assessment of the suitability of cryptographic mechanisms was deemed out of scope of CC

Different national policies impose requirements on products for sale in those countries

Area of Divergence

A survey of Different National Approaches to Cryptography

- CC Producing Countries Surveyed

Australia

Canada

France

Germany

United Kingdom

United States

Area of Divergence

A survey of Different National Approaches to Cryptography

- Differing approaches to cryptographic requirements in CC Schemes results in
 - Unique national cryptographic policies
 - Unconstrained search and testing for cryptographic vulnerabilities
 - Policies that require compliance with hard to locate external publications
 - Certification that is considered sufficient for one scheme may not be accepted by other schemes only for certain assurance levels

Area of Divergence

A survey of Different National Approaches to Cryptography

- Characteristics of National Cryptographic Policies

- Lists of permitted algorithms
- Schedule of required security strengths
- Certification required

FIPS 140-2

DCE

CAPS

- Crypto in Protection Profiles
- On algorithms and security strengths there is general consensus, but different national policies impose different schedules for strengthening cryptography.
 - Example: NIST SP 800-131 versus BSI requirements on security strengths for use with signatures (next slide)

Area of Divergence

Germany Security Strength Requirements for Signatures

**Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen**

**Bekanntmachung zur elektronischen Signatur
nach dem Signaturgesetz und der Signaturverordnung
(Übersicht über geeignete Algorithmen)**

Vom 06. Januar 2010

Die folgende Tabelle fasst die minimalen Bitlängen zusammen.

Zeitraum	bis Ende 2010	bis Ende 2016
Parameter		
n	1728 (Mindestw.) 2048 (Empf.)	1976 (Mindestw.) 2048 (Empf.)

Die folgende Tabelle fasst die Eignung der Hashfunktionen zusammen.

Erzeugung qualifizierter Zertifikate*:	Erzeugung qualifizierter Zertifikate**:	geeignet bis Ende 2010	geeignet bis Ende 2015	geeignet bis Ende 2016
geeignet bis Ende 2009	geeignet bis Ende 2010			
SHA-1	SHA-1	RIPEMD-160	SHA-224 (SHA-1, RIPEMD-160)***	SHA-256, SHA-384, SHA-512

*d.h. zur Erzeugung qualifizierter Zertifikate, nicht aber zur Erzeugung und Prüfung anderer qualifiziert signierter Daten.

** d.h. zur Erzeugung qualifizierter Zertifikate mit mindestens 20 Bit Entropie der Seriennummer, nicht aber zur Erzeugung und Prüfung anderer qualifiziert signierter Daten.

***ausschließlich zur Prüfung qualifizierter Zertifikate.

You read that correctly – SHA-1 is not permitted in digital certificate generation after 2010.

Area of Divergence

A survey of Different National Approaches to Cryptography

- Australia and New Zealand

 - Australia has published no PPs to date, but if crypto is in the product a DCE is required

- Canada

 - Does not promulgate crypto policy by protection profile
 - Mutual Recognition on FIPS 140-2

- France

 - PPs require compliance with unique national cryptographic policies

- Germany

 - Few or no FCS requirements in Protection Profiles for most technologies, but PPs exist for cryptographic modules of various security strengths.

 - Appear to map nicely to FIPS 140-2

- United Kingdom

 - A CAPS is required – Requirements are not publicly listed

Area of Divergence

A survey of Different National Approaches to Cryptography

■ United States

Cryptographic Requirements are generally present in CCEVS PPs, how it is required varies greatly

- Some PPs require FIPS 140-2 in the environment
- Some PPs explicitly stipulate required security strengths
- More recent PPs require a FIPS 140-2 validated module in the TOE
- Some PPs exceed FIPS 140-2 in explicitly stated cryptographic requirements – even basic robustness PPs

Examples: Wireless Access System PP requiring multiple overwrites of keys, key integrity checks on all internal transfers, etc.

Area of Divergence

A survey of Different National Approaches (United States)

- ‘FIPS Plus” in the TOE example

Wireless LAN Client PP:

FCS_BCM_(EXT) requires FIPS 140-2

Security levels spelled out for software/hybrid/hardware that exceed the Army Letter

Other FCS requirements exceed FIPS 140-2

Key generation requirements cite FIPS and add SP 800-57 key integrity protections

Persistent keys must be stored encrypted or in split knowledge when not in use

Keys must be destroyed after an admin specified period of inactivity

Area of Divergence – Crypto

A survey of Different National Approaches (United States)

- Downside of ‘FIPS Plus’

Reuse of FIPS 140-2 certification is impossible because the PP’s cryptographic functional requirements exceed FIPS 140-2

A certified module needs to be modified to meet the PP, and then FIPS 140-2 certified again

- Additional vendor cost
- Additional time

Use of Certification in CC Evaluation

- Government Policies governing the purchase of trusted products require products certification
- In the US for example, government policies require
 - FIPS 140-2
 - SCAP
 - WiFi
 - IPv6
- Where possible certification reuse would lessen the burden on vendors and

CC and Crypto – Reuse Scenarios

- Certify crypto in the TOE Environment
 - Easier to evaluate
 - Quite suitable for external crypto modules (e.g. HSMs)
- Include validated module as a component in the TOE
FCS requirements will be met by default
- Keep FCS requirements from PP
- An international set of common cryptographic requirements should become standard

CC and Crypto – Reuse Scenarios

- Follow the model of the German CSP PPs (or use them if suitable)

Is it possible to model FIPS 140-2 with those PPs?

Products could claim conformance to a Crypto PP and also the PP for their technology type

Structure Crypto PPs to permit national policies on algorithms and security strengths by reference.

Structure non-Crypto PPs to allow the ST to be written to a Crypto PP of the appropriate level

Summary

- Mutual Recognition has been a tremendous boost to the success of Common Criteria
 - Instant global market for certified products
 - Evaluation labs and evidence developers have an international customer base
 - Vendors have numerous labs and schemes to choose from
- Proliferation of one-time or incompatible certification requirements for cryptography or anything else will reduce those benefits
 - Certified products might not meet local requirements
 - Vendors will have incentive to stick with evaluation labs in their primary markets
- We need find a way to express cryptographic requirements in a mutually recognized and consistent manner

Contact Information

- Scott Shorter, Global Certifications Team, Cisco, scoshort@cisco.com
- Eve Pierre, AT&E Lab, SAIC, marie.e.pierre@saic.com