# Purpose-driven development of cPPs and related documents

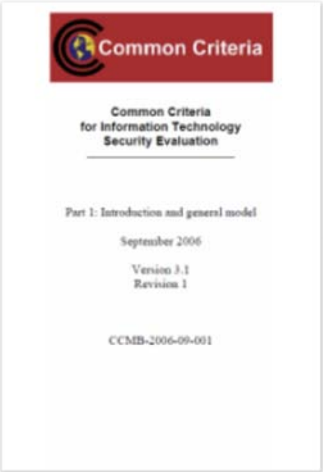
RICOH
imagine. change.

12 September, 2013

Brian Smithson
Senior Security Architect
Global Solutions Engineering
Ricoh Americas

iccc
SEPTEMBER 10-12 • ORLANDO
INTERNATIONAL COMMON CRITERIA CONFERENCE
2013

# Purpose of a Protection Profile



Common Criteria

Common Criteria
for Information Technology
Security Evaluation

Part 1: Introduction and general model

September 2006

Version 3.1
Revision 1

CCMB-2006-09-001

TECHNICAL REPORT

ISO/IEC
TR
15446

First edition
2004-07-01

Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets

Technologies de l'information — Techniques de sécurité — Guide pour la production de profils de protection et de cibles de sécurité

Reference number
ISO/IEC TR 15446:2004(E)

© ISO/IEC 2004

- “an implementation-independent structure for consumer groups and communities of interest to express their security requirements in an unambiguous manner”

- “a document that defines the customer’s security requirements in a formalised, standardised way”

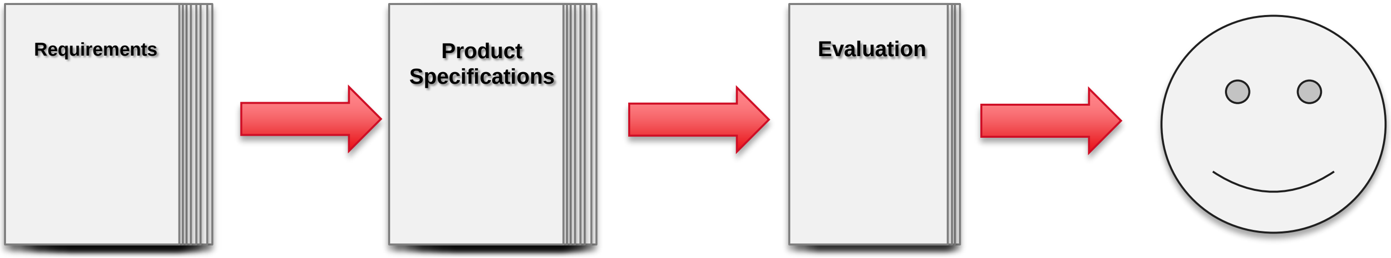
- “states a security problem rigorously for a given collection of system or products […] and to specify security requirements to address that problem without dictating how these requirements will be implemented.”

# It’s a simple idea

- Customers (or their representatives) specify security requirements in a common format
- Product vendors respond by designing products that fulfill the requirements
- Those products are evaluated using a common methodology
- Result: customers have some assurance that certified products fulfill their security requirements

# It’s not new

- Removing “Common” from Common Criteria:
  - Individual nations expressed their individual requirements
  - Vendors responded with products
  - Nations evaluated them using their individual methods and criteria
  - And then they bought the products



# “Common” made it complex

- After nations agreed on a Common Criteria:
  - PPs must use a common expression and format for requirements
  - Nation-specific requirements must be harmonized, or they are left out of the process
  - Certificate-issuing schemes list PPs that they’ve developed and products that they’ve validated
  - The CC Portal collects every nation’s PPs and products
  - CCRA nations mutually recognize PPs and certified products

***But do they actually agree with the PPs and purchase the certified products?***

**PP := Protection Profile  CC := Common Criteria  CCRA := Common Criteria Recognition Arrangement**

# A focus on procurement

- In the new CC Recognition Arrangement:
  - PPs are intended to be used for procurement purposes by multiple nations
  - To do that, cPPs will be proposed for types of products
  - CCRA nations will express their level of commitment to proposed cPPs
  - ESRs will be written to broadly describe the security problem
  - iTCs will be formed to create cPPs and Supporting Documents

- Result:
  - ***cPPs are more likely to be accepted by CCRA nations***
  - ***Products conforming to cPPs are more likely to be purchased***

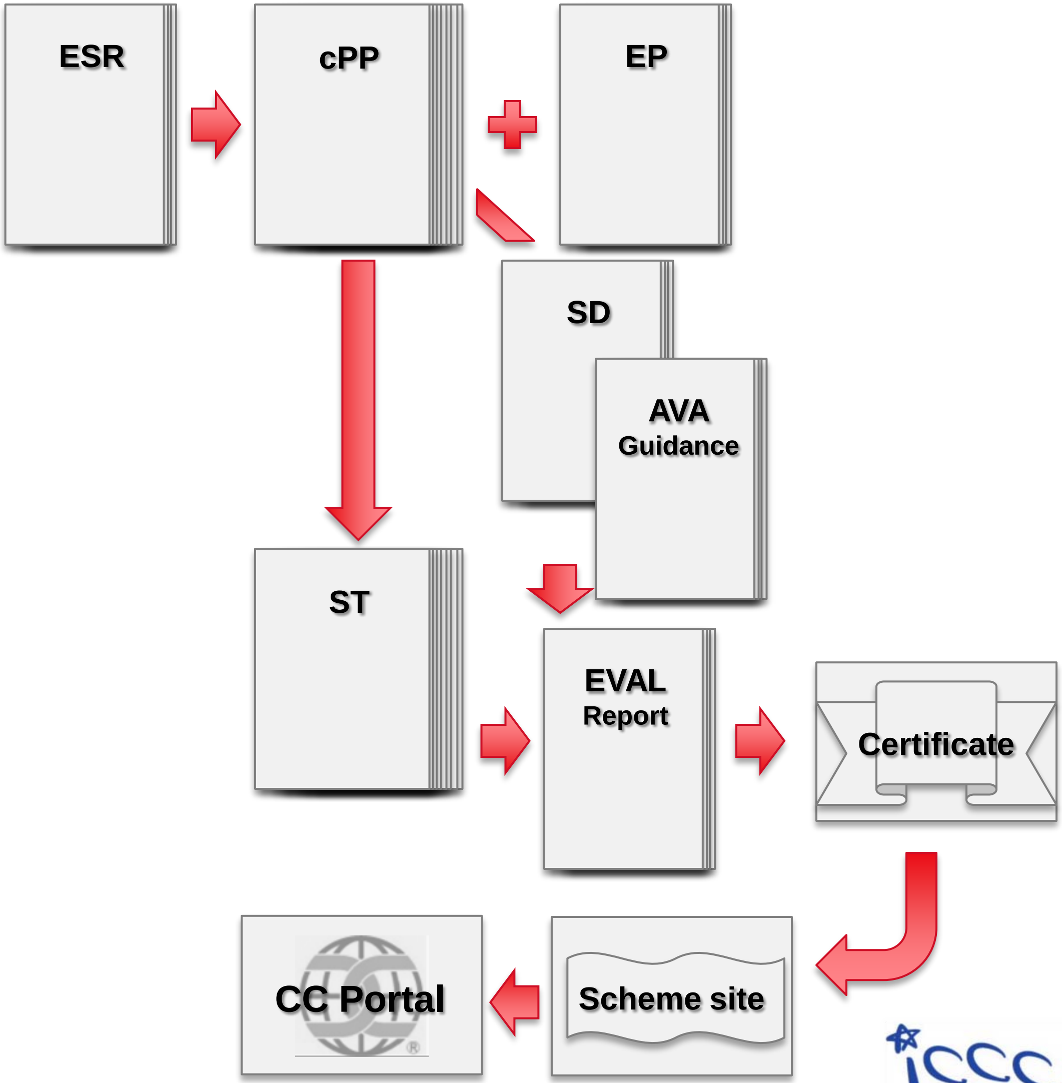
**cPP := Collaborative Protection Profile ESR := Essential Security Requirements iTC := International Technical Community**

# To make that work…

- iTCs are composed of a variety of subject matter experts, not all of whom are CC experts
  - The Security Problem Definition is written in a less formal, narrative style, and then formalized in CC constructs later
  - This makes it understandable to the non-CC experts in the iTC and to customers who want to know if it fulfills their requirements
- cPPs facilitate objective evaluations that generate reproducible results
  - Technology-specific assurance activities embedded in the cPPs
  - Vulnerability assessment is addressed in more detail
  - Technology-specific evaluation methodologies may be written in Supporting Documents

# It’s not so simple anymore

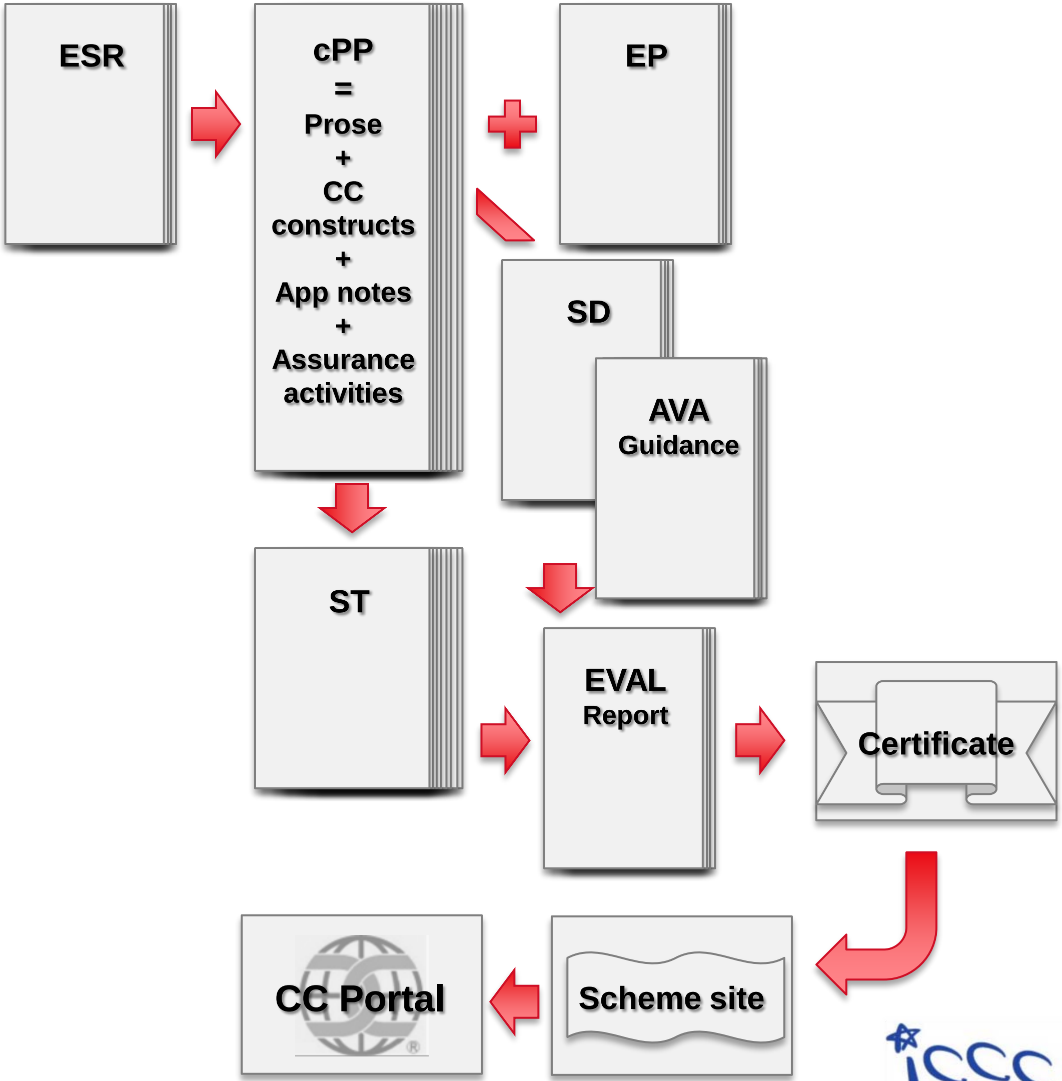
- There are lots of documents



EP := Extended Package  SD := Supporting Document AVA := Vulnerability Assessment (assurance class) ST := Security Target

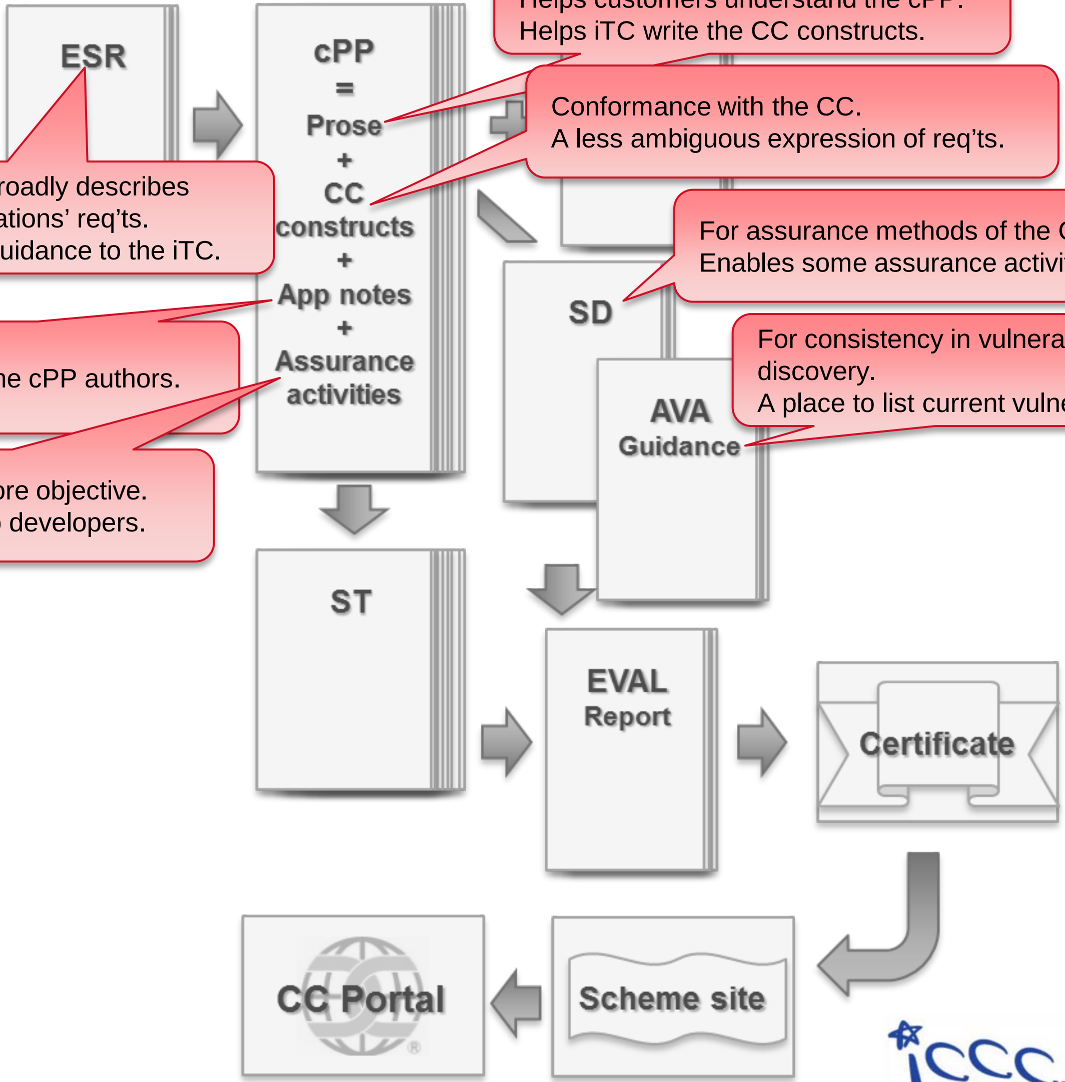
# It’s not so simple anymore.

- There are lots of documents ...
- and document parts



# It’s not so simple anymore..

- There are lots of documents ...
- and document parts
- They serve multiple purposes



For non-CC-experts to contribute.
Helps customers understand the cPP.
Helps iTC write the CC constructs.

Conformance with the CC.
A less ambiguous expression of req’ts.

Broadly describes nations’ req’ts.
Guidance to the iTC.

For assurance methods of the CEM.
Enables some assurance activities.

For consistency in vulnerability discovery.
A place to list current vulnerabilities.

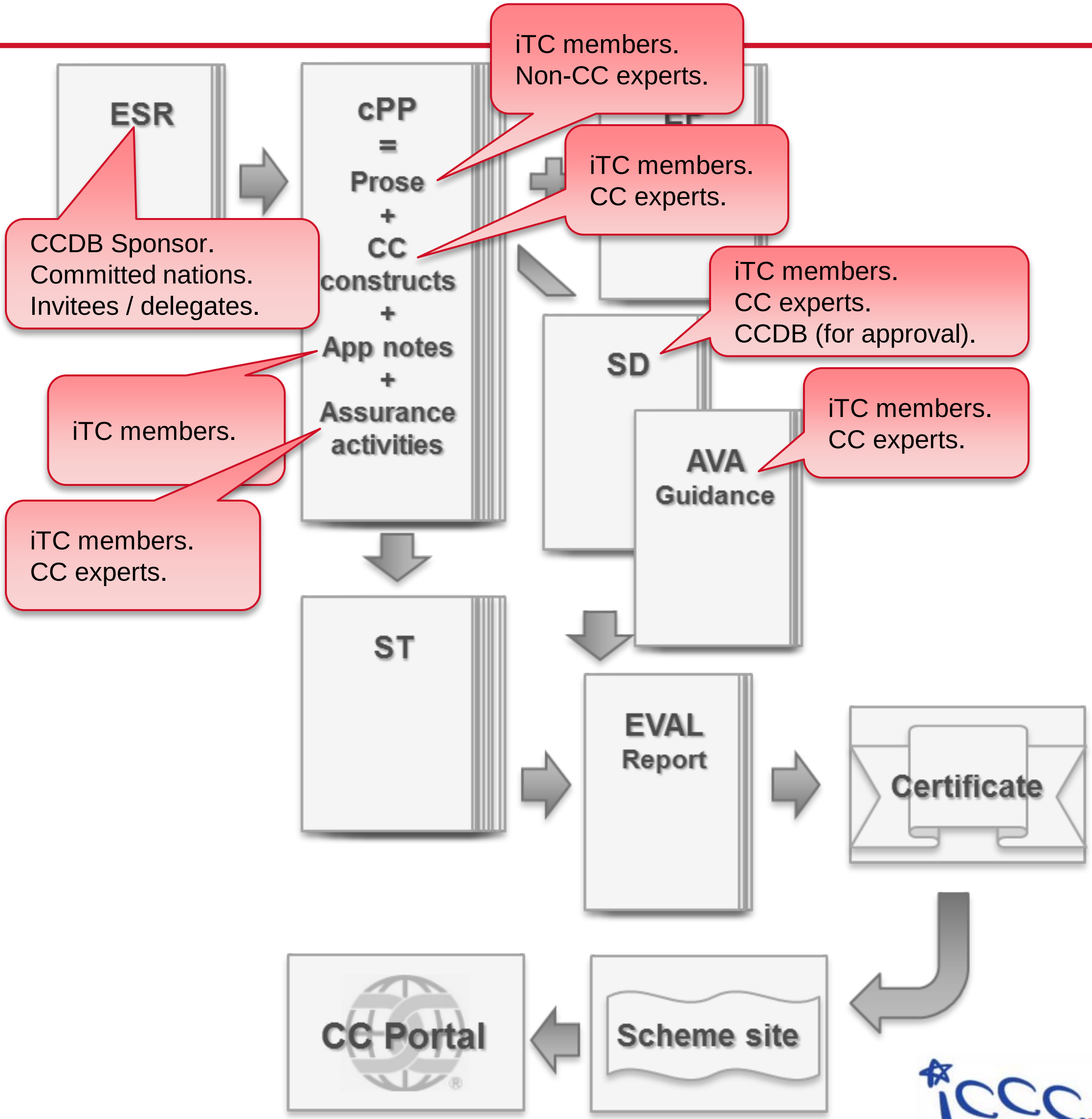
Clarifies intent of the cPP authors.

Makes evaluation more objective.
Provides guidance to developers.

CEM:= Common Evaluation Methodology

# It’s not so simple anymore…

- There are lots of documents ...
- and document parts
- They serve multiple purposes
- There are written by a variety of authors



ESR

CCDB Sponsor.
Committed nations.
Invitees / delegates.

cPP
=
Prose
+
CC constructs
+
App notes
+
Assurance activities

iTC members.
Non-CC experts.

iTC members.
CC experts.

iTC members.

iTC members.
CC experts.

SD

iTC members.
CC experts.
CCDB (for approval).

AVA Guidance

iTC members.
CC experts.

ST

EVAL Report

Certificate

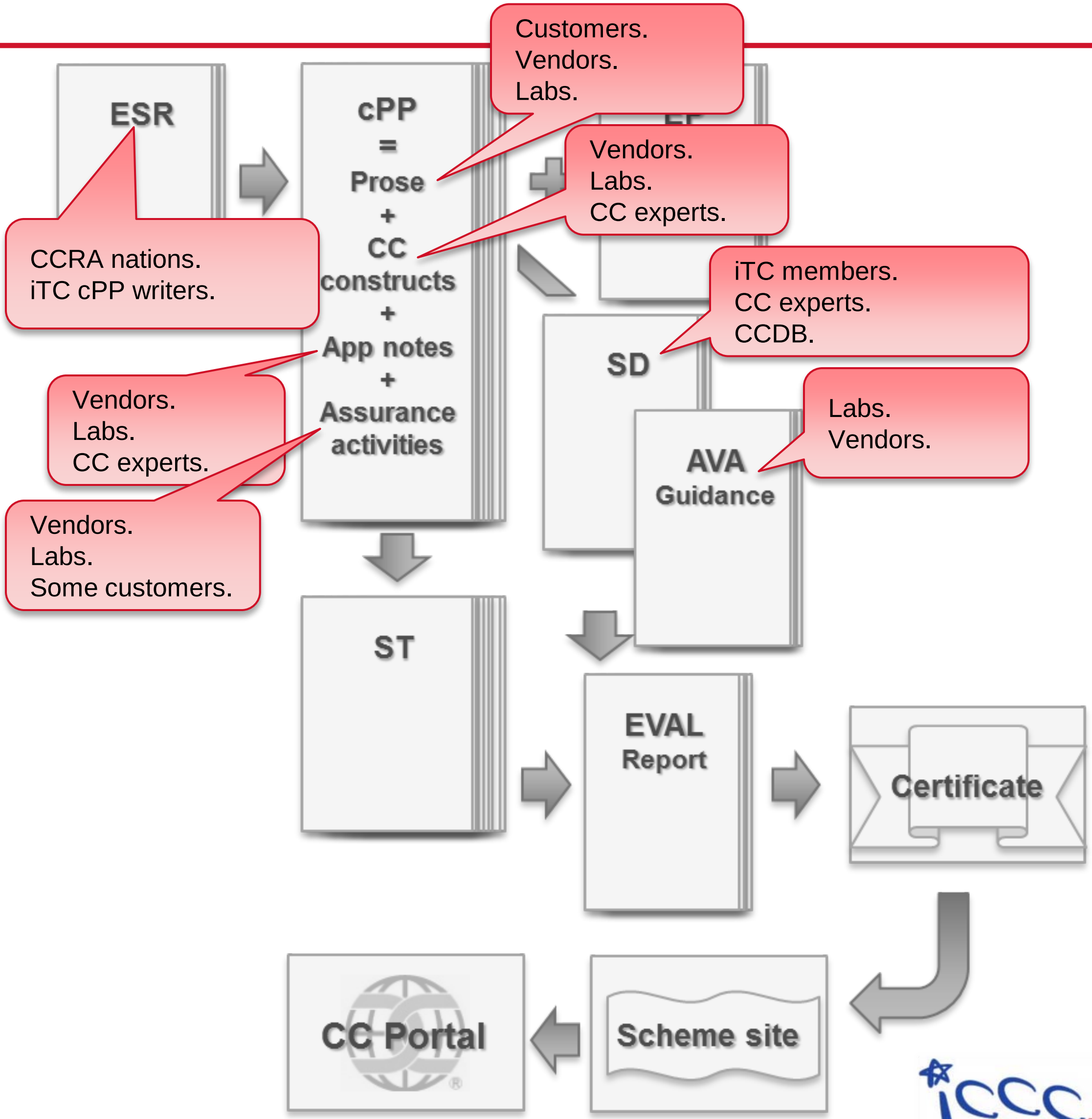
Scheme site

CC Portal

CCDB := Common Criteria Development Board

# It’s not so simple anymore….

- There are lots of documents ...
- and document parts
- They serve multiple purposes
- There are written by a variety of authors
- There have multiple audiences



ESR

CCRA nations.
iTC cPP writers.

cPP = Prose + CC constructs + App notes + Assurance activities

Customers.
Vendors.
Labs.

Vendors.
Labs.
CC experts.

Vendors.
Labs.
CC experts.

Vendors.
Labs.
Some customers.

EP

SD

iTC members.
CC experts.
CCDB.

AVA Guidance

Labs.
Vendors.

ST

EVAL Report

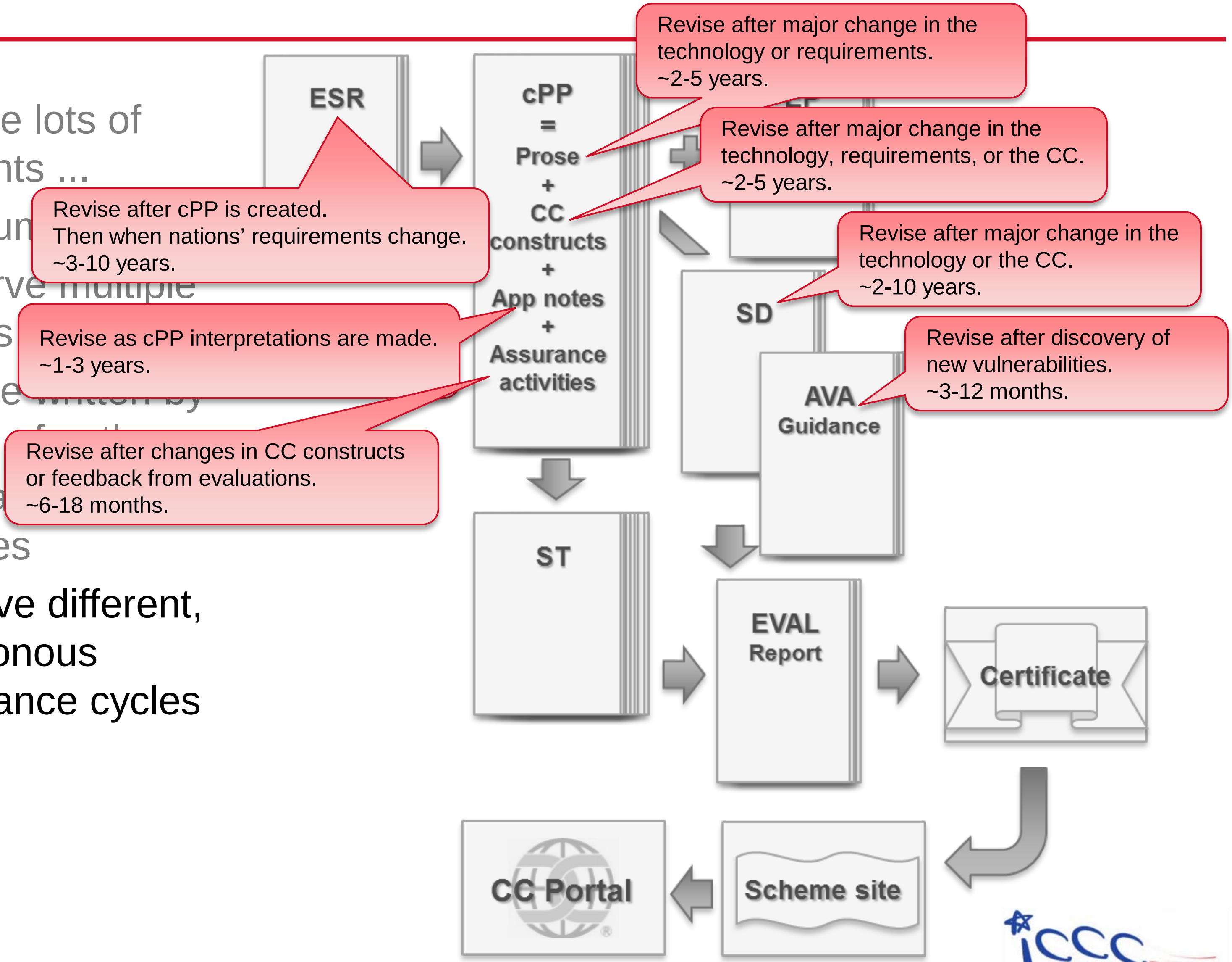
Certificate

Scheme site

CC Portal

# It’s not so simple anymore…..

- There are lots of documents ...
- and docun
- They serve multiple purposes
- There are written by a variety
- There ha audiences
- They have different, asynchronous maintenance cycles


ESR
cPP = Prose + CC constructs + App notes + Assurance activities
SD
AVA Guidance
ST
EVAL Report
Certificate
Scheme site
CC Portal

Revise after major change in the technology or requirements.
~2-5 years.

Revise after major change in the technology, requirements, or the CC.
~2-5 years.

Revise after cPP is created.
Then when nations’ requirements change.
~3-10 years.

Revise after major change in the technology or the CC.
~2-10 years.

Revise as cPP interpretations are made.
~1-3 years.

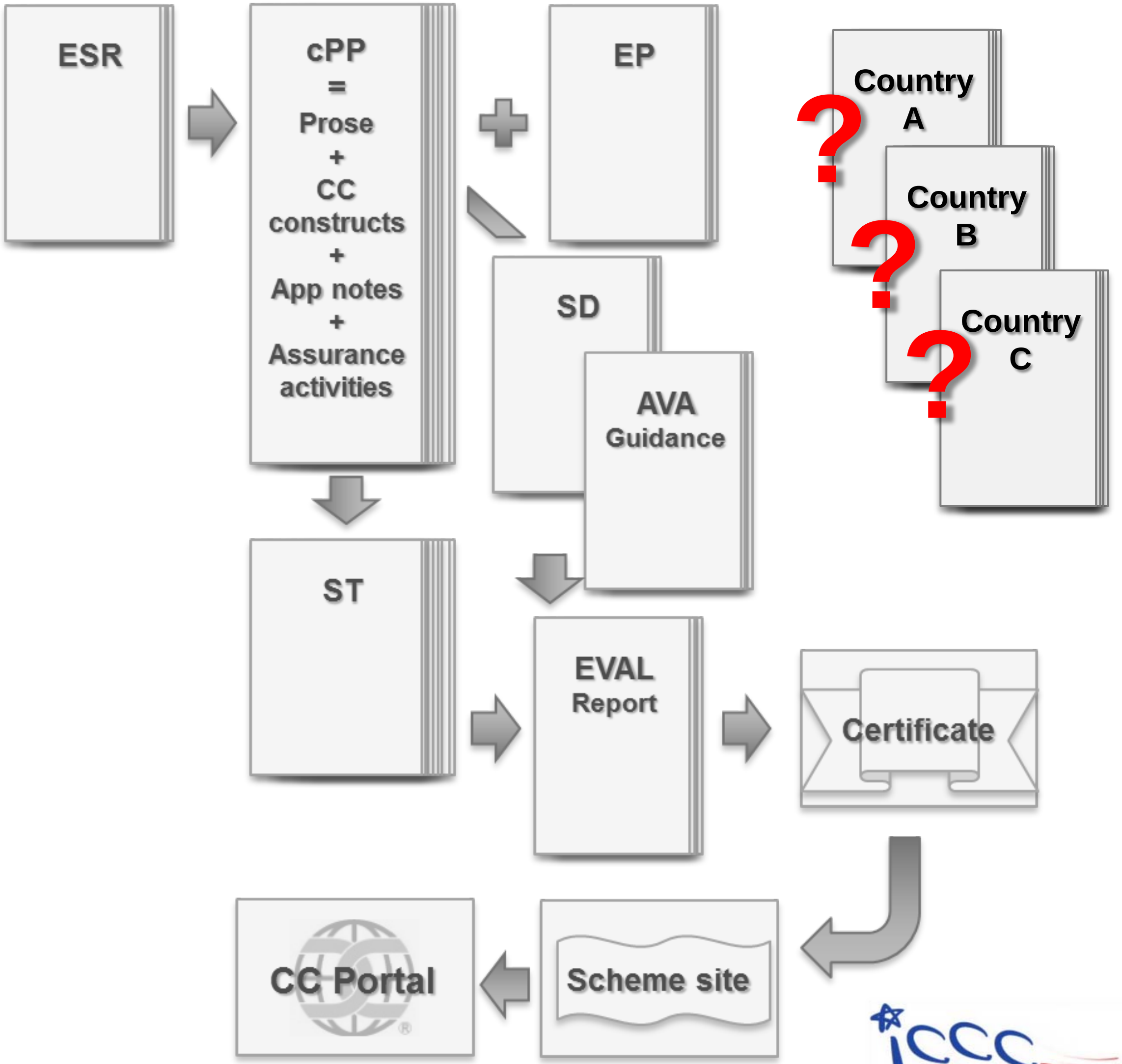
Revise after discovery of new vulnerabilities.
~3-12 months.

Revise after changes in CC constructs or feedback from evaluations.
~6-18 months.

# It’s not so simple anymore…..!

RICOH imagine. change.

- There are lots of documents ...
- and document parts
- They serve multiple purposes
- There are written by a variety of authors
- There have multiple audiences
- They have different, asynchronous maintenance cycles
- And they *still* don’t have a place for nation-specific requirements!



ICCC 2013 SEPTEMBER 10-12 • ORLANDO INTERNATIONAL COMMON CRITERIA CONFERENCE

# Proposals for ESRs

- Embed the ESR in the cPP introduction (APE_INT)
  - Write it as a separate document , then use it as part of the cPP
  - This ensures that it stays in sync with the cPP
- In the “use case” section of the ESR, describe the users’ security expectations for each case
  - This makes the ESR more relevant to end customers who may not be security experts
- Consider different user perspectives
  - Using the product
  - Managing the product
  - Managing the environment in which the product is used

APE := protection profile evaluation (assurance class)  INT := introduction

# Proposals for cPPs

- Maintain the fundamental parts of the cPP (APE_INT, CCL, SPD, OBJ, ECD, REQ) separately from Application Notes and Assurance Activities
  - Try to keep the fundamentals frozen even if application notes or assurance activities are updated (in a cPP “dot release”)
  - Revise Application Notes to document cPP-specific interpretations
  - Revise Assurance Activities to document lessons learned from evaluation experience
- Consider making Assurance Activities a separate document
  - Assurance Activities add a great deal of volume to the cPP but serves only a specialized audience

**CCL := conformance claims SPD := security problem definition OBJ := objectives ECD := extended component definitions**
**REQ := security functional and assurance requirements These are families in the profile evaluation assurance class**

# Proposal for AVA guidance

- Vulnerability assessment guidance should be separate from the cPP
  - It needs to be updated much more frequently as new vulnerabilities or attack methods are discovered
- Maintaining AVA guidance is a good way to keep the iTC alive in between cPP revisions
  - The iTC could have a quarterly teleconference to see if there are any new vulnerabilities or exploits to consider

# Proposals for national req’ts

- Create a way for nation-specific requirements to be documented and associated with cPPs
- Security Targets claiming cPP conformance can also claim conformance to one or more nation’s requirements
- Include national endorsements on CC certificates for products that conform to the cPP and fulfill those nations’ requirements (and for Committed Nations that have not expressed additional requirements for that cPP)

# Example

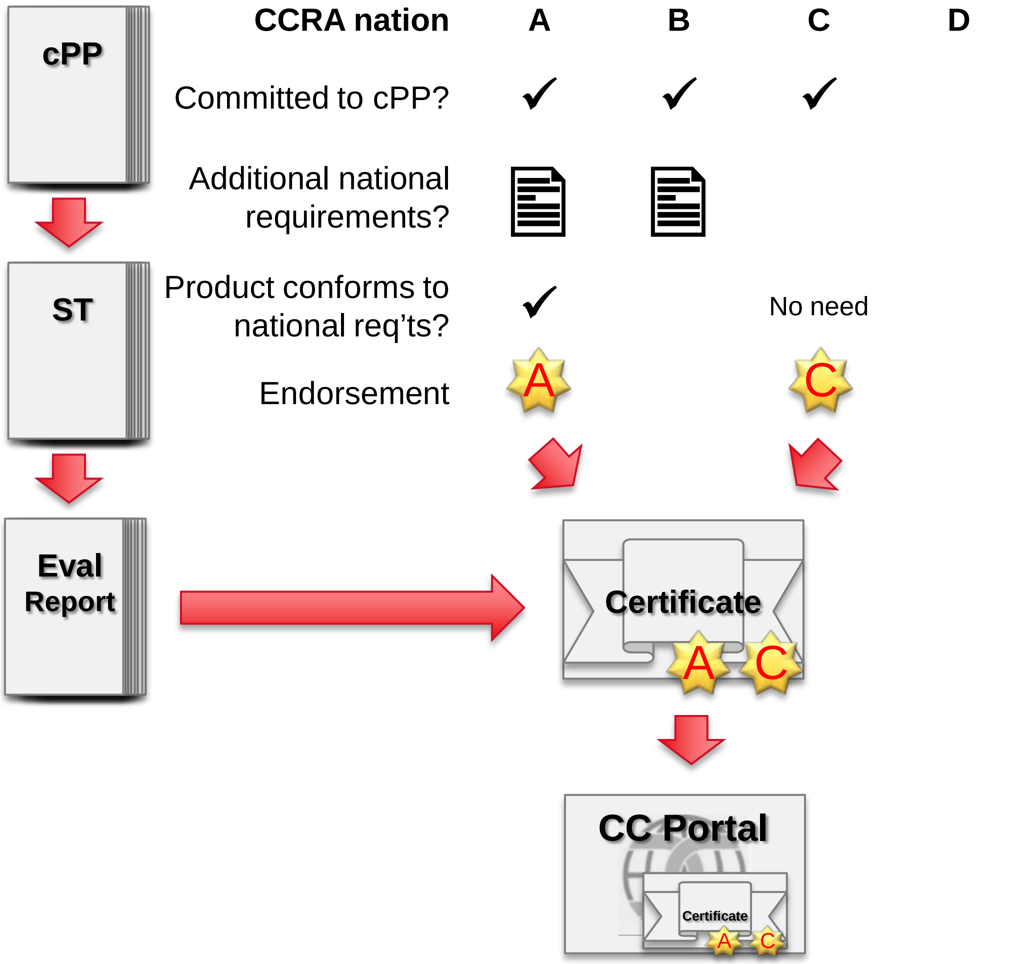
- Some nations commit to a cPP
- Some of them have national requirements associated with that cPP

- A product conforming to the cPP can choose to also conform to national requirements

- Endorsements are given by committed nations if:
  - They have no additional requirements

    — OR —

  - The product conforms to their additional requirements



| CCRA nation | A | B | C | D |
|---|---|---|---|---|
| Committed to cPP? | ✓ | ✓ | ✓ | |
| Additional national requirements? | 📄 | 📄 | | |
| Product conforms to national req'ts? | ✓ | | No need | |
| Endorsement | A | | C | |

# Proposals for the CC Portal

- Include national endorsements in portal listings
  - For protection profiles: based on a nation’s cPP Commitment
  - For certified cPP-conforming products: based on a nation’s cPP Commitment and conformance to its national requirements
  - Schemes could endorse “legacy” PPs and products, based on their own policies and preferences
- Add a feature to filter portal listings by nation
  - It makes it easy for procurers and other interested parties to see only PPs and products that are endorsed by a particular nation
  - Schemes would no longer need to worry about listing products approved for procurement that were evaluated elsewhere
  - The CC Portal would become what it is supposed to be: **a single destination for finding CC certified products**

# Conclusion

- Many documents are needed in support of the new Common Criteria and CCRA
  - They have different authors, purposes, and audiences.
  - They require maintenance, often with different update frequencies.
- If we do not actively consider these things, we risk creating a new CC that is as inconsistent, as inefficient, and for some, as inaccessible as the old CC.

Questions? Comments?

*Thank you.*

ICCC
SEPTEMBER 10-12 • ORLANDO
INTERNATIONAL COMMON CRITERIA CONFERENCE
2013

Brian Smithson
Ricoh Americas
bsmithson@ricohsv.com