
jtsec
BEYOND IT SECURITY

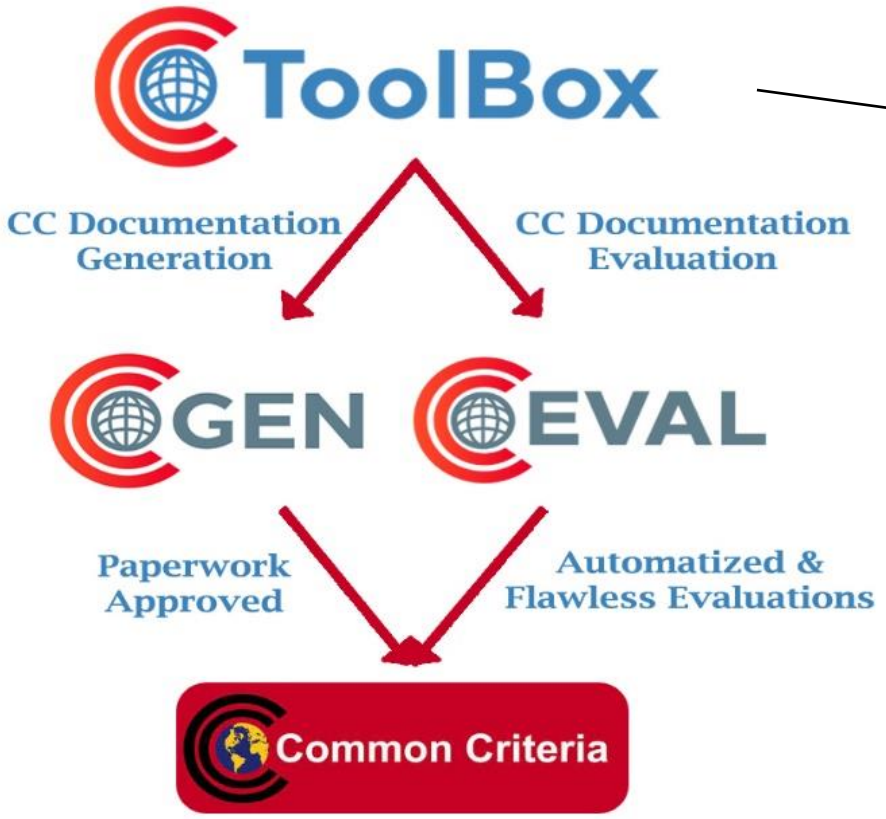
Creating cPPs with CCgen
2020/11/12

CCUF 2020

Contents

- Brief introduction to CCGen
- cPP creation with CCGen
- Handling cPP SFRs with CCGen
- Handling SARs in cPPs
- Inclusion / Exclusion conditions
- Conclusions and future work

Brief introduction to CCGen



- Unique & innovative framework to smooth the Common Criteria certification process
- Easy in-house Installation
- Intuitive and attractive user interface
- Support for EAL-Dependent, NIAP PP or cPP projects
- Integrated in-line CC requirements with CC Expert tips
- Advanced Editors
- Centralized Dashboard
- Centralized Glossary, Acronyms and References
- Integrated Document Management System
- Web Edition, docx output
- Your project in a single file

cPP creation with CCGen

- CCGen can be used to create
  - Regular Protection Profiles
  - Collaborative Protection Profiles
  - Create PP-conformant Security Targets
  - Other evaluation documents: AGD, ADV, ATE, ALC…
- Once a PP is created with CCGen, we can create any conformant ST with it
- Exact conformance is supported, required by most cPPs

Handling cPP SFRs with CCGen

- All CCp2 SFRs available in a dedicated editor
- Almost every SFR in a cPP is refined… CCGen supports all kind of refinements

> ***FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)***
>
> **FCS_COP.1.1(b) Refinement:** The TSF shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [***selection: SHA-256, SHA-384, SHA-512***] ~~and cryptographic key sizes [*assignment: cryptographic key sizes*]~~ that meet the following: [*ISO/IEC 10118-3:2004*].

- Support for optional SFRs (Annex A)
- Support for selection-based SFRs (Annex B)
- Support for objective SFRs

Handling cPP SFRs with CCGen

- CCGen Extended SFR Editor supports every extended SFR in any cPP

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection:

- one, using a submask as the BEV;
- intermediate keys generated by the TSF using the following method(s): [selection:
  - asymmetric key generation as specified in FCS_CKM.1(a),
  - symmetric key generation as specified in FCS_CKM.1(b)];
- intermediate keys originating from one or more submask(s) to the BEV using the following method(s): [selection:
  - key derivation as specified in FCS_KDF_EXT.1,
  - key wrapping as specified in FCS_COP.1(d),
  - key combining as specified in FCS_SMC_EXT.1,
  - key transport as specified in FCS_COP.1(e),
  - key encryption as specified in FCS_COP.1(g)]]

while maintaining an effective strength of [selection: 128 bits, 256 bits] for symmetric keys and an effective strength of [selection: not applicable, 112 bits, 128 bits, 192 bits, 256 bits] for asymmetric keys.

Handling cPP SARs with CCGen

- UI available for handling SARs assignments
  - Don't worry again about
- CCGen supports refinements in SARs
- Extended SARs supported for additional activities

21 **Note to ST authors: There is a selection in the ASE_TSS that must be completed. One**
22 **cannot simply reference the SARs in this cPP.**

ASE_TSS.1.1C Refinement: The TOE summary specification shall describe how the TOE meets each SFR, **including a proprietary Key Management Description (Appendix E), and [selection: Entropy Essay, list of all of 3rd party software libraries (including version numbers), 3rd party hardware components (including model/version numbers), no other cPP specified proprietary documentation].**

Inclusion / Exclusion conditions

- Include / exclude elements based on conditions
  - Threats, policies, security objectives…
  - For example, include / exclude a threat based on if a SFR included in the ST

10 **B.1 Class: Cryptographic Support (FCS)**

11 If FCS_VAL_EXT.1 is included in the ST, the evaluator shall add the following threat to the
12 ST:

13 (T.AUTHORIZATION_GUESSING) Threat agents may exercise host software to
14 repeated guess authorization factors, such as passwords and pins. Successful guessing
15 of the authorization factors may cause the TOE to release DEKs or otherwise put it in
16 a state in which it discloses protected data to unauthorized users.

Conclusions

- CCgen supports key features used in cPPs:
  - Advanced SFR/SAR refinements
  - Extended SFR/SARs
  - Exact conformance
  - Optional SFRs
  - Selection-Based SFRs
  - Inclusion and exclusion conditions

- The tool is not flawless! But it meets our requirements (cPPs added on demand)
- The most critical features are already implemented
- The CCToolBox framework allows easy implementation of new features
- Roadmap is defined

Future work

- Add more complex conditions for selection-based SFRs -> under testing
- Support for PP modules -> under development
- Enhanced GUI for advanced refinements
- **If any technical group wants to use CCGen it for the creation of a cPP, we are happy to provide support!**
- **Contact us for a free demo! (hello@jtsec.es)**

Contact

jtsec: Beyond IT Security

Granada & Madrid – Spain

hello@jtsec.es

@jtsecES

www.jtsec.es

"Any fool can make something complicated. It takes a genius to make it simple."
Woody Guthrie