The Printer Working Group

Imaging Device Security

November 15, 2023

PWG November 2023 Virtual Face-to-Face

Agenda

Please Note: This PWG IDS Meeting is Being Recorded

When	What
10:45 – 10:50	Introductions, Agenda review
10:50 – 11:40	Discuss status of HCD iTC, HIT and plans for future HCD cPP/HCD SD releases
11:40 – 12:00 12:45 – 1:15	Debrief on Fall 2023 CCUF Workshop and ICCC 2023
1:15 – 1:40	ICAM 2023 Presentation
1:40 – 1:45	HCD Security Guidelines v1.0 Status
1:45 – 2:25	TCG/IETF Liaison Reports
2:25 – 2:30	Wrap Up / Next Steps

Antitrust and Intellectual Property Policies

"This meeting is conducted under the rules of the PWG Antitrust, IP and Patent policies".

- Refer to the Antitrust, IP and Patent statements in the plenary slides

Officers

- Chair:
  - Alan Sukert
- Vice-Chair:
  - TBD
- Secretary:
  - Alan Sukert
- Document Editor:
  - Ira McDonald (High North) – HCD Security Guidelines

ICCC2023

ICCC 2023 (International Common Criteria Conference 2023)
October 31-November 2, 2023 | Marriott Metro Center, Washington DC, USA

Hardcopy Devices iTC Update

Kwangwoo Lee

Security Mater Architect, HP

HCD iTC chair

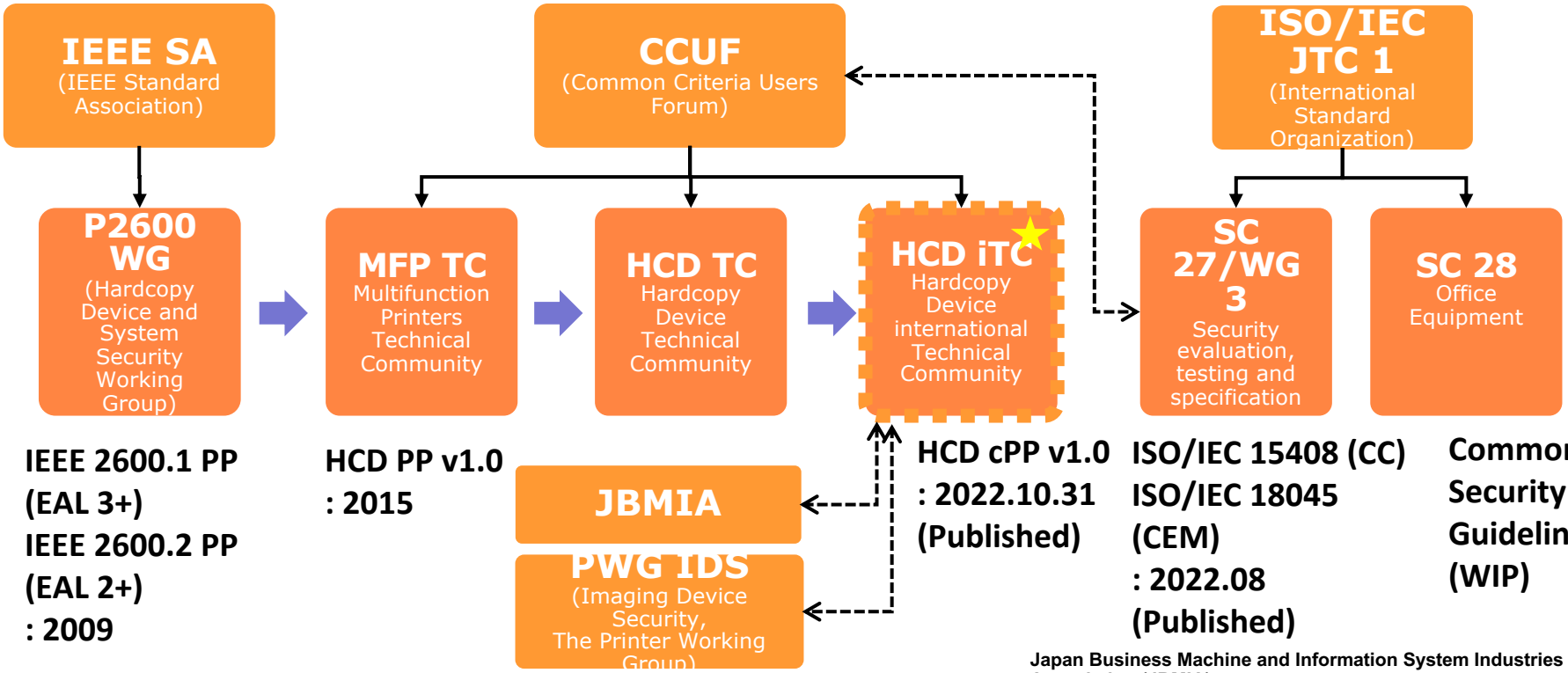
Alan Sukert

HCD HIT chair

HCD international Technical Community (iTC) Status

- Since last IDS F2F on August 10, 2023 HCD iTC meetings have been held on:
  - August 21st
  - Sep 25th
  - Oct 27th

  NOTE: Since publishing the HCD cPP v1.0 and HCD SD v1.0 in Oct 2022 the HCD iTC has gone to meeting once a month
- Current focus is on:
  - Developing a release plan for future versions of the HCD cPP and HCD SD
  - Determining content for and then implementing the next HCD cPP / HCD SD release
  - Addressing issues against HCD cPP / SD v1.0

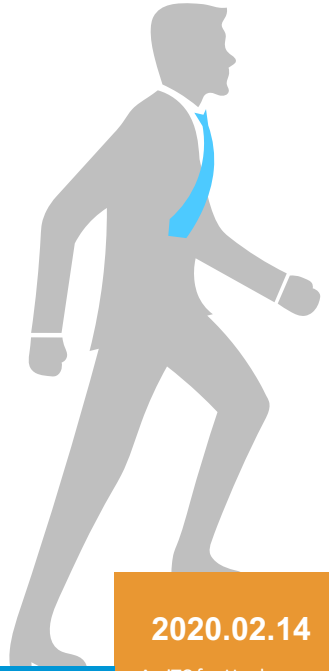

IEEE SA
(IEEE Standard Association)
CCUF
(Common Criteria Users Forum)
ISO/IEC JTC 1
(International Standard Organization)
P2600 WG
(Hardcopy Device and System Security Working Group)
MFP TC
Multifunction Printers Technical Community
HCD TC
Hardcopy Device Technical Community
HCD iTC
Hardcopy Device international Technical Community
SC 27/WG 3
Security evaluation, testing and specification
SC 28
Office Equipment
IEEE 2600.1 PP (EAL 3+)
IEEE 2600.2 PP (EAL 2+)
: 2009
HCD PP v1.0
: 2015
JBMIA
PWG IDS
(Imaging Device Security, The Printer Working Group)
HCD cPP v1.0
: 2022.10.31
(Published)
ISO/IEC 15408 (CC)
ISO/IEC 18045 (CEM)
: 2022.08
(Published)
Common Security Guideline (WIP)
Japan Business Machine and Information System Industries Association (JBMIA)
The Printer Working Group (PWG)

ICCC2023

Step by Step

SOG-IS
EUCC
CCRA

National/Region Security Certification +



2018.10

CCDB at its Oct 2018 Meeting chartered a CCDB Working Group (WG) containing the Korean and Japanese schemes

2020.02.14

An iTC for Hardcopy Devices endorsed by CCMC in February 14th, 2020. The ESR was produced by the HCD WG with HCD TC collaboration

2020.02.15

CCMC chair shared vote results regarding CCMC endorsement of a new iTC for hardcopy devices and associated rationale for Supporting Documents. A majority of the CCRA members voted YES for endorsing the new iTC for hardcopy devices and associated rationale for Supporting Documents.

2020.03.20

HCD iTC kick-off meeting

Consensus for:

- objective
- key person/SMEs
- collaboration tool
- regular meeting
- sub WG
- schedule
- deliverable
- action item
- iTC operational rules

2020.05.08

- **Essential Security Requirements** version 0.7 (dated 8 May 2020)
- **Position Statements published**
- Japan IPA (14 May 2020)
- Korea ITSCC (16 Sept 2020)
- US NIAP (25 Sept 2020)

2022.10.31

- HCD iTC SME meeting (Biweekly)
- HCD iTC Editors meeting (Biweekly)
- HCD iTC Comment Resolution meeting for cPP & SD (Weekly)
- **HCD cPP v1.0**
- **HCD SD v1.0**

ICCC2023

Master Comment Spreadsheet & Github issue

546+

12+ comments	157 + comments	95+ comments	84+ 79+ comments	9+ 29+ comments	10+ 43+ comments	9+ 38+ comments
SPD (Public Review)	**cPP** (Internal Draft)	**SD** (Internal Draft)	**cPP** (Public Review Draft 1 & 2)	**SD** (Public Review Draft 1 & 2)	**cPP** (Public Review Draft Final)	**SD** (Public Review Draft Final)

Publication of HCD cPP v1.0 / Supporting Document v1.0

31 Oct 2022

The HCD iTC has published their collaborative Protection Profile and Supporting Document v1.0.

Please visit the **HCD iTC home page** for more information and to access the published documents.

Multi-Function Devices – 1 Protection Profile

Protection Profile	Version	Assurance Level	Issued	Certified
collaborative Protection Profile for Hardcopy Devices • Protection Profile • Supporting Document • Endorsement Statement	1.0	None	2022-10-31	No *

The iTC has worked on the following items:

- Complete Evaluation Activity Development
- Reviewing, comparing, and collaborating with OTHER iTCs
- Planning setup of an HCD Interpretations Team
- Establishing Interpretation Team (HIT)

Review date : 2022-10-31

Title	Hardcopy Devices
Workspace	(OnlyOffice) https://ccusersforum.onlyoffice.com (Github) https://github.com/HCD-iTC (CC Portal) https://www.commoncriteriaportal.org/communities/hardcopy_devices.cfm
Chair / Vice-chair Technical Editors	Kwangwoo Lee / Alan Sukert Alan Sukert; Brian Volkoff; Gerardo Colunga
Sub WG leads	Tom Benkart (Network SG); Gerardo Colunga (Hardware-anchored Integrity Verification SG); Anantha Kandiah (Secure Erase SG)
Scheme Involved	Japan, Republic of Korea (CCDB iTC Liaison: Eunkyoung Yi, KR)
ToRs	**v0.5 approved by the CCDB on 2019.08 [Link]**
Essential Security Requirements	**v0.7, 2020-05-08 [Link]**
Position Statements [Link]	Japan, Republic of Korea, US
Security Problem Definition	Initial Release for HCD iTC internal Review (v0.3, 2021-04-06) **Public Review Draft (v0.4, 2021-05-09)**

Review date : 2023-10-06

Title	Hardcopy Devices
Current Version of cPP [Link]	Initial Release for HCD iTC internal Review (v0.6, 8 June 2020) Second Release for HCD iTC internal Review (v0.7, 18 October 2020) Third Release for HCD iTC internal Review (v0.8, 2021-06-09) Final Release for HCD iTC internal Review (v0.9, 2021-08-16) Public Review Draft 1 (v0.10, 2021-08-30) [Link] Public Review Draft 2 (v0.11, 2021-12-14) [Link] Final Public Review (v0.13, 2022-07-25) [Link] **cPP v1.0 (2022-10-31) https://hcd-itc.github.io/cPP/cPP_HCD_V1.0.pdf** Latest published versions can be found at https://hcd-itc.github.io/
Current Version of SD [Link]	Initial Release for HCD iTC internal Review (v0.4, 2020-08-26) Second release for HCD iTC internal Review (v0.8, 2020-11-18) Third Release for HCD iTC internal Review (v0.87, 2021-06-29) Final Release for HCD iTC internal Review (v0.9, 2021-09-29) Public Review Draft 1 (v0.91, 2021-10-08) [Link] Public Review Draft 2 (v0.98, 2022-02-24) [Link] Final Public Review (v0.99, 2022-07-29) [Link] **SD v1.0 (2022-10-31) https://hcd-itc.github.io/SD/SD_HCD_V1.0.pdf** Latest published versions can be found at https://hcd-itc.github.io/
Current Issues	The iTC has worked on the following items: 1. Complete Evaluation Activity Development 2. Reviewing, comparing, and collaborating with OTHER iTCs 3. Planning setup of an HCD Interpretations Team 4. Establishing Interpretation Team (HIT)

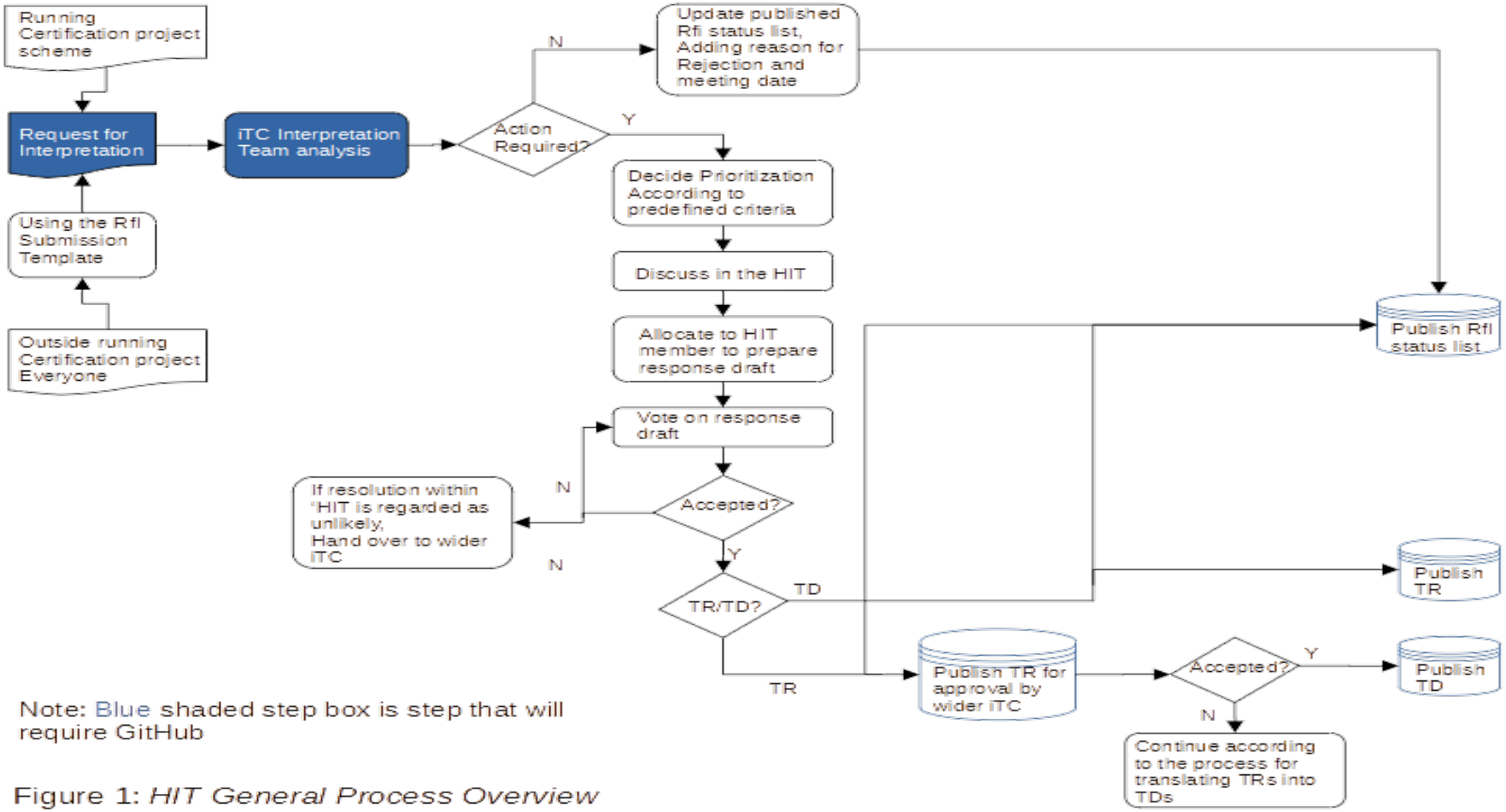
HCD HIT Update

- HIT now has 12 members
  - Current HIT membership consists of HCD vendors (6), Evaluation Labs (2), PWG (1) and Schemes (NIAP and Canadian) (3)
- HIT procedures v1.0 were finalized and infrastructure set up
  - Use of GitHub for documenting Requests for Interpretation (RfIs) and for creating and tracking changes to HCD cPP v1.0 and HCD SD v1.0 for approved RFIs has led to development of new process for creating updated cPP and SD; will require updated to the HIT Procedures to reflect the new process
  - First iTC to use GitHub for the full end-to-end HIT Process
    - Still facing some procedural issues associated with this "first time" use of GitHub, especially in the area of linking the Technical Decision (TD) to the file containing the actual fix in the proper baselines
  - Created new HCD-IT repository and Integration baseline for changes approved by the HIT
- Have had 10 HIT Meetings to date to review and process RFIs submitted as GitHub issues and to approve HIT procedures v1.0

Scope of HIT

- Theoretically the HIT should be able to handle any issue, so everything is in scope
- Real question is what can the HIT resolve by itself and what does the HIT have to let the full HCD iTC resolve
- The general consensus seems to be:
  - HIT should be able to resolve any issue that involves clarification of existing requirements in either the HCD cPP v1.0 or HCD SD v1.0
  - For any issue that involves new content to either the HCD cPP or HCD SD, the HIT should make a recommendation to the full HCD iTC, which would then have the responsibility to resolve the issue

HCD Interpretation Team (HIT) Process



Note: Blue shaded step box is step that will require GitHub

Figure 1: *HIT General Process Overview*

HIT Issue Statistics

HCD-IT	Editorial	Technical	cPP	SD
#1		√	√	
#2		√		√
#3	√		√	
#4	√		√	
	√		√	
	√		√	
	√		√	
	√		√	
	√		√	
	√		√	
#5	√		√	
#6	√		√	
#7	√		√	
#8		√	√	
#9		√		√
#10		√	√	
#11		√	√	
#12		√	√	
#13	√		√	√
#14	√		√	√
#15	√		√	
#16	√		√	
	√		√	
		√	√	
#17		√		√
#18		√		√
#19		√		√
#20		√		√
#21		√		√
Totals	16	13	22	9

HIT Issue Summaries

Issue #	Issue Summary	Status
HCD-IT #1	CFB is the only AES mode allowed by the TPM 2.0 specification but it is not included as n allowable mode in SFR FCS_COP.1/KeyEnc	Potential Solution being reviewed by HIT
HCD-IT #2	In HCD SD Section 2.6.1 FPT_SBT_EXT.1 Extended: Secure Boot, 2.6.1.3 Tests, need clarification that the algorithm verification for Root of Trust should be avoided	Solution developed; Technical Decision being prepared
HCD-IT #3	In Section 5.3.5, FCS_CKM.4 Cryptographic key destruction, in the last requirement "…that meets the following: [selection: no standard]" the selection should be deleted	This issue was closed because it duplicated another comment
HCD-IT #4-HCD-IT #7	These four issues were a set of four comments from NIAP stating areas such as improperly defined Extended Component Definitions and bolding of the selection prompt where the HCD cPP did not follow the conventions stated in Section 5.1	The issues cited by NIAP have mostly been fixed. Remaining concern is how to address the comment on Extended Components
HCD-IT #8	Requested that the Application Notes in SFR FPT_KYP_EXT.1 be modified to more clearly explain what each of the conditions for key storage in that SFR mean	This issue is linked to Issue HCD-IT #11 and will be fixed jointly with that issue

HIT Issue Summaries

Issue #	Issue Summary	Status
HCD-IT #9	This issue is about the test cases for SFR FDP_DSK_EXT.1 in the HCD SD requiring an "operational TSFI" (i.e., an external human interface such as a web interface) when user and confidential data stored on nonvolatile data on the HCD is only accessed by the OS and required no human interface	Working on a proposed solution to be presented to the HIT at our next meeting
HCD-IT #10	This issue is for the Security Objective an O.KEY_MATERIAL being mapped to a Conditionally Mandatory SFR FPT_KYP_EXT.1 when it should be mapped to a Mandatory SFR, because protection of keys and key material should be a mandatory security objective	The solution for this issue is known and is being worked jointly by the HIT at a HIT meeting
HCD-IT #11	This issue deals with FCS_CKM.4 and whether encrypted keys are within the scope of key destruction. The real issue, though, is the fact that FCS_CKM_EXT.1 states that only plaintext keys and key material must be destroyed, whereas other cPPs require all keys and key material must be destroyed	Resolution of this issue is on hold while we determine why the HCD cPP only required plaintext keys to be destroyed; HiT divided on this issue
HCD-IT #12	This issue is from the Canadian Scheme and was for the fact that three threats - T.TSF_FAILURE. T.UNAUTHORIZED_UPDATE, and T.WEAK_CRYPTO did not have the required asset information in their definition	This issue is being worked by the HCD cPP Editor and Canadian Scheme Representative

HIT Issue Summaries

Issue #	Issue Summary	Status
HCD-IT #13	This issue stated that the title of SFR FDP_DSK_EXT.1 - Protection of Data on Disk – was misleading as it might lead someone to assume it only applied to HCDs that had a hard disk drive.	Solution is to change title so it is clear this SFR applies to any HCD that stores data in Nonvolatile Storage
HCD-IT #14	This issue is a simple issue where the sections where the SFRs FIA_AFL.1 and FCS_CKM.1/AKG reside are different between the HCD cPP and the HCD SD	Issue has been assigned to a HIT member to resolve
HCD-IT #15	This issue is a case where the title of the SFR FCS_COP.1/CMAC is correct where it is defined in Section A,,3, but is incorrect when FCS_COP.1/CMAC is included in a dependency list for another SFR	Issue has been assigned to a HIT member to resolve
HCD-IT #16	This issue documents three comments – two editorial and one technical – from the required CCMB review of the HCD SD v1.0	The CCMB comments are under review by the HIT for assignment to a HIT member(s) to analyze and resolve

HIT Issue Summaries

Issue #	Issue Summary	Status
HCD-IT #17	This issue documents three comments – two editorial and one technical – from the required CCMB review of the HCD SD v1.0	This issue was closed because it duplicated of Issue HCD-IT #16
HCD-IT #18	The issue is that the TSS Assurance Activity for SFR FCS_CKM.1/SKG Cryptographic key generation (Symmetric Keys) has to clarify a disconnect how the TOE obtains a symmetric key through direct generation from a random bit generator between the two standards referenced in the SFR.	Issue has been assigned to a HIT member to resolve
HCD-IT #19	This issue is whether Tests 1 and 2 for SFR FCS_CKM.4 Cryptographic key destruction apply to only volatile memory	Issue has been assigned to a HIT member to resolve. Solution appears to be a simple one to implement
HCD-IT #20	This issue is whether for Test 2 for SFR FDP_DSK_EXT.1 Protection of Data on Disk decryption of the data is not required if the data is encrypted by “another key”	Issue is being reconsidered as to whether it is a valid issue
HCD-IT #21	This issue is to clarify when Tests 3 and 4 for SFR FDP_DSK_EXT.1 are required to be run	Concern is whether Tests 3 and 4 are “out of scope” for this SFR and why they were added in the first place

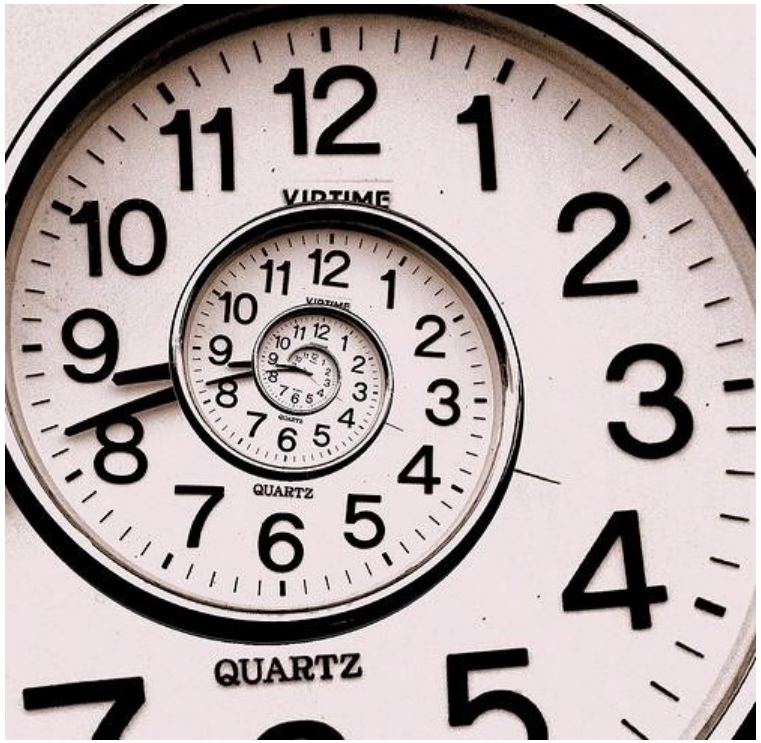
HIT Release Plan

- Will definitely need an Errata release ASAP to address, as a minimum, the comments from the NIAP and Canadian Schemes and the CCDB comments against HCD SD v1.0
  - May also include fixes for one or more of the open issues (at the time of release) against HCD cPP v1.0 and HCD SD v1.0
- There may be additional standalone HCD cPP or HCD SD v1.0.x releases after the initial Errata release. If so and how many of these releases will occur likely depend on the comments we get from:
  - The review of the HCD cPP from the other Schemes and
  - The current Lexmark and Japan certification and future certifications against HCD cPP v1.0 or HCD SD v1.0 from the applicable Evaluation Lab or applicable Scheme

  Note: The nature and severity of the comments will probably determine whether comments against HCD cPP or HCD SD v1.0 get fixed in a v1.0 release or get fixed in a later version of the HCD cPP and HCD SD

- It took much longer than we expected or planned to create or update the PP, so don’t expect a new or update PP to be developed quickly either.

  - Alan Sukert (2018)



- The Schemes that sponsor an PP or cPP need to commit the necessary resources support from the beginning to the TC/iTC to address questions/concerns/issues as they come up.

- If you pull in requirements into a PP from other PPs or cPPs, ensure these requirements are assessed to make sure they apply to the PP they are being inserted into or modify them so they apply.

- Have a plan and process in place from the beginning for updating a PP once it is approved, because updates will be needed.
- Make sure you get the involvement from vendors, consultants, and CCTLs as well as the Schemes in developing the requirements that are to go into a PP.
- Make sure assurance activities are consistent with their corresponding requirements and can be performed by vendors and CCTLs
- Have a process in place from the beginning to obtain interpretations and questions on requirements or assurance activities as the PP is being created, and more importantly, as the PP is being implemented.

HCD iTC
Issues Post-Version 1.0 – Release Plan

- In the past release plans have been based on whether to have major releases on maybe a 2-3 year bases and minor releases on possibly 12 - 15 month basis as needed
- Now, several factors have forced release plans to be based on five major factors that will help govern the future content on the HCD cPP and SD and the timing of that content:
  - CCDB Specification of Functional Requirements for Cryptography
  - CC:2022 Compliance
  - Syncing with ND cPP / SD v3.0
  - CNSA 2.0
  - Mutual Recognition with EUCC

HCD cPP/SD Content Post-Version 1.0 Potential V1.1 Content

- Incorporate SFRs from the CCDB Specification of Functional Requirements for Cryptography once it is published and we get a transition plan
- Updates for the relevant changes in CC:2022
- Update for then relevant changes in ND cPP v3.0e
- Initial CNSA 2.0 Implementation – Removal of SHA-1
- Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
  - NC iTC and NIAP are developing competing TLS Packages
  - NIAP wants to standardize on a common TLS Package
  - May not come in V1.1 timeframe
- Incorporate the NIAP Functional Package for SSH so can claim conformance to it
- Inclusion of AVA_VAN and ALC_FLR.*
- Sync with new EUCC
- Initial implementation of CNSA 2.0 algorithms
- Changes due to any approved RfIs (Issues) to HCD cPP/SD v1.0
- Inclusion of NTP
- Changes due to requests from JISEC, ITSCC, NIAP, Canada and possible other Schemes due to on-going certifications against HCD cPP/SD v1.0

HCD cPP/SD Content Post-Version 1.0 Potential for Inclusion in Later Versions

- **Full implementation of CNSA 2.0**
- **Support for Cloud Printing**
- **Incorporate NIAP Functional Package for X.509 when it becomes available**
- **Support for post quantum and other new crypto algorithms**
- **Any other new NIAP Packages**
- **Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, and NIAP TDs**
- **Updates to Address 3D printing and the Digital Thread to Additive Manufacturing**
- **Support for Artificial Intelligence**
- **Support for Wi-Fi**
- **Any new CCDB Crypto WG or CCUF Crypto WG Packages or Specifications**

HCD cPP/SD Content Post-Version 1.0 Potential for Inclusion in Later Versions

- Support for Security Information and Event Monitoring (SIEM) and related systems
- Support for SNMPv3
- Support for NFC
- Updates based on new technologies, customer requests or government mandates
- Syncing with NIAP / ND iTC / Other iTCs such as DSC iTC and FDE iTC

HCD iTC Status
Key Next Steps

- Continue HIT activities for maintaining HCD cPP/SD v1.0 and issue the necessary TDs/TRs and Errata to address all documented RfIs
- Get HCD cPP/SD v1.0 certified by June 30, 2024
- Get HCD cPP/SD v1.0e published be the end of 2023
- Develop an HCD cPP/HCD SD release plan for future versions of the HCD cPP and HCD SD
- Determine the content for and then create the next HCD cPP/SD version after HCD cPP/SD v1.0e
- Fully engage the HCD iTC to work on the next update to the HCD cPP and HCD SD
- Engage in long-range planning to determine what content will be needed in the HCD cPP/SD in the 3-5 year range and beyond

HCD iTC Status
Some More Lessons Learned from 19 Years of Developing PPs and cPPs (My Take)

- The toughest thing to do is to resist the urge to add more into a release than you can reasonably address. Sometimes "you just have to get the release out even if it doesn't contain everything you want "
- This may sound confusing, but I've learned that in trying to develop PPs sometimes "the best you can do is the best you can do", and that's OK
- One regret in developing the HCD PP and now the HCD cPP/SD is that we didn't celebrate enough or appreciate enough as a team what we had accomplished. We (I mean the global "we') need to celebrate our victories more because they are so few and far between

EUCC Implementing Regulation

EUCC Implementing Regulation

- Draft EUCC Implementing Regulation was issued for public comments that were due on Oct 31, 2023
- There were a lot of issues with the draft regulation
- The main issues are on the next two slides

EUCC Implementing Regulation Main Issues

1. Mutual Recognition Agreements with Third Countries
   - "Third countries willing to certify their products in accordance with this Regulation, and who wish to have such certification recognised within the Union, shall conclude a (separate) mutual recognition agreement with the Union"
   - The CCRA wants a mutual recognition agreement between the EU and the entire CCRA as a group, not separate mutual agreements with each CCRA member nation
2. Transition to the EUCC
   - "This Regulation shall apply 12 months after its entry into force. The requirements of Chapter IV (Conformity Assessment Bodies) and Annex III (Content of a certification report) do not require a transition period and should therefore apply as of the entry into force of this Regulation"
   - NIAP and others feel 1 year is too short to handle transition to EUCC

EUCC Implementing Regulation (IR) Main Issues

3. Continued EU association with the CCRA
   - This is the #1 issue that even blind-sided the EU Member Nations
   - "This Regulation sets out conditions for mutual recognition agreements with third countries. Such mutual recognition agreements should replace similar agreements currently in place, such as SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and Common Criteria Recognition Arrangement (CCRA).

     In a number of Member States Common Criteria certificates are issued under national schemes using mutual recognition rules established in SOG-IS MRA and CCRA. This Regulation should provide an indicative list of existing national schemes which will cease to produce effects. **Member States should end their participation in the CCRA in the areas covered by this Regulation**."
   - No one is happy with this new policy that got put in without anyone's knowledge

Basically, the CCMB and CCRA as well as the EU Member Nations are fighting these changes as well as other issues with the IR

Fall 2023 CCUF Workshop and 2023 International Common Criteria Conference

Fall 2023 CCUF Workshop and 2023 International Common Criteria Conference

Will show selected slides from the PDF versions of the following presentation:

- An Update on EUCC
- 2023 NIAP Update
- CC 2022 IN ACTION: SECURING CRYPTOGRAPHIC PROTOCOLS AND THEIR IMPLEMENTATIONS
- Post Quantum Cryptography: A Quintessential Quagmire
- CCDB Crypto Working Group Status
- Network Device iTC Update
- Application of Common Criteria in Cooperative Intelligent Transportation Systems

2023 CC Statistics Report

About me

- **José Manuel Pulido:**
- Common Criteria expert and Lead Consultant in jtsec.
- CCToolbox developer
- Contributor to ENISA, Eurosmart and ISO projects and CEN/CENELEC.
- More than 12 years of experience in cybersecurity technologies
- Speaker at several conferences including CCUF20, ICCC20, ICCC21 and ICC22

About us

jtsec Applus

- jtsec is part of the A+ group along with Lightship Security. We have labs in Canada, USA and Spain.
- Cybersecurity **evaluation** & consultancy **services**
- Common Criteria, LINCE and ETSI EN 303 645 accredited lab.
- Developers of the most powerful tool for Common Criteria, CCToolbox.
- **Involved in standardization** activities (ISO, CEN/CENELEC, ISCI WGs, ENISA CSA WGs, CCUF, CMUF, ERNCIP, …)
- Members of the SCCG (Stakeholder Cybersecurity Certification Group)

ICCC2023

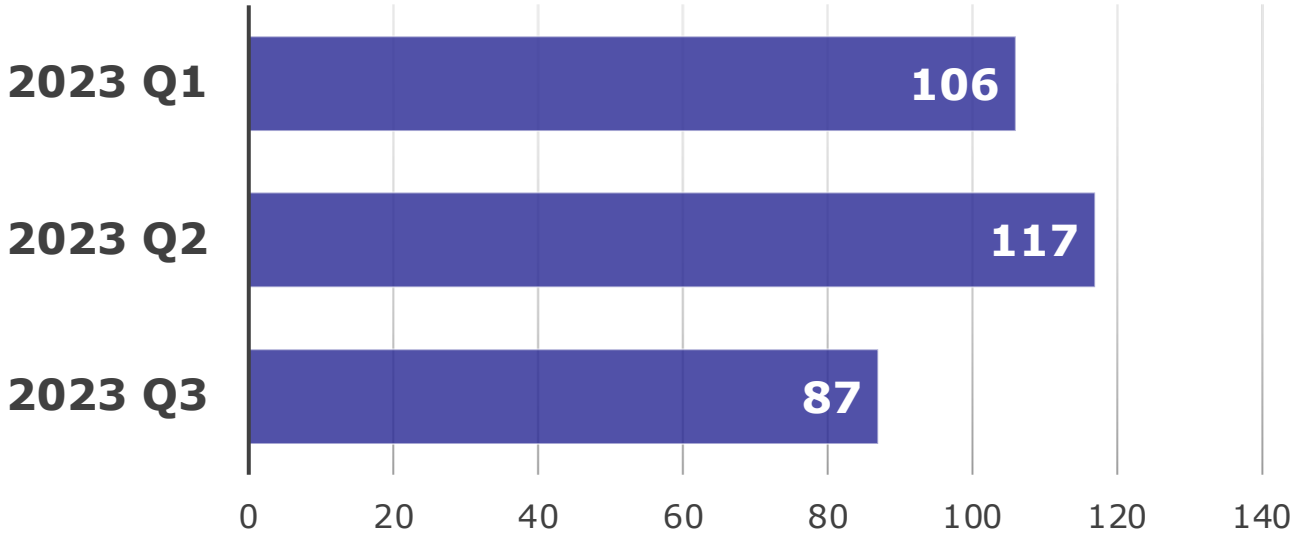
jtsec Applus

Common Criteria Statistics for 2023

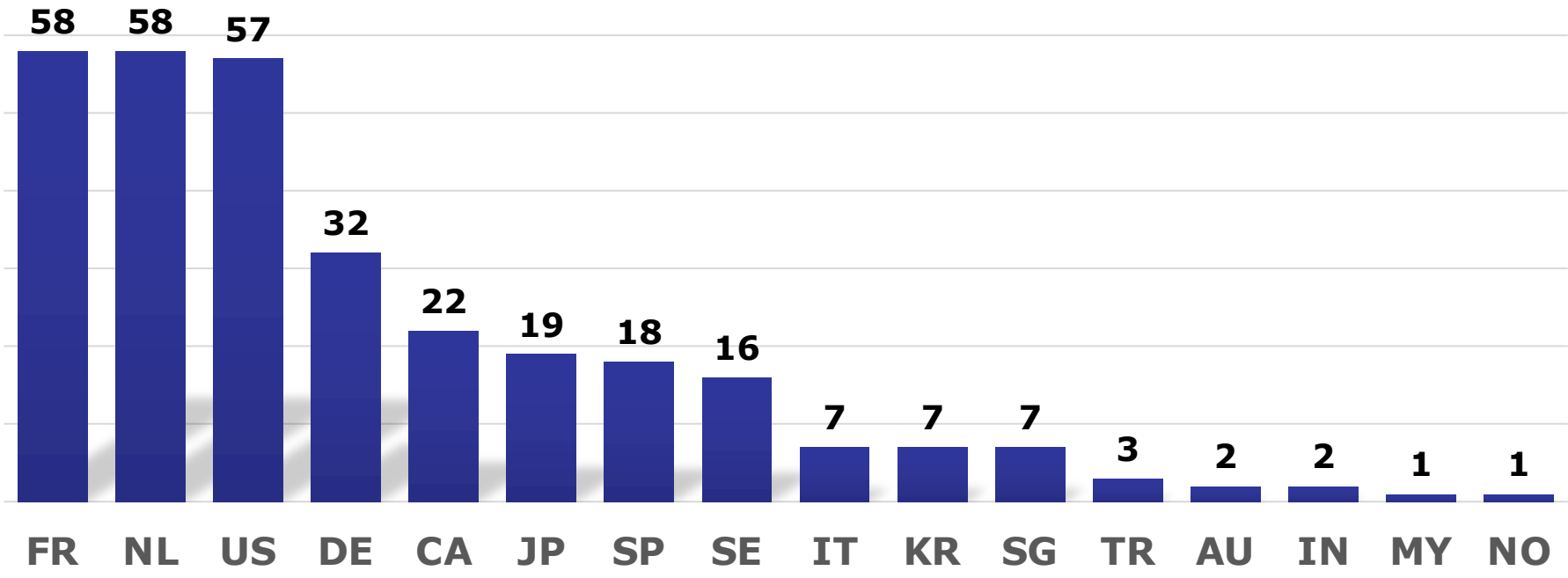
***Disclaimer**: CC scraper was run on 29th of September 2023. The statistics are calculated with the data for the first 9 months of the year.*

Number of CC certificates in 2023

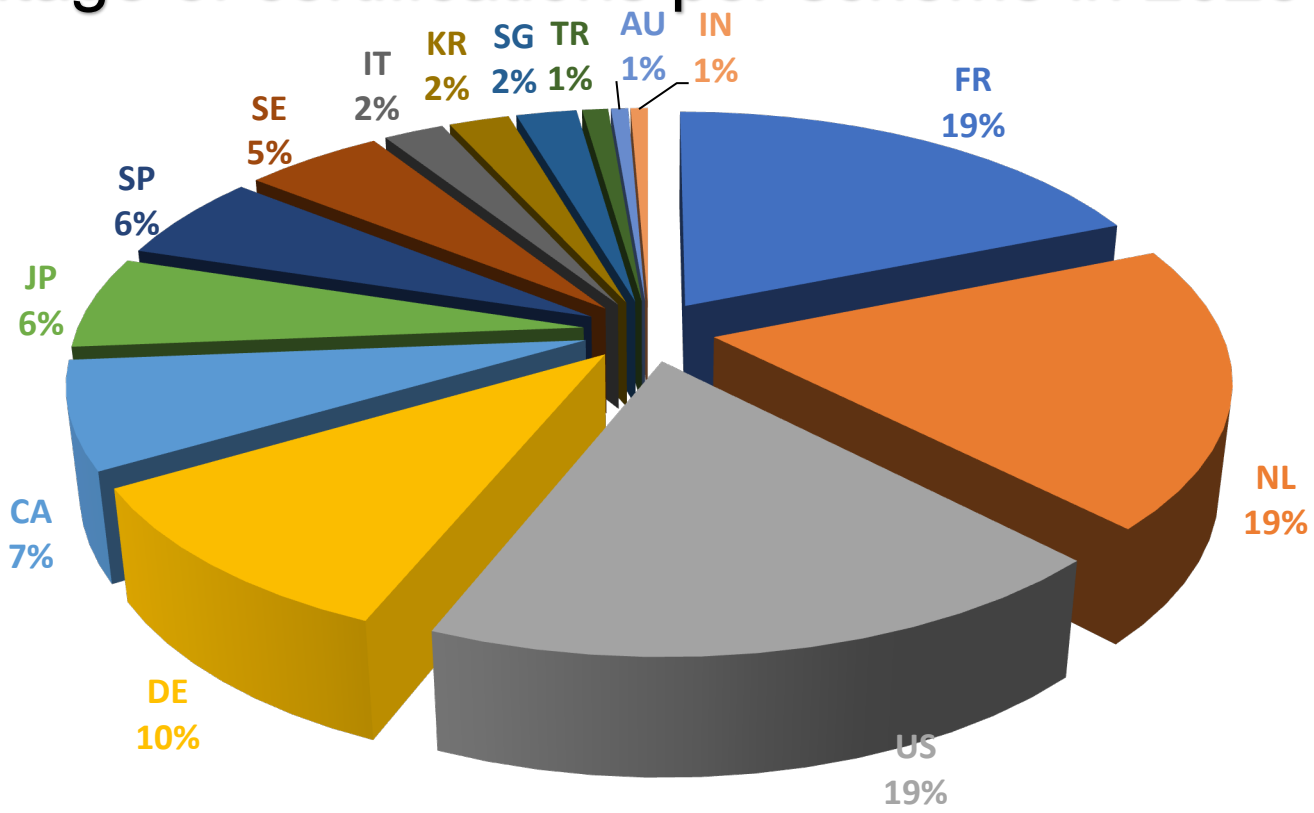
- **310** products were CC certified during 2023 (data until 29/09/2023)



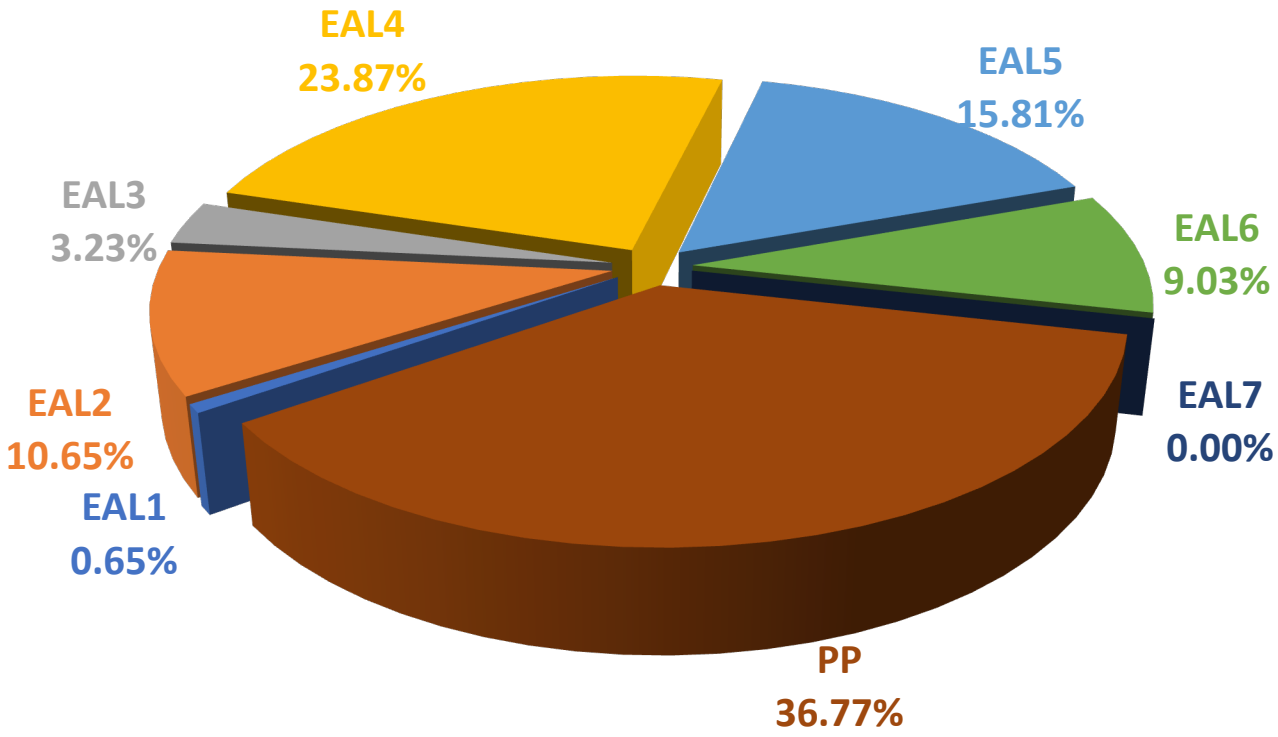
Top certifier schemes in 2023



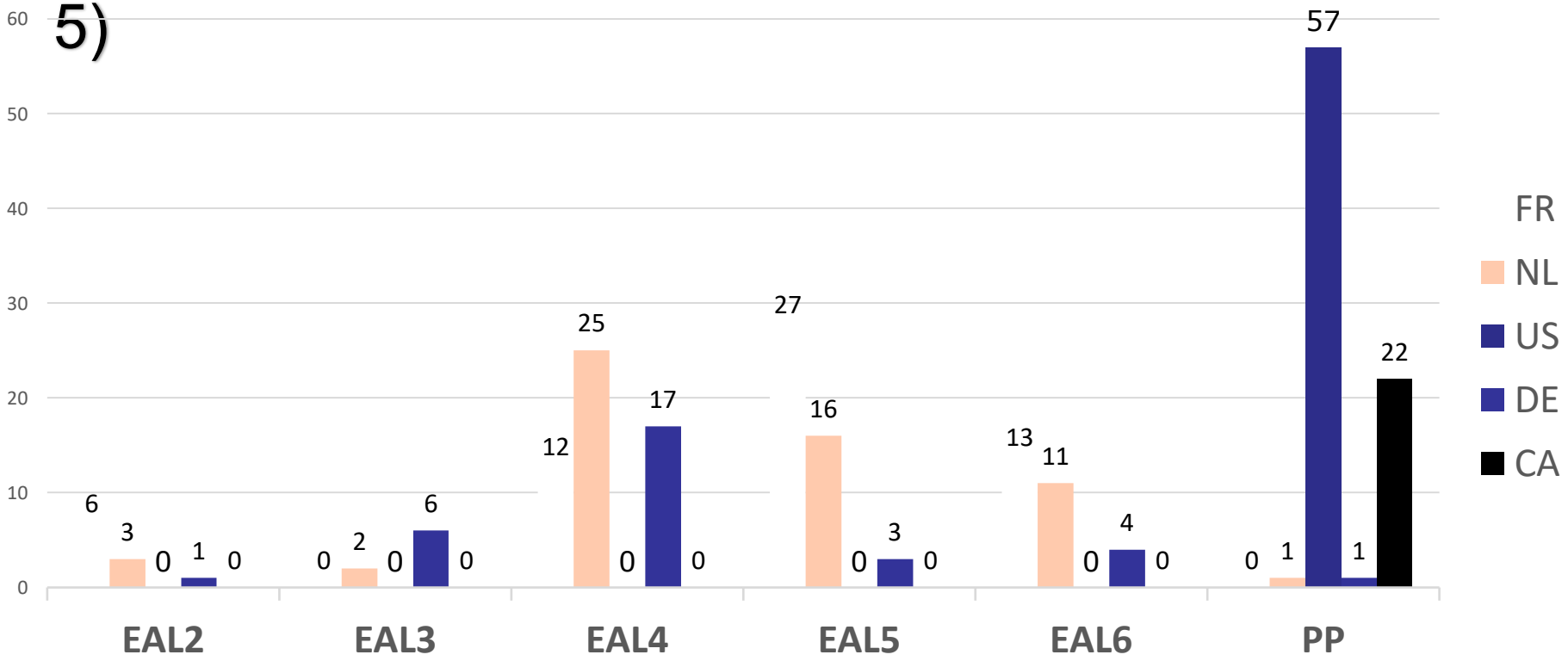
Percentage of certifications per scheme in 2023



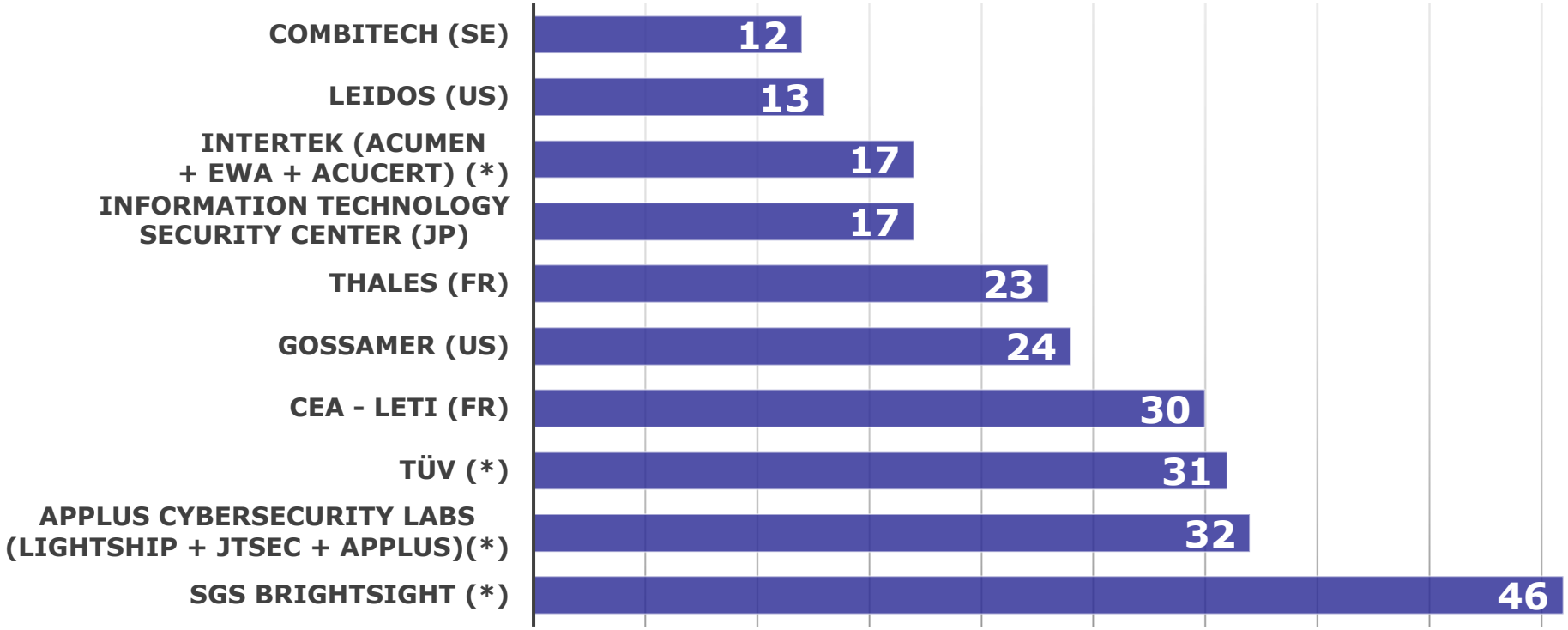
Assurance levels used in 2023



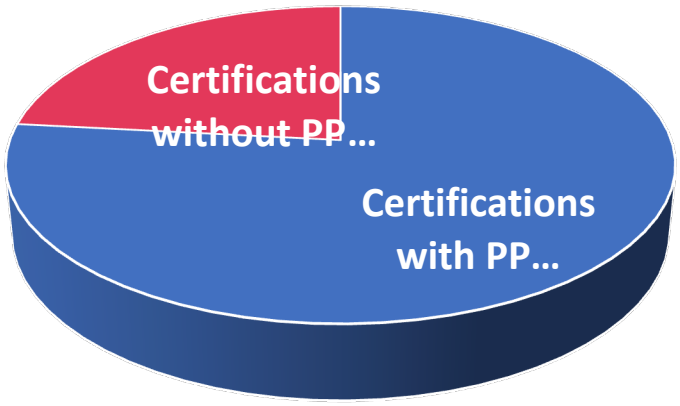
Product assurance level per country in 2023 (top 5)

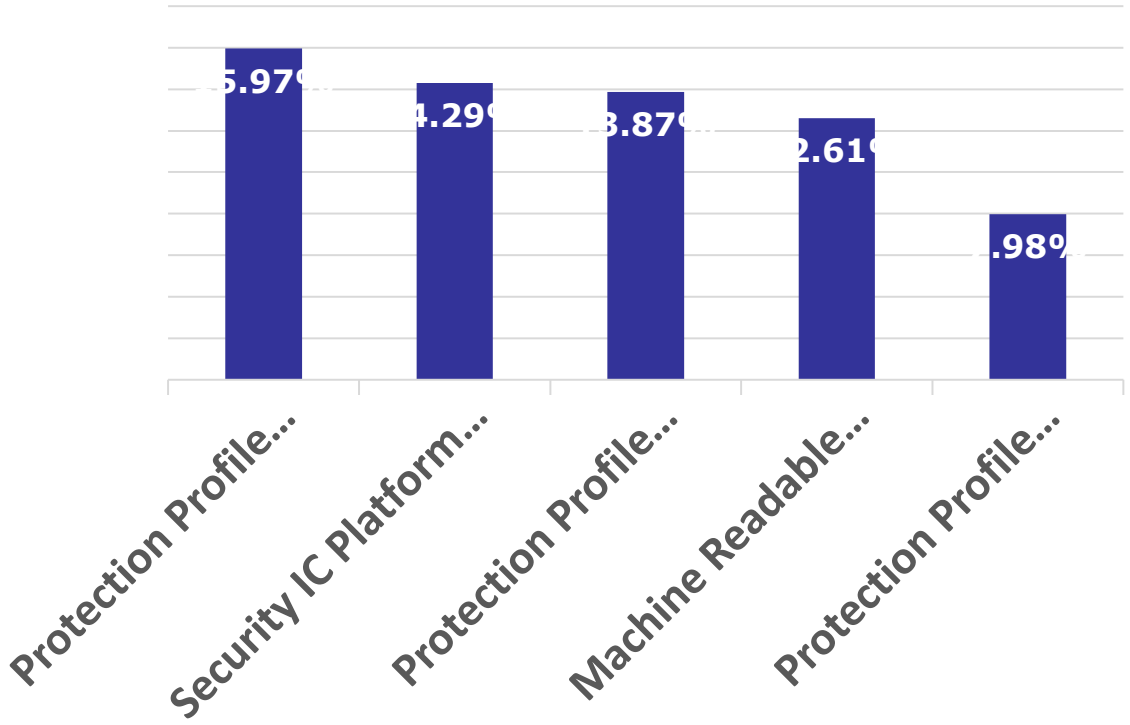


Top 10 laboratories in 2023



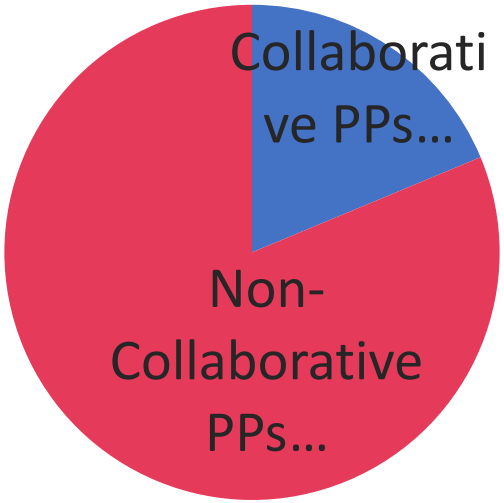
Use of PPs in 2023 / Top PPs



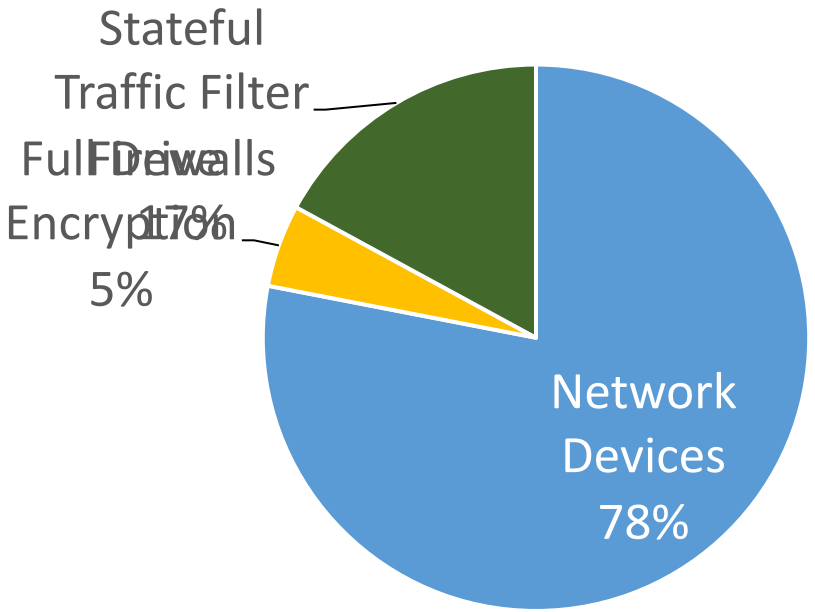


Use of collaborative PPs

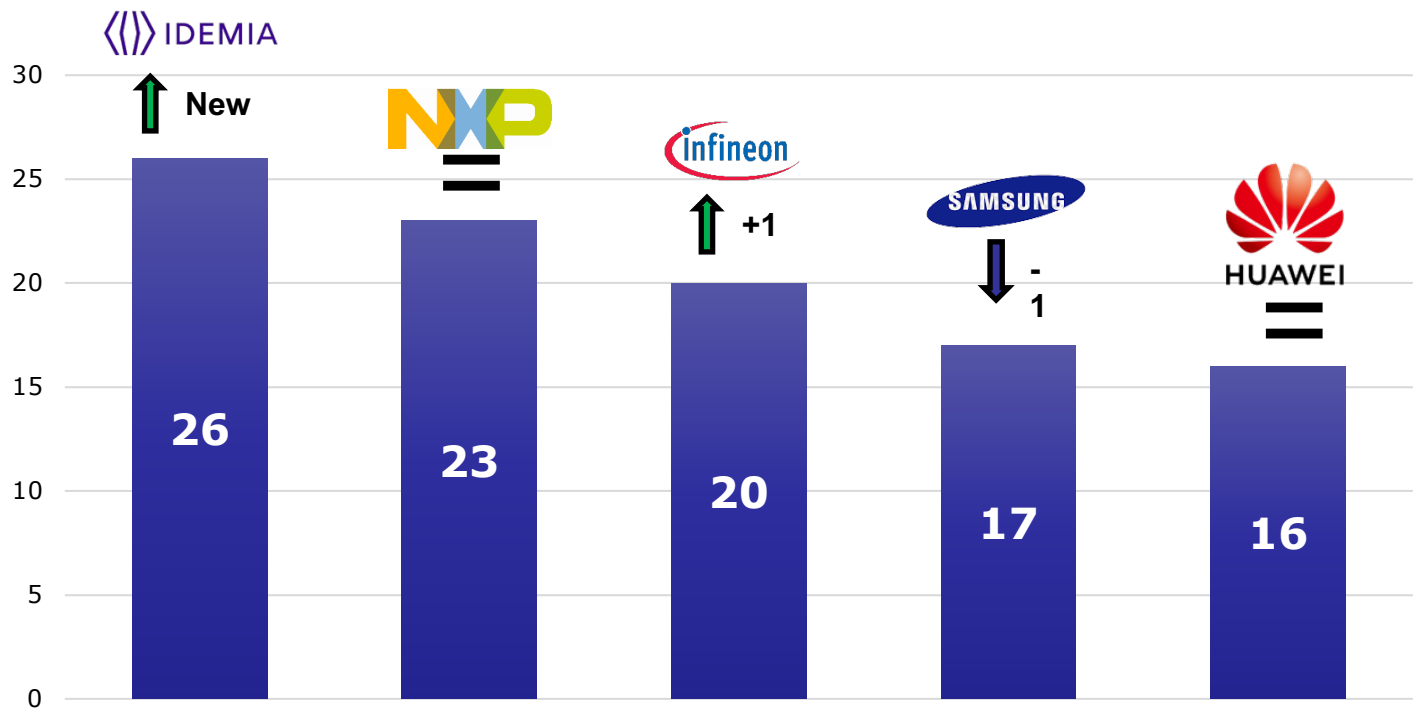
Collaborative PPs vs Non-Collaborative PPs



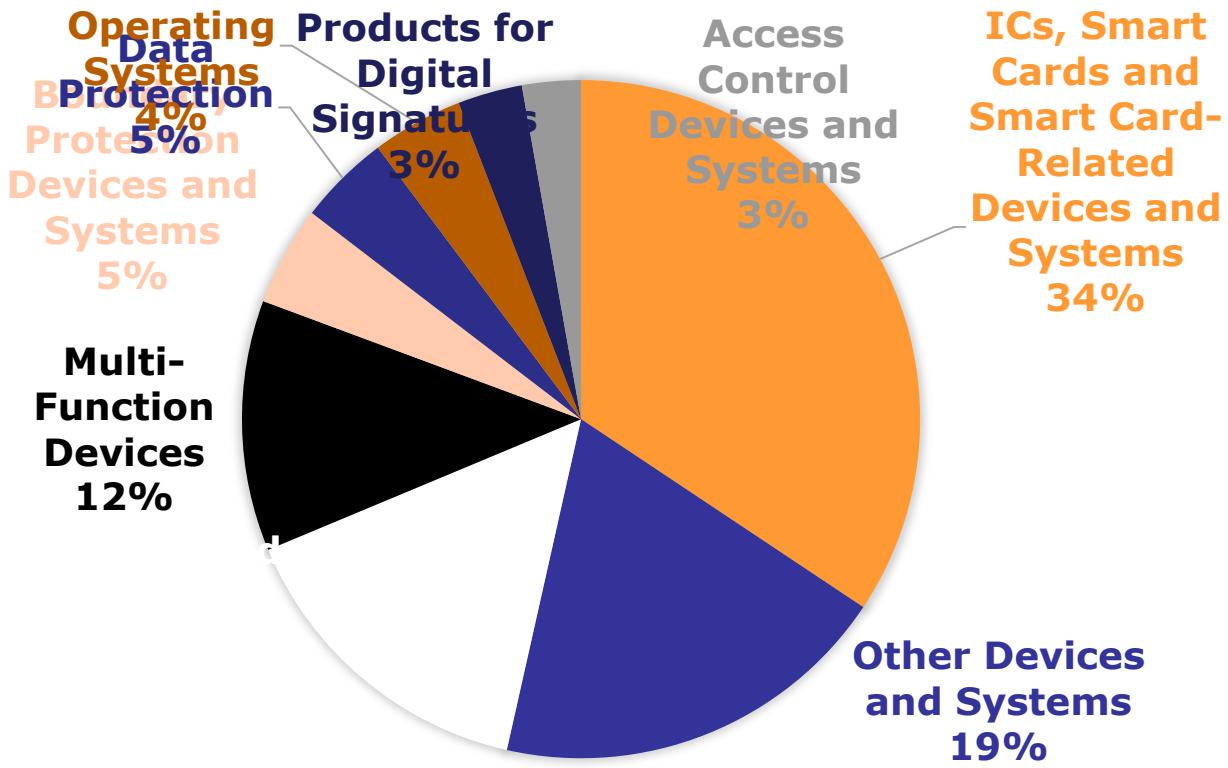
cPP certifications 2023



Top manufacturers of certified products in 2023

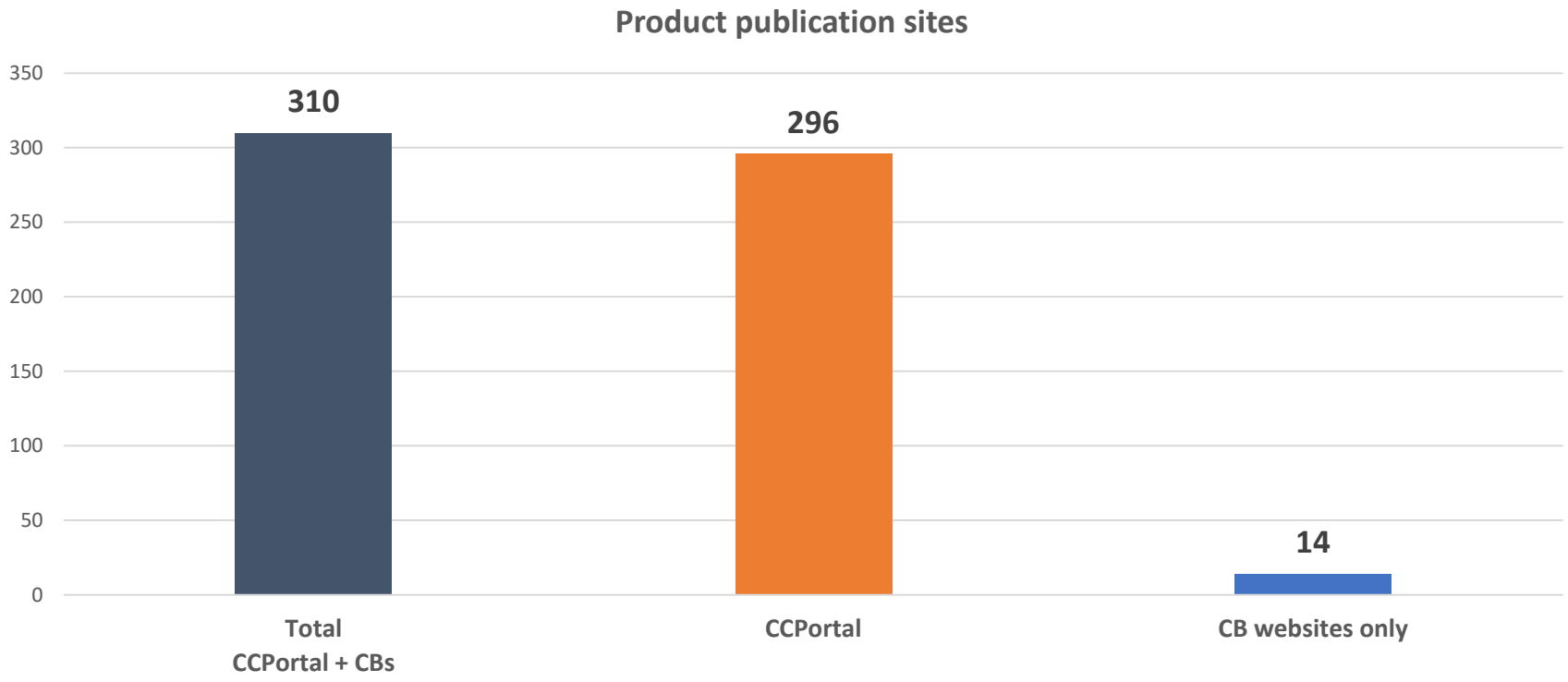


Top certified categories in 2023



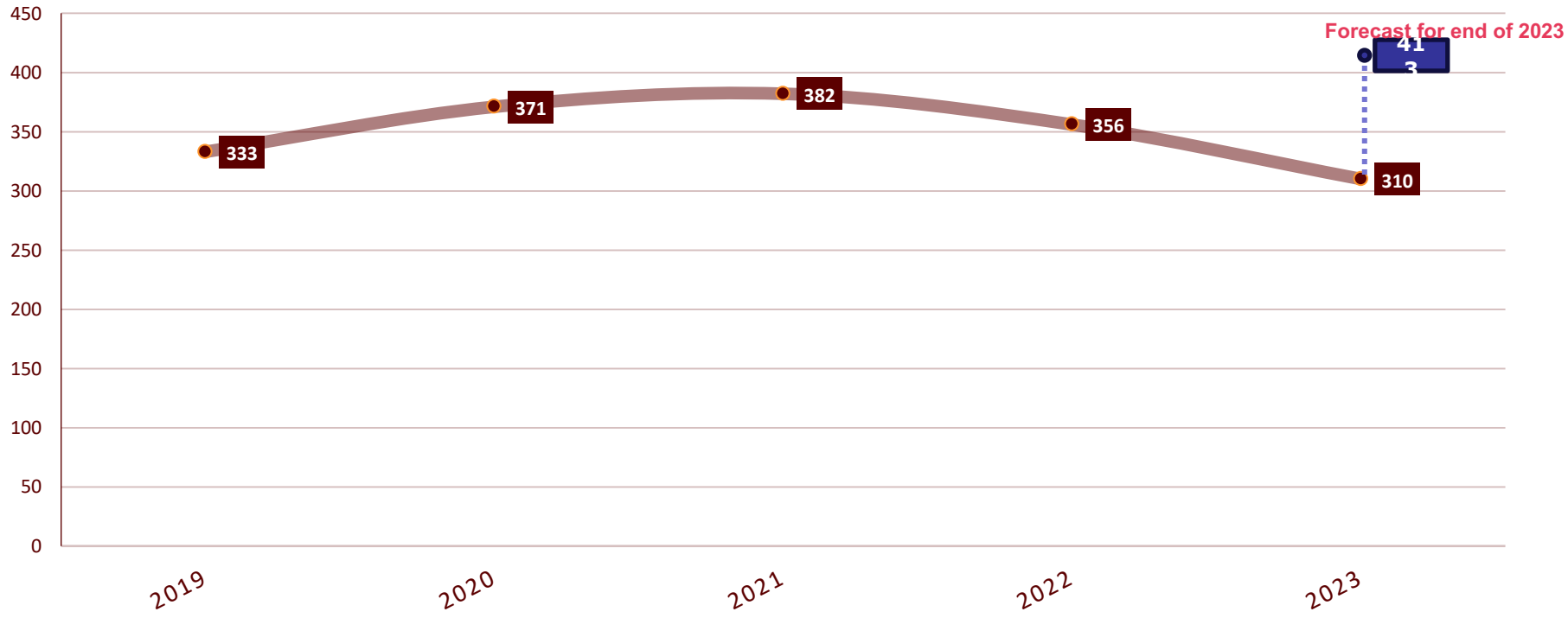
Note: categories with less than 3% were omitted for readability

Products uploaded from CB websites to CC Portal

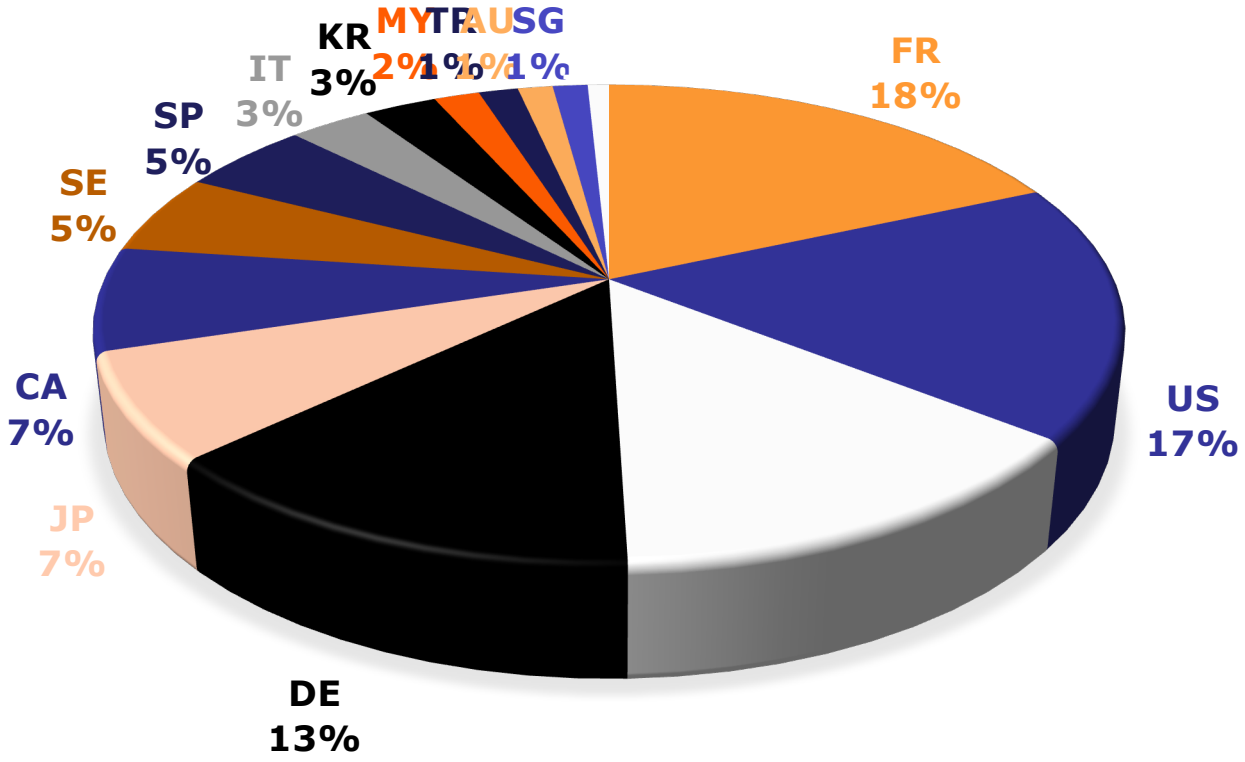


CC Statistics for 5 years

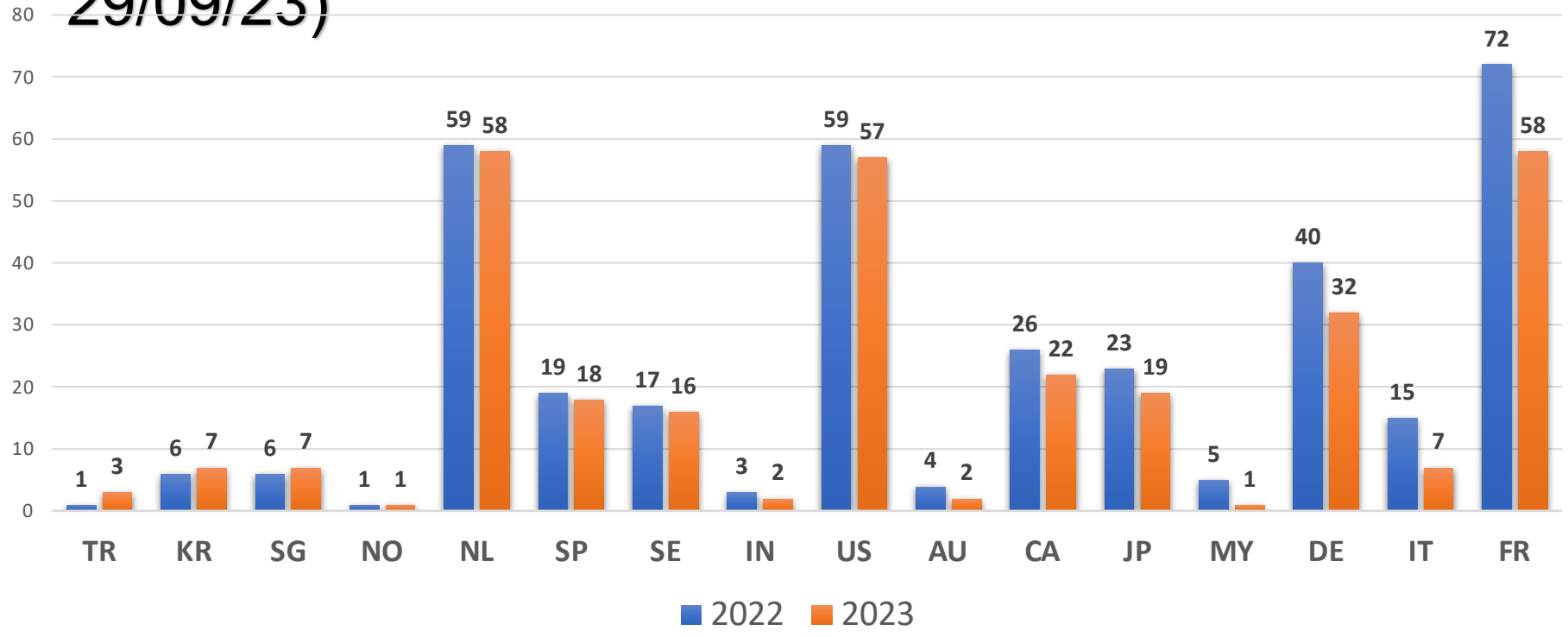
Number of certifications in the last 5 years



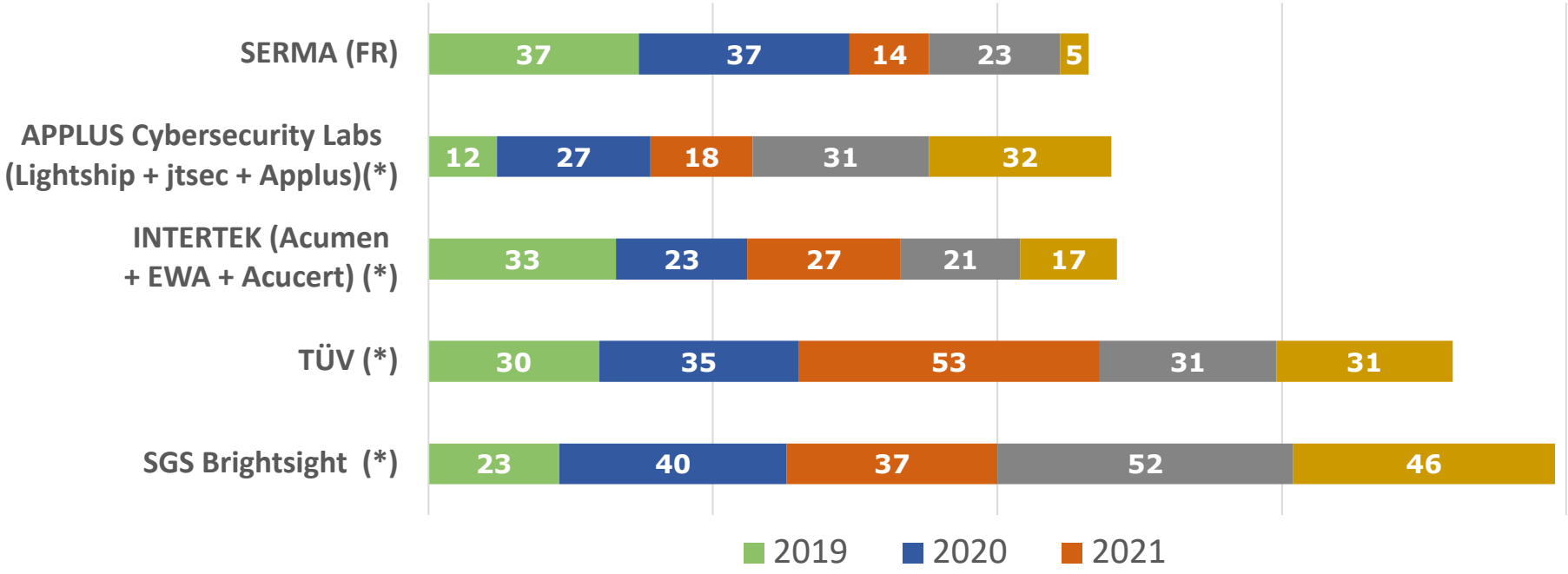
Certifications per scheme – last 5 years



Scheme growth 2022-2023 (until 29/09/23)

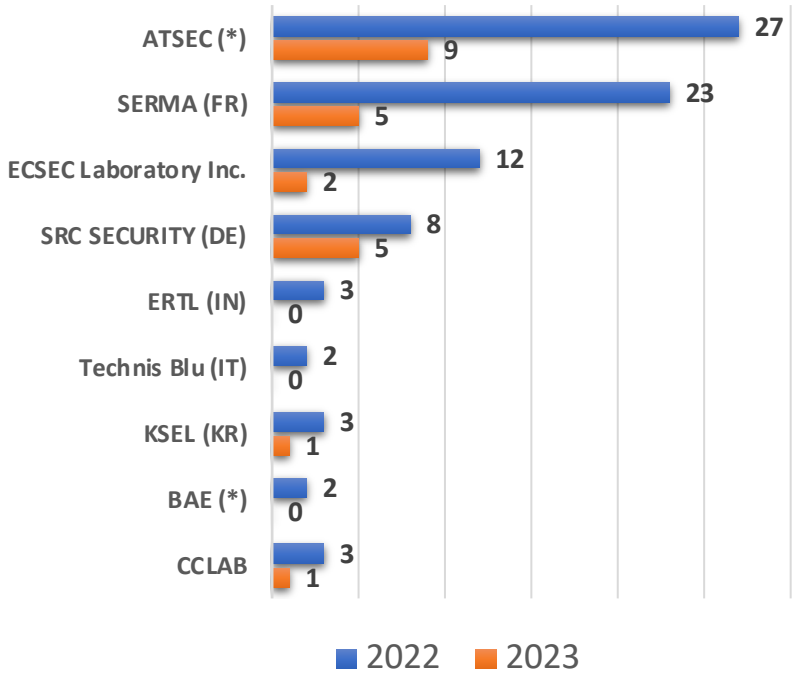


Evolution of top 5 laboratories in the last 5 years

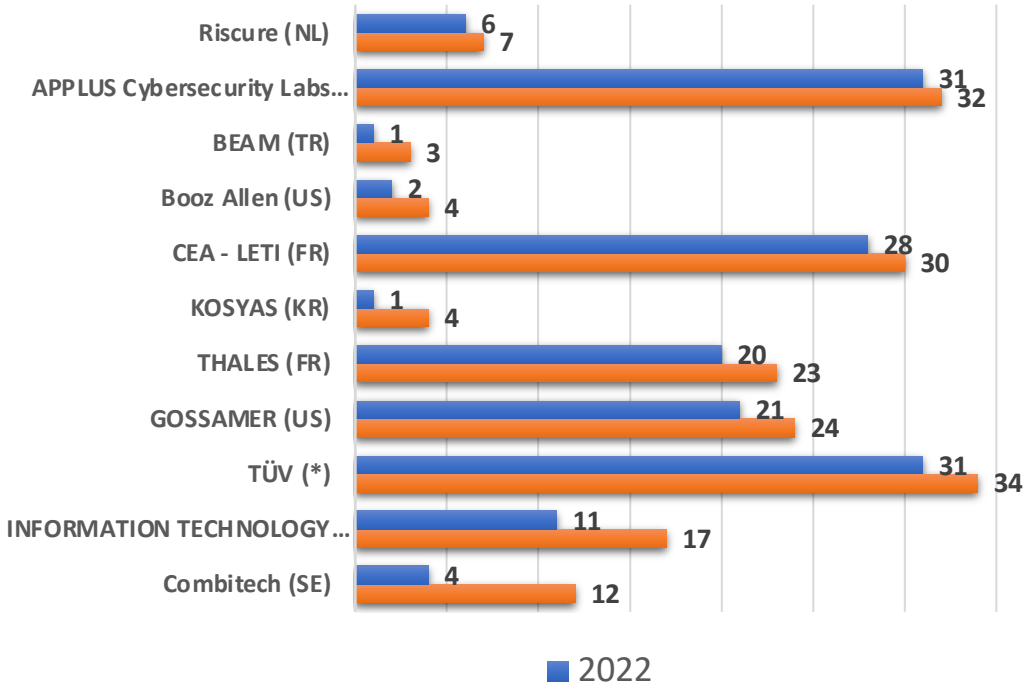


Lab growth 2022-2023 (until 29/09/23)

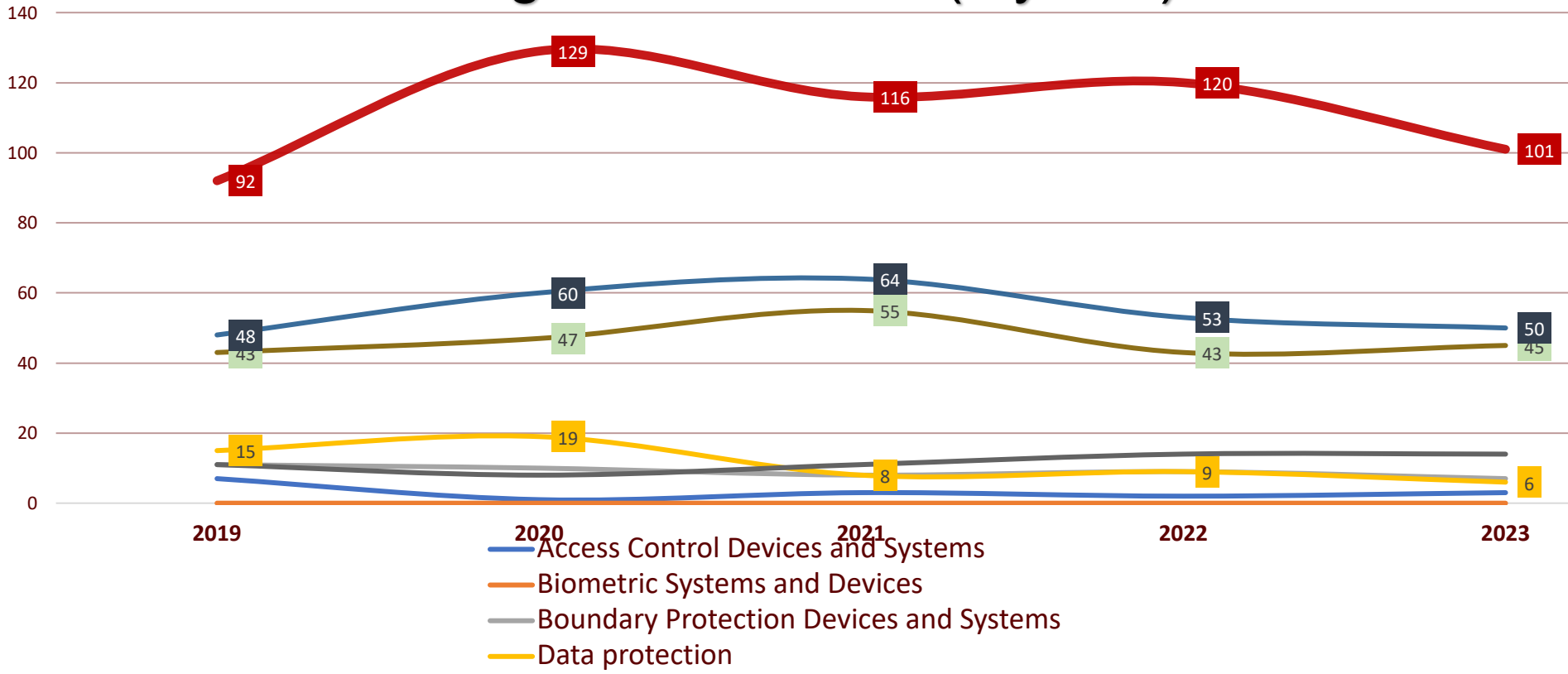
Lab negative growth 2022-2023



Lab positive growth 2022-2023 (sept)



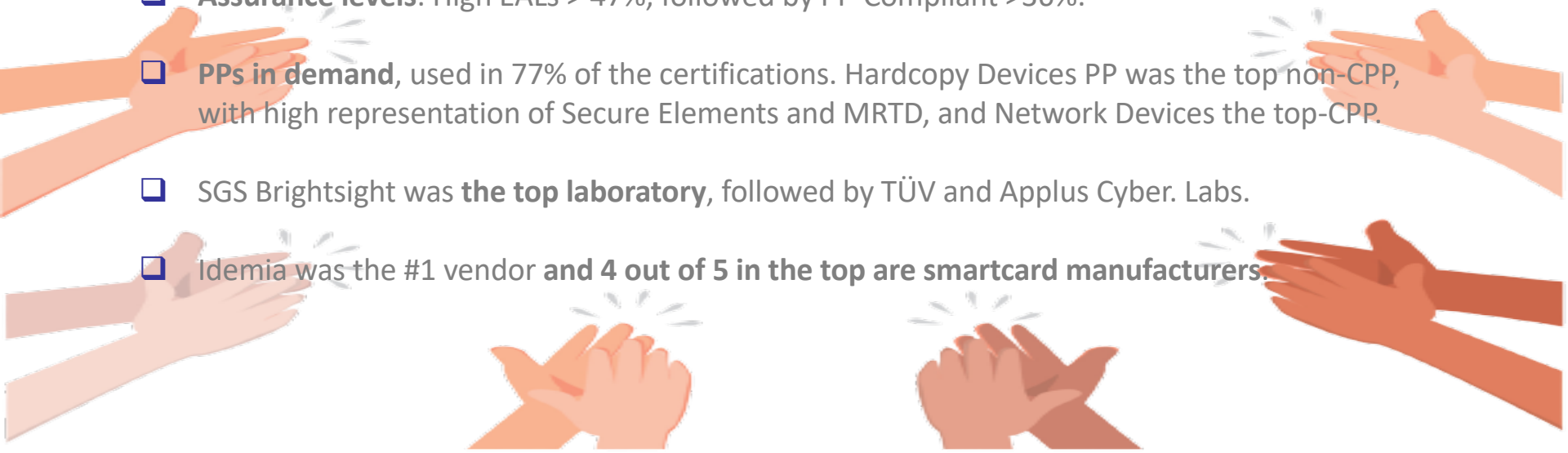
Statistics – Categories evolution (5 years)



Conclusions

CC Certification Industry in 2023

- **Strong Year**: 2023 performance probably will end as **the best year of the last 5.**
- **The top-3 schemes dominate** (FR, NL, USA), tied up, with difference over the rest.
- **Assurance levels**: High EALs > 47%, followed by PP-Compliant >36%.
- **PPs in demand**, used in 77% of the certifications. Hardcopy Devices PP was the top non-CPP, with high representation of Secure Elements and MRTD, and Network Devices the top-CPP.
- SGS Brightsight was **the top laboratory**, followed by TÜV and Applus Cyber. Labs.
- Idemia was the #1 vendor **and 4 out of 5 in the top are smartcard manufacturers.**

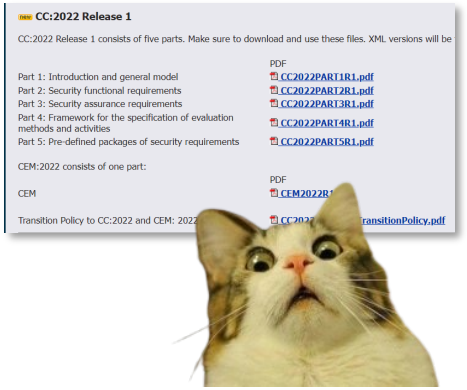


The near future brings changes to CC industry

- In ICCC 2022 we already highlighted the growing importance of national **lightweight certifications** and the shifting of the industry **to cloud-based** certifications… but it hasn't affected the numbers so far.

- **CC2022** will impact labs and vendors
  - New evaluations with CCv3.1 R5 will be admitted only until 30 June 2024.
  - PPs need to be migrated to CC2022 before end of 2027.
  - Will PP0117 start replacing PP0084 for some products in 2024?

- **EUCC** could significantly change the CC certification landscape in Europe:
  - Implementing act draft already published. After 1 year transition period, EU countries will no longer issue certificates under CCRA.
  - Some vendors could slow down their certification roadmap during that period.
  - We still need to see how American and Asian CC market will react.



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

ASTM ICAM 2023 Presentation

The Printer Working Group

- November 2, 2023

APPLYING COMMON CRITERIA TO THE DIGITAL THREAD AND 3D PRINTING?

What is Common Criteria?

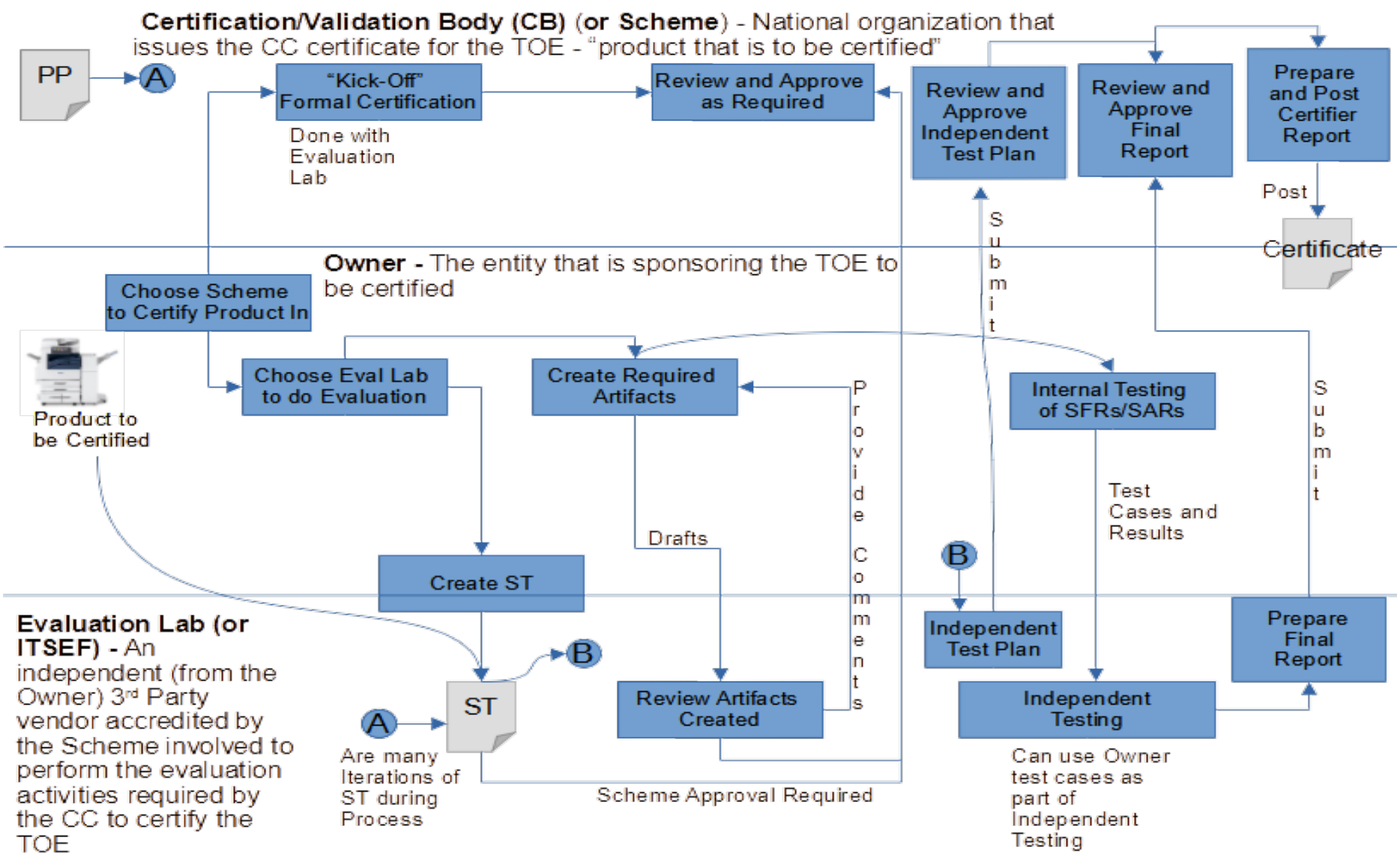
- The Common Criteria for Information Technology Security Evaluation (or Common Criteria (CC)) is an international standard (ISO/IEC Standard 15408-1:2009) for security certification of information security products.
- Common Evaluation Methodology (CEM) is the document that defines how to apply CC to evaluate a product
- CC is governed by a Common Criteria Recognition Arrangement (CCRA) signed by 31 countries

Common Criteria Certification Key Terminology

- **Target of Evaluation (TOE):** A set of software, firmware and/or hardware possibly accompanied by guidance.

  The TOE is what gets certified. It can be anything from a piece of hardware, a software application, part of a product, an operation system to a complete software/hardware/system product
- **Protection Profile:** Implementation-independent statement of security needs for a TOE type (in this case the TOE type will be "3D printers")
- **Security Target:** Implementation-dependent statement of security needs for a specific identified TOE
- **Evaluation Scheme:** Administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community

Common Criteria Certification Process



Common Criteria Certification of Hardcopy Devices (2D Printers)

- Developed and published a collaborative Protection Profile for Hardcopy Devices (HCD cPP)
- In the HCD cPP the following were identified as part of the Security Problem Definition:
  - Key Security Threats to HCDs (and 2D printers in general)
  - Key Assumptions about the Operational Environment necessary so Key Threats can be mitigated
  - Key Organizational Security Policies (OSPs) that have to be in place in an organization to support the security of HCDs
  - Key Security Functions that the HCD has to perform to support the security of HCDs

Digital Thread for Additive Manufacturing and Common Criteria Certification

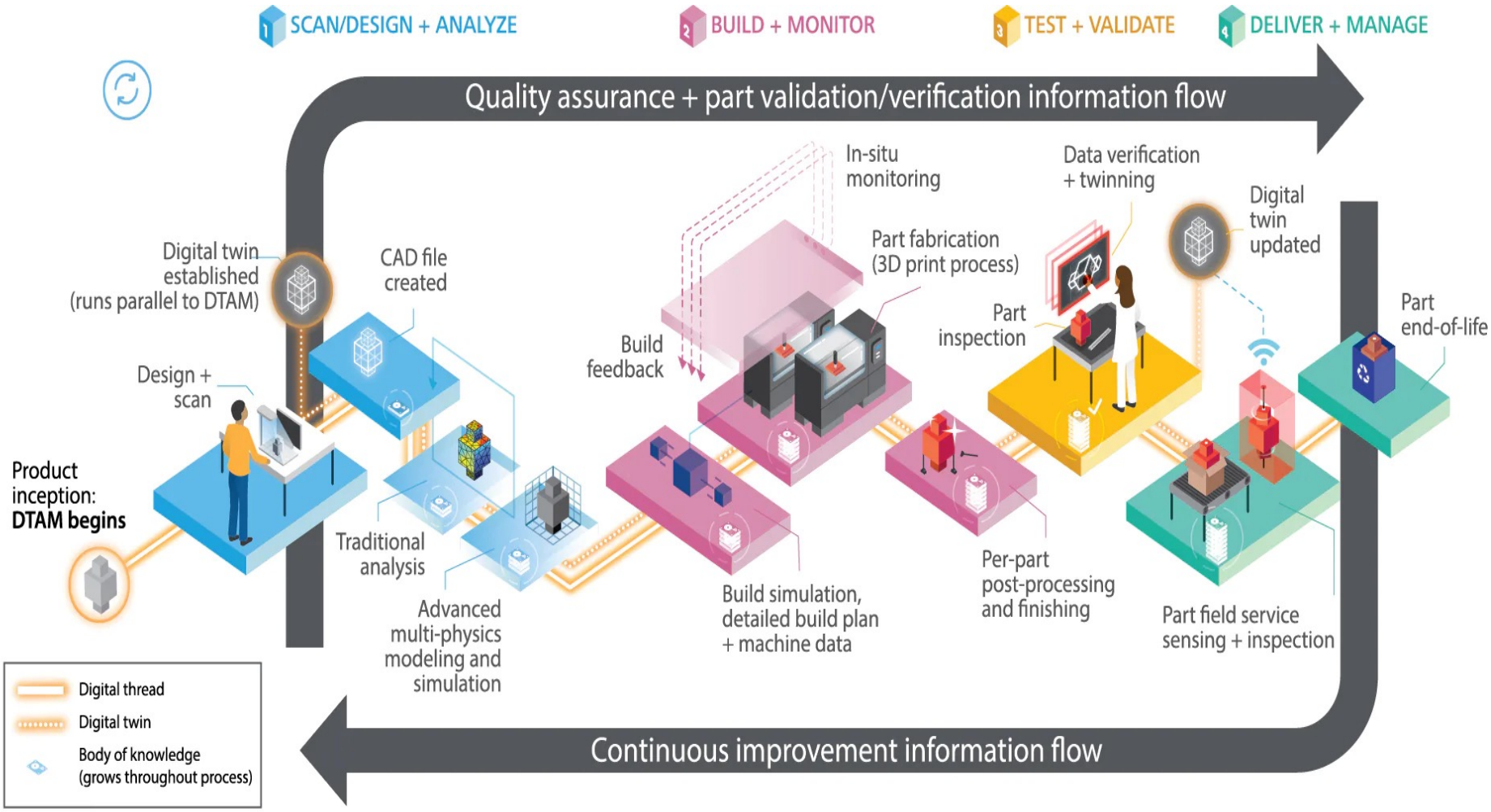
Could the Common Criteria Certification process that was used to certify Hardcopy Devices be used to perform a similar security certification for the Digital Thread for Additive Manufacturing?

We think the answer is '**YES IT CAN BE**' because:

- Both have major assets that must be protected from unauthorized disclosure or modification
- Both have similar security threats that these assets must be protected from
- Both have similar security objectives that have to be performed to support the security of the HCDs or Digital Thread

HOW CHANGES TO COMMON CRITERIA IN 2022 IMPROVE ABILITY TO CERTIFY THE DIGITAL THREAD

Digital Thread for Additive Manufacturing



Common Criteria 2022 (CC:2022)

•A new version of the Common Criteria (denoted as CC:2022) was issued in November 2022

- The Common Criteria standard is now broken up into 5 Parts:
  - Part 1: Introduction and General Model - Same as before
  - Part 2: Security Functional Components – Same as before
  - Part 3: Security Assurance Components – Some important changes from previous version
  - Part 4: Framework for the specification of evaluation methods and activities – All new
  - Part 5: Pre-defined packages of security requirements – Mostly new, but includes parts of what was in Part 3 in previous version
- Part 2 contains some new and modified Security Functional Requirements (SFRs) from previous version

Why the CC:2022 Changes Are Significant For the Digital Thread

- CC:2022 defines the concept of a "composite Target of Evaluation (TOE)", which is defined as "comprising solely two or more separately identified components with a security relationship between their *TOE security functionality (TSFs)"*
  - This may allow us to define the Digital Thread as a composite TOE between the 3D Printer and the computer containing the CAD file and build simulations and then develop a Protection Profile for the composite TOE based on the composite evaluation techniques in CC:2022 Part 5
-

Why the CC:2022 Changes Are Significant For the Digital Thread

- CC:2022 also defines the concept of a PP-Configuration and PP-Module that could be used to define a Protection Profile for the full Digital Thread, The idea would be that you:
  1. Define a base configuration (the full Digital Thread in this case without considerations for the 3D Printer and Computer with the CAD file) with a Security Problem Definition and a set of applicable functional and assurance requirements to form a PP called the base PP
  2. The 3D Printer and Computer with the CAD file/Build Simulation, etc. would each be treated as a separate PP-Module, each with its own Security Problem Definition and set of functional and Assurance requirements in the form of PP
  3. The sum of the base PP and the PPs for the two PP-Modules would comprise the PP-Configuration

Why the CC:2022 Changes Are Significant For the Digital Thread

- CC:2022 Part 2 includes several new Security Functional Requirements (SFRs) that, in addition to many of the SFRs that are in the published version of the HCD cPP, could be applicable to the eventual PP for the Digital Thread:
  - New cryptographic SFRs dealing with Random bit generation and Random number generation, Cryptographic key derivation and Timing and event of cryptographic key destruction
  - New Trusted channel protection, TSF initialization and Stored data confidentiality SFRs
- The new CC:2022 Part 4 defines a general model for defining a unique evaluation method and evaluation activities not in Parts 3 or 5 that can apply to an PP, PP-Module or PP-Configuration
  - This could be used to develop evaluation methods and activities that reflect the unique aspects of the Digital Thread

Digital Thread and Common Criteria Certification Next Steps

- Identify one or more National Bodies to sponsor and then create a 3D Printing Technical Community (TC) to develop a Protection Profile (PP) for the Digital Thread (or separately for 3D Printers)
- Determine who the customers/audience for this TC would be
- Determine what are the following for the Digital Thread (or for 3D printers alone):
- Threats
- Key assumptions that must be upheld
- Organizational Security Policies that must be upheld
- Security Objectives
- Generate an approved Digital Thread/3D Printing Protection Profile. Our initial thought is that it could be a PP-Module based off of the HCD collaborative PP that is currently being developed for publication in 4Q 2022
- Recognize this will take a minimum of two – four years to complete
- Once we have a Digital Thread/3D Printing PP we can start certifying 3D Printers or the entire Digital Thread against that PP

BACKUP

Digital Thread vs. HCDs

From a security certification perspective, at the 10,000 foot Level, the Digital Thread and HCDs are not that dissimilar

- Both have major assets that must be protected from unauthorized disclosure or modification. In the case of the Digital Thread, assets can include things like:
  - CAD model
  - Build Simulations
  - STL file the CAD model is transformed into
- Both have similar security threats that these assets must be protected from such as:
  - Unauthorized access to the CAD model and build simulations
  - Unauthorized access to the STL file created from the CAD file
  - Unauthorized access to the STL file while in transit between the computer hosting the CAD model and the 3D printer if stored on separate computers
  - Unauthorized access to the build simulation and slicer software stored on the 3D printer
  - Unauthorized software upgrade of either the computer hosting the CAD model or the 3D printer

Digital Thread and Common Criteria Certification

- Similarly, the following HCD Security Objectives might also apply in total or in part to the Digital Thread for Additive Manufacturing:
  - User Authorization
  - User Identification and Authentication
  - Access Control
  - Communications Protection
  - Auditing
  - Storage Encryption
  - Firmware/Software Update Verification
  - Protection of Key Material
  - Authentication Failures
  - Strong Cryptography

Common Criteria Terminology

- **CC:** Common Criteria for Information Technology Security Evaluation, the title of a document describing a particular set of *IT Security Evaluation Criteria*
- **CEM:** Common Methodology for Information Technology Security Evaluation, the title of a technical document describing a particular set of *IT Security Evaluation Methods*
- **Certification/Validation Body (CB):** An organisation responsible for carrying out *Certification/Validation* and for overseeing the day-today operation of an *Evaluation and Certification/Validation Scheme*
- **Common Criteria Certificate:**
  A public document issued by a *Compliant CB* and authorised by a *Participant* which confirms that a specific *IT Product* or *Protection Profile* has successfully completed *Evaluation* by an *ITSEF*.
- **Evaluation:** The assessment of an *IT Product* or a *Protection Profile* against the *Common Crit*eria using *Common Evaluation Methodology* to determine whether or not the claims made are justified
- **Evaluation and Certification/Validation Scheme:** The systematic organisation of the functions of *Evaluation* and *Certification/Validation* under the authority of a *CB* in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved

Common Criteria Terminology

- **ITSEF:** IT Security *Evaluation Facility*, an *Accredited Evaluation Facility*, *Licensed* or *Approved* to perform *Evaluations* within the context of a particular *IT Security Evaluation and Certification/Validation Scheme* (Note: Also known as the "Evaluation Lab" or "Common Criteria Test Lab")
- **Protection Profile:** A formal document defined in *CC,* expressing an implementation independent set of security requirements for a category of *IT Products* that meet specific consumer needs
- **collaborative Protection Profile (cPP):** A *Protection Profile* collaboratively developed by an *International Technical Community* endorsed by the *Management Committee*. A *cPP* and related *Supporting Documents* define the minimum set of common security functional requirements and the *Achievable Common Level of Security Assurance*. It addresses vulnerability analysis requirements to ensure certified products reach an *Achievable Common Level of Security Assurance*
- **Security Target (ST):** An implementation-dependent statement of security needs for a specific identified *Target of Evaluation*
- **Supporting Document:** A document that specifies the use of the Common Criteria or *Common Methodology for Information Technology Security Evaluation* in a particular field or domain of technology. Such documents may be either mandatory or guidance and generally specify the *Interpretations* of the *CC* and/or *CEM* when necessary

Common Criteria Terminology

- **Target of Evaluation (TOE):** An *IT Product* and its associated administrator and user guidance documentation that is the subject of an *Evaluation*
- **IT Product:** A package of IT software and/or hardware, providing functionality designed for use or incorporation within a multiplicity of *IT Systems*
- **International Technical Community (iTC):**A group of technical experts including *Participants*, *Certification/Validation Bodies*, *ITSEFs*, developers and users which are:
  a) working in manners that promote fair competition;
  b) working in some specific technical area in order to define *cPPs*;
  c) endorsed for this purpose by the *Management Committee*; and
  d) establishing *Interpretations* of the application of the *CC* and *CEM* necessary for *cPPs* through *Supporting Documents* which are subject to the CCRA approval process
- **TOE Security Functionality (TSF)**: Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

HCD Security Guidelines

Liaison Status

Trusted Computing Group (TCG)

- **Recent and Next TCG Members Meetings**
  - **TCG Hybrid F2F (Kirkland, WA) – 24-26 October 2023 – Ira called in**
  - **TCG Hybrid F2F (Tokyo, Japan) – 27-29 February 2024 – Ira to call in**
- **Trusted Mobility Solutions (TMS) – Ira is co-chair and co-editor**
  - **Formal Liaisons – GP (TEE, SE, TPS), ETSI (NFV/SAI Security and Privacy)**
  - **Informal Liaisons – 3GPP, GSMA, IETF, ISO, ITU-T, SAE, US NIST**
  - ***TCG TMS Use Cases v2 – published September 2018***
- **Mobile Platform (MPWG) – Ira is co-editor**
  - **Formal and Informal Liaisons – jointly with TMS WG above**
  - ***TCG Mobile Reference Architecture v2 – published August 2023***
  - ***TCG MARS 1.0 Mobile Profile – new work-in-progress Q4 2023***
  - ***TCG TPM 2.0 Mobile Common Profile – work-in-progress deferred to Q1 2024***
  - ***TCG Runtime Integrity Preservation for Mobile Devices – published Nov 2019***
  - ***GP TPS Client API / Entity Attestation Protocol / COSE Keystore – joint work***
- **Recent Specifications**
  - **http://www.trustedcomputinggroup.org/resources**
  - ***TCG MARS Serialization Interface v1 – public review October 2023***
  - ***TCG PC Client Reference Integrity Manifest v1.1 – public review October 2023***
  - ***TCG Reference Integrity Manifest (RIM) Info Model v1.1 – public review October 2023***
  - ***TCG Storage Component Class Registry v1 – public review September 2023***
  - ***TCG Mobile Reference Architecture v2 – published August 2023***
  - ***TCG Algorithm Registry v1.34 – public review June 2023***
  - ***TCG MARS API v1 – published May 2023***
  - ***TCG Measurement and Attestation RootS (MARS) Library v1 – published January 2023***

Internet Engineering Task Force (IETF) (1 of 4)

- **Recent and Next IETF Members Meetings**
  - **IETF 118 Hybrid F2F (Prague, Czech Republic) – 6-10 November 2023 – Ira called in**
  - **IETF 119 Hybrid F2F (Brisbane, Australia) – 18-22 March 2024 – Ira to call in**
  - **IETF 120 Hybrid F2F (Vancouver, Canada) – 22-26 July 2024 – Ira to call in**
- **Transport Layer Security (TLS)**
  - **IETF Delegated Credentials for TLS and DTLS – RFC 9345 – July 2023**
    https://datatracker.ietf.org/doc/rfc9345/
  - **IETF Exported Authenticators in TLS – RFC 9261 – July 2022**
    https://datatracker.ietf.org/doc/rfc9261/
  - **IETF Compact TLS 1.3 – draft-09 – October 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-ctls/
  - **IETF Well-known URI for publishing ECHConfigList Values – draft-04 – October 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-wkech/
  - **IETF IANA Registry Updates for TLS/DTLS – draft-05 – October 2023 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8447bis/
  - **IETF Return Routability Check for DTLS 1.2/1.3 – draft-10 – October 2023 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-tls-dtls-rrc/
  - **IETF TLS Encrypted Client Hello – draft-17 – September 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-esni/
  - **IETF Deprecating Obsolete Key Exchange in TLS 1.2 – draft-03 – Sept 2023 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-tls-deprecate-obsolete-kex/
  - **IETF Hybrid key exchange in TLS 1.3 – draft-09 – September 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
  - **IETF TLS Protocol 1.3 – draft-09 – July 2023 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8446bis/

Internet Engineering Task Force (IETF) (2 of 4)

- **Concise Binary Object Representation (CBOR)**
  - **IETF Stable Storage for Items in CBOR – RFC 9277 – August 2022**
    https://datatracker.ietf.org/doc/rfc9277/
  - **IETF CBOR tags for IPv4/v6 Adresses – RFC 9164 – December 2021**
    https://datatracker.ietf.org/doc/rfc9164/
  - **IETF CBOR Time, Duration, Period – draft-12 – October 2023 – IETF Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-time-tag/
  - **IETF CBOR DNS Messages – draft-05 – October 2023**
    https://datatracker.ietf.org/doc/draft-lenders-dns-cbor/
  - **IETF CBOR Ext Diagnostic Notation – draft-05 – October 2023 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-edn-literals/
  - **IETF Feature Freezer for CDDL – draft-12 – September 2023**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-freezer/
  - **IETF CDDL 2.0 Draft Plan – draft-03 – August 2023**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-2-draft/
  - **IETF Notable CBOR Tags – draft-09 – August 2023**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-notable-tags/
- **Network Time Protocols (NTP)**
  - **IETF Secure Selection and Filtering for NTP with Khronos – draft-25 – Oct 2023 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-ietf-ntp-chronos/history/
  - **IETF Network Time Protocol v5 – draft-01 – October 2023**
    https://datatracker.ietf.org/doc/draft-ietf-ntp-ntpv5/
  - **IETF NTP Over PTP – draft-01 – October 2023**
    https://datatracker.ietf.org/doc/draft-ietf-ntp-over-ptp/
  - **IETF Roughtime – draft-08 – October 2023**
    https://datatracker.ietf.org/doc/draft-ietf-ntp-roughtime/
  - **IETF NTPv5 Use Cases and Requirements – draft-03 – September 2023**
    https://datatracker.ietf.org/doc/draft-ietf-ntp-ntpv5-requirements/

Internet Engineering Task Force (IETF) (3 of 4)

- **Remote ATtestation ProcedureS (RATS)**
  - **IETF RATS Architecture – RFC 9334 – January 2023**
    https://datatracker.ietf.org/doc/rfc9334/
  - **IETF Concise Reference Integrity Manifest (CoRIM) – draft-03 – October 2023**
    https://datatracker.ietf.org/doc/draft-ietf-rats-corim/
  - **IETF Epoch Markers – draft-08 – October 2023**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-epoch-markers/
  - **IETF EAT Attestation Results – draft-02 – October 2023**
    https://datatracker.ietf.org/doc/draft-fv-rats-ear/
  - **IETF X.509-based Attestation Evidence – draft-00 – October 2023**
    https://datatracker.ietf.org/doc/draft-ounsworth-rats-x509-evidence/
  - **IETF ARM PSA Attestation Token – draft-14 – October 2023**
    https://datatracker.ietf.org/doc/draft-tschofenig-rats-psa-token/
  - **IETF RATS Endorsements – draft-03 – October 2023**
    https://datatracker.ietf.org/doc/draft-dthaler-rats-endorsements/
  - **IETF EAT Profile for Intel® TDX Attestation Result – draft-00 – October 2023**
    https://datatracker.ietf.org/doc/draft-kdyxy-rats-tdx-eat-profile/
  - **IETF Entity Attestation Token (EAT) – draft-22 – October 2023 – IETF Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat/
  - **IETF RATS Conceptual Messages Wrapper – draft-04 – October 2023**
    https://datatracker.ietf.org/doc/draft-ftbs-rats-msg-wrap/
  - **IETF Direct Anonymous Attestation for RATS Architecture – draft-04 – September 2023**
    Direct Anonymous Attestation for the Remote Attestation Procedures Architecture
  - **IETF Attestation Event Stream Subscription – draft-04 – September 2023**
    https://datatracker.ietf.org/doc/draft-ietf-rats-network-device-subscription/
  - **IETF Reference Interaction Models for RATS– draft-08 – September 2023**
    https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/

Internet Engineering Task Force (IETF) (4 of 4)

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **IRTF RSA Blind Signatures – RFC 9474– October 2023**
    https://datatracker.ietf.org/doc/rfc9474/
  - **IRTF SPAKE2, a Password-Authenticated Key Exchange – RFC 9382 – September 2023**
    https://datatracker.ietf.org/doc/rfc9382/
  - **IRTF Verifiable Random Functions (VRFs) – RFC 9381 – August 2023**
    https://datatracker.ietf.org/doc/rfc9381/
  - **IRTF Hashing to Elliptic Curves – RFC 9380 – August 2023**
    https://datatracker.ietf.org/doc/rfc9380/
  - **IRTF BBS Signature Scheme – draft-04 – October 2023**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/
  - **IRTF Merkle Tree Ladder Mode (MTL) Signatures – draft-01 – October 2023**
    https://datatracker.ietf.org/doc/draft-harvey-cfrg-mtl-mode/
  - **IRTF Mastic VDAF – draft-01 – October 2023**
    https://datatracker.ietf.org/doc/draft-mouris-cfrg-mastic/
  - **IRTF Deterministic Nonce-less Hybrid Public Key Encryption – draft-03 – October 2023**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-dnhpke/
  - **IRTF Properties of AEAD algorithms – draft-02 – October 2023**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-properties/
  - **IRTF Secp256k1-based DHKEM for HPKE – draft-01 – October 2023**
    https://datatracker.ietf.org/doc/draft-wahby-cfrg-hpke-kem-secp256k1/
  - **IRTF AEGIS Family of Authenticated Encryption Algorithms – draft-05 – October 2023**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aegis-aead/
  - **IRTF OPAQUE Asymmetric PAKE Protocol – draft-12 – October 2023**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-opaque/

Next Steps – IDS WG

- Next IDS WG Meeting– November 30, 2023
- Next IDS Face-to-Face Meeting likely February 8, 2024 at PWG February 2024 F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG

Backup

HCD iTC
Issues Post-Version 1.0 – CNSA 2.0

- Commercial National Security Algorithm (CNSA) 2.0 released by NSA Sep 2022
- Addresses problem that future deployment of a cryptanalytically relevant quantum computer (CRQC) would break public-key systems still used today
- Need to plan, prepare, and budget for an effective transition to quantum-resistant (QR) algorithms, to assure continued protection of National Security Systems (NSS) and related assets
- Is an update to CNSA 1.0 Algorithms
- Applies to all NSS use of public cryptographic algorithms (as opposed to algorithms NSA developed), including those on all unclassified and classified NSS
- Using any cryptographic algorithms the National Manager did not approve is generally not allowed, and requires a waiver specific to the algorithm, implementation, and use case
- Per CNSSP 11, software and hardware providing cryptographic services require NIAP or NSA validation in addition to meeting the requirements of the appropriate version of CNSA

Commercial National Security Algorithm (CNSA) Suite 2.0 Algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels SHA256/192 recommended
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels

Transitioning to CNSA Suite 2.0

- The timing of the transition depends on the proliferation of standards-based implementations
- NSA expects the transition to QR algorithms for NSS to be complete by 2035 in line with NSM-10.
- NSA urges vendors and NSS owners and operators to make every effort to meet this deadline.
- Where feasible, NSS owners and operators will be required to prefer CNSA 2.0 algorithms when configuring systems during the transition period.
- When appropriate, use of CNSA 2.0 algorithms will be mandatory in classes of commercial products within NSS, while reserving the option to allow other algorithms in specialized use cases

Detailed NIAP Transition Plan for CNSA Suite 2.0

- Currently all NIAP PPs must have CNSA 1.0 algorithms
- Will add SHA-512 to all NIAP PPs
- Will require either CNSA 1.0 or CNSA 2.0 be mandatory on all NIAP PPs
- Will implement CNSA asymmetric algorithms for software/firmware signing per following
  - LMS – 1H 2023
  - XMSS – 2H 2023
- Will implement following Key Establishment CNSA 2.0 algorithms in all NIAP PPs when they are standardized and all relevant Assurance Activities have been defined and agreed upon:
  - CRYSTALS - Kyber
  - CRYSTALS – Dilithium (used for Digital Signatures)
- Will deprecate CNSA 1.0 in 2030 – 2033 timeframe
- No current timeline established to make CNSA 2.0 mandatory
  - Will make use of CNSA 2.0 mandatory to be listed on PCL at some point
- Will work with vendors to help try to meet NSA schedule
- Will discuss with CCRA and engage with iTCs how best to integrate CNSA 2.0 into cPPs