# IDS WG Meeting Minutes
# December 14, 2023

This IDS WG Meeting was started at approximately 3:00 pm ET on December 14, 2023.

**Attendees**

| | |
|---|---|
| Graydon Dodson | Lexmark |
| Smith Kennedy | HP |
| Jeremy Leber | Lexmark |
| Ira McDonald | High North |
| Alan Sukert | |
| Mike Trent | Xerox |

**Agenda Items**

1. The topics to be covered during this meeting were:
   - Latest updates on the HCD HIT
   - Special Topic on updates to the recently published EU AI Act
2. Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust-policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. AI began by discussing the results of the December 4th and 11th HCD Interpretation Team (HIT) Meetings:
   - The December 4th HIT Meeting was primarily to review the fixes Brian Volkoff made in the HCD cPP to address the four NIAP comments made in its review of HCD cPP v1.0. Brian provided a diff file showing the HCD cPP v1.0 text and the updated text Brian fixed, and we did a comparison to verify the fixes were made correctly. Note: This activity continues after the regularly scheduled time of the meeting.
   - Other items of note from the 12/4/23 HIT Meeting:
     - We processed issue HCD-IT#22 cPP **Clarification of Test Requirements and Context of FPT_TST_EXT.1**:

       cPP Section 5.8.4. "FPT_TST_EXT.1 Extended: TSF testing" has the following two paragraphs under Application Note, which has minor consistency among each other:

       **Application Note:**
       Power-on self-tests may take place before the TSF is operational, in which case this SFR can be satisfied by verifying the TSF image by digital signature as specified in FCS_COP.1/SigGen, or by hash specified in FCS_COP.1/Hash.

       Self-test is intended to detect malfunctions which may compromise the TSF. Since the integrity of the firmware/software is guaranteed by FPT_SBT_EXT, the function for FPT_TST_EXT should
       address the malfunction detection like DRBG self-test defined in ISO/IEC 18031:2011.

       Is it sufficient to only run an integrity test (no other tests) on start-up/power on?

       **Suggestions:**

       1. If integrity of TOE image is sufficient to meet the intent of FPT_TST_EXT.1, then the SFR should be reworded as:
          *FPT_TST_EXT.1.1 The TSF shall run **an integrity test** on TOE software/firmware during initial start-up (and power on) to*
          *demonstrate the correct operation of the TSF.*
       2. If testing of TOE image integrity is not in scope of FPT_TST_EXT.1 (as it's covered under FPT_SBT_EXT.1 as per Application Note provided above), the testing requirement in the SD should be updated accordingly.

*Note: The Application Note was initially changed as a result of the following Issue raised against the draft cPP: HCD-iTC/HCD-iTC-Template#261*

We gave this issue Priority 1 and assigned it to Brian Volkoff to review. .

- We processed HCD-IT #23: **Missing option in then selection in SFR FIA_X509_EXT.2 X.509 Certificate Authentication in HCD cPP v1.0**

  A comment from Shin-ichi Inoue, ECSEC laboratory against HCD cPP v1.0:
  Section A.5.1.2 FIA_X509_EXT.2 X.509 Certificate Authentication, FIA_X509_EXT.2.2 - Usage of an offline CRL (CRL may be imported to TOE by USB memory) is not considered as an option in this SFR. In this case, TOE doesn't need to establish a connection.

  Solution: Add the option "allow the Administrator to import CRL file and perform OFFLINE-validation of a certificate" in the selection in this SFR.

  We gave this issue Priority 1 .It is awaiting an assignment to a HIT member for review.

- HCD-IT #20: This submitter of the issue requested via email that this issue be withdrawn because it turns out not to be a valid issue. Al had the action to close this issue on that basis.
- HCD-IT #9: Sato-san has sent a proposal via email to the Al and Jerry on how to address this issue. We did not review this proposal at this meeting because most of the HIT members have not seen it. Al agreed to send the proposal out to the full HIT membership before the next HIT Meeting, and then we will review the proposal as the first topic of the next meeting.
- HCD-IT #9: Sato-san sent a proposal via email to Al and Jerry Colunga on how to address this issue. We did not review this proposal at this meeting because most of the HIT members have not seen it. Al agreed to send the proposal out to the full HIT membership before the next HIT Meeting, and then we would review the proposal as the first topic at the next HIT meeting.
- It was mentioned during this review that the completed Errata will have to go to NIAP for review before we publish it.

- Items of note from the 12/11/23 HIT Meeting:
  - Sato-san's Proposal to address HCD-IT #9 **Modification proposal : tests for FDP_DSK_EXT.1**

    The latest version of the proposal we reviewed at the meeting can be found at Proposal for No.9 on HIT 20231208 Response2.docx.

    Part of Sato-san's proposal was to add the following paragraph to the TSS Assurance Activities for SFR FDP_DSK_EXT.1:

    If any User document or Confidential TSF data are potentially transparently encrypted and written to disk via mechanisms other than the operating TSFI, the evaluator shall verify that the TSS identifies those mechanisms and describes at a high level how the associated data are encrypted. Examples of such mechanisms could include swap files and core dump

    The team focused on the word "potentially" in the paragraph and felt it would cause confusion as to what files required mechanisms other than the operating TSFI to be transparently encrypted. We agreed that "potentially" should be removed and the last sentence rewritten to better clarify exactly what files are involved, and that this paragraph is just basically stating the case where certain types of files like swap files and core dumps require mechanisms other than the operating TSFI to be transparently encrypted and written on the disk.

    We also agreed the word "potentially" should be removed from the new Test 5 and Test 6 added to the Test Assurance activities for SFR FDP_DSK_EXT.1 by this proposal.

With these changes the HIT members present at the meeting agreed to accept the modified proposal as the solution for HCD-IT #9.

- Brian indicated he would have the final diff file for all the fixes for the four NIAP issues ready for final review by Tuesday 11/12.
- HCD-IT #18: **Technical issue in the TSS Assurance Activities for SFR FCS_CKM.1/SKG in HCD SD v1.0Colunga**

  We got into a long discussion on this issue and the direct generation of keys. Jerry Colunga brought up the issue because SFR **FCS_CKM.1/SKG Cryptographic Key Generation (Symmetric Keys)** includes the following requirements:

  The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [selection: *128 bits, 192 bits, 256 bits*] that meet the following: [selection: *ISO/IEC 18031:2011 (Clause 9) [DRBG], NIST SP 800-133 Rev.2 Section [selection: 6.1, 6.3]]***

  Jerry looked into NIST SP 800-133 Rev 2 and found that Section 6.1 deals with direct generation of keys using a Random Bit Generator (RBG), but Section 6.3 deals with combining multiple keys with other data into a new key. Based on that Jerry felt that "direct" should not be deleted because of the second case of a new key generated by a concatenation of other keys and other data (one of the cases listed in NIST SP 800-133 Rev 2 Section 6.3).

  We discussed the aspects of this issue for several minutes and finally came to the conclusion that the cases discussed in either NIST SP 800-133 Rev 2 Section 6.1 or 6.3 ultimately result in using direct output of an RBG to generate the key. As a result, the requirements in **SFR FCS_CKM.1/SKG** are correct as is and do not need to be changed.

  As for the HCD SD, which is what this issue was against, to address the case of keys generated by multiple keys and other data, the HIT agreed that the TSS Assurance Activities for **SFR FCS_CKM.1/SKG** should add a paragraph that addresses this "second" case. The HIT also felt the current test cases in the Test Assurance Activities for **SFR FCS_CKM.1/SKG** were sufficient to cover this "second" case.

4. Al then presented his special topic for the day, which is a closer look at the updated EU Artificial Intelligence (AI) Act. The slides for this special topic can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/AI Act Update.pdf.

   The reason Al brought the EU AI Act up was that on Dec 9th, 2023 the EU and its 27 Member Nations came to a provisional agreement on the final wording of the EU AI Act, which is a key step in the eventual publishing and implementation of this act. The provisional agreement did result in several key changes from the initial text of the act that Al reviewed at the 6/22/2023 IDS Meeting.

   The key points from the review of the EUCC IR were:

   - The purpose of the EU AI Act remained the same – to establish
     - Harmonized rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union
     - Prohibitions of certain artificial intelligence practices
     - Specific requirements for high-risk AI systems and obligations for operators of such systems
     - Harmonized transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorization systems, and AI systems used to generate or manipulate image, audio or video content
     - Rules on market monitoring and surveillance
   - Similarly, the scope of the AI Act remained the same – the EU AI Act applies to:

- Providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country
- Users of AI systems located within the Union
- Providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union
- Not apply to AI systems developed or used exclusively for military purposes
- Not apply to public authorities in a third country nor to international organizations falling within the scope of this Regulation, where those authorities or organizations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States

- At a high-level, three key changes to the AI Act from its initial text are:
  - Rules on high-impact general-purpose AI models that can cause systemic risk in the future, as well as on high-risk AI systems
  - A revised system of governance with some enforcement powers at EU level extension of the list of prohibitions but with the possibility to use remote biometric identification by law enforcement authorities in public spaces, subject to safeguards
  - Better protection of rights through the obligation for deployers of high-risk AI systems to conduct a fundamental rights impact assessment prior to putting an AI system into use

  Al noted that the AI Act still focuses on high-risk AI systems but now there is more attention to AI models that were not mentioned at all in the initial draft.

- Another key chance in the AI Act from the provisional agreement was that the list of intrusive and discriminatory uses of AI systems was amended now include:
  - “Real-time” remote biometric identification systems in publicly accessible spaces;
  - “Post” remote biometric identification systems, with the only exception of law enforcement for the prosecution of serious crimes and only after judicial authorization;
  - Biometric categorisation systems using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation);
  - Predictive policing systems (based on profiling, location or past criminal behaviour);
  - Emotion recognition systems in law enforcement, border management, workplace, and educational institutions; and
  - Indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases (violating human rights and right to privacy)

  Al noted that there still is a focus in the AI Acton on human rights and privacy, which are both huge issues in the EU.

- The key provisions in the updated AI Act per the provisional agreement are that it:
  - Imposes legally binding rules requiring tech companies to notify people when they are interacting with a chatbot or with biometric categorization or emotion recognition systems
  - Requires tech companies to label deepfakes and AI-generated content, and design systems in such a way that AI-generated media can be detected

    These first two are very important given the concern today about the potential misuse of AI
  - Requires all organizations that offer essential services, such as insurance and banking, to conduct an impact assessment on how using AI systems will affect people’s fundamental rights
  - Requires foundation models and AI systems built on top of them to draw up better documentation, comply with EU copyright law, and share more information about what data the model was trained on

    Transparency of AI models is another important new inclusion in the AI Act

- Tech companies have to share how secure and energy efficient their AI models are
- Applies a stricter set of rules to only the most powerful AI models, as categorized by the computing power needed to train them

  This was a point of controversy. Many Member Nations wanted this provision to apply to all models but ended up compromising to what it is here. Categorizing on computing power doesn't seem like the right way to determine what is a "powerful" AI model
- Enforces binding rules on AI
- The AI Act's governance mechanism includes a scientific panel of independent experts to offer guidance on the systemic risks AI poses, and how to classify and test models

  Al noted this is a good thing to make sure independent guidance on AI development, so there is a check on AI development
- The fines for noncompliance are steep: from 1.5% to 7% of a firm's global sales turnover, depending on the severity of the offense and size of the company.

  The fins do seem substantial
- EU citizens will be able to launch complaints about AI systems and receive explanations about how AI systems came to the conclusions that affect them

  Another good new provision allowing citizens to formally complain when AI systems negatively impact them.
- Some AI uses are now completely banned in the EU:
  - biometric categorization systems that use sensitive characteristics;
  - untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases like Clearview AI;
  - emotion recognition at work or in schools;
  - social scoring;
  - AI systems that manipulate human behavior;
  - and AI that is used to exploit people's vulnerabilities.

  These prohibitions speak for themselves
- Predictive policing is also banned, unless it is used with "clear human assessment and objective facts, which basically do not simply leave the decision of going after a certain individual in a criminal investigation only because an algorithm says so

  The concept of "predictive policing" is interesting and somewhat akin to "police profiling"; it is also scary.
- The AI Act does not apply to AI systems that have been developed exclusively for military and defense uses

  This was in the scope
- European police forces will only be able to use biometric identification systems in public places if they get court approval first, and only for 16 different specific crimes, such as terrorism, human trafficking, sexual exploitation of children, and drug trafficking

  It is good the AI Act puts limits on the uses of AI by law enforcement
- Law enforcement authorities may also use high-risk AI systems that don't pass European standards in "exceptional circumstances relating to public security"

- What comes next for the EU AI Act now that the provisional agreement has been reached is:
  - Following the provisional agreement, work will continue at technical level in the coming weeks to finalize the details of the new regulation
  - The presidency will submit the compromise text to the member states' representatives for endorsement once this work has been concluded.

- The agreed text will have to be formally adopted by both Parliament and Council to become EU law.
- The Artificial Intelligence Act will become law 20 days after its publication in the Official Journal of the European Union (the official publication for EU legal acts, other acts and official information from EU institutions, bodies, offices and agencies).
- This will likely happen during the summer of 2024 (although I read other estimates that this will happen in 2025)
- Once it is in force, tech companies have two years to implement the rules. The bans on AI uses will apply after six months, and companies developing foundation models will have to comply with the law within one year

So, it will take at least 6 months, and maybe up to a year or more, before the EU AI Act actually becomes law.

- After Al finished his presentation Smith asked a question that resulted in a lively conversation to end the meeting. Smith's question was "How does the AI Act related to HCDs?".

  The general view was that any impact would be indirect. The idea is that given the increasing popularity of AI and the fact that HCDs today (especially Multi-Function Devices) do support apps. It is only a matter of time before someone develops if they haven't done so already) Al apps for HCDs. Al's thoughts were that these AI apps would allow a user to, for example, enter in the necessary information and the AI app would then generate and automatically print or scan to a file/destination or email a standard type of letter or a standard legal document like a will.

  An application like this brings up all then AI issues that are of concern today, and if the HCD is in Europe the EU AI Act would apply to it. And as Ira pointed out, if something goes wrong and the app prints something it is not supposed to or something that violates a provision of the AI Act, the printer manufacturer could (and probably would) be liable for the fines mentioned above.

  The bottom line is that HCD manufacturers have to be very careful what, if any, AI-related apps or products that allow their devices to access.

5. **Actions:** None

**Next Steps**

There is no future IDS WG Meeting scheduled at this time. Al will be unavailable to lead IDS until May 2024 and the Steering Committee is looking for someone to temporarily take over IDS until Al returns in May.