EUCC ISAC

EUCC ISAC Joint Hardware Attack Subgroup (JHAS)

Terms of Reference

V.01

1st December 2025

Traffic Light Protocol (TLP)

TLP LEVEL	DESCRIPTION	SHARING SCOPE
TLP:CLEAR	Disclosure is not restricted.	May be shared freely and published without limitation.

Table of Contents

1. Introduction

The EUCC ISAC is as a non-for-profit association governed by Belgium law, the Joint Hardware Attack Subgroup or JHAS is a technical group of the EUCC ISAC. Terms of Reference provide practicalities, details and procedure in relation with the working of JHAS which are not specified by the statutes of the EUCC ISAC.

JHAS has been originally addressing the concerns of vendors and SOG-IS national schemes related to Common Criteria methodology about state-of-the art attacks, mainly driven historically by the banking and governmental market products. Gradually, JHAS has been widening its scope to the development of the smartcard industry with further referential schemes, i.e. EMVCo, IPA and members provided they could share the same values about high-level security evaluation approach and agree to the rules of collaboration. Recognized schemes refer to those pre-cited schemes.

The JHAS is recognized in the industry for its harmonization added value in the CC and EMVCo domains. The harmonization work at JHAS is essential to preserve the ITSEFs applying equal methods and evaluation scale. This is crucial for acknowledgement of certificates coming from other participating certification countries and/or schemes.

The mission is that all participants gain an agreed common understanding of the evaluation of certain attacks.

Within the last decade, the Security Evaluation standards evolved towards several directions:

- Changing form factors and business models (Smartcards to Secure ICs, Secure Element to Secure Subsystem within an SoC…)
- New markets growing with shorter timeframe and different levels of security (from traditional Banking, Passport to mobile Security, TPM and IoT …)
- Emergence of main regional actors creating or influencing the standards (China, US, …),
- Evolution of CCRA,
- Evolution of European cybersecurity regulations

Meanwhile, the JHAS still targets a worldwide harmonization and standardization of how emerging attacks and new analysis methods are to be evaluated throughout all participating evaluation and certification schemes. Its mission is that all participants apply the same scale of evaluation metric for a certain identified attack or analysis method. This is fundamental for the mutual acceptance of certificates among the participating schemes, respectively countries. For this reason, the group consists of certification bodies, respectively authorities, accredited evaluation laboratories (CAB/ITSEFs), hardware and software vendors.

This group is driven by the vendors and schemes and has no educational mission.

The JHAS collaboration is conformant with European antitrust laws as it is managed as an ISAC subgroup under the ISAC antitrust bylaws.

This document contains the mission statement, organization and functioning rules for this subgroup.

The compliance to ToR by each JHAS member is required to preserve each member's sensitive assets, guarantee the trustworthiness in the subgroup exchanges and enable JHAS productivity. It is essential that JHAS members share the same values and work towards agreed shared objectives.

2. Guiding principles

JHAS is led by voluntary consensus principles in accordance with the following attributes:

- Openness – the procedures or processes used for creation, revision, reaffirmation, and withdrawal of JHAS' technical documents are transparent and open to all the members. JHAS members are provided meaningful opportunities to participate in the definition of the technical documents on a non-discriminatory basis.
- Balance and Lack of Dominance – JHAS' decision-making process, and the development of deliverables should be balanced; there should be meaningful involvement from a broad range of parties, with no single interest dominating the decision-making.

- Due Process – due process shall include procedures, adequate notice of meetings and documentation development, a defined adequate period to review drafts and prepare views and objections, access to views and objections of other participants, within the limits imposed by the confidentiality of information and the strict respect of the antitrust compliance guidelines.
- Procedural Appeals – an appeal process shall be available for the impartial handling of procedural appeals.
- Consensus – consensus is the rule (general agreement, but not necessarily unanimity); during the development of consensus, comments and objections are considered using fair, impartial, open, and transparent processes. To validate this general agreement, votes can be organized pursuant to the following JHAS' Terms of Reference (ToR).

3. Mission and powers

3.1. Tasks

JHAS is tasked with:

- Owning, maintaining, and evolving the methodology to rate attack paths of security IC hardware and embedded security firmware and software,
- Giving guidance to interpret the rating methodology,
- Considering and monitoring state of the art attack paths and emerging attack techniques,
- Aligning the application of the methodology in security evaluations from low attack potential (AVA_VAN.2) up to high attack potential level (AVA_VAN.5),
- Contributing to updates of ISCI outcomes such as the Minimum Lab Requirements for JHAS qualified labs. In particular, it supports evaluations for secure ICs like smart cards, secure elements, secure processing units and enclaves within SoCs and similar technology, corresponding security and cryptographic firmware, security IC operating systems, and security applications,
- JHAS consists of global experts from certification bodies (CAB/CBs), liaised security certification schemes and bodies, related security evaluation facilities, developers and end-user organisations as set out in Article 6 of the EUCC ISAC statutes.
- JHAS contributes to the security community, particularly by publishing and consulting about the attack rating methodology and its interpretation. For clear delimitation, this group is neither a community of certifiers nor a community of security architects,
- Aiming to harmonise attack evaluation methods and ratings, thereby creating a fair and equal framework for all stakeholders. This enables certification schemes, policy makers, and users to robustly evaluate the security solutions they select, both in current and emerging domains.

3.2. Scope Limitations and Exclusions:

- JHAS can neither provide decision about product certificates nor provide threat analysis of a product case or product feature.
- This group is not intended to educate public to attack method details. Other schemes are welcome to use JHAS methodologies and outcomes but can only be recognized as such with formal and official authorization from ECCG (EsEm) or ENISA - ECCG authorities.

4. Membership

Members of JHAS are members of the EUCC ISAC and shall follow its Statutes. Membership to JHAS is open to those EUCC ISAC members who meet the criteria set out in Article 6 of the EUCC ISAC Statutes, as complemented by Terms of Reference (ToR).

JHAS membership is made of:

4.1. Executive members with voting rights:

a. **National Cybersecurity Certification Authorities (NCCAs)**
b. **National Conformity Assessment Bodies (CAB/CBs) operated by a NCCA**
c. **Private CAB/CB, acting on behalf of a National Cybersecurity Certification Authority (NCCA),**
d. **Labs and Information Technology Security Evaluation Facilities (CAB/ITSEFs) that operate within the European Union and supported by an NCCA**
e. **Manufacturers or providers of ICT products**
f. **End-User groups and organisations** (e.g. Telco's, Payment System/Scheme, European and global technical bodies)

With reference to the intention to have one vote per member state, the NCCA shall designate who has the one vote under a) through c). In cases where multiple private CAB/CBs are designated to participate in JHAS activities on behalf of the NCCA, only one CAB/CB shall be granted voting rights, in accordance with the principle of "one Member State represented, one vote." The remaining CAB/CBs may participate, but without voting rights.

4.2. Associate Members with no voting right:

a. **National Cybersecurity Certification Authorities (NCCA)**
b. **National Conformity Assessment bodies (CAB/CBs) operated by an NCCA**
c. **National Accreditation Bodies (NABs)**
d. **One or several representatives of ECCG subgroup for EUCC maintenance and review (EsEm)**

4.3. Observers:

a. **Cybersecurity certification authority operating outside the European Union**
b. **Non-European consortium made of laboratories, conformity assessment bodies, vendors and led by a third-country national cybersecurity certification authority.**

5. Liaisons

JHAS may request the Steering Committee to establish transient or permanent liaison with any other entities. To this end, JHAS defines the conditions of participation and the content of the liaison statement to be submitted to the Steering Committee for approval pursuant to article 23 of the EUCC ISAC Statutes.

6. Other conditions specific to the group

Information discussed in the meetings or communicated in the reports is considered confidential and treated as such. JHAS discussions shall be free without suppressing opinions and meanings:

- Conflicts shall be discussed on technical level only,
- Individual business and other interests are not subject of JHAS discussions,
- Carrying out competitive relations by discrediting or blaming other members or influencing others against a certain member are against the collaboration rules. This should be immediately stopped by the chair and should result in consequences in form of penalty for the initiator.

The information discussed in the meetings or communicated in the documents may not be used for commercial activities other than the intended mission of JHAS.

Each member can provide topics to the chair, vice-chair or secretary for the agenda any time prior to a meeting.

- Whether a topic could be managed in the next meeting is matter of time remaining prior to the meeting and of remaining meeting time of an already given agenda.
- The chair cannot guarantee that a late topic is included in the next meeting, but if not, it shall be a part of the agenda of one of the next meetings. Its urgency can be discussed in the plenary.

The collaboration using electronic media shall be based on encrypted transfer when applicable according to the JHAS asset policy in section 12 output material. Alternatively, the JHAS repository can be used for upload and download.

The JHAS repository keeps a database of

- The public keys of
  - all acting members,
  - of members which have left JHAS,
  - of obsolete keys just to have the possibility to verify old documents or emails,
- Meeting minutes,
- Presentations held.

Acting members means individuals, main representatives and their back-up for each member entity that is actually participating to plenary or subgroup meetings. Acting means actively involved.

Access and account to the JHAS repository have only acting members. Participants being in the trial period gain access when they become acting members.

7. Applications

Applications are subject to validation procedure by the JHAS and information of the Steering Committee of the EUCC ISAC.

JHAS members are accepted according to the conformance to JHAS specific criteria.

- Each JHAS member is providing the JHAS application form correctly filled in with representative's coordinates and PGP keys to JHAS chairman and JHAS repository responsible.
- Each organization agrees by signing in as member to the rules described in JHAS ToR described in this document. This form shall be updated at each member change or at latest every 3 years. Applications from an authorized CB will follow a different process and have to be submitted to the chair of the ISAC Steering Committee.

The members should represent a spectrum as wide as possible of the parties involved in Secure IC products certification with interest in high security evaluation (Common Criteria…). The main groups so far identified are: IC vendors, SW vendors, card vendors, certification bodies, evaluation laboratories, service providers and end-users.

The acceptance criteria for new member application are based on the following main paradigms that are JHAS specific:

1. Applicant profile, technical skills and competence
2. Motivation/Reciprocity Benefit
3. Acceptance of JHAS rules for collaboration
4. Acceptance of JHAS results for their own evaluation, respectively certification

7.1. Applicant profile, technical skills and competence

The new applicant is expected to provide a comprehensive presentation of its entity:

- Entity status such as, but not limited to: vendor, laboratory.

- When the member application decision has to be done at JHAS plenary, eligibility criterion for the application acceptance must be taken into account as follows:
    - NCCA – without restriction
    - CAB/CB authorized and notified bodies to issue EUCC certificates – without restriction
    - CAB/ITSEF authorized to evaluate, also known as ITSEF – without restriction
    - Vendors (IC, SW, card) submitting products (at least 1) to an EUCC certification at level high
        - High means PP with physical resistance AVA_VAN.3 - AVA_VAN.5, certified under EUCC scheme)
        - The ToE must claim SFR against physical attacks
    - Government bodies sponsored by NCCA (liaison)
    - Non-EUCC scheme owners issuing certificates endorsing EUCC evaluation results (e.g. payment schemes)
- Organization, regional origin, business profile, link to other company/schemes/University
- Related product and markets,
- Entity experience in the domain:
    - Product Security
    - Security certification/ used certification schemes…
    - Confidentiality management
- Entity representative for the JHAS (member expertise and experience, technical publications)
- Sponsorship from an existing JHAS member. For Observer, sponsorship shall be supported by at least one NCCA.

7.1.1. Objectives:

Assess the trustworthiness of the entity and the relevance to JHAS discussion. Avoid malicious members.

7.1.2. Metrics:

The elements provided by the applicant:

- Guaranties brought by the member to preserve information confidentiality (provided by the signed JHAS application forms),
  Note: A direct link to a university or a spin-off is a blocking point, as well as known representatives, instances or organizations of hacker groups. JHAS has no educational mission.
- Sufficient skills and experience for active contribution to state-of-the-art attacks. Examples below could be provided as evidence (not exhaustive):
    - the entity has more than one security expert that performs attacks in-house,
    - the entity has lab capabilities (that could be reviewed, if necessary, by CB's schemes already active in JHAS),
    - the entity works with several labs active in JHAS,
    - the entity is a laboratory, and it is compliant with Minimum Lab Requirements [MinLabReq].
- Sufficient interest in higher evaluation levels and CC/EMVCo methodologies,
  Examples below could be provided as evidence (not exhaustive):
    - the entity is currently running at least one on-going certification by a trusted laboratory which is an active JHAS member and on a scheme recognized at the higher level for the certification scheme,
    - additionally, the entity may also have certified products within the EUCC recognized schemes,
    - the entity is a developer who is a major market player in its domain, it is already involved in secure products development, and the security of its products is known by several JHAS members.
- Provide evidence of CC evaluation activity within EUCC scheme (at least started). CC evaluation shall target high level of resistance. Members shall provide evidence of interest and skills in evaluations targeting at least high level of resistance, and potentially also from medium to low resistance levels. CC evaluations shall be based on JHAS-related Technical Domains relevant PP (such as BSI-CC-PP-0084, BSI-CC-PP-0117, BSI-CC-PP-0099, ANSSI-CC-PP-2020/01, ANSSI-CC-PP-2018/04…),
- Provide technical proofs of their skills. A presentation of an attack or recent technical publication must be done at a JHAS meeting. Success criterion is: attack level not below current AM document,

- JHAS member sponsorship must be provided in an official letter from the supporting entity.

Additional requirements/metrics

- Conformance to "Minimum ITSEF Requirements" (optional, for laboratory applicant)

7.2. Motivation / Reciprocal benefit

Applicants have to declare how they intend to contribute to JHAS and for what purpose. They are expected to detail how they would use JHAS results in their context (own certification, scheme).

7.2.1. Objectives

- Ensure an active and valuable contribution to the JHAS,
- Check reciprocal benefit of applicant and JHAS,
- Check recognition of JHAS works,
- Show long term interest about high-level security evaluation approach,
- Discard applicants that would not or could not participate actively to the JHAS working group or that are interested by a short-term participation.

7.2.2. Metrics

The applicant has to provide commitment (reciprocal benefit letter) on its:

- Understanding and sharing of JHAS missions,
- Regular attendance to JHAS plenary meetings. Full participation is requested (100% of hybrid or physical) with a minimum participation of 80% to plenary hybrid or physical. Physical participation at plenary is strongly encouraged,
- Quality and quantity of contribution: in JHAS decision, approval of JHAS documentation release, participation to the JHAS subgroups (if committed),
- Positive behaviour within JHAS. If the following behaviour is observed, the JHAS organization may apply penalties that could lead to exclusion:
    - rude or aggressive attitude,
    - repeated infringement of the JHAS working rules,
    - disclosing JHAS internal documentation or discussion without authorization from the assembly,
    - Improper use of JHAS information in a nasty way towards another JHAS member,
    - using JHAS to promote a proprietary product or solution.
- Sharing and harmonization of attack techniques and rating
- Acceptance of trial period. Soft skills (reliability/trustworthiness, active participation) will be evaluated during the 1-year observation.
- Recognition (for any member):
    - Recognition of JHAS rules and assets (JHAS reference documentation) = right to discuss, decide in JHAS, modify them
    - No recognition of JHAS ToR or working rules = no membership acceptance
    - No recognition of JHAS assets = right to discuss in JHAS but no decision role

7.3. Member Approval process

There are 3 sequential steps in the new applicant process:

7.3.1. Step1: Interview with JHAS chairman

New applicant must take contact with JHAS chairman. Interviews are set up to explain the Terms of Reference to new applicant. JHAS chairman shall verify potential blocking points with EUCC ISAC JHAS ToR. At this level, each applicant must provide the JHAS subgroup application form and a reciprocal benefit letter to the JHAS Chairman.

Upon positive feedback of JHAS chairman, the candidate can be proposed to present its membership application in front of JHAS plenary meeting. A dedicated slot in the next JHAS agenda is defined. It is underlined that the applicant will be invited only for this sole purpose and cannot attend the rest of the JHAS plenary meeting.

Whatever the decision, JHAS chairman informs the JHAS audience about new application status. JHAS chairman may pre-check non-trivial cases with the ISAC Steering Committee.

7.3.2. Step2: Presentation to JHAS plenary

New JHAS applicants are invited to present their company profile, expertise and motivation (reciprocal benefits) in front of the whole plenary audience.

Applicants shall show their skills, experience in certification, interest in higher level evaluation and potential contributions. Technical presentation of attack capabilities and security experience is expected.

After the applicant presentation and without its presence, JHAS audience debriefs of each application file and concludes with an acceptance or refusal verdict.

7.3.3. Step3: Presentation to ISAC Steering Committee

Upon acceptance by JHAS audience, the JHAS chairman submits the complete file (application form, presentation material) to ISAC Steering Committee for final approval.

Upon ISAC Steering Committee acceptance, the applicant becomes a JHAS member with the status of MITS (Membership In Trial Status) and can be invited to the next plenary meetings.

At any stage and whatever the conclusion, the JHAS chairman cares for informing back the new applicant.

The JHAS may decide to grant a Membership In Trial Status according to the article 9.6 of the Articles of Association of the EUCC ISAC.

7.3.4. Trial period rules

If an applicant has passed and accepted the previously described conditions the applicant is JHAS Member In Trial Status (MITS). As per section 9.6 of [ISAC Bylaws], this can be applied to entities including, but not limited to, manufacturers, providers or end-users of ICT products.

- MITS shall take active part in discussions and working groups and have equal rights regarding input of topics, discussion of topics and collaboration in subgroups, and MITS can also lead subgroups,
- MITS have no voting rights,
- MITS have no election rights,
- MITS cannot be elected for the role of chair, vice chair and secretary,
- MITS have no account and access to the JHAS repository,
- The trial period lasts at least 9 meetings within a time frame of up to two years. If the 9 meetings in two years were not attended the membership is lost. The applicant losing the trial membership can re-apply after a further period of one year,
- Validation of this trial period is based on factual contributions, evidence of reciprocal behavior and regular attendance,
- The count begins with the next meeting after MITS status has been achieved,
- In the 1st JHAS plenary meeting after the trial period ends, JHAS members shall discuss and decide whether the MITS can become an acting member,
- For this discussion, all MITS participants must leave the room,
- If no consensus can be achieved the rules for anonymous voting apply.

8. Members obligations

It is expected that all members work actively towards the goals of JHAS. This can take various forms such as regularly participating in the meetings, taking on – and delivering – specific work packages, representing JHAS at conferences and other forums, etc.

It is discouraged to be merely an entry in the JHAS e-mail distribution list, and membership status may be under review by the JHAS subgroup should the latter be the case. Normal consensus rules apply here.

As defined by ToR, the confidentiality within the group is based on:

- Confidence and trustworthiness of JHAS member attendants,
- Provided by JHAS membership and identification of attendants appointed by each JHAS member,
- The application form reminds the confidentiality obligation to the member representatives,
- Commitment from each JHAS member to respect basic rules:
    - Information discussed in the meetings or communicated in the reports is considered confidential and treated as such,
    - The organisations and companies of the JHAS members can use information discussed in the meetings or communicated in the reports internally,
    - The information discussed in the meetings or communicated in the reports may not be used for commercial activities other than the intended usage: methodology for Common Criteria evaluations for smartcard developers and evaluators,
    - Handle accordingly topics related to cryptography, cryptographic analysis and high-end measurement equipment.
- Awareness to Wassenaar arrangement related impact (confidentiality of discussion for some cryptographic & high-end measurement equipment).

9. Exclusion

In case a JHAS member does not respect the JHAS working rules, the JHAS chairman has to warn the JHAS member about the infringement of the rules.

If normal behaviour does not resume, penalties based on JHAS group exclusion may be taken depending on the seriousness and the harm of the facts. The exclusion can be temporary (gradually 3 meetings/6 months then, 5 meetings/1 year) or permanent. Returning from temporary exclusion, JHAS members will be considered as MITS.

The decision should be taken by a JHAS vote and applied by the JHAS chairman.

Pursuant to the article 11.2 of the statutes of the EUCC ISAC, JHAS chairman will apply the JHAS group decision to exclude any Member, MITS or Observer, which does not fulfil the above obligation or does not conform to the statutes of the EUCC ISAC, after giving that Member be heard in its defence.

10. Meetings

JHAS plenary meetings are held several times a year with required attendance for each member. Plenary face-to-face attendance is preferred and at least, hybrid participation is required for each company. JHAS assembly decides the necessary number of sessions (typically every 2 months, at least 5 plenary sessions per year, at least 2 subgroup sessions per year) and length of the agenda (1 or 2 days). The scheduling shall be done at least 4 months before the meeting date to ease travel organization.

Face to Face meetings should be held at least 5 times per year.

JHAS expenses (plenary or subgroup meetings…) are sponsored by ISAC. Meetings can be punctually sponsored by one JHAS member or non-profit organizations such as Eurosmart.

11. Late Membership fee policy

The following policy applies where membership fees due by a member have not been received by EUCC ISAC within the timeframe aforementioned:

a) After 60 days of the due date set in the invoice, the Secretariat sends a reminder letter or email to the member that the payment is now 60 days past due and notifies the Board.

b) 45 days after the reminder letter or email (1) the Secretariat sends a letter or email that the membership rights and benefits will be temporarily suspended if payment is not received within 30 days and notifies the Board.
c) 30 days after the reminder letter or email (2) the membership rights and benefits are suspended. According to the bylaws, the Board may waive (or delay) the suspension based on individual case.

The Secretariat may use the services of a recovery fee company to collect unpaid membership fees, subject to approval from the Board.

12. Voting rules

JHAS formal decisions will be made by consensus. If total consensus cannot be achieved a decision can be accepted with a vote.

Where a decision has been put to a vote, the result of the vote will be announced at the next JHAS meeting. The decision will take account of votes received by email and votes from the meeting attendees. Formal decisions will be made for at least the following:

- Acceptance of new members,
- JHAS tasks,
- Release of JHAS outputs (including classification rules),
- Changes to JHAS ToR.

Formal decisions are accepted with a remote decision process. For each topic submitted to JHAS formal decision, this process is in 2 rounds:

- 1 round with potential feedback,
- 1 round for final acceptance.

As a pre-requisite, topics shall be prepared enough to avoid several iterations of rounds with potential feedback.

Each JHAS member must provide feedback on each proposed topic. Each round of the process is initiated and followed up by the JHAS chairman or any assigned backup. He/she provides the topic of approval, the related documentation and the deadline for answer.

The result of each vote is communicated to the JHAS audience by email 5 days after the deadline and the resulting decision can be executed consequently (approval or refusal).

In case of sending one topic for remote decision for the first time, it should go for remote decision by consensus in 2 rounds (as described above). In this case, silence is seen as 'Acceptance' after deadline.

In case the consensus is not reached (after the 2nd round), a vote has to be initiated. Voting should be applied only as last possible tool to come to a conclusion. The JHAS group should rather strive for consensus by open discussion before voting.

In general, it depends on the type of topic whether anonymous voting (voting sheets) or a simple and obvious hand-count voting is appropriate. If voting cannot be avoided the following rules apply:

1. The plenary shall be asked for the type of vote.
   1.1. All acting members shall provide opinion, physically or virtually present in the meeting, or at last before next plenary meeting. Opinion can express acceptance, refusal or abstention. If one member does not show up at those 2 plenary sessions, the voting process will be done anyway in order not to block JHAS activity,
   1.2. Each member organization with voting right (see section 2) has one vote,
   1.3. Decision can be accepted with a majority of 2/3 of votes received,
   1.4. If only one acting member requests anonymous voting then the voting shall be anonymous,
   1.5. In case of anonymous voting the chair must take care that a present party has only one vote even if a party appears with two (or more) representatives that day.
2. Liaison and MITS have no right to vote.

13. Alteration to the Terms of Reference

In order to validate any alteration to the Terms of Reference, the decision shall be taken by consensus by default or if no consensus can be reached, at least with 2/3 of total JHAS members with voting rights.

14. Output Materials

Documents generated by JHAS are owned by the EUCC ISAC and are made available to the members or public for non-commercial purposes.

Documents generated by the subgroups of JHAS shall be returned to the main group for final approval.

Classification of information and results is subject of JHAS. In case of differences the voting rules apply.

JHAS provides its classification, and related protection means as recommendations to the ISAC Steering Committee for any documentation usage. It is expected that those recommendations shall be passed any other users beyond.

The JHAS and subgroup discussion contents, results and meeting notes are considered to be JHAS-confidential and must be carefully controlled by each JHAS member.

The members can use information discussed in the meetings or communicated in the documents in their respective organization.

Nothing in this document shall cause prejudice to national laws and regulations of the Member States, including regarding public access to documents, government access to documents, the protection of personal data or the protection of classified information.

The finalized JHAS document output is accepted or returned for rework to JHAS by the ISAC Steering Committee.

The ISAC Steering Committee is interfacing with ECCG (EsEm) organization for the publication of JHAS final output documents.

The communication of JHAS information shall be managed by any member according to Transfer Light Protocol (TLP). The TLP levels are defined as follows:

TLP LEVEL	DISTRIBUTION RULE	PROTECTION MEANS
WHITE	Public information	No encryption
GREEN	Shared within the broader EUCC ISAC Community (ISCI…), ECCG, GP (tbc) and other interested stakeholders. Not public but no specific restriction in distribution within these defined communities.	No encryption, not distributed through public channel.
AMBER	Restricted JHAS audience and, upon need, accepted third parties (ISAC Steering Committee, ISCI, EsEm, ECCG), only.	Encryption when out of JHAS and respective member repositories
RED	Restricted strictly to JHAS members (no specific restriction inside each member company).	Encryption when out of JHAS and respective member repositories

14.1. JHAS documentation output (main documents):

The JHAS assets are defined over three main categories:

ASSETS	CLASSIFICATION LEVEL/TLP	CONTENT SUBJECT TO CLASSIFICATION
[AAP] DOCUMENT	Public / TLP WHITE	None, already published
[AM] DOCUMENT	Restricted (JHAS audience) / TLP AMBER (JHAS audience, ISAC Steering Committee, European Commission, EsEm)	• Added-value of this doc for its completeness • Detailed attack path scenario: no specific lab know-how but educational value for newcomers • Case of some specific attacks taken as examples (ROM reverse…) • Section 3: HW & SW counter measure list • …
CONTRIBUTION TO ISCI [MINLABREQ] DOCUMENT	Public / TLP WHITE	• Definition of minimum capabilities (include the knowledge and the skills of their evaluators and the necessary equipment to conduct the aforementioned attacks) to perform the evaluation of an Integrated Circuit (IC), a crypto library, a Platform and Integrated Circuit Card (ICC) with sufficient guarantees • …

All output materials in DRAFT or in Approval phase shall be considered as TLP AMBER.

14.2. JHAS Support Documents

The JHAS produces documents from results of their internal working groups. These possibly separated documents can provide information related to certifications and evaluations and can be used in combination with attack method and attack potential documents.

14.3. Internal JHAS exchanges or working units (non-exhaustive list)

ASSETS	CLASSIFICATION LEVEL / TLP
JHAS MEETING TECHNICAL PRESENTATIONS	Restricted (JHAS audience) TLP RED (by default)
JHAS SUBGROUP STATUS (NON TECHNICAL)	TLP GREEN (by default)
JHAS TECHNICAL DOCUMENTATION EXTRACTS/DRAFT PROPOSAL	Depend on the JHAS output material it is related to. e.g : TLP AMBER if related to AM TLP WHITE if related to AAP
COMPANY PRESENTATION TO JHAS	Restricted (JHAS audience) TLP RED (by default)
JHAS MEETING DISCUSSION	Restricted (JHAS audience) TLP RED (by default)
JHAS MINUTES	Restricted (JHAS audience) TLP RED (by default)
JHAS ARCHIVE SITE	Restricted (JHAS audience) TLP RED (by default))
JHAS TOR	Public TLP WHITE
JHAS ACTIVITY STATUS/REPORTING TO ISAC STEERING COMMITTEE OR ESEM	Restricted to relevant audience TLP GREEN

14.4. Data protection. Handling of confidentiality

Any JHAS classified information (“Restricted” or similar) shall be exchanged in an encrypted way or through JHAS protected repository.

15. Chairman of JHAS

The Chairpersons oversee steering meetings and subgroup activities. The Chairman is responsible for chairing meetings and ensuring minutes of each meeting are recorded and distributed. The Chairman proposes the agenda for each meeting.

JHAS assembly is led and organized by a chair, a vice-chair and a secretary, that are elected each year by the JHAS voting members.

The chair is accountable to gather and achieve the JHAS group objectives. These objectives can be self-assigned, or assigned to JHAS by ISAC Steering Committee, ECCG (EsEm). The chair is also accountable for JHAS outputs (in

terms of operations/timing, not in terms of technical content[1]), JHAS way of working (checking member participation, creation of subgroup, moderation of JHAS plenary meeting, the respect of Terms of Reference ...) and any external communication with all stakeholders (ISAC steering, ECCG (EsEm), Eurosmart...).

The vice-chair is the chair deputy, assisting the chair in its tasks and in particular the consolidation and review of JHAS outputs.

The secretary is in charge of JHAS plenary minutes of meetings.

The chairman seats at the Steering Committee of the EUCC ISAC.

15.1. Election procedure:

- The chair, vice-chair and secretary roles are renewed annually by JHAS plenary. If several candidates are applying for role, a voting process shall be organized by the chairman.
- The election of those roles shall be anonymous.
- Each acting member of JHAS must provide a vote and should be present at the voting date to keep the anonymity status of the vote.
- The election result is valid if at least 75% of the listed members are present.
    - If there are less members present, no election can take place and the election is automatic part of the agenda of the next meeting.
- The chair must take care that each party has only one vote.
    - The number of vote sheets must match with present parties.
    - A present party has only one vote even if a party is represented by two (or more) representatives that day.
    - Liaison and MITS have no right to vote.

16. Subgroups of JHAS

Subgroups can be created to work on specific topics which cannot be managed during ordinary meeting of JHAS. Subgroups are subject to prior validation of the Group members pursuant to article 8 and shall be validated by the Steering Committee of the EUCC ISAC. The competence of the subgroup shall be limited to the scope of JHAS to avoid any prejudice to the work of the other EUCC ISAC technical groups.

JHAS defines the subgroups' roadmap. Subgroups report at every plenary session.

A subgroup chairman drives and is accountable for the work of the subgroup. He/She shall be appointed by JHAS pursuant to article 8. There is no specific limit in time for such role.

17. Intellectual Property Rights (IPR) policy

JHAS' activities are conducted in strict compliance with the IPR policy of the EUCC ISAC.

Each Member shall use its reasonable endeavours to timely inform the JHAS of that Member's Essential IPR that the Member is aware of and believes to be likely to fully or partially cover elements of Specifications that are being developed by a Member of JHAS prior to such Specifications being submitted to a voting procedure. In particular, each Member submitting a technical proposal for development of a Specification shall timely and on a bona fide basis draw the attention of JHAS to the IPR of that Member which might be Essential if the proposal is adopted.

[1] Technical content accountability is conferred by the expertise of the members.

18. Antitrust Compliance

The EUCC ISAC and JHAS's activities are conducted in strict compliance with applicable antitrust laws. JHAS members shall respect the Antitrust Compliance Guidelines.

The JHAS activities must not lead to a restriction of competition between members, nor must meetings of members organized or supported by JHAS be used by members to discuss or coordinate market behavior resulting in a restriction of competition. More generally, the platform offered by JHAS to its members must not be misused for activities prohibited by antitrust laws.

A reminder of general rules including antitrust will be done at each meeting start and in the minutes of meeting.

19. Confidentiality and Information Protection

Members of JHAS shall endorse the confidentiality clause as guarantee to preserve sensitive information developed and shared in this organization.

Members of JHAS acknowledge that participation to its activities may involve access to confidential information. Members shall agree to treat all such information with the same degree of care as they would their own confidential information, but in any case, no less than reasonable care. Confidential information shall not be disclosed to any third party except as expressly permitted by the JHAS confidentiality provisions.

Members shall ensure that their representatives respect these confidentiality obligations. Information shared within JHAS shall be presumed non-confidential unless designated otherwise in writing and accepted as such by the Chair.

Any confidential information disclosed remains the property of the disclosing party and must not be copied, used, or disseminated beyond the agreed scope.

These obligations shall survive the termination of a member's participation for a period of **15 years** from the date of disclosure, unless explicitly released in writing by the disclosing party.

20. Complaint Procedure

This section details procedures for complaints and appeals that concern the actions and decisions of JHAS and its subgroups related to the release of a specification, a technical document or a publication.

20.1. Conditions

Complaints may only be submitted by persons or organizations that are directly, materially, or adversely affected by the activities related to the complaint.

Complaints filed with the EUCC ISAC must:

- be introduced within 30 days after the EUCC ISAC has officially communicated a specification or a technical document or a publication;
- be accompanied by documentation providing all relevant details of the complaint;
- include any supporting evidence or documentation, such as statements and explanations related to the issue; and
- not be repeated unless a minimum of 6 weeks has passed.
- pay attention on that the complainant (person or organization) shall not derive any rights or presume the validity of the claim based on the fact that the EUCC ISAC is investigating the complaint.

20.2. Process

The complaint shall be submitted by e-mail sent to the JHAS Secretariat (chair, vice-chair and secretary email).

The complaint, along with the personal and/or company information of the complainant (full name, address, and other contact details), shall include the complainant's personal opinion about the assessment and/or conclusion, the reasons for disapproval with the decision reached, as well as the settlement being sought.

The Secretariat will acknowledge receipt of the complaint, assign a complaint reference number (CPYYYYMMnn) the Board appoints the person responsible for investigating and assessing the complaint, The selection is based upon competence, independence and impartiality. Then, the Secretariat notifies the person of the complaint.

The person responsible will investigate and assess the complaint, considering advice from the technical experts, where necessary, to determine the facts of the case and an appropriate response or resolution.

This investigation will be completed within 30 days of receipt of the complaint. If more time is needed, the complainant will be notified of progress and estimated timeline.

Proposed resolutions will be reviewed and ratified by the Steering Committee to determine a final decision prior to onward communication.

The Secretariat will communicate outcomes or proposed resolutions to the complainant.

If the complainant agrees with the outcome at this stage, then the complaint does not proceed to further stages and the complaint is closed.

If the complainant is not satisfied with the outcome, then he/she may submit an Appeal.

Records of complaints, investigations, and proposed resolutions will be provided to and maintained by the Secretariat.

21. Appeal Procedure

This procedure stipulates the way in which an appellant may appeal a decision of the EUCC ISAC with respect to a complaint.

21.1. Filing

Appeals may only be submitted by persons or organizations that are directly, materially, or adversely affected by the activities related to the initial complaint / appeal.

The appeal must be submitted within 14 days after the decision on the disputed complaint is communicated to the complainant.

The appeal shall be submitted by e-mail sent to the JHAS Secretariat (chair, vice-chair and secretary email).

21.2. Acceptance

The appellant can only submit an appeal after the Secretariat has communicated a final decision on the complaint.

If the appeal is submitted within the required timeline and by the appropriate person or organization and no prior appeal has been submitted, the appeal will be accepted by the EUCC ISAC, with no undue burden imposed on the appellant.

When an appeal has been accepted by the EUCC ISAC, the appeal is considered formal and will be dealt with according to this procedure.

21.3. Process

Upon acceptance of an appeal, the Secretariat will promptly acknowledge receipt and assign an appeal reference number (APYYYYMMnn). The Steering Committee selects the person responsible for investigating and assessing the appeal. The selection is based upon competence and independence/impartiality.

The person responsible for investigating and assessing appeals will be notified of the filed appeal.

The person responsible will investigate and assess the appeal, taking into account advice from the technical experts where necessary, to determine the facts of the case and an appropriate response or resolution. This investigation will be completed within 30 days of receipt of the appeal. If more time is needed, the appellant will be notified of progress and estimated timeline.

All appeals will be handled by the relevant parties promptly and in a fair, unbiased, and impartial manner.

Proposed resolutions will be reviewed and decided expeditiously by the Steering Committee prior to onward communication.

The Secretariat will communicate outcomes of final decision to the appellant, and the appeal is closed. Note that appeals may not be repeated or re-submitted.

Records of appeals, investigations, and proposed resolutions will be provided to and maintained by the Secretariat.

22. Reference documentation

[MinLabReq] Minimum ITSEF Lab Requirements

[AAP] Attack Potential for Smartcard and similar devices

[AM] Attack Method for Smartcard and similar devices

[ISAC Bylaws] ISAC Bylaws

23. Annexes

Annex A: IPR Policy of the EUCC ISAC

See the ISAC website for the latest update.

https://ccisac.eu/wp-content/uploads/2025/07/2024_11_25_EU-CC-ISAC-IPR-policy.pdf

Annex B: Antitrust guidelines

See the ISAC website for the latest update.

https://ccisac.eu/wp-content/uploads/2025/09/EUCCISAC_Antitrust-Compliance-Guidelines_.pdf

About us

The EU Common Criteria Information Sharing and Analysis Centre (EUCC ISAC) is an international non-profit association dedicated to fostering collaboration, harmonization, and excellence in cybersecurity certification.

The EUCC ISAC acts as a central hub for collaboration between public and private stakeholders, ensuring the effective and consistent implementation of the EU Common Criteria (EUCC) certification scheme. It provides essential input to key entities—including the ECCG subgroup for EUCC maintenance (EsEm), the European Commission, ENISA, and Member States—to support the ongoing development and maintenance of the EUCC scheme. We aim to maintain state-of-the-art practices by providing technical interpretations, methodologies, attack quotations, and an up-to-date attack catalogue.

EUCC ISAC | Avenue de Broqueville, 66 - 1200 Brussels – Belgium | contact@ccisac.eu

EUCC ISAC