Documentation available under confidentiality

The three levels of documentation, what is provided in an evaluation session and the procedure: request, confidentiality agreement, supervised session without copies and record in the log.

Three levels of documentation

Product documentation is classified into three levels. This classification is public: it classifies without revealing.

Public documentation

May circulate without additional procedure. It comprises the product identity and sheet, architecture at design level, the algorithm inventory with its scheme status, the existence of each protection mechanism, the headline data of the evidence — identifier, date, methodology and results — and the **public** verification keys. This library forms part of that level.

Confidential documentation, under evaluation

Shown or provided to the accredited evaluator during an evaluation, under a confidentiality agreement, and does not circulate outside it. It comprises the detail whose open disclosure would degrade a specific protection or expose the operating instance.

Material that, by design, does not exist in documents

There is material that cannot be delivered even under a confidentiality agreement, **because the system is built so that it does not exist outside its place**: custody shares and protected keys, unopened envelopes, printed ceremony codes and the private keys of each custodian's authenticators. Shares are never stored — only metadata and fingerprint are retained —, the reconstructed key lives only during the ceremony, printed codes reside in the system only as one-way fingerprints, and the private key of an access key never leaves its holder's authenticator. No agreement can promise to deliver what the system does not keep.

What is provided in an evaluation session

Under confidentiality, and only by its generic title, the following may be provided:

- The complete design of the Key Custody Protocol.
- The full validation and security audit reports.
- The operational parameters for ceremony and custody oversight.
- The source code, examined in session or through contractual deposit in third-party escrow.
- The laboratory detail of point-in-time recovery verification.

Provision procedure

1. **Request.** The institution or the evaluator requests access, identifying the material by its title.
2. **Confidentiality agreement.** Access requires the confidentiality agreement signed by the accredited evaluator who will examine the material.
3. **Supervised session.** Provision takes place in an evaluation session, in person or supervised remote, with read access to the document or the system, **without copies, without download and without photography**, except with recorded written authorisation.
4. **Record.** Each provision is entered in the **dossier log**: what material, to whom, in what session, with what scope and with what authorisation. The log demonstrates the traceability of provision without revealing the content provided.
5. **Closure.** On closing the evaluation, access is revoked and the log is archived with the dossier. An evaluator's own report may cite the material provided by its title, without reproducing its content.