

Digital fingerprints

How OPEREX shows that a signed permit, an approved risk assessment or a recorded action has been changed after the fact — and where the limits are.

CONTENTS

1. What is a digital fingerprint?
2. Lock, chain, outside witness — the three layers
3. The permit to work: chain and paper
4. Where it works — and what we do not claim

IN SHORT

- Every signature on permits and maintenance work orders — and every risk assessment at approval — gets a digital fingerprint: the smallest later change can be detected.
- The signatures of a permit form a chain — editing, deleting or inserting a step breaks it, and the check says where.
- Every day, the fingerprints of the previous day's audit trail, permit signatures and approvals are stored off-server, per organisation and chained.
- The QR code on a printed permit points to the organisation's own address: a phone opens the live status without signing in — whether work may proceed on it now, and whether the paper is the latest version.

What is a digital fingerprint?

After an accident or an inspection, the first question is: is what we see now what was signed back then? A digital fingerprint gives a machine-checkable answer.

A digital fingerprint (technically: a cryptographic hash) is a short, unique string computed from the data by a standard procedure. OPEREX uses the internationally standardised SHA-256: data of any size yields a fingerprint of 64 characters.

When a record is signed or approved, the system computes and stores its fingerprint. A later check recomputes it from today's data with the same procedure: if the two match, the data has not changed since; if they differ, the change has been detected.



A single different character (18:00 instead of 16:00) gives a completely different fingerprint. The two fingerprints in this figure were computed from the text above with SHA-256 when this sheet was generated.

Same data, same fingerprint

The same data yields the same fingerprint on every machine, every time — so the check can be repeated at any point.

Any change, a new fingerprint

Changing a single digit, accent or space gives a completely different fingerprint: a change cannot hide.

Cannot be reversed

The data cannot be recovered from the fingerprint, and in practice no other content can be made with the same fingerprint.

No secret involved

Computing it needs no key: anyone can recompute it. That makes it a check — not just the system's claim.

Lock, chain, outside witness

A fingerprint detects a change but does not prevent it. So three layers work together: the lock prevents it, the chain detects it, and the outside witness records it beyond the server.

1 Lock — append-only records

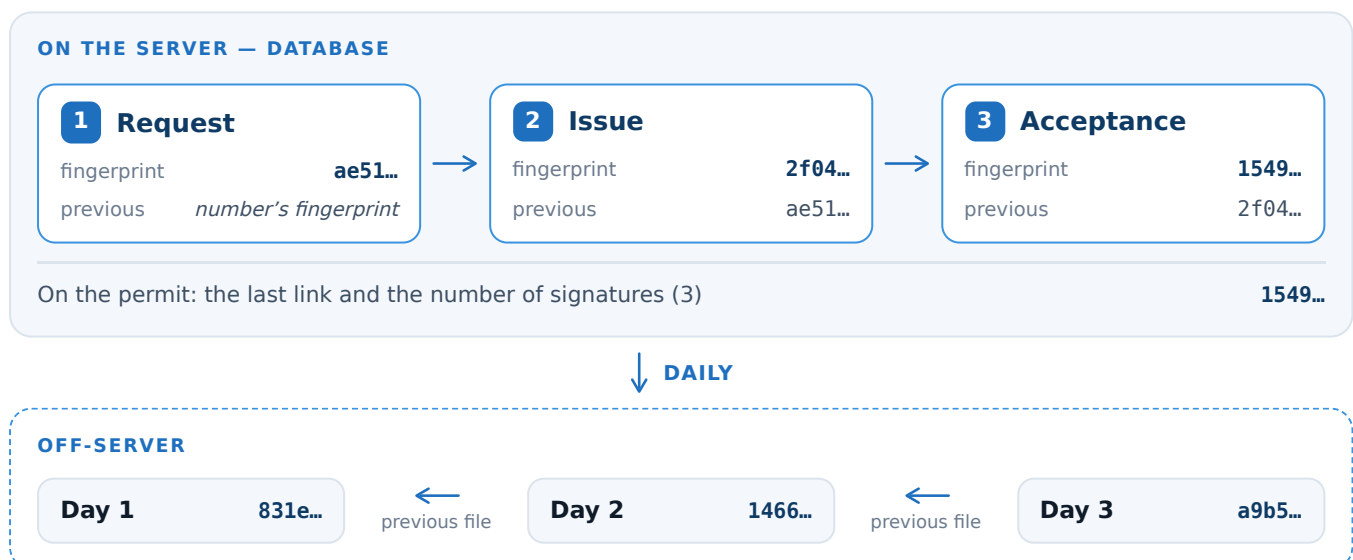
The database refuses every role permission to modify or delete the audit trail and the signatures — including the owner account we operate with. Lawful, contractual deletion is an explicit, logged exception.

2 Chain — every step points to the previous one

Each permit signature stores the fingerprint of the previous signature — a new signature's fingerprint also covers that link, the sequence number and the signing time — and the permit itself holds the last link and the number of signatures. Editing, deleting or inserting a step breaks the chain — and the check names the signature and the reason.

3 Outside witness — a daily fingerprint off-server

Every day, a per-organisation fingerprint of the previous day's audit trail, permit signatures and approved risk assessments is stored off-server, each daily file pointing to the previous one. A later change to an already recorded day — even one made with owner rights inside the database — can thus be detected.



The chain lives on the server, the daily fingerprint off-server. Only fingerprints, counts and organisation identifiers leave the server — no personal data. (The shortened fingerprints in the figure are illustrative.)

The permit to work: every step is a signature

The permit is the most scrutinised document — after an accident it is the first thing to be pulled. Here all three layers work together, and the paper can be checked too.

- After the first signature — the request — the content of the permit cannot change. Every further step (issue, countersignature, acceptance, suspension, extension, closure...) is another signature in the chain.
- Each signature's fingerprint covers the full content of the permit and the step itself: who did what, in which role, with which validity window.
- On the permit page both the server and the browser check the chain, stating their results separately. The evidence check reviews the permits and assessments of the accessible sites in one run; the report downloads as CSV and PDF, and the run itself is audited.
- A risk assessment is fingerprinted at approval (answers, prescription, the job safety analysis steps); from then on the database refuses any change to the approved content, and its own paper carries a QR code too.



- | | |
|--|---|
|  Work may proceed
The permit is active, within its validity window, and its chain is intact: work may proceed now. |  Do not work
The page says why: not issued yet, suspended, expired, closed... It never says yes to a broken chain. |
|  Outdated paper
The paper was printed from an earlier version — the page shows how many changes happened since. Today's state is what counts. |  Unknown
The paper fits none of the versions, or the code is unknown: do not start work, contact the issuer. |

There is no visible fingerprint string on the paper: the machine evidence is a single QR code, printed only once there is something to check. The QR is a link to the organisation's own address — a random 96-bit code (not the permit number) plus the start of the chain's last fingerprint at printing. A phone opens it: the verdict appears without signing in and without personal data; a signed-in colleague can also open the permit in the system. Older papers with a text QR can still be checked on the paper check page. The QR code in the figure is real, but it decodes to an example organisation's link — no permit belongs to it.

Where the fingerprint works

The evidence fingerprints share one common implementation, with the same rule everywhere. Where a hash only measures copy integrity, we say so.

AREA	WHAT THE FINGERPRINT RECORDS	WHERE IT CAN BE CHECKED
Permit to work	every signature: the permit content and the step, chained	the permit page · the paper's QR (live status) · evidence and paper check · daily off-server fingerprint
Risk assessment	the approved content, at the moment of approval	the assessment page · evidence and paper check · daily off-server fingerprint
Maintenance work order	the handover, test and acceptance signatures, chained	the work order page
Audit trail — every module	every recorded action of the day per organisation, the shift log's too	daily off-server fingerprint — comparable with the live database to the day and organisation
Exit and deletion	every exported file, the file inventory and the deletion certificate	by the recipient, on their own machine (SHA-256 per file)
Backup	the backup uploaded off-server	integrity check: is the copy intact — not tamper protection

What we do NOT claim

- No machine authenticates the text on the paper. The QR says what the permit's current state is and which version the sheet was printed from; whether the paper says the same is compared by a person against the title, location and status on the live page — a genuine QR code can be copied onto a forged sheet.
- The live status is shown without signing in, but only with network coverage (without it, ask the issuer). The per-signature chain check, the evidence report and checking old text QRs require signing in with view rights.
- The daily off-server fingerprint is made the next day — until then, the day's data is protected by the lock and the chain.
- The outside witness detects a later change made inside the database; protection against a full takeover of the server does not come from it.
- A signature is a recorded step by a user identified in the system (signed in, with two-step verification depending on the organisation's settings) — not a qualified electronic signature.

We are happy to demonstrate the checks on a live system — including when preparing for an audit or a procurement questionnaire.