

ISO 11770-8 kit specimen

Password-based key derivation: the register, the evidence and the plan

ISO/IEC FDIS 11770-8, edition 1, 22 pages, ISO/IEC JTC 1/SC 27. Stage 50.20 on 2026-09-21. Expected publication 16 February 2027, an estimate, not an ISO date.

SPECIMEN. Three rows only. This is not the paid kit.

Not legal advice; does not certify. The ISO text is not reproduced. Requirements are stated in our own words and every field carries a source pointer. Where the public record is silent the text says so.

How to read this file

- Public fact: stated plainly and cited to the clause or the ISO record. The public preview carries clauses 1 to 3 only.
- Labelled reading: our interpretation of what a clause or annex implies for a build, an evidence file or a test. It is not the standard wording.
- Named gap: the normative clauses 4 to 7 and annexes A to D are behind the paywall. The row says so and does not invent a requirement.
- Every evidence row names the artefact and why a reviewer asks for it. Every unit ends with a test you can run this week.

The register

Ref	Citation	Title	Kind	Public status	Binding party	Requirement (our words)	Evidence to keep	Test	Source	Owner	Due	Status
U-01	Clause 1	Scope	normative clause	The scope is in the public preview and is quoted in our own words below.	The organisation that derives a cryptographic key from a human-memorised password, and anyone asked to show that its derivation follows this part.	This part covers one narrow family: functions that turn a human-memorised password into a cryptographic key. It applies where a key has to be produced from a password.	A one-page scope memo that names each password-derived key and the algorithm or store it protects; A list of password verification paths that are excluded, with the reason; The data flow from password entry to derived key to protected asset	Name one place where a password-derived value is used as a key for another algorithm, and one place where a password is only verified. If the two cannot be separated, the inventory is not ready.	https://www.iso.org/standard/87940.html			Open
U-02	Clause 2	Normative references	normative clause	The reference list is in the public preview. The editions and the dated or undated treatment are shown below.	The implementer and the assessor, because the references decide which vocabulary and which prior mechanisms are indispensable.	Three documents are indispensable: ISO/IEC 11770-1:2010, ISO/IEC 11770-4:2017, and ISO/IEC 20009-4. The first two are dated, so only those editions apply. The third is undated, so its latest edition, including amendments, applies.	A reference register with the three citations, their editions and the date checked; A note on the undated 20009-4 reference and the edition in force when the assessment was done; The national adoption preface if one applies in your market	Open the conformity statement and check that each of the three references is named with its edition or marked as the latest edition.	https://www.iso.org/standard/87940.html			Open

Ref	Citation	Title	Kind	Public status	Binding party	Requirement (our words)	Evidence to keep	Test	Source	Owner	Due	Status
U-03	Clause 3	Terms and definitions	normative clause	All five entries and the inherited definitions are in the public preview. They are summarised, not reproduced.	The organisation that derives a cryptographic key from a human-memorised password, and anyone asked to show that its derivation follows this part.	Clause 3 adopts the vocabulary of ISO/IEC 11770-1:2010 and adds five terms of its own: hash-function, key derivation function (KDF), weak secret, password, and salt.	A project glossary mapped to the five defined terms and to the inherited 11770-1 vocabulary; A review note that distinguishes the salt from any secret key or pepper; The password entropy assumption stated in the design record	Ask three engineers to define salt and pepper without notes. If the answers disagree, the glossary is not in use.	https://www.iso.org/standard/87940.html			Open

Evidence list

One row per evidence artefact. The paid XLSX carries the same rows with an owner and a status column.

Ref	Unit	Citation	Title	Artefact	Why it is asked for	Source	Owner	Status
E-01	U-01	Clause 1	Scope	A one-page scope memo that names each password-derived key and the algorithm or store it protects	Shows the boundary was decided from the use of the output, not from the library in use.	https://www.iso.org/standard/87940.html		Open
E-02	U-01	Clause 1	Scope	A list of password verification paths that are excluded, with the reason	Lets an assessor see that the exclusion was deliberate and not an omission.	https://www.iso.org/standard/87940.html		Open
E-03	U-01	Clause 1	Scope	The data flow from password entry to derived key to protected asset	Proves the key exists and is used as a key, which is what brings the work into scope.	https://www.iso.org/standard/87940.html		Open
E-04	U-02	Clause 2	Normative references	A reference register with the three citations, their editions and the date checked	The starting point for any review of whether the reading is current.	https://www.iso.org/standard/87940.html		Open