e-QR Operator Certification Criteria v0.1

Criteria and evidence for certification as an e-QR operator

Document name	e-QR Operator Certification Criteria
Version	v0.1
Date	2026-11-17
Published by	e-QR Payment Standard MTÜ, 17 November 2026
Applies to	Applicants for certification and certified e-QR operators
Related documents	e-QR Scheme Rules v0.1; e-QR Technical Specification v0.1; Signed-URL Carrier Profile v0.1
Owner	e-QR Payment Standard MTÜ, registry code 80666291
Published at	eqrstandard.com

Version history

Version	Date	Change
v0.1	2026-11-17	First version

Each criterion is a yes/no check; the applicant supplies the evidence named. The Association decides within 30 days of a complete application.

A. Entity

#	Criterion	Evidence
A1	Legal person registered in the EU or EEA	Registry extract
A2	Named responsible person and an incident e-mail answered within two working days	Contact sheet
A3	Not subject to insolvency proceedings; no board member with a payment-fraud conviction	Written declaration

B. Technical conformance

Checked against the e-QR Technical Specification v0.1 (operator conformance, s. 12.1) and the Signed-URL Carrier Profile v0.1.

#	Criterion	Evidence
B1	Resolver at `POST https://<host>/1/m/<opid>` in proxy mode: JSON body, no redirects, `pi` validated, both-`mid`-and-`tok` rejected, error codes 400/404/410/429/500/503 as specified (Spec s. 9, 12.1)	The Association's conformance run against the operator host, using the Spec's test vectors (s. 13)
B2	Resolver success responses and printed codes are signed JWS ES256; resolver responses over the JCS form (Spec s. 9.4), codes per the Carrier Profile	Two sample codes and two resolver responses verified by the Association
B3	Signing keys are EC P-256, held in a hardware or cloud key-management service, private key not exportable; public keys supplied as JWK for the Operator Directory	KMS configuration screenshot or attestation; JWK
B4	A signature is produced only for a merchant record approved under operator controls independent of the registry data store (Spec s. 5.1, payout integrity): by a named person, or automatically when every check in section C has passed and the name and IBAN signed into the code are those in the merchant's own qualified-signed application. Each approval, with who or what gave it, is logged outside the merchant table; an IBAN change never reuses a MID	Procedure; audit-log extract
B5	Hosts served over TLS 1.2 or later; token secrets, if token mode is offered, never logged (Spec s. 11)	Live test
B6	Operator endpoints `/.well-known/eqr/jwks.json` and `/.well-known/eqr/revoked.json` served per the Carrier Profile; a revoked MID is on the list within one hour and the resolver stops answering for it within one working day	Live test
B7	Codes use only a payer host listed in the Directory's `payer_hosts`, never a host of the operator's own; the operator accepts scan counts from the payer page at `POST /1/log` (Carrier Profile s. 3, 7)	Two sample codes; live test
B8	Availability of resolver, key and revocation endpoints ≥ 99.5 % per calendar month, measured and kept for 12 months	Monitoring description

C. Merchant verification baseline

#	Criterion	Evidence
C1	Application is digitally signed (a qualified electronic signature: ID-card, Mobile-ID, Smart-ID or an eIDAS equivalent, made online or as a signed container uploaded by the applicant) by a person listed as a representative of the merchant in the business register, checked against the register before the code is issued	Procedure + one redacted example
C2	The IBAN passes format and check-digit validation (ISO 13616) and belongs to a SEPA country; the merchant confirms it in the signed application and is responsible for its correctness under the operator's terms	Procedure + screenshot of the confirmation step
C3	Sole proprietors (FIE): same as C1–C2 with the person's name. Private persons are not eligible (Rules s. 1.4)	Procedure
C4	Records of C1–C2 kept for the life of the registration plus 7 years (accounting law)	Retention statement

D. Terms, price, privacy

#	Criterion	Evidence
D1	Published merchant terms comply with Scheme Rules s. 4 (tier ceilings, no per-transaction fees, no payer fees, free portability)	Link
D2	Published privacy notice naming the operator as controller, covering merchants and the requests its registry receives	Link
D3	Current price published on the operator's site	Link
D4	The Mark used only as Scheme Rules s. 2.3 allows: the operator badge, the codes and the printed materials that carry them, and text; never in or next to the operator's own logo, or in its company, product or domain names	Site review

E. Ongoing

#	Criterion	Evidence
E1	Quarterly count of active merchants and revocations	E-mail
E2	Notification to the Association within 5 working days of any change in control, key compromise, or data breach affecting merchants	Procedure

How to apply

During the Association's bootstrap phase an application is accepted only for a country that has no certified operator (Scheme Rules s. 2.5). The certification fee in Scheme Rules Annex B is payable with the application.

E-mail info@eqrstandard.com with the evidence in the tables, as one PDF or a shared folder. The Association confirms within 5 working days whether the application is complete; the 30-day decision period runs from that confirmation.

Decision

Certification is granted when every criterion is met. The decision names the certificate number, the OPID issued, the registry address and the signing keys entered in the Operator Directory; the signed decision document is the certificate. Where an applicant is controlled by a board member, the conflict is stated in the decision text (Rules s. 6.4, Governance Note s. 3).