

QUANTUM CORE INSTITUTE

Identity and the Double Migration

Human and workload identity under QCI-QS1 Annex G domain 9

Field	Value
Document ID	QCI-QS1-C5
Version	V1.2 – September 23, 2026. Clause references are QCI requirement identifiers from QCI-QS1 v2.3 (September 23, 2026).
Applies to	QCI-5.2-02 (human and workload identity), Annex G domain 9; Practitioner Handbook chapter 10. Companions C2 and C4.
Status	Informative client handout. Nothing in this handout creates, modifies, or interprets a requirement. Where this handout and the standard differ, the standard governs.
Endorsement	None. Providers named are unranked. Quantum Core Institute does not endorse, resell, or certify any provider and has not independently tested any product.
License	Free. Attribution required. May not be modified and redistributed.
Publisher	Quantum Core Institute Inc.

1 Read this first

Identity is the domain where most organizations are least able to fix things themselves and most likely to do the work twice. The signing algorithm behind SAML assertions, OIDC tokens and passkeys lives inside a vendor's federation product, and no identity provider has shipped post-quantum federation signing as a default. At the same time, many organizations are running identity modernization programmes (passkeys, new IAM platforms, credential re-issuance) that will issue credentials on classical algorithms and then have to issue them again.

QCI-5.2-02 separates human identity from workload identity in the QASI because the two change through different products on different timelines, and because workload identity is where AI agents authenticate. This handout covers both and the seam between the identity programme and the PQC programme.

COMMON MISTAKE

The double migration. Institutions running identity modernization separately from PQC planning are scheduled to issue the same credentials twice and reconcile the inventories never. The cheapest available decision is one shared inventory, one re-issuance plan, and one named owner for the seam between the programmes, made before the identity programme ships.

2 Where the cryptography sits

Function	Cryptography today	Quantum exposure	Who controls the change
Federation signing (SAML, OIDC, JWT)	RSA-2048 or ECDSA P-256 signing keys at the identity provider	Assertion and token forgery once the adversary can forge; no HNDL exposure	Identity provider vendor
Passkeys and FIDO2	ECDSA P-256 (ES256) credentials on authenticators; attestation certificates	Credential forgery; attestation chain forgery	FIDO Alliance, browser and authenticator vendors
Smart cards and PIV	RSA and ECC key pairs on the card; certificate chains to an issuing CA	Same as PKI (domain 5), with card replacement cycles of 3 to 5 years	Card manufacturers, issuing CA, PIV standards
Workload identity (service accounts, SPIFFE, mTLS)	X.509 certificates on ECDSA or RSA; short-lived tokens	Certificate forgery; agent impersonation	Platform team, CA, identity broker
Directory and Kerberos	Symmetric (AES) tickets; PKINIT on RSA or ECC	PKINIT and certificate logon only; ticket encryption survives	Directory vendor

3 Providers and their published position

Provider	Published position, as of the cover date	What to ask
Microsoft	PQC APIs generally available in Windows Server 2025, Windows 11 and .NET 10; ML-DSA in AD CS from May 2026; Quantum Safe Program targets critical services by 2029 and Entra and Microsoft 365 by 2033	The date for ML-DSA signing of Entra tokens and SAML assertions
Okta	Targeting 2026 to 2027 for initial PQC support, with administrative controls to move tenants to PQC-ready defaults	Which functions ship first and whether hybrid signing is offered
Ping Identity	Evaluating NIST PQC integration; publishing migration playbooks	A dated roadmap; whether federation signing keys can be rotated to ML-DSA in place
FIDO Alliance	PQC Study Group scoping post-quantum extensions to WebAuthn; initial browser and authenticator support expected late 2027 to 2028	Nothing to ask yet; record the wait under QCI-T4 with the specification as the revisit condition
Yubico	ML-KEM and ML-DSA prototypes on security keys; not product-ready; new hardware required	Firmware upgrade path for keys bought in 2026 to 2027, or plan replacement in 2027 to 2030
IDEMIA	First complete PIV application running on a smart card with post-quantum cryptography, demonstrated June 2026	Product availability and certification dates
Thales SafeNet IDPrime PIV	Current cards support RSA and ECC only per the product brief	The PQC applet roadmap
SPIFFE/SPIRE, HashiCorp Vault, cloud IAM	Workload identity that follows the CA and TLS library underneath; PQC-capable identity on SPIRE being built by Entrust and others	Whether the issuing CA can issue ML-DSA workload certificates and the clients can verify them

4 The seam: identity programme meets PQC programme

Most organizations have an identity programme in flight. The seam between it and the PQC programme has three questions, and the answer to each is a decision record under QCI-T4.

Question	If the answer is no	Decision to record
Are the credentials the identity programme is about to issue on an algorithm that will need replacing before their natural expiry?	Proceed; note the expiry in the QASI	None needed

Question	If the answer is no	Decision to record
Can those credentials be re-issued on a post-quantum scheme without a second enrolment event for the user or the workload?	The programme will run twice	Delay issuance until the vendor ships, or accept the double issuance with a dated re-issuance plan and an owner
Is there one inventory of credentials that both programmes read?	The two inventories will never reconcile	Merge into the QASI now; name the owner of the seam

WHAT THE ASSESSOR WILL ASK

Show me the QASI row for the identity provider, with human and workload identity separated, and show me who owns the seam between the passkey rollout and the PQC roadmap. The Handbook's second worked example, hard-coded RSA-2048 in federation config with 47 service certificates of unclear ownership, is what this row usually looks like on the first pass.

5 What to do now

1. Split identity dependencies in the QASI into human and workload, per QCI-5.2-02, and name an owner for each. Workload identity is where AI agents will authenticate; give it its own owner.
2. Inventory federation signing keys, their algorithm, and whether the algorithm is configurable. Hard-coded is a rigid-component exposure flag under QCI-5.3-01.
3. Send the pack to the identity provider, the authenticator vendor and the card issuer. Score the responses; a provider that cannot date ML-DSA signing is an exception with a contractual milestone at the next renewal.
4. Record the passkey wait under QCI-T4 with the FIDO specification as the revisit condition, and require a confirmed firmware upgrade path for any hardware token bought in 2026 to 2027.
5. Move workload identity first where the CA and the TLS library allow it; it is inside the organization's control and it is the identity path AI agents use.
6. Name the seam owner, merge the credential inventories, and decide whether the identity programme ships before or after the vendor does.

Sources

- [Microsoft PQC APIs GA](#) · [Microsoft AD CS ML-DSA](#) · [Microsoft Quantum Safe Program timeline](#)
- [Okta on post-quantum identity](#) · [Ping Identity on quantum](#)
- [FIDO and post-quantum passkeys](#) · [Yubico on PQC](#) · [IDEMIA PQC PIV](#) · [Thales IDPrime PIV](#)
- QCI-QS1 v2.3 (September 23, 2026); Practitioner Handbook chapter 10; QCI-M1; QCI-T4