

ENCIPHER SYSTEMS

PQC Readiness Pack

Sample Sequence

A fictional unclassified listing for one system boundary, split into an external edge and an internal operations set. Not a customer file.

Sample number	PQC-SAMPLE-001
Version	Sample 0.2
Date	25 September 2026
Preparer	Encipher Systems
Cover hash	bbf21510d3b05bbd0e6a806d2442fcb64281d5c2dd859cb0912aec86a9f9bbca

Boundary. One fictional system. Unclassified. No high-value-asset flag. No key material accepted.

Portable. A published path exists. The increment is Confirm.

Rewrite. The row has to move. The increment is Move First or Later.

Blocked. No published path. The increment is Market Research.

Refused is not a class. That row was not read.

The sequence does not name a product. It is not an authorization and not a compliance certification.

Cryptographic Bill Of Materials

Input. Eighteen readable rows, plus one row that was not read.

Row	Use	Algorithm	Size
TLS-001	External HTTPS	RSA	2048
GRP-038	38 endpoints, one build	RSA	2048
CERT-014	Public certificate	RSA	2048
VPN-007	Site tunnel	ECDH	P-256
SSH-011	Jump-host signature	RSA	Host key
MAIL-004	Mail gateway	RSA	2048
ADM-009	Admin portal certificate	RSA	2048
VPN-012	Remote access	ECDH	P-256
TLS-002	Internal mTLS	ML-KEM hybrid	1024
KEM-003	Application library	ML-KEM	FIPS 203
SIGN-002	Firmware signing	LMS / XMSS	Stateful
LIB-021	12 internal applications	RSA	2048
SIGN-006	Code signing	RSA	2048
CTL-015	Building controller	RSA	End of support
DB-018	Database TLS	RSA	2048
BKP-002	Backup transport	RSA	2048
MON-011	Monitoring agent	ML-KEM	FIPS 203
SSH-022	Internal bastion	RSA	Host key
HSM-001	Not read	Not recorded	Private key material

HSM-001 is listed only to show the row arrived. The algorithm was not recorded.

Sequence

Output. Class and the funding increment.

Row	Class	Increment	Action
External edge			
TLS-001	Rewrite	Move First FY27 Q2	Replace RSA key establishment.
GRP-038	Rewrite	Move First FY27 Q2	One action for 38 endpoints on one library build.
CERT-014	Rewrite	Later FY28	Reissue with the external endpoint.
VPN-007	Rewrite	Move First FY27 Q2	Hybrid key establishment on the next refresh.
SSH-011	Rewrite	Later FY28	Rotate the host key.
MAIL-004	Rewrite	Move First FY27 Q2	Replace RSA on the mail gateway.
ADM-009	Rewrite	Later FY28	Reissue the admin certificate.
VPN-012	Rewrite	Move First FY27 Q2	Hybrid key establishment for remote access.
Internal operations			
TLS-002	Portable	Confirm	Confirm the hybrid setting.
KEM-003	Portable	Confirm	Confirm the published build.
SIGN-002	Portable	Confirm	Keep. State stays with the owner.
LIB-021	Rewrite	Later FY28	One action for 12 internal applications.
SIGN-006	Rewrite	Later FY28	Reissue the code-signing certificate.
CTL-015	Blocked	Market Research FY27 Q2	No published path. End of support.
DB-018	Rewrite	Move First FY27 Q2	Replace database key establishment.
BKP-002	Rewrite	Move First FY27 Q2	Replace backup key establishment.
MON-011	Portable	Confirm	Confirm the published build.
SSH-022	Rewrite	Later FY28	Rotate the bastion host key.

Phase view

Move First - FY27 Q2 - 2030 key establishment

TLS-001, GRP-038, VPN-007, MAIL-004, VPN-012, DB-018, BKP-002.

Later - FY28 - 2031 signatures

CERT-014, SSH-011, ADM-009, LIB-021, SIGN-006, SSH-022.

2035 - What remains

No remaining row in this sample.

Confirm

TLS-002, KEM-003, SIGN-002, MON-011. A published path exists.

Market Research - FY27 Q2

CTL-015. Blocked. The controller is at end of support and has no published path.

Exposure

CERT-014 moves with TLS-001. GRP-038 is one action, not 38. LIB-021 is one action for 12 applications.

Refuse list

HSM-001. The listing said private key material. It is not Blocked. No path was guessed.

Narrative

Fund Move First in FY27 Q2: the external RSA endpoints, both tunnels, the database, and the backup path. GRP-038 is a single line because those 38 endpoints share one library build. Hold the 2031 signature work for FY28. Confirm the four rows that already have a published path. CTL-015 is Blocked. Open market research in FY27 Q2. Do not name a replacement in this pack. HSM-001 stays on the refuse list. This sample is not an authorization.