SYMBEEO

PUBLIC

DESIGN STUDY

Cryptographic inventory and post-quantum roadmap for an insurer under DORA

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Consulting & Engineering	Financial Services	Composite insurer
DOCUMENT	**VERSION**	**DATE**
CON-003	1.1	Oct 10, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	CON-003	Version	1.1
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Sep 27, 2026
Capability	Consulting & Engineering	Industry	Financial Services
Author	David Morgan	Role	Principal Security Architect
Credentials	CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before the engagement starts."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 7
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure or clause read from the standards body's or publisher's own current page on Sep 24, 2026 · [S*] figure from the page summary where the page itself could not be opened · [A] assumption about the typical buyer, to be confirmed by the signing engineer · [T] design target taken from the design's stated outcome or derived from it. Every figure carries one tag. No figure comes from any prior engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Sep 27, 2026	1.0	First issue.
Oct 10, 2026	1.1	Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author.

1 · Scope

Who it is for. The CISO of an insurer who has been asked by the board when the company's encryption stops being safe against a quantum-capable adversary, cannot answer because nobody knows where RSA and elliptic-curve keys are used, and must show the supervisor a plan that sits inside the insurer's DORA ICT risk framework.

Typical buyer [A]. A composite insurer in one EU member state: 2,400 staff, two data centers, one hyperscaler tenancy, 310 externally reachable endpoints (portals, broker APIs, VPN concentrators, mail gateways), an internal PKI issuing about 18,000 certificates, and 140 ICT third-party service providers in its DORA register of information.

What is in. A cryptographic inventory of external endpoints and internal management planes, recorded as a machine-readable cryptography bill of materials; a replacement horizon for every quantum-vulnerable entry; the supplier questions that follow from the third-party register; a costed, sequenced roadmap in three horizons; a risk register entry per gap on the insurer's own criteria. SRA-CON-001 Model A, with R4 as the lead requirement. **What is out.** Replacing any algorithm, certificate or device; source-code cryptography review of in-house applications; penetration testing; the DORA register of information itself, which the insurer maintains.

Assumptions. The insurer is a financial entity under DORA [A]. Scans run only in authorized windows and read handshakes; no key material is collected [A]. Suppliers answer a written questionnaire within 30 days [A]. The insurer's risk criteria are a 5 × 5 likelihood and impact matrix [A].

Related documents, read Sep 24, 2026. SRA-CON-001, SDD-CON-001, STP-CON-001 (this capability) · NIST IR 8547 initial public draft, Transition to Post-Quantum Cryptography Standards, https://csrc.nist.gov/pubs/ir/8547/ipd · European Commission, EU reinforces its cybersecurity with post-quantum cryptography (Jun 23, 2025), https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography · A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography · CycloneDX v1.7 release note (Oct 21, 2025), https://cyclonedx.org/news/cyclonedx-v1.7-released/ · ECMA-424 2nd edition (December 2025), https://ecma-international.org/publications-and-standards/standards/ecma-424/ · Commission Implementing Regulation (EU) 2024/2956, register of information templates, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402956 · DORA, Regulation (EU) 2022/2554, https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.

© 2026 Symbeeo. All rights reserved. · Public

1c · Public implementations this design follows

Each row is labeled. **Public deployment**: a named operator's real deployment, published and dated by the operator, its vendor or a partner, used where one exists. **Our own design**: the dated vendor or standards documentation this design was built from, where no public deployment of the design exists. Labels and dates checked Sep 27, 2026.

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Our own design, built from published documentation. Coordinated implementation roadmap for the transition to PQC: member states start transitioning by the end of 2026; critical infrastructures transition as soon as possible and no later than the end of 2030	European Commission and the NIS Cooperation Group · Jun 23, 2025	R6 and §4.4: the 2030 horizon for high-risk use is the published EU date, not this document's choice; finance is a critical-infrastructure sector in it	`https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography`
Our own design, built from published documentation. NIST IR 8547 (initial public draft): dates set by security strength — RSA, ECDSA, finite-field and elliptic-curve Diffie-Hellman at 112 bits deprecated after 2030 and disallowed after 2035; at 128 bits or more disallowed after 2035 (Tables 2 and 4)	NIST · Nov 12, 2024, still the initial public draft on Sep 27, 2026 (comments closed Jan 10, 2025)	R5: the strength-dependent dates give each CBOM entry a horizon; the draft status is stated wherever the date is used	`https://csrc.nist.gov/pubs/ir/8547/ipd`
Our own design, built from published documentation. CycloneDX 1.7, adopted as ECMA-424 2nd edition: standard lists of algorithm families and elliptic curves for CBOM and PQC-readiness assessments	OWASP CycloneDX · Oct 21, 2025; Ecma International · December 2025	R3 and §4.2: the inventory format is an international standard the insurer's own tools can read, not a Symbeeo spreadsheet	`https://cyclonedx.org/news/cyclonedx-v1.7-released/`

No public, dated record of an insurer's or bank's cryptographic inventory was found on Sep 27, 2026; every row is documentation used to build our own design.

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Scope	310 external endpoints; internal PKI; management planes of 2 data centers and 1 tenancy	[A]
R2	External coverage	100 % of the 310 external endpoints scanned for TLS, SSH and IPsec	[T]
R3	Inventory format	CBOM in CycloneDX 1.7 (ECMA-424 2nd ed.), validated against the published schema	[S] CycloneDX; Ecma
R4	Entry content	protocol, algorithm, key size, certificate issuer and expiry, owner, supplier where one runs it	[T]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R5	Horizon per entry	each RSA, ECDH or ECDSA entry dated to the IR 8547 draft by its security strength: 112 bits, deprecated after 2030 and disallowed after 2035; 128 bits or more, disallowed after 2035	[S] IR 8547 ipd
R6	High-risk horizon	every entry on a critical business service scheduled for migration by the end of 2030	[S] EU PQC roadmap
R7	Target algorithms	ML-KEM (FIPS 203) and ML-DSA (FIPS 204); SLH-DSA (FIPS 205) for long-lived signatures	[S] FIPS 203/204/205
R8	Supplier coverage	the 40 providers supporting critical or important functions asked for their PQC plan, from the 140 in the register	[A]
R9	Internal PKI	CA hierarchy, issuance profiles and the 18,000 certificates summarized by algorithm and validity	[A]
R10	Risk register	every quantum-vulnerable entry on a critical service entered as a risk with owner and treatment on the 5 × 5 criteria	[T]
R11	Roadmap	every item in one horizon (0–6, 6–18, 18–36 months) and linked to ≥ 1 CBOM entry	[T] from SRA-CON-001 R11
R12	Re-scan check	10 external endpoints re-scanned independently; 10 of 10 match the CBOM	[T] from STP-CON-001 T4
R13	Evidence handling	scan data held in the insurer's tenancy; no key material collected	[A]
R14	Turnaround	report issued ≤ 20 working days after scan authorization	[T]

Fourteen rows; four carry a published figure, four are design assumptions, six are design targets.

3 · Architecture overview

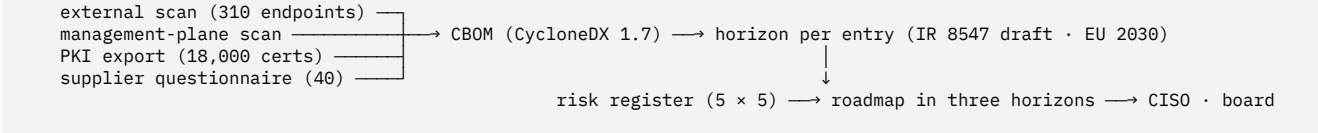


Figure 1. Cryptographic inventory to roadmap

One inventory in an open format, every entry given a date by a published horizon, every date turned into a risk someone owns.

© 2026 Symbeeo. All rights reserved. · Public

Table 4. Architecture overview

Role	Component (exact name)	Qty	Capacity used	Why this unit
Inventory format	CycloneDX 1.7 CBOM, ECMA-424 2nd edition	1	310 endpoints plus internal planes [A]	International standard; algorithm and curve lists built in [S]
Horizon source, US	NIST IR 8547 ipd	1	every quantum-vulnerable entry	by strength: 112-bit deprecated after 2030 and disallowed after 2035; 128-bit or more disallowed after 2035; draft [S]
Horizon source, EU	Coordinated Implementation Roadmap for the Transition to PQC	1	critical services	End-2030 for critical infrastructures [S]
Target algorithms	FIPS 203 ML-KEM · FIPS 204 ML-DSA · FIPS 205 SLH-DSA	3	replacement path per entry	Final standards since August 2024 [S]
Supplier list	the insurer's DORA register of information (ITS 2024/2956 templates)	1	40 of 140 providers [A]	The supplier list already exists and is supervised [S]

4 · Design by subsystem

4.1 Scan.

External endpoints first: TLS versions and cipher suites, certificate key types, SSH host-key and key-exchange algorithms, IPsec proposals (R2). Then the management planes of both data centers and the tenancy. Handshake reads only; no private key leaves any device (R13). Rejected: agent-based host scanning on day one — it reaches application cryptography but needs a change per host; it is a horizon-2 roadmap item [A].

4.2 CBOM.

Every finding written as a CycloneDX 1.7 cryptographic-asset component with the fields of R4, then validated against the schema (R3). The CBOM is the insurer's, stored in its tenancy, readable by any tool that reads ECMA-424 [S]. An endpoint found by the scan but absent from the CMDB is a finding, not dropped.

4.3 PKI and certificates.

Export of the internal CA's issuance data summarized by algorithm, key size and validity (R9). A certificate valid past 2030 on an RSA or elliptic-curve key of 112-bit strength is flagged: it outlives the draft deprecation date for that strength [S] IR 8547 ipd; mapping key size to strength follows NIST SP 800-57 Part 1 [A].

4.4 Horizons and priority.

Each entry gets two dates: the IR 8547 draft date (R5) and, where it serves a critical business service, the EU end-2030 date (R6). Priority is the earlier date, then data lifetime: policy and claims data kept for decades is the harvest-now, decrypt-later exposure, so the channels carrying it go first [A]. Replacement path per entry: ML-KEM for key establishment, ML-DSA for signatures, hybrid where the platform supports it (R7).

4.5 Suppliers.

The 40 providers behind critical or important functions (R8) receive a questionnaire: which algorithms their service uses today, their published PQC plan, and the date they will support ML-KEM on the interface the insurer uses. An unanswered questionnaire is a risk entry, not a blank [A].

© 2026 Symbeeo. All rights reserved. · Public

4.6 Risk and roadmap.

Each gap on a critical service becomes a risk on the insurer's 5 × 5 criteria (R10), owned and treated. The roadmap puts the work in three horizons (R11): horizon 1, inventory upkeep and crypto-agile requirements in every new purchase; horizon 2, external key-exchange migration on the highest-priority channels; horizon 3, PKI re-issue and signature migration [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Endpoint refuses the scan or is outside the window	entry marked "not observed" with reason; coverage below R2 reported	[A]
Supplier does not answer	entry held as a risk with the supplier named; escalated through the insurer's vendor management	[A]
IR 8547 finalized with different dates before issue	horizons recomputed from the final text; roadmap re-dated	[A]
CBOM fails schema validation	fixed before issue; the insurer's tools must read it unaltered	[T]
Internal PKI export unavailable	R9 reported partial; horizon-3 PKI items carry a stated uncertainty	[A]
Algorithm hidden in application code	not seen by a network scan; listed as a limit and a horizon-2 discovery item	[A]

6 · Limits

- A network scan sees cryptography on the wire, not inside applications or databases.
- IR 8547 is a draft; its 2030 and 2035 dates are proposals, stated as such wherever used.
- The EU roadmap addresses member states and critical infrastructures; how the insurer's supervisor applies it is the insurer's question.
- The roadmap is costed as bands; supplier dates drive horizons 2 and 3 more than the insurer's own work does.
- This is a finding on cryptography, not legal advice on DORA.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

© 2026 Symbeeo. All rights reserved. · Public

8 · The author

WRITTEN BY

David Morgan

Principal Security Architect

CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)

Signed off by Edwin Ozer, Founder.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

CON-003 · Version 1.1 · Oct 10, 2026