KILDE

SWIFT CSP Attestation Evidence Pack — CSCF v2026

Edition 1.0 · current to 21 August 2026

General information and document templates only. Not legal advice; no compliance outcome is guaranteed. Licensed for single-organisation use — see the Licence at the end of this document. Independent publication. Not affiliated with, endorsed by, or approved by S.W.I.F.T. SC. SWIFT is a registered trademark of S.W.I.F.T. SC. © 2026 Kilde.

START HERE — Your architecture type, your v2026 changes, and your clock

SWIFT CSP Attestation Evidence Pack · CSCF v2026 · current to 21 August 2026. General information and document templates only — not security consulting, not an independent assessment, not legal advice; no compliance outcome is guaranteed. Your independent assessor and your own copy of the framework are authoritative. First step for every file in this pack: download the CSCF v2026 yourself from SWIFT's Knowledge Centre (publication page cscf_dd/70.0 — free, no login) and verify every item in this pack against it. Independent publication by Kilde. Not affiliated with, endorsed by, or approved by S.W.I.F.T. SC. SWIFT is a registered trademark of S.W.I.F.T. SC.

The single thing to understand first: the 2026 attestation window runs 1 July – 31 December 2026, and your attestation must be backed by a mandatory independent assessment that finishes before you submit. The deadline that matters is therefore not 31 December — it's the day your assessor needs to start, and the day before that, when your evidence has to exist. This pack is that evidence, pre-structured. As one assessor firm puts it publicly: most controls fail on evidence, not on implementation.

Step 1 — Your architecture type in 10 minutes (this decides everything else)

Your type decides which controls apply, so it's the first thing your assessor checks — and v2026 moved the line. Work the tree, then verify the result against the architecture descriptions and the control-applicability grid in your own CSCF download (file 02 goes deeper).

```
Which architecture type are you THIS year? (revalidate — don't carry forward)
│
├─ Do you run your own communication interface — your infrastructure
│  connects directly to SWIFT?
│   ├─ YES → A1. Your messaging + communication stack is yours to secure.
│   └─ NO ↓
├─ Do you run your own messaging interface, while a provider owns the
│  communication layer?
│   ├─ YES → A2.
│   └─ NO ↓
├─ Is there a SWIFT-footprint connector installed on your premises —
│  Alliance Cloud SIL, Direct Link, Lite2 AutoClient, Microgateway?
│   ├─ YES → A3. (Lite2 with AutoClient is A3, not B.)
│   └─ NO ↓
├─ THE v2026 CONNECTOR SELF-TEST — answer honestly:
│  Does ANY software your institution owns make the connection to SWIFT
│  or to your provider application-to-application? Look for:
│    · a file-transfer client or server (SFTP scripts count)
│    · MQ / middleware / an integration layer talking to the provider
│    · an in-house app calling SWIFT's or the provider's API
│    · a webserver fronting WebAccess for your users
│   ├─ ANY YES → A4 — even if you attested B last year. v2026 pulled
│   │          customer connectors into mandatory scope (file 01).
│   └─ ALL NO → B. Humans in a browser GUI only. Your operator PCs are
│              STILL in scope as general-purpose machines.
```

Two rules that decide edge cases: what a component does and how it connects determines the type — not the mere fact that it exists; and ownership follows your BIC — where the thing is hosted is irrelevant. Write your

answer and your reasoning into templates/scoping-memo.md now; your assessor will ask for exactly this rationale.

Step 2 — What changed for you in v2026 (60 seconds per type)

- Everyone: 32 controls, now 26 mandatory + 6 advisory (v2025 was 25+7). The one promotion: 2.4 Back Office Data Flow Security is now mandatory — the flow-inventory and diagram work in file 03 is the biggest new lift for most buyers.
- Type B last year: run the connector self-test above. If anything you own connects app-to-app, you are now A4, with a materially larger control set. This is the reclassification SWIFT's own change material points to.
- A4: your connector — file-transfer client, middleware, API integration — is now a mandatory in-scope component of 14 controls (table in file 01). Plus A4-only 1.5 Customer Environment Protection.
- A1/A2/A3: 2.4 promotion + the minor tightenings (hardening now names WMI/PowerShell, MFA for remote privileged access, non-Windows malware scope, crypto expectations — file 01).
- Service-bureau / Lite2 / Alliance Cloud users: none of this transfers to your provider. File 07.

Step 3 — The window clock (work backwards from 31 December)

By when	What must be true	Pack file
31 Dec 2026	Attestation submitted and approved in KYC-SA	06
~Dec	Approver (CISO-level — see below) has reviewed and signs off	06
before submission	Independent assessment complete — it is mandatory, and it comes first	05
~Oct	Assessor engaged (internal 2nd/3rd line or external) — calendars fill in Q4	05
before day one with the assessor	Evidence exists: scoping memo, registers, 2.4 flow work, per-control evidence set	02, 03, 04
this week	Architecture type revalidated + scoping memo drafted	00, 02

Miss the window and the consequences are not abstract: counterparties see your status color-coded in KYC-SA (green valid / amber expired / grey none), and SWIFT reserves the right to report late or absent attestation — and missing independent assessments — to your supervisor, who can watch in real time via KYC-SA for Supervisors. File 06 has the full list.

Step 4 — Who must sign

The attestation Approver must be your CISO — or CIO, CRO, chief auditor, or an officer of similar seniority; CEO as last resort. The approver's name and function are visible to your counterparties. Decide the person now, brief them with file 06, and put the December sign-off in their calendar this week. (A Submitter prepares; the Approver owns it.)

Step 5 — The pack map

File	What it does for you
01	v2026 delta map — what actually changed, per control, with the operational move
02	Architecture + scoping — the memo and registers that anchor everything
03	Control 2.4 evidence workbook — flow inventory, bridging servers, diagrams, risk memos
04	Evidence checklist for all 26 mandatory controls — what assessors typically ask for
05	Independent assessment runbook — internal vs external, procurement, back-planner
06	KYC-SA submission runbook + log
07	Service-bureau / Lite2 / B-and-A4 specifics
08	Update tracker (the $49/mo tier) — v2027 watch, tentative-2028 legacy date, crypto KB
templates/	The registers and memos as fill-in files

Reminder before you start: this pack is general information and templates — it is not an assessment, not consulting, and not legal advice, and it guarantees no compliance outcome. Only your own CSCF v2026 download and your independent assessor are authoritative; verify everything here against both.