NIS2 and DORA: FairSSL ACME and API

For your supplier assessment of FairSSL: what the API and ACME server do, where data is stored, the controls built into the product and those we apply, and what you are responsible for. The page and PDF have the same content.

Documentation for your supplier assessment under the NIS2 Directive and DORA Regulation

Version 1.5
Date 01-11-2026

Support for your work with NIS2 and DORA, not legal advice.

Applies to FairSSL's API and ACME server on the date above. The latest version is at fairssl.dk/en/nis2-dora/.

FairSSL A/S, CVR no. 33075782, Åbrovej 29, 8586 Ørum Djurs, Denmark

Contents

1. The service and FairSSL's role
2. The data we process and where it is stored
3. Subcontractors for your register of information
4. Changes, access, updates, incidents and insurance
5. Controls in the ACME server and control panel
6. Private keys
7. Exit and concentration risk
8. External checks and security contact
9. DORA
10. NIS2 Article 21(2)(a)-(j)
11. Completed supplier questionnaire

1. The service and FairSSL's role

API and control panel	Ordering certificates from DigiCert, GlobalSign and Sectigo, monitoring certificates and expiry, users with permissions per account, monitoring CT logs for your domains, and AutoDNS, which sets up DNS validation with your DNS provider.
ACME server	An ACME server compliant with RFC 8555 at fairssl.dk/acme with External Account Binding (EAB) and ACME Renewal Information (ARI, RFC 9773). Your own ACME clients obtain and renew the certificates.
FairSSL's own status	FairSSL itself is not subject to NIS2: the certificates are issued by the CAs, and FairSSL is not a trust service provider under eIDAS. This page supports your supply chain obligations under NIS2 Article 21(2)(d) and (3), and DORA Articles 28-30. For financial entities, DORA takes precedence over NIS2 (NIS2 Article 4).
Legal basis	NIS2 Directive (EU) 2022/2555 as transposed in each member state. DORA Regulation (EU) 2022/2554 with RTS (EU) 2024/1774 and ITS (EU) 2024/2956. For customers in digital infrastructure or providing managed services: Implementing Regulation (EU) 2024/2690.

Sources
- NIS2 Directive (EU) 2022/2555: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- DORA Regulation (EU) 2022/2554: https://eur-lex.europa.eu/eli/reg/2022/2554/oj
- RFC 8555 (ACME): https://www.rfc-editor.org/rfc/rfc8555

2. The data we process and where it is stored

Most of it is certificate data that becomes public in CT logs when the certificate is issued. Personal data is limited to billing, contacts, login and the IP addresses of ACME clients. Data about your internal environment stays with you, apart from what the installation script reports back.

- The websites, control panel, API, ACME server and database run at Amazon Web Services EMEA SARL in the AWS region eu-central-1 (Frankfurt, Germany). Encrypted database backups are stored in eu-north-1 (Stockholm, Sweden).
- We are actively working to move operational and business systems hosted or owned outside the EU to services both hosted and owned in the EU. The certificate authorities (CAs) depend on the chosen product and are not part of the move.
- Automated system emails are sent via Lettermint B.V. (Netherlands); data is processed and stored in the EU.
- Data minimisation is a control in itself (NIS2 Article 21(2), GDPR Articles 25 and 32): with ACME, FairSSL never has your private key, and your internal environment is only visible through what the installation script reports back. This gives a low risk profile for confidentiality. It does not change the availability requirements under DORA.

Data	Where	Public?
Certificate data: domain names and, for OV/EV, company name and address	FairSSL (AWS Frankfurt) and the issuing CA	Yes, in CT logs after issuance
Order and validation data for OV/EV: company details and contact	FairSSL (AWS Frankfurt) and the validating CA	Company details yes, contact no
Billing, contacts and login	FairSSL (AWS Frankfurt); invoices in Visma e-conomic	No
Server name, thumbprint, result and error text from the installation; the ACME client's IP address and version in the event log	FairSSL (AWS Frankfurt), sent by the installation script in the simple-acme download	No

Data	Where	Public?
Private keys	With ACME, on your systems. Only when you ask FairSSL to generate the key and CSR is the key stored encrypted at FairSSL for a limited period (see the section on keys)	No

3. Subcontractors for your register of information

For the register of information under DORA Article 28(3) and Implementing Regulation (EU) 2024/2956. Your direct supplier is FairSSL A/S, CVR no. 33075782, Denmark: reseller of TLS certificates, ACME server and API for certificate management. The table lists FairSSL's sub-processors, the same as on the sub-processor list. The certificate authorities DigiCert, GlobalSign and Sectigo act as independent controllers under their own agreements; they and our other suppliers are listed in the privacy policy. You assess whether the service supports a critical or important function in your organisation.

Supplier	Service for FairSSL	Where data is stored and processed	Transfer basis
UpCloud Ltd (Finland)	From 11 November 2026: hosting of websites, control panel, API, ACME server and database	EU (Copenhagen and Amsterdam)	EU
mailbox.org (Heinlein Hosting GmbH, Germany)	From 11 November 2026: email	Germany	EU
OVHcloud (OVH SAS, France)	From 11 November 2026: locked backups and encryption key management	France	EU
Lettermint B.V. (Netherlands)	Automated system emails	EU	EU
Amazon Web Services EMEA SARL (Luxembourg)	Hosting of websites, control panel, API, ACME server and database; AWS WAF; log files in Amazon S3	eu-central-1 (Frankfurt); database backups in eu-north-1 (Stockholm)	EU; DPF and SCC for the group in the USA
Microsoft 365 and Azure	Office and cloud infrastructure	EU (Ireland and the Netherlands)	DPF and SCC
Freshdesk (Freshworks Inc., USA)	Helpdesk	AWS Frankfurt	DPF

4. Changes, access, updates, incidents and insurance

- All changes go through version control, and every deployment to production is traceable in the history.
- Administrative access is restricted to key personnel with role-based access control (RBAC) and least privilege.
- Security updates for systems and dependencies are installed on an ongoing basis.
- We notify the customer without undue delay and no later than 48 hours after a security incident has affected the customer's data or the service. This sentence also appears in the terms of sale. A vulnerability resolved without affecting data or the service is not an incident within the meaning of NIS2 (Article 6(6) and (15)).
- The customer is responsible for backing up its own systems and data, including before FairSSL carries out an installation or remote assistance.
- FairSSL A/S has public liability, product liability and professional indemnity insurance for IT companies with If. Proof of insurance is available on request.
- FairSSL is not ISO 27001 certified. The controls are mapped to ISO/IEC 27001:2022 Annex A and CIS Controls v8.1. An independent assurance report, such as ISAE 3000, can be included in a customer agreement at the customer's expense, subject to agreement.

5. Controls in the ACME server and control panel

The controls you manage in the control panel. The default is shown in the last column.

Control	What it does	Default
Single-use EAB	A new ACME client needs an EAB key. A key for a single client is deleted in the same transaction that creates the client's account, so it cannot be reused.	The wizard defaults to "One client"; "Many clients" must be selected explicitly
Lock on names and wildcards per client	When the lock is enabled, a client with a valid certificate can only renew and reissue its existing names, or fewer, and cannot order wildcards. Attempts are rejected and logged as an event. Initial setup with EAB may use any name the account can validate, so a new server can get started without waiting for approval; you then lock the client.	Locked on the profile; enabled per client
Profiles and accounts	Clients are grouped into profiles, each with its own product, locks and notifications. FairSSL accounts each have their own AutoDNS settings, so production and testing, for example, can be kept separate.	As configured by you
CAA	The ACME server checks CAA records for all names against the CA that will issue the certificate and rejects the order with a CAA error when CAA does not allow that CA. CAA lets you control which CAs may issue certificates for your domains.	Always
Notifications per profile	Event emails at six levels: critical, errors, warnings, orders, information and debugging. Each level includes those below it.	Orders (level 200): errors, warnings, new orders and new certificates
Warning when a client stops using ARI	A daily check warns when a client that has used ARI has not queried it for 3 days, and again after 7 days. This detects a client that has stopped before the certificate expires.	Always
Installation feedback	After each renewal, simple-acme from FairSSL reports whether the certificate was installed, with the server name and thumbprint. The result appears as an event on the client in the control panel.	Enabled in the simple-acme download
Monitoring API v1	Read access using a token to the overview, certificates, ACME clients and events as JSON, PRTG or Prometheus, so your own monitoring can track the certificates.	You create the token
Two-factor login	The account can require two-factor login for all users in the control panel.	Two-factor login can be required per account

6. Private keys

- With ACME, your ACME client generates the private key on your own server, and the key stays there. The ACME server only receives the certificate signing request (CSR) and has no function that accepts a private key.
- If you order a certificate without ACME, FairSSL's CSR service can generate the key and CSR for you. The key is stored encrypted with AES-256, using a key derived from the order and a download password. The password is stored encrypted separately from the key, and downloading requires both the link and the password.
- An hourly job deletes the key 48 hours after the first download, and no later than 60 days after it was generated (30 days if the order is cancelled or the certificate is revoked). You can also delete it yourself using the link and password. Each deletion is logged on the order.
- If you do not want FairSSL ever to have your private key, generate the key yourself or use ACME.

7. Exit and concentration risk

- ACME is an open standard (RFC 8555) supported by all major CAs and ACME clients.
- Switching to another provider requires a new account and EAB with the new provider, validation of the domains, possibly new DNS and CAA records, and the new provider's URL in your ACME client.
- Installed certificates work until they expire, even if FairSSL no longer provides the service. The certificates are stored on your systems and with the CA that issued them.
- The overview of your certificates and ACME clients can be retrieved through the monitoring API, so you have your inventory outside FairSSL.

8. External checks and security contact

- fairssl.dk and fairssl.se undergo DigiCert's external vulnerability scan weekly without login. The latest report is available on request. The ACME server responds at fairssl.dk/acme on the same servers as fairssl.dk.
- The CAs are audited annually under WebTrust for CAs or ETSI EN 319 411. The audit covers the CAs' operations and issuance, not FairSSL.
- Send security enquiries and vulnerabilities to info@fairssl.dk. The contact is also listed in /.well-known/security.txt (RFC 9116) on fairssl.dk and fairssl.se.

Sources
- RFC 9116 (security.txt): https://www.rfc-editor.org/rfc/rfc9116
- CCADB: CA audit reports: https://www.ccadb.org/resources

9. DORA

Article 7 of RTS (EU) 2024/1774 on cryptographic key management requires financial entities to renew certificates before expiry (paragraph 5) and maintain a register of certificates and devices that store certificates (paragraph 4).

- Paragraph 5: the ACME client renews automatically before expiry, and ARI tells the client when to renew. The warning about a client that has stopped using ARI and expiry monitoring detect a renewal that does not happen.
- Paragraph 4, partially: the control panel and monitoring API provide an overview of certificates and ACME clients. You register the devices that store certificates (servers, HSMs, load balancers) yourself.

DORA Articles 28-30 and where to find the answer on this page:

DORA	Topic	Section
Art. 28(1)-(2)	Your policy on ICT third-party risk	Your responsibility; this page provides input
Art. 28(3)	Register of information	Subcontractors
Art. 28(4)-(5)	Assessment before entering into an agreement	Data, controls, keys, external checks
Art. 28(8)	Exit strategy	Exit and concentration risk
Art. 29	Concentration risk and subcontractors	Exit; subcontractors
Art. 30(2)(a)	Description of the service and subcontractors	The service; subcontractors
Art. 30(2)(b)	Where data is processed and stored	Data and location
Art. 30(2)(c)	Availability, integrity, confidentiality	Controls; keys; changes and access
Art. 30(2)(d)	Access to data on termination	Exit (monitoring API)
Art. 30(2)(e)	Service level	Terms of sale, section 12: no SLA
Art. 30(2)(f)	Assistance with ICT incidents	Incidents (48 hours)
Art. 30(2)(g)-(i)	Cooperation with authorities, termination, training	Terms of sale; other points on request
Art. 30(3)	Critical or important functions	The full package addresses the applicable points; the rest on request

Sources
- RTS (EU) 2024/1774: https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj

- ITS (EU) 2024/2956: https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj

10. NIS2 Article 21(2)(a)-(j)

Three layers in each row: what the product helps you with, our own controls, and what you are responsible for.

Point	The product	Our controls	Your responsibility
a) Risk analysis and policies	The data and subcontractor tables for your risk analysis of FairSSL.	Data minimisation; controls mapped to ISO/IEC 27001:2022 Annex A and CIS Controls v8.1.	Your risk analysis and policies.
b) Incident handling	Notifications about errors, rejected orders and failed installations.	Notification no later than 48 hours after incidents affecting your data or the service.	Your incident procedure and reporting.
c) Business continuity and backup	Installed certificates work without FairSSL; ARI and renewal before expiry.	Database in Frankfurt with encrypted backups in Stockholm.	Backups of your own systems, including before installation or remote assistance.
d) Supply chain security	CAA restricts which CAs may issue certificates.	Subcontractors with locations and transfer bases.	Your assessment of FairSSL as a supplier.
e) Security in acquisition, development and maintenance	ACME under RFC 8555 and ARI under RFC 9773.	Version control with traceable deployments; ongoing security updates; weekly external scans; security.txt.	Updating your ACME clients and servers.
f) Assessing effectiveness	The monitoring API for your own monitoring of certificates and clients.	Scan report on request.	Your own measurement of the controls.
g) Cyber hygiene and training	Automatic renewal instead of manual steps.	Least privilege for administrative access.	Training your own staff.
h) Cryptography	The private key stays with you when using ACME.	Keys from the CSR service are encrypted with AES-256 and deleted automatically.	Your cryptography policy and key lengths.
i) Human resources security, access control and assets	Users with permissions per account; single-use EAB; lock per client; overview of certificates and clients.	Role-based access control (RBAC) with least privilege.	Who in your organisation has access to the control panel and ACME clients.
j) Multi-factor authentication	Two-factor login, which the account can require for all users.	Access based on role and least privilege.	Enabling the two-factor requirement for your account.

11. Completed supplier questionnaire

The questions a supplier assessment typically asks, with our answers. Also available as CSV.

Question	Answer	Section
Supplier name and registration number	FairSSL A/S, CVR no. 33075782, Åbrovej 29, 8586 Ørum Djurs, Denmark	Subcontractors
What service is provided?	TLS certificates from DigiCert, GlobalSign and Sectigo, ACME server and API for certificate management	The service

Question	Answer	Section
Is the supplier itself subject to NIS2?	No. The CAs issue the certificates, and FairSSL is not a trust service provider under eIDAS	The service
Where is data stored and processed?	AWS eu-central-1 (Frankfurt); encrypted database backups in eu-north-1 (Stockholm); subcontractors as listed in the table	Data and location
Is data processed outside the EU?	Yes, by the sub-processors listed in the table, and by the CAs DigiCert and Sectigo in the USA under DPF	Subcontractors
Does the supplier have access to our private keys?	Not with ACME. With the CSR service, encrypted for no more than 60 days	Private keys
How are changes managed?	All changes go through version control, and every deployment to production is traceable in the history.	Changes
How is administrative access managed?	Administrative access is restricted to key personnel with role-based access control (RBAC) and least privilege.	Changes
How are systems kept up to date?	Security updates for systems and dependencies are installed on an ongoing basis.	Changes
When are we notified of incidents?	Without undue delay and no later than 48 hours after a security incident has affected your data or the service	Incidents
Does the supplier hold a certification?	Not ISO 27001. The controls are mapped to ISO/IEC 27001:2022 Annex A and CIS Controls v8.1; ISAE 3000 by agreement at the customer's expense	Changes
External testing?	Weekly external vulnerability scans of fairssl.dk and fairssl.se without login; report on request	External checks
Insurance?	Public liability, product liability and professional indemnity insurance with If; proof on request	Insurance
Can we require two-factor login?	Yes, for all users on the account	Controls
Exit?	ACME is an open standard; installed certificates work until expiry	Exit
Does the supplier offer an SLA?	No. See section 12 of the terms of sale	DORA
Security contact	info@fairssl.dk and /.well-known/security.txt	External checks

Frequently asked questions

Is FairSSL subject to NIS2?

No. FairSSL resells certificates issued by the CAs and is not a trust service provider under eIDAS. This page exists because you, as a customer, must assess your suppliers under NIS2 Article 21(2)(d) and (3), or DORA Articles 28-30.

Should FairSSL be included in our DORA register of information?

Yes, if you are a financial entity and use FairSSL's API or ACME server. The subcontractor section contains the information the register requires. You assess whether the service supports a critical or important function.

Can FairSSL see our private keys?

Not with ACME: the key is generated and stays on your server. Only if you order using FairSSL's CSR service is the key stored encrypted until it is deleted automatically.

What happens if FairSSL cannot provide the service?

Installed certificates work until they expire. You can switch to another ACME provider with a new account, EAB, validation and the new URL in your ACME client.

Will you complete our supplier questionnaire?

We do not complete the customer's own questionnaire. The supplier questionnaire on this page and the full package answer the questions an assessment typically asks.

The full package

If you need the documentation for a supplier assessment under NIS2 or DORA, write to us with your company name and what the assessment needs to cover. We will then send the full package with the scan report and our completed supplier questionnaire.

info@fairssl.dk