NIS2 and DORA documentation

What your supplier assessment under NIS2 or DORA needs about sslbrain, for businesses across the EU. On Professional and above, the appliance also creates your own documentation.

sslbrain: documentation for your supplier assessment under NIS2 and DORA

Version 1.6
Date 06-11-2026

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

Applies to sslbrain on the date above. The latest edition is always at sslbrain.com/en/nis2/.

FairSSL A/S, publisher of sslbrain

Contents

1. The service and our role
2. Data and where it is stored
3. Subcontractors for your register
4. Operations: changes, access, updates and incidents
5. Controls in the product
6. Keys and cryptography
7. Exit and concentration risk
8. External checks, certification and insurance
9. DORA
10. NIS2 Article 21(2)(a)-(j)
11. Residual risks and mitigations
12. Completed supplier questionnaire
13. Frequently asked questions

1. The service and our role

About sslbrain in one page

What it does	Obtains, renews and installs TLS certificates on your servers, load balancers and firewalls, and shows where each certificate is installed and when it expires.
Where keys and data are stored	On-Premise in your appliance: private keys (generated on the appliance and stored encrypted in the vault), certificates, installation plans, audit log and settings.
What sslbrain Cloud (EU) holds	Your account and licence, a key to the appliance vault (section 5), accounts with CAs and, if you choose, DNS API keys. Cloud is hosted in the EU by the sub-processors in section 3.
What leaves your network	Only connections initiated by the appliance. Over HTTPS: to cloud.sslbrain.com, acme.sslbrain.com, registry.sslbrain.com and dns-proxy.sslbrain.com, and to the CAs and DNS providers you choose. Also DNS lookups through 1.1.1.1, 8.8.8.8 and 9.9.9.9 (port 53 and DNS over HTTPS), Ubuntu security updates from archive.ubuntu.com (port 80) and time synchronisation (NTP). The appliance's own firewall allows only these. Sent to Cloud: counts and versions (servers, certificates, installation plans, service agents, disk usage), certificate requests for certificates from Cloud, and diagnostics only if you enable them. Never private keys.
What comes in	No inbound connections. The appliance web interface responds only on your own network. The appliance and service agents only initiate outbound connections, and neither FairSSL nor Cloud can log in to the appliance.

NIS2, DORA and the other frameworks

- NIS2 is an EU directive, and each country has its own law, for example the Danish NIS 2 Act (Act no. 434 of 6 May 2025) and the Swedish Cybersecurity Act (Cybersäkerhetslag (2025:1506)). The Danish Act entered into force on 1 July 2025. The articles here are the directive's, so the documentation can be used anywhere in the EU.
- Financial entities follow DORA, Regulation (EU) 2022/2554, which takes precedence over NIS2 where it covers the same matters (NIS2 Article 4).
- Customers that are themselves digital infrastructure or MSPs also follow Implementing Regulation (EU) 2024/2690.
- FairSSL itself is not subject to NIS2. This documentation supports your supply chain obligations: NIS2 Article 21(2)(d) and (3), and DORA Articles 28 to 30.
- The same controls cover GDPR Articles 28 and 32 (the data processing agreement and security of processing).
- FairSSL does not hold an ISO 27001 certification. The controls are mapped to ISO/IEC 27001:2022 Annex A and CIS Controls v8.1.
- sslbrain is developed in line with the Cyber Resilience Act, Regulation (EU) 2024/2847.

- NIS2 Directive (EU) 2022/2555: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
- DORA, Regulation (EU) 2022/2554: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
- RTS (EU) 2024/1774 on ICT risk management: https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj/eng
- ITS (EU) 2024/2956 on the register of information: https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj/eng
- Implementing Regulation (EU) 2024/2690: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng
- Cyber Resilience Act, Regulation (EU) 2024/2847: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

2. Data and where it is stored

Most of it is certificate data that is already public in Certificate Transparency logs. Personal data is limited to billing, contacts and login. Data about your internal environment stays with you. Cloud receiving so little is a control in itself (data minimisation, NIS2 Article 21(2) and GDPR Articles 25 and 32).

Data	Where it is stored	Classification

Data	Where it is stored	Classification
Private keys	Generated on the appliance and stored encrypted in the vault on your systems. Never sent to Cloud.	Confidential
Credentials: server logins, DNS API keys, CA accounts on the appliance	Encrypted in the appliance vault. A DNS API key is stored in Cloud only if you choose this for ACME from Cloud.	Confidential
Internal certificates, server names, IP addresses and software	In the appliance inventory on your systems. Selected information (e.g. server name, IP address and operating system) is sent to FairSSL support only if you enable diagnostics.	Internal
Counts and versions	Cloud: counts of servers, certificates, installation plans and service agents, versions and disk usage. Used for licensing and operations.	Internal
Certificate requests for certificates from Cloud	Cloud and the CA you choose: the names in the certificate and validation (AutoDNS or DNS API key).	Public
Notifications you send through Cloud	Cloud and the email service Lettermint: subject and text, which may mention server names and certificates. Lettermint deletes message content, recipients and metadata automatically 28 days after sending. Notifications through your own SMTP server or webhooks do not pass through Cloud.	Internal
Messages to service agents via Cloud	Encrypted end to end between appliance and service agent. Cloud sees who, when and how much, not the content.	Confidential
Audit log	In the appliance. On Professional and above, the latest hash in the chain is stored in Cloud every hour.	Internal
Account, login, contacts and billing	sslbrain Cloud (EU) and the sub-processors in section 3.	Personal data

3. Subcontractors for your register

- sslbrain Cloud is hosted in the EU by the sub-processors in the table.
- Certificate authorities (CAs): Independent data controllers for issuance, validation and Certificate Transparency logging of the certificates the customer orders. The CA follows the certificate profile the customer chooses.
- The names in a certificate are public: the CA writes them to Certificate Transparency logs.

Supplier	Ownership	Data stored in	Used for
UpCloud	Finland	EU	Server and database hosting
OVHcloud	France	EU	Server and database hosting
mailbox.org	Germany	EU	Email
Microsoft 365	USA	EU	Email and office systems
Lettermint	Netherlands	EU	System emails

The customer may object within 30 days of the notice by writing to info@fairssl.dk.

Change log

- No changes yet.

4. Operations: changes, access, updates and incidents

FairSSL as a supplier

- Changes: Updates to the appliance, service agents and deployment agents are signed with a hardware key, and the appliance installs only updates with a valid signature.
- Access: Administrative access is limited to key personnel with role-based access control (RBAC) and least privilege.
- Updates: Security updates to systems and dependencies are installed continuously.
- Incidents: We notify the customer without undue delay and at the latest within 48 hours if a security incident has affected the customer's data or the service. This is also stated in the terms and the data processing agreement. A vulnerability that has been fixed without affecting the customer's data or the service is not an incident (NIS2 Article 6, points 6 and 15).
- sslbrain is developed in line with the Cyber Resilience Act.

Incidents and contract

- We notify the customer without undue delay and at the latest within 48 hours if a security incident has affected the customer's data or the service (terms, section 16, and data processing agreement, section 8).
- Personal data breaches: FairSSL informs you without undue delay and no later than 48 hours after becoming aware of the breach (data processing agreement, section 8).
- Security notices that require action from you are emailed to the account's security recipients, and all notices are at sslbrain.com/en/security-notices/.
- Sub-processors: a new or replaced sub-processor is announced by email and in the change log in section 3. You can object within 30 days of the notice, and if no solution is found, you can terminate the affected services without a remaining contractual commitment.
- Changes that require action from you are announced at least 30 days in advance.
- When you stop: your subscription runs until the end of the paid period, then switches to Free. Closing the Cloud account does not affect data already held on your systems.
- Personal data that FairSSL processes for you is deleted or returned on termination. Deletion from active systems takes place within 30 days; backups are deleted in the regular rotation.
- FairSSL's total liability is limited to what you have paid in the last 12 months.
- Our notification does not replace your own deadlines for significant incidents under NIS2 Article 23 or DORA Article 19: under NIS2, early warning within 24 hours, incident notification within 72 hours and a final report no later than one month after the notification.

5. Controls in the product

Your supplier assessment of sslbrain

Article 21(2)(d) and (3) of the NIS2 Directive and DORA Article 28 ask you to assess your ICT suppliers. The table shows what FairSSL and sslbrain Cloud can and cannot do in your network, alongside an ACME client using a public CA.

	sslbrain	**An ACME client (e.g. Certbot with Let's Encrypt)**
Supplier code running on your systems	The appliance, service agents and integrations run on your systems. They are restricted to what FairSSL has signed and what you sign yourself with the appliance key (section 7), just as an ACME client runs what it was built to do.	The ACME client runs on your systems with the permissions you give it.
Supplier control	No commands. Cloud cannot run anything on the appliance or service agents. Cloud can refuse to unlock the appliance or lock it (section 5), and offer a new signed version that the appliance installs itself if you have chosen automatic updates.	No commands.

	sslbrain	An ACME client (e.g. Certbot with Let's Encrypt)
Updates	Updates to the appliance, service agents and deployment agents are signed with a hardware key, and the appliance installs only updates with a valid signature. A version that cannot be verified will not start. Automatic updates can be disabled locally. The operating system underlying the appliance (Ubuntu LTS) downloads only Ubuntu security updates, signed by Canonical, and restarts at 03:00 UTC if needed.	Depends on the client. Certbot updates itself when installed as recommended.
Issuance for your domains	Issuance through Cloud requires the name to be validated with AutoDNS (one CNAME per name) or with a DNS API key you have stored in Cloud. Names validated with a DNS API key in the appliance cannot be issued by Cloud. You decide per name. CAA records also restrict which CAs and accounts may issue.	Whoever controls the ACME account and validation can obtain certificates for your names. CAA records restrict this in the same way.
Renewals stopping	If Cloud or your subscription stops, installed certificates work until they expire, and the data in the appliance belongs to you and stays with you. Section 7 describes each situation.	If the CA or client stops, installed certificates work until they expire.
Access into your network	None. SSH access for troubleshooting by FairSSL support can only be enabled for 24 hours from the appliance's local console. Even then, access to the appliance on your network is required.	None.
DNS API keys	Stored encrypted in the appliance vault, in one place in your network. Calls to the DNS provider pass through an encrypted connection that Cloud cannot read. For ACME from Cloud, you can choose to store the key in Cloud.	Stored on every server that issues certificates. certbot, acme.sh and lego keep it in plain text in a file or environment variable. win-acme encrypts it by default with the server's own Windows key.

The vault key in sslbrain Cloud

Security reviewers ask about it first. Here is exactly what it can and cannot do.

- The appliance vault encrypts private keys with a 256-bit master key generated on the appliance and never sent to Cloud.
- The master key is stored on the data disk only in encrypted form: copies locked with keys from Cloud (the current key and the most recently replaced ones) and one copy locked with the 12 backup words. While the appliance is running, the unencrypted master key is held in memory, not on disk.
- Cloud generates a random key (32 bytes) for each installation and stores it encrypted.
- The key is replaced every time the vault is unlocked through Cloud and every 6 hours.
- Cloud alone decrypts nothing: Cloud holds neither the master key nor your private keys.
- Cloud plus a copy of the data disk or a backup unlocks the keys as long as Cloud still holds the key that locks the copy. Protect the data disk and backups as you would private keys.
- Cloud controls the vault's availability, not its contents: Cloud can refuse to unlock it or lock the appliance. The 12 backup words always unlock it, including a locked appliance, without Cloud. The appliance then stays unlocked until the next restart; anything that goes through Cloud stops, and the emergency account cannot download private keys or backups.
- If Cloud does not respond, an unlocked vault keeps running. After a restart, Cloud or the backup words unlock it.
- If two copies of the same installation are running, you choose in Cloud which one continues. FairSSL support can also approve a takeover from Cloud, and the account's recipients receive an email. The other copy is

locked.
- After a restore from a backup, Cloud asks for your approval (or approval from FairSSL support) before unlocking. The 12 backup words unlock it immediately. Cloud deletes replaced keys when they are more than 7 days old and not among the 10 newest, so an older backup or disk copy can only be unlocked with the backup words.

The NIS2 package from your appliance (Professional)

Your own documentation, signed by the appliance: audit log with chain verification, inventory, renewals and failures, policies on the selected date, completed cryptography policy, risk worksheet and incident procedure. On Professional and above, the appliance creates the NIS2 package: one signed file for the period you choose, ready for your auditor.

- The audit log with hashes and the result of chain verification.
- Certificate inventory on the selected date: names, CA, key type and size, expiry and where each certificate is installed.
- Renewals and failures during the period.
- Policies on the selected date: roles and users, who can download private keys, domain lock and update mode.
- Appliance and service agent versions, and whether the signatures are valid.
- A cryptography policy under Commission Implementing Regulation (EU) 2024/2690, point 9.2 of the Annex, completed with your settings.
- A risk worksheet, an incident procedure with the Article 23 deadlines, and the division of responsibilities between you and FairSSL.
- As a PDF and as files you can edit in Word and spreadsheets.
- Every row in the audit log is sent to your SIEM using syslog over TLS, and the latest hash in the chain is stored in sslbrain Cloud.

Regulation (EU) 2024/2690 is binding only on the entities listed in its Article 1 (e.g. cloud, DNS, MSPs, data centres and trust service providers). For others, it is a useful reference.

6. Keys and cryptography

- Data in the appliance: private keys and other secrets are encrypted with XChaCha20-Poly1305 and a 256-bit key.
- The 12 backup words: 96 bits, converted to a key with Argon2id.
- Messages between the appliance and service agents: signed with ECDSA (P-384, or P-256 depending on the service agent's key) and encrypted with AES-256-GCM (JWE, ECDH-ES). This also applies to messages via sslbrain Cloud (EU), which cannot read them.
- Appliance versions and integrations: signed with ECDSA P-384 and SHA-384.
- Downloaded backup files: encrypted with XChaCha20-Poly1305 and a key derived from your password (Argon2id). The password is required and must be at least 12 characters.
- Certificate keys: generated on the appliance, RSA 2048 to 4096 bits or ECDSA P-256 and P-384. The certificate profile and the servers the certificate will be installed on determine which types are allowed. Certificates you upload yourself retain their key.
- The appliance web interface and Cloud services use TLS 1.2 and 1.3 and reject TLS 1.0 and 1.1 (measured 25-10-2026).

Measured 25-10-2026: TLS 1.3 and hybrid post-quantum key exchange (X25519MLKEM768).

Component	TLS 1.3	X25519MLKEM768
Appliance web interface	Yes	Yes
sslbrain Cloud (cloud.sslbrain.com)	Yes	Yes
acme.sslbrain.com, registry.sslbrain.com, dns-proxy.sslbrain.com	Yes	Yes
Linux service agent (uses the server's OpenSSL)	Yes	Yes with OpenSSL 3.5 or later (e.g. Debian 13), otherwise X25519
Windows service agent (uses Windows' own TLS)	From Windows Server 2022	From Windows Server 2025, when Windows has it switched on

7. Exit and concentration risk

What happens when sslbrain Cloud or FairSSL is unavailable. Private keys, certificates and data remain On-Premise on your systems in all four situations, and installed certificates work without Cloud: they are files on your servers that nothing in sslbrain removes when Cloud is unavailable.

- Local ACME source (Professional and above): the appliance issues directly with the CA, e.g. Let's Encrypt or your own ACME CA, without going through Cloud. Validation with AutoDNS or a DNS API key in Cloud still requires Cloud; a DNS API key in the appliance does not.
- The Local ACME server add-on (Enterprise) is different: an ACME server on the appliance that your internal ACME clients use and that relays requests to your own CA or an external ACME CA.
- Multiple CAs in order: a profile can have several certificate sources, and if the first fails, the next takes over.
- Your own signing key: the appliance has its own key, generated on the appliance. If you set its public part locally on a server with a service agent, the service agent runs your own agents and your own changes to agents, signed by the appliance. The key cannot approve FairSSL's packages or updates.
- Service agents can be installed manually on the server from a version you build or obtain yourself (MSI on Windows, a package or source code on Linux). Enrolment is with your appliance.
- If the appliance runs in Docker, you can download and update the image yourself. The signature can be checked locally with sslbrain-sigverify before starting the image.
- By default, the appliance is unlocked through Cloud, or with the 12 backup words without Cloud. If you want to operate entirely without Cloud, you can purchase the 100% local On-Premise edition (the Offline operation add-on).
- What requires Cloud today: appliance enrolment and activation, Cloud login, licence renewal, unlocking after a restart (otherwise the backup words), issuance through Cloud with AutoDNS, DNS API keys in Cloud and dns-proxy.sslbrain.com, service agent enrolment via Cloud and messages via Cloud, updates and integrations from the catalogue, notifications through Cloud, the audit log hash in Cloud and the code for the console's root shell.

Situation	What works	What stops
Cloud does not respond (outage)	The appliance keeps running with the vault unlocked. Users log in with the password known to the appliance. With Local ACME source and DNS API keys in the appliance, certificates are renewed directly with the CA and installed. Directly connected service agents and notifications through your own SMTP server or webhooks work.	Issuance through Cloud and AutoDNS, messages to service agents via Cloud, Cloud login, updates, notifications through Cloud and licence renewal. These resume when Cloud responds again.
Restart while Cloud is unavailable	By default, the vault is unlocked through Cloud. Without Cloud, you unlock it with the 12 backup words, and the appliance stays unlocked until the next restart. It then behaves as during an outage.	The same as during an outage. The emergency account cannot download private keys or backups.
The subscription has expired	You are notified at least 28 days before expiry. The appliance continues as Free: the oldest servers up to the Free limit still receive renewals and installations. Other servers remain in the inventory, retain their keys and are still discovered.	Renewal and installation on servers beyond the Free limit, and features and modules that Free does not include.

Situation	What works	What stops
FairSSL is permanently gone	Keys, certificates and inventory belong to you and stay with you. The appliance keeps running, and the 12 backup words unlock it after a restart. Local ACME source renews directly with the CA until the licence period expires. After that, the appliance itself removes the Professional modules, and Free renews through Cloud, so renewals stop; installed certificates work until they expire. Should development of sslbrain ever stop, we will release the software as open source first. The code is readable (source-available), and ACME is an open standard (RFC 8555), so switching requires a new account with the new provider, validation and new installations.	Everything that requires Cloud (see the list below), updates from FairSSL, licence renewal and, once the licence period has expired, certificate renewal.

8. External checks, certification and insurance

Development and vulnerabilities

- Updates to the appliance, service agents and deployment agents are signed with a hardware key, and the appliance installs only updates with a valid signature.
- The operating system underlying the appliance (Ubuntu LTS) installs Ubuntu security updates automatically and restarts at 03:00 UTC if needed.
- A version that cannot be verified will not start, and the version that was running is started again. An integration that cannot be verified does not replace the installed one.
- You choose manual or automatic updates on the appliance.
- The code is readable (source-available), so you or a third party can review it.
- Report vulnerabilities to info@fairssl.dk; the contact is listed in sslbrain.com/.well-known/security.txt. Security notices are at sslbrain.com/en/security-notices/.
- We support the latest and previous major versions and give at least 90 days' notice before a version stops receiving security fixes.

Certification and insurance

- FairSSL does not hold an ISO 27001 certification. The controls are mapped to ISO/IEC 27001:2022 Annex A and CIS Controls v8.1.
- FairSSL A/S holds general liability, product liability and professional liability insurance for IT companies with If.

9. DORA

DORA and RTS 2024/1774, Article 7

DORA, Regulation (EU) 2022/2554, applies to financial entities and takes precedence over NIS2 for them (NIS2 Article 4). Article 7 of Commission Delegated Regulation (EU) 2024/1774 on ICT risk management sets requirements for cryptographic keys and certificates. Here are the three paragraphs concerning certificates, verbatim, and how sslbrain covers them.

RTS 2024/1774, Article 7	How sslbrain covers it

RTS 2024/1774, Article 7	How sslbrain covers it
Paragraph 1: "Financial entities shall include in the cryptographic key management policy referred to in Article 6(2), point (d), requirements for managing cryptographic keys through their whole lifecycle, including generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking, and destroying those cryptographic keys."	Generating: the key is generated on the appliance. Renewing: each new version gets a new key by default, and a policy can require it. Storing: encrypted in the vault. Backing up: included in the appliance backup. Retrieving: only the roles you allow can download a key. Transmitting: encrypted to the service agent. Revoking: with the CA through ACME or the CA's API. The audit log shows each step. Professional completes the cryptography policy with your settings.
Paragraph 4: "Financial entities shall create and maintain a register for all certificates and certificate-storing devices for at least ICT assets supporting critical or important functions. Financial entities shall keep that register up to date."	The inventory is the register: each certificate with its CA, key type, expiry and every server, service and device it is installed on. Discovery finds certificates on your network that you did not know about. The register is kept up to date with every renewal and installation.
Paragraph 5: "Financial entities shall ensure the prompt renewal of certificates in advance of their expiration."	Automatic renewal before expiry, at the time recommended by the CA (ARI, RFC 9773), and the new version is installed everywhere the certificate is used. If a renewal fails, you are notified.

Paragraphs 2 and 3 (protecting the keys and replacing them in the event of loss or compromise) are covered by the vault and by the ability to renew a certificate with a new key and install it everywhere at once.

DORA Articles 28 to 30: where to find the answer

The section numbers are the same on the page and in the PDF. Whether the service supports a critical or important function is for you to assess.

DORA	Requirement	Answer
Art. 28(1) and (2)	General principles: managing ICT third-party risk	Sections 5 (supplier assessment and the key in Cloud) and 11 (residual risks).
Art. 28(3)	Register of information	Section 9 (the register under ITS 2024/2956).
Art. 28(4) and (5)	Assessment before entering into an agreement and information security at the supplier	Sections 4 (FairSSL as a supplier), 6 (cryptography) and 8 (development and vulnerabilities).
Art. 28(7) and (8)	Termination and exit strategy	Sections 4 (incidents and contract) and 7 (exit).
Art. 29	Preliminary assessment of ICT concentration risk at entity level	Sections 3 (sub-processors) and 7 (exit and concentration risk).
Art. 30	Key contractual provisions	Section 4 (incidents and contract): the terms and the data processing agreement.

The register of ICT suppliers

Information for your register of information under Implementing Regulation (EU) 2024/2956.

Field	sslbrain
Legal name	FairSSL A/S
Identification	CVR no. 33075782 (VAT no. DK33075782). FairSSL does not have an LEI.
Country	Denmark. Åbrovej 29, 8586 Ørum Djurs.
Type of ICT service	Certificate management software running on your systems (appliance and service agents), and sslbrain Cloud (EU) as a service: licensing, issuance through CAs and ACME, AutoDNS and relaying encrypted messages.

Field	sslbrain
Where data is stored	Appliance: on your systems. sslbrain Cloud (EU): in the EU by the sub-processors in section 3.
Where data is processed	The same locations.
Sub-processors	UpCloud, OVHcloud, mailbox.org, Microsoft 365, Lettermint. Purposes and countries in section 3.
Certificate authorities (independent controllers)	DigiCert, Inc. (USA; DPF) for certificates from DigiCert. Let's Encrypt (Internet Security Research Group, USA) and Google Trust Services (USA) for free certificates. The CA follows the certificate profile you choose.
Critical or important function	Your assessment.

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

The ten measures in Article 21: what the product helps you with, our own controls, and what you do yourself. NIS2 does not approve suppliers; you assess them.

Article 21(2)	What the product helps you with	Our own controls	What you do
a) Risk analysis and information system security policies	An overview of all certificates, where they are installed and when they expire. Policies set in one place: who can download private keys, which domains can have certificates, manual or automatic updates. Professional: a risk worksheet completed with your settings.	The controls are mapped to ISO/IEC 27001:2022 Annex A and CIS Controls v8.1.	Your overall risk assessment. Approve and review the policies.
b) Incident handling	Alerts for failures and expiry. A new version of a certificate is installed everywhere it is used. The audit log shows what happened. Professional: an incident procedure with the Article 23 deadlines.	We notify the customer without undue delay and at the latest within 48 hours if a security incident has affected the customer's data or the service.	Assess and report significant incidents: early warning within 24 hours, incident notification within 72 hours and a final report no later than one month after the notification.
c) Business continuity, backup management and crisis management	Backup and restoration of the appliance. The 12 backup words unlock it without Cloud. Profiles with multiple CAs in order. Installed certificates work even if Cloud does not respond (section 7).	sslbrain Cloud (EU) is hosted in the EU by the sub-processors in section 3. Backups are always stored in one or more EU countries, separate from the country where the backup is taken.	Back up the appliance, and store backup files and backup words outside it. Practise a restore.
d) Supply chain security	Everything that runs on your systems is signed and has readable code. Sections 5 and 11 describe what FairSSL and Cloud can and cannot do.	Sub-processors from a single list (section 3). You can object within 30 days of the notice.	Assess sslbrain and the CAs you use as suppliers.
e) Security in acquisition, development and maintenance, including vulnerabilities	Signed versions; a version that cannot be verified will not start. Manual or automatic updates. Security notices and security.txt.	Updates to the appliance, service agents and deployment agents are signed with a hardware key. Security updates to systems and dependencies are installed continuously.	Choose how to update and install security updates.

Article 21(2)	What the product helps you with	Our own controls	What you do
f) Assessing the effectiveness of measures	An audit log with a hash chain and chain verification, export for a selected period. Professional: the NIS2 package, signed by the appliance.	The controls are mapped to ISO/IEC 27001:2022 Annex A and CIS Controls v8.1, and this documentation is versioned.	Review the documentation with your auditor.
g) Cyber hygiene and cybersecurity training	Certificates are renewed automatically before expiry and as recommended by the CA (ARI), so shorter lifetimes (200, 100 and 47 days) do not create manual work.	Security updates to systems and dependencies are installed continuously.	Train your staff.
h) Cryptography and encryption	Private keys are generated and remain On-Premise. Vault: XChaCha20-Poly1305 with 256 bits. Messages to service agents: AES-256-GCM. Versions: ECDSA P-384. Professional: a cryptography policy under Commission Implementing Regulation (EU) 2024/2690, point 9.2 of the Annex, completed with your settings.	TLS 1.2 and 1.3 with hybrid post-quantum key exchange on Cloud (section 6).	Approve the cryptography policy. Choose key types in your certificate profiles.
i) Human resources security, access control policies and asset management	Roles: Free has Owner, Basic has Owner and Administrator, Professional and Enterprise have all four (Owner, Administrator, Operator, Viewer). AD login on Professional and above. Private key downloads are controlled by role and limited per hour. An inventory of servers, services and certificates.	Administrative access is limited to key personnel with role-based access control (RBAC) and least privilege.	Assign roles and remove users who leave.
j) Multi-factor authentication and secured communication	Two-factor authentication (TOTP) can be enabled per user when logging in through sslbrain Cloud. Login with a local password or AD login on the appliance has no two-factor authentication. Downloading private keys and backups requires a fresh login confirmation, valid for 5 minutes. Messages to service agents are encrypted end to end.	Messages to service agents are signed and encrypted end to end; the appliance and Cloud speak TLS 1.2 and 1.3.	Enable two-factor authentication for each user in Cloud. If you require two-factor authentication, use only Cloud login on the appliance.

11. Residual risks and mitigations

Residual risk	Mitigation
Cloud plus a copy of the data disk or a backup unlocks the private keys as long as Cloud holds the key that locks the copy.	Protect the data disk and backups as you would private keys. Downloaded backups are encrypted with your password. Cloud does not hold the master key, and replaced keys are deleted after 7 days.

Residual risk	Mitigation
A snapshot of the running virtual machine that includes memory contains the unencrypted master key.	Take snapshots without memory, and protect snapshots as you would private keys. Swap is disabled on the appliance.
Cloud controls whether the vault can be unlocked.	The 12 backup words always unlock it, including a locked appliance, without Cloud.
AutoDNS: whoever controls Cloud can obtain certificates for the names pointing to AutoDNS.	CAA records with accounturi, Certificate Transparency monitoring, and AutoDNS only for the names that need it.
If you choose to store a DNS API key in Cloud, whoever controls Cloud can change DNS in that zone.	Keep the key in the appliance, where it goes through dns-proxy.sslbrain.com without Cloud seeing it. Use a key that can only write _acme-challenge where the provider offers this.
The appliance's TLS key, identity key and Cloud token are stored unencrypted on the data disk and in every backup, protected by file permissions.	Protect the data disk. Downloaded backups are encrypted with your password.
The audit log is hash-chained, so changes can be detected but not prevented: whoever has full access to the appliance can rewrite it.	Chain verification on the appliance. On Professional and above, the latest hash in the chain is stored in Cloud every hour, and every row is sent to your SIEM using syslog over TLS, so a rewritten log is detected outside the appliance.
A signed but malicious update.	Signing requires a physical hardware key. Choose manual updates if you want to review each version first. The code is readable.
Messages via Cloud: Cloud sees who, when and how much, not the content.	Connect service agents directly to the appliance where your network allows it.
Concentration: Cloud is a single supplier for licensing, issuance through Cloud and messages.	Local ACME source, DNS API keys in the appliance, multiple CAs in order and directly connected service agents (section 7).

12. Completed supplier questionnaire

Answers to the questions in a supplier assessment.

Question	Answer
Legal basis	The NIS2 Directive (EU) 2022/2555, in Denmark the NIS 2 Act (Act no. 434 of 6 May 2025). Financial entities: DORA (EU) 2022/2554 and RTS (EU) 2024/1774. Personal data: GDPR Articles 28 and 32 in the data processing agreement.
Supplier	FairSSL A/S, CVR no. 33075782, Denmark. Product: sslbrain (On-Premise appliance and sslbrain Cloud (EU)).
Where is the service hosted, and in which country?	sslbrain Cloud (EU) is hosted in the EU by the sub-processors in section 3. The appliance runs on your systems.
What data does the supplier process?	In Cloud: account, licence, the key to the appliance vault, accounts with CAs, DNS API keys if you choose, certificate requests for certificates from Cloud, notifications sent through Cloud, and counts and versions from the appliance. Private keys, certificates, inventory and the audit log are stored in the appliance (section 2).
Does the supplier have access to your systems?	No. No connections into your network. SSH access for FairSSL support can only be enabled from the appliance's local console, for 24 hours.
Administrative access at the supplier	Administrative access is limited to key personnel with role-based access control (RBAC) and least privilege.
Encryption at rest	XChaCha20-Poly1305 with 256 bits in the appliance vault; downloaded backups encrypted with your password.

Question	Answer
Encryption in transit	HTTPS with TLS 1.2 and 1.3 on the appliance and Cloud, TLS 1.3 with X25519MLKEM768 (measured 25-10-2026). Messages to service agents are also signed and encrypted with AES-256-GCM.
Access control and MFA	Roles (Owner, Administrator, Operator, Viewer), AD login on Professional and above, two-factor authentication per user when logging in through sslbrain Cloud (not with a local password or AD login), fresh confirmation before downloading private keys.
Logging	Hash-chained audit log in the appliance; export (CSV, JSON) and SIEM using syslog over TLS on Professional and above.
Incident notification	We notify the customer without undue delay and at the latest within 48 hours if a security incident has affected the customer's data or the service. Security notices at sslbrain.com/en/security-notices/.
Vulnerability handling	Report to info@fairssl.dk (security.txt). Security updates to systems and dependencies are installed continuously. Ubuntu security updates are installed automatically on the appliance.
Change management	Updates to the appliance, service agents and deployment agents are signed with a hardware key, and the appliance installs only updates with a valid signature.
Secure development	Signing with a physical hardware key; a version that cannot be verified will not start; readable code. sslbrain is developed in line with the Cyber Resilience Act.
Certification	FairSSL does not hold an ISO 27001 certification. The controls are mapped to ISO/IEC 27001:2022 Annex A and CIS Controls v8.1.
Insurance	FairSSL A/S holds general liability, product liability and professional liability insurance for IT companies with If.
Sub-processors	UpCloud, OVHcloud, mailbox.org, Microsoft 365, Lettermint. List: sslbrain.com/en/nis2/#sub-processors. Objection within 30 days of the notice.
Exit	Keys, certificates and data in the appliance belong to you and stay with you; installed certificates work until expiry. Section 7 describes outages, restarts, an expired subscription and a supplier that is gone. Personal data in Cloud is deleted from active systems within 30 days.
Data processing agreement	Created for your account in sslbrain Cloud.
Security contact	info@fairssl.dk

13. Frequently asked questions

Is sslbrain a supplier you need to assess?

Yes. Article 21(2)(d) and (3) of the NIS2 Directive and DORA Article 28 ask you to assess your ICT suppliers. The PDF has what you need: what FairSSL and sslbrain Cloud can and cannot do, exit, residual risks, the register and a completed supplier questionnaire.

Does the documentation cover DORA?

Yes. It quotes RTS 2024/1774 Article 7(1), (4) and (5) and shows how inventory, automatic renewal, the vault, a new key on renewal and revocation cover them. It includes the register under ITS 2024/2956 and a table covering DORA Articles 28 to 30.

What happens if FairSSL disappears?

Keys, certificates and data remain on your systems, installed certificates work, and the appliance keeps running. After a restart, the 12 backup words unlock it. Section 7 describes each situation and what requires Cloud today.

How long is the audit log kept?

On the appliance according to your plan: Free 30 days, Basic 90 days, Professional 2 years and Enterprise 7 years. If you need to keep it longer, export it or send it to your SIEM.

Which export formats are available?

CSV and JSON on Professional and above. Each event includes the time, user, action, object, IP address, values before and after, and its position in the hash chain.

Can FairSSL access your private keys?

No. Your private keys are generated and stored encrypted in your own appliance and its backup, and are sent end-to-end encrypted to the servers they are installed on. FairSSL and sslbrain Cloud have no copy of them. The keys can only be opened with the encrypted data plus either your 12 backup words, which only you know, or the rotating key that sslbrain Cloud issues to your appliance. Otherwise they can only be exported in the appliance by a user with the right to export keys, who must first confirm their identity again.

Do you need more detail?

If you are subject to rules that require more than this page and our completed supplier questionnaire, you can apply for access to more detailed documentation at info@fairssl.dk. We assess each application individually.

Contact

Questions about this documentation go to FairSSL A/S at:

info@fairssl.dk