NIS2- og DORA-dokumentation

Det, jeres leverandørvurdering efter NIS2 eller DORA skal bruge om sslbrain, for virksomheder i hele EU. Fra Professional laver appliancen også jeres egen dokumentation.

sslbrain: dokumentation til jeres leverandørvurdering efter NIS2 og DORA

Version 1.6
Dato 06-11-2026

Støtte til jeres arbejde med NIS2 og DORA, ikke juridisk rådgivning.

Gælder for sslbrain på datoen ovenfor. Den nyeste udgave ligger altid på sslbrain.com/nis2/.

FairSSL A/S, udgiver af sslbrain

Indhold

1. Tjenesten og vores rolle
2. Data, og hvor de ligger
3. Underleverandører til jeres register
4. Drift: ændringer, adgang, opdateringer og hændelser
5. Kontroller i produktet
6. Nøgler og kryptografi
7. Exit og koncentrationsrisiko
8. Ekstern kontrol, certificering og forsikring
9. DORA
10. NIS2 artikel 21, stk. 2, litra a-j
11. Rest-risici og hvad der dæmper dem
12. Udfyldt leverandørskema
13. Ofte stillede spørgsmål

1. Tjenesten og vores rolle

Om sslbrain på én side

Hvad den gør	Henter, fornyer og installerer TLS-certifikater på jeres servere, load balancere og firewalls, og viser, hvor hvert certifikat sidder, og hvornår det udløber.
Hvor nøgler og data ligger	On-Premise i appliancen hos jer: private nøgler (laves på appliancen og ligger krypteret i vaulten), certifikater, installationsplaner, revisionslog og indstillinger.
Hvad sslbrain Cloud (EU) har	Jeres konto og licens, en nøgle til appliancens vault (afsnit 5), konti hos CA'erne og, hvis I vælger det, DNS-API-nøgler. Cloud hostes i EU hos underleverandørerne i afsnit 3.
Hvad der går ud af netværket	Kun forbindelser, appliancen selv åbner. Over HTTPS: til cloud.sslbrain.com, acme.sslbrain.com, registry.sslbrain.com og dns-proxy.sslbrain.com, og til de CA'er og DNS-udbydere, I vælger. Desuden DNS-opslag hos 1.1.1.1, 8.8.8.8 og 9.9.9.9 (port 53 og DNS over HTTPS), Ubuntu's sikkerhedsopdateringer fra archive.ubuntu.com (port 80) og tidssynkronisering (NTP). Appliancens egen firewall tillader kun disse. Til Cloud sendes antal og versioner (servere, certifikater, installationsplaner, service-agenter, diskforbrug), CSR'er for certifikater fra Cloud, og diagnostik kun, hvis I slår det til. Aldrig private nøgler.
Hvad der kommer ind	Ingen forbindelser udefra. Appliancens webflade svarer kun på jeres eget netværk. Appliancen og service-agenterne åbner kun forbindelser udad, og hverken FairSSL eller Cloud kan logge ind på appliancen.

NIS2, DORA og de andre rammer

- NIS2 er et EU-direktiv, og hvert land har sin egen lov. I Danmark er det NIS 2-loven (lov nr. 434 af 6. maj 2025), som trådte i kraft 1. juli 2025. Artiklerne her er direktivets, så dokumentationen kan bruges i hele EU.
- Finansielle virksomheder følger DORA, forordning (EU) 2022/2554, som går forud for NIS2, hvor den dækker det samme (NIS2 artikel 4).
- Kunder, der selv er digital infrastruktur eller MSP, følger desuden gennemførelsesforordning (EU) 2024/2690.
- FairSSL er ikke selv omfattet af NIS2. Dokumentationen findes for at understøtte jeres forpligtelser i leverandørkæden: NIS2 artikel 21, stk. 2, litra d, og stk. 3, og DORA artikel 28 til 30.
- De samme kontroller dækker GDPR artikel 28 og 32 (databehandleraftalen og behandlingssikkerhed).
- FairSSL har ikke en ISO 27001-certificering. Kontrollerne er kortlagt til ISO/IEC 27001:2022 bilag A og CIS Controls v8.1.
- sslbrain udvikles efter Cyber Resilience Act, forordning (EU) 2024/2847.

- NIS2-direktivet (EU) 2022/2555: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/dan
- DORA, forordning (EU) 2022/2554: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/dan
- RTS (EU) 2024/1774 om IKT-risikostyring: https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj/dan
- ITS (EU) 2024/2956 om informationsregistret: https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj/dan
- Gennemførelsesforordning (EU) 2024/2690: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/dan
- Cyber Resilience Act, forordning (EU) 2024/2847: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/dan

2. Data, og hvor de ligger

Det meste er certifikatdata, som i forvejen er offentlige i Certificate Transparency-logs. Persondata er kun fakturering, kontaktpersoner og login. Data om jeres interne miljø bliver hos jer. At Cloud modtager så lidt, er en kontrol i sig selv (dataminimering, NIS2 artikel 21, stk. 2, og GDPR artikel 25 og 32).

Data	Hvor det ligger	Klassifikation
Private nøgler	Laves på appliancen og ligger krypteret i vaulten hos jer. Sendes aldrig til Cloud.	Fortroligt
Adgange: serverlogins, DNS-API-nøgler, CA-konti på appliancen	Krypteret i appliancens vault. En DNS-API-nøgle ligger kun i Cloud, hvis I selv vælger det til ACME fra Cloud.	Fortroligt

Data	Hvor det ligger	Klassifikation
Interne certifikater, servernavne, IP-adresser og software	I appliancens inventar hos jer. Kun hvis I slår diagnostik til, sendes udvalgte oplysninger (fx servernavn, IP-adresse og styresystem) til FairSSL's support.	Internt
Antal og versioner	Cloud: antal servere, certifikater, installationsplaner og service-agenter, versioner og diskforbrug. Bruges til licens og drift.	Internt
CSR'er for certifikater fra Cloud	Cloud og den CA, I vælger: navnene i certifikatet og valideringen (AutoDNS eller DNS-API-nøgle).	Offentligt
Notifikationer, I sender gennem Cloud	Cloud og mailtjenesten Lettermint: emne og tekst, som kan nævne servernavne og certifikater. Lettermint sletter beskedernes indhold, modtagere og metadata automatisk 28 dage efter afsendelse. Notifikationer over jeres egen SMTP-server eller webhooks går ikke gennem Cloud.	Internt
Beskeder til service-agenter via Cloud	Krypteret hele vejen mellem appliance og service-agent. Cloud ser hvem, hvornår og hvor meget, ikke indholdet.	Fortroligt
Revisionslog	I appliancen. Fra Professional gemmes kædens seneste hash i Cloud hver time.	Internt
Konto, login, kontaktpersoner og fakturering	sslbrain Cloud (EU) og underdatabehandlerne i afsnit 3.	Persondata

3. Underleverandører til jeres register

- sslbrain Cloud hostes i EU hos underleverandørerne i tabellen.
- Certifikatudstedere (CA'er): Selvstændige dataansvarlige for udstedelse, validering og Certificate Transparency-logning af de certifikater, kunden bestiller. CA'en følger den certifikatprofil, kunden vælger.
- Navnene i et certifikat er offentlige: CA'en skriver dem i Certificate Transparency-logs.

Leverandør	Ejerskab	Data ligger i	Bruges til
UpCloud	Finland	EU	Server- og databasehosting
OVHcloud	Frankrig	EU	Server- og databasehosting
mailbox.org	Tyskland	EU	E-mail
Microsoft 365	USA	EU	E-mail og kontorsystemer
Lettermint	Holland	EU	Systemmails

Kunden kan gøre indsigelse inden 30 dage efter varslet ved at skrive til info@fairssl.dk.

Ændringslog

- Ingen ændringer endnu.

4. Drift: ændringer, adgang, opdateringer og hændelser

FairSSL som leverandør

- Ændringer: Opdateringer til appliance, service-agenter og deploy-agenter signeres med en hardwarenøgle, og appliancen installerer kun opdateringer med gyldig signatur.
- Adgang: Administrativ adgang er begrænset til nøglepersoner med rollebaseret adgang (RBAC) og mindst mulige rettigheder.

- Opdateringer: Sikkerhedsopdateringer til systemer og afhængigheder installeres løbende.
- Hændelser: Vi varsler kunden uden unødig forsinkelse og senest inden for 48 timer, hvis en sikkerhedshændelse har påvirket kundens data eller tjenesten. Det står også i vilkårene og databehandleraftalen. En sårbarhed, der er lukket uden at have påvirket kundens data eller tjenesten, er ikke en hændelse (NIS2 artikel 6, nr. 6 og 15).
- sslbrain udvikles efter Cyber Resilience Act.

Hændelser og kontrakt

- Vi varsler kunden uden unødig forsinkelse og senest inden for 48 timer, hvis en sikkerhedshændelse har påvirket kundens data eller tjenesten (vilkårene, afsnit 16, og databehandleraftalen, afsnit 8).
- Brud på persondatasikkerheden: FairSSL informerer jer uden ugrundet ophold og senest 48 timer efter at være blevet bekendt med bruddet (databehandleraftalen, afsnit 8).
- Sikkerhedssager, der kræver noget af jer, får kontoens sikkerhedsmodtagere på mail, og alle står på sslbrain.com/sikkerhedsmeddelelser/.
- Underleverandører: en ny eller udskiftet underleverandør varsles pr. mail og i ændringsloggen i afsnit 3. I kan gøre indsigelse inden for 30 dage efter varslet, og findes der ingen løsning, kan I opsige de berørte tjenester uden binding.
- Ændringer, der kræver noget af jer, varsles mindst 30 dage før.
- Når I stopper: abonnementet løber til udgangen af den betalte periode, derefter Free. Lukning af Cloud-kontoen påvirker ikke data, der allerede ligger hos jer.
- Personoplysninger, FairSSL behandler for jer, slettes eller returneres ved ophør. Sletning fra aktive systemer sker inden for 30 dage; backups slettes i den løbende rotation.
- FairSSL's samlede erstatningsansvar er begrænset til det, I har betalt de seneste 12 måneder.
- Vores varsling erstatter ikke jeres egne frister for væsentlige hændelser efter NIS2 artikel 23 eller DORA artikel 19: under NIS2 tidlig varsling inden 24 timer, underretning inden 72 timer og endelig rapport senest en måned efter underretningen.

5. Kontroller i produktet

Jeres leverandørvurdering af sslbrain

NIS2-direktivets artikel 21, stk. 2, litra d, og stk. 3 og DORA artikel 28 beder jer vurdere jeres IKT-leverandører. Tabellen viser, hvad FairSSL og sslbrain Cloud kan og ikke kan i jeres netværk, ved siden af en ACME-klient mod en offentlig CA.

	sslbrain	**En ACME-klient (fx Certbot mod Let's Encrypt)**
Kode fra leverandøren hos jer	Appliance, service-agenter og integrationer kører hos jer. De er låst til det, FairSSL har signeret, og til det, I selv signerer med appliancens nøgle (afsnit 7), ligesom en ACME-klient kører det, den er bygget til.	ACME-klienten kører hos jer med de rettigheder, I giver den.
Styring fra leverandøren	Ingen kommandoer. Cloud kan ikke køre noget på appliancen eller service-agenterne. Det, Cloud kan: nægte oplåsning og låse appliancen (afsnit 5), og tilbyde en ny signeret version, som appliancen selv installerer, hvis I har valgt automatisk opdatering.	Ingen kommandoer.

	sslbrain	En ACME-klient (fx Certbot mod Let's Encrypt)
Opdateringer	Opdateringer til appliance, service-agenter og deploy-agenter signeres med en hardwarenøgle, og appliancen installerer kun opdateringer med gyldig signatur. En version, der ikke kan verificeres, starter ikke. Automatisk opdatering kan slås fra lokalt. Styresystemet under appliancen (Ubuntu LTS) henter kun Ubuntu's sikkerhedsopdateringer, signeret af Canonical, og genstarter ved behov kl. 03:00 UTC.	Afhænger af klienten. Certbot, installeret som anbefalet, opdaterer sig selv.
Udstedelse til jeres domæner	Udstedelse via Cloud kræver, at navnet valideres med AutoDNS (én CNAME pr. navn) eller med en DNS-API-nøgle, I har gemt i Cloud. Navne, der valideres med en DNS-API-nøgle i appliancen, kan Cloud ikke udstede til. I vælger pr. navn. CAA-poster begrænser desuden, hvilke CA'er og konti der må udstede.	Den, der styrer ACME-kontoen og valideringen, kan få udstedt certifikater til jeres navne. CAA-poster begrænser det på samme måde.
Stop af fornyelser	Stopper Cloud eller jeres abonnement, virker de installerede certifikater, til de udløber, og data i appliancen er jeres og bliver hos jer. Afsnit 7 beskriver hver situation.	Stopper CA'en eller klienten, virker de installerede certifikater, til de udløber.
Adgang ind i jeres netværk	Ingen. Kun med adgang til appliancens lokale konsol kan man åbne SSH til FairSSL's support til fejlfinding i 24 timer. Også da kræver det adgang til appliancen på jeres netværk.	Ingen.
DNS-API-nøgler	Gemmes krypteret i appliancens vault, ét sted i jeres netværk. Kaldene til DNS-udbyderen går gennem en krypteret forbindelse, som Cloud ikke kan læse. Til ACME fra Cloud kan I vælge at gemme nøglen i Cloud.	Gemmes på hver server, der udsteder certifikater. certbot, acme.sh og lego gemmer den som klartekst i en fil eller miljøvariabel. win-acme krypterer den som standard med serverens egen Windows-nøgle.

Nøglen til vaulten i sslbrain Cloud

Sikkerhedsgodkendere spørger først til den. Her er præcis, hvad den kan og ikke kan.

- Appliancens vault krypterer private nøgler med en hovednøgle på 256 bit, som laves på appliancen og aldrig sendes til Cloud.
- Hovednøglen ligger kun krypteret på datadisken: kopier låst med nøgler fra Cloud (den nuværende og de senest udskiftede) og én kopi låst med de 12 backup-ord. Mens appliancen kører, ligger den åbne hovednøgle i hukommelsen, ikke på disken.
- Cloud laver nøglen tilfældigt (32 byte) for hver installation og gemmer den krypteret.
- Nøglen udskiftes ved hver oplåsning gennem Cloud og hver 6. time.
- Cloud alene dekrypterer intet: Cloud har hverken hovednøglen eller jeres private nøgler.
- Cloud plus en kopi af datadisken eller en backup åbner nøglerne, så længe Cloud stadig har den nøgle, der låser kopien. Beskyt datadisk og backup som private nøgler.
- Cloud styrer vaultens tilgængelighed, ikke dens indhold: Cloud kan nægte oplåsning eller låse appliancen. De 12 backup-ord åbner altid, også en låsning, uden Cloud. Appliancen er så åben til næste genstart; det, der går gennem Cloud, står stille, og nødkontoen kan ikke hente private nøgler eller backup.
- Svarer Cloud ikke, kører en åben vault videre. Efter en genstart låser Cloud eller backup-ordene op.
- Kører to kopier af samme installation, vælger I i Cloud, hvilken der fortsætter. FairSSL's support kan også godkende en overtagelse fra Cloud, og kontoens modtagere får en mail. Den anden kopi låses.
- Efter en gendannelse fra backup beder Cloud om jeres godkendelse (eller FairSSL's support), før den låser op. De 12 backup-ord åbner straks. Cloud sletter udskiftede nøgler, når de er over 7 dage gamle og ikke

blandt de 10 nyeste, så en ældre backup eller diskkopi åbner kun med backup-ordene.

NIS2-pakken fra jeres appliance (Professional)

Jeres egen dokumentation, signeret af appliancen: revisionslog med kædekontrol, inventar, fornyelser og fejl, politikker på dagen, udfyldt kryptografipolitik, risikoark og hændelsesprocedure. Fra Professional laver appliancen NIS2-pakken: én signeret fil for det tidsrum, I vælger, klar til revisor.

- Revisionsloggen med hashes og resultatet af kædekontrollen.
- Certifikatinventar på dagen: navne, CA, nøgletype og -størrelse, udløb og hvor hvert certifikat sidder.
- Fornyelser og fejl i tidsrummet.
- Politikker på dagen: roller og brugere, hvem må hente private nøgler, domænelås og opdateringsform.
- Versioner af appliance og service-agenter, og om signaturerne er gyldige.
- Kryptografipolitik efter Kommissionens gennemførelsesforordning (EU) 2024/2690, bilagets punkt 9.2, udfyldt med jeres indstillinger.
- Risikoark, hændelsesprocedure med fristerne i artikel 23 og opdeling af ansvar mellem jer og FairSSL.
- Som PDF og som filer, I kan redigere i Word og regneark.
- Hver række i revisionsloggen sendes til jeres SIEM med syslog over TLS, og kædens seneste hash gemmes i sslbrain Cloud.

Forordning 2024/2690 binder kun de enheder, der står i dens artikel 1 (fx cloud, DNS, MSP, datacentre og tillidstjenesteudbydere). For andre er den en god reference.

6. Nøgler og kryptografi

- Data i appliancen: private nøgler og andre hemmeligheder krypteres med XChaCha20-Poly1305 og en nøgle på 256 bit.
- De 12 backup-ord: 96 bit, gjort til nøgle med Argon2id.
- Beskeder mellem appliance og service-agenter: signeret med ECDSA (P-384, eller P-256 efter service-agentens nøgle) og krypteret med AES-256-GCM (JWE, ECDH-ES). Det gælder også beskeder via sslbrain Cloud (EU), som ikke kan læse dem.
- Appliance-versioner og integrationer: signeret med ECDSA P-384 og SHA-384.
- Hentede backup-filer: krypteret med XChaCha20-Poly1305 og en nøgle fra jeres adgangskode (Argon2id). Adgangskoden er påkrævet og mindst 12 tegn.
- Certifikatnøgler: laves på appliancen, RSA 2048 til 4096 bit eller ECDSA P-256 og P-384. Profilen og de servere, certifikatet skal ud på, bestemmer, hvilke typer der er tilladt. Certifikater, I selv uploader, beholder deres nøgle.
- Appliancens webflade og Cloud-tjenesterne taler TLS 1.2 og 1.3 og afviser TLS 1.0 og 1.1 (målt 25-10-2026).

Målt 25-10-2026: TLS 1.3 og hybrid post-kvante-nøgleudveksling (X25519MLKEM768).

Del	TLS 1.3	X25519MLKEM768
Appliancens webflade	Ja	Ja
sslbrain Cloud (cloud.sslbrain.com)	Ja	Ja
acme.sslbrain.com, registry.sslbrain.com, dns-proxy.sslbrain.com	Ja	Ja
Linux-service-agenten (bruger serverens OpenSSL)	Ja	Ja med OpenSSL 3.5 eller nyere (fx Debian 13), ellers X25519
Windows-service-agenten (bruger Windows' egen TLS)	Fra Windows Server 2022	Fra Windows Server 2025, når Windows slår det til

7. Exit og koncentrationsrisiko

Hvad der sker, når sslbrain Cloud eller FairSSL ikke er der. Private nøgler, certifikater og data ligger On-Premise hos jer i alle fire situationer, og installerede certifikater virker uden Cloud: det er filer på jeres servere, som intet i sslbrain fjerner, når Cloud er væk.

- Lokal ACME-kilde (fra Professional): appliancen udsteder direkte hos CA'en, fx Let's Encrypt eller jeres egen ACME-CA, uden om Cloud. Validering med AutoDNS eller en DNS-API-nøgle i Cloud kræver stadig Cloud; en DNS-API-nøgle i appliancen gør ikke.

- Tilkøbet Lokal ACME-server (Enterprise) er noget andet: en ACME-server på appliancen, som jeres interne ACME-klienter bruger, og som formidler til jeres egen CA eller en ekstern ACME-CA.
- Flere CA'er i rækkefølge: en profil kan have flere certifikatkilder, og fejler den første, tager den næste over.
- Jeres egen signeringsnøgle: appliancen har sin egen nøgle, som laves på appliancen. Sætter I dens offentlige del lokalt på en server med service-agent, kører service-agenten jeres egne agenter og jeres egne ændringer af agenter, signeret af appliancen. Nøglen kan ikke godkende FairSSL's pakker eller opdateringer.
- Service-agenter kan installeres manuelt på serveren fra en version, I selv bygger eller får (MSI på Windows, pakke eller kildekode på Linux). Tilmeldingen sker mod jeres appliance.
- Kører appliancen i Docker, kan I selv hente og opdatere imaget. Signaturen kan kontrolleres lokalt med sslbrain-sigverify, før imaget startes.
- Som standard åbnes appliancen via Cloud, uden Cloud med de 12 backup-ord. Vil I helt uden Cloud, kan I købe den 100 % lokale On-Premise-udgave (tilkøbet Offline drift).
- Det kræver Cloud i dag: tilmelding og aktivering af appliancen, login via Cloud, licensfornyelse, oplåsning efter genstart (ellers backup-ordene), udstedelse via Cloud med AutoDNS, DNS-API-nøgler i Cloud og dns-proxy.sslbrain.com, tilmelding af service-agenter via Cloud og beskeder via Cloud, opdateringer og integrationer fra kataloget, notifikationer gennem Cloud, revisionsloggens hash i Cloud og koden til konsollens root-shell.

Situation	Det virker	Det står stille
Cloud svarer ikke (udfald)	Appliancen kører videre med åben vault. Brugere logger ind med den adgangskode, appliancen kender. Med Lokal ACME-kilde og DNS-API-nøgler i appliancen fornyes og installeres certifikater direkte hos CA'en. Service-agenter, der er forbundet direkte, og notifikationer over jeres egen SMTP-server eller webhooks virker.	Udstedelse via Cloud og AutoDNS, beskeder til service-agenter via Cloud, login via Cloud, opdateringer, notifikationer gennem Cloud og licensfornyelse. Det genoptages, når Cloud svarer igen.
Genstart, mens Cloud er væk	Som standard låses vaulten op via Cloud. Uden Cloud låser I op med de 12 backup-ord, og appliancen er åben til næste genstart. Derefter som ved udfald.	Det samme som ved udfald. Nødkontoen kan ikke hente private nøgler eller backup.
Abonnementet er udløbet	I får besked senest 28 dage før udløb. Appliancen fortsætter som Free: de ældste servere op til Free's grænse får stadig fornyelser og installationer. Øvrige servere bliver i inventaret, beholder deres nøgler og opdages stadig.	Fornyelse og installation på servere ud over Free's grænse, og funktioner og moduler, som Free ikke har.
FairSSL er væk for altid	Nøgler, certifikater og inventar er jeres og bliver hos jer. Appliancen kører videre, og de 12 backup-ord låser op efter genstart. Lokal ACME-kilde fornyer direkte hos CA'en, til licensperioden udløber. Derefter fjerner appliancen selv Professional-modulerne, og Free fornyer via Cloud, så fornyelserne stopper; installerede certifikater virker til udløb. Skulle udviklingen af sslbrain nogensinde stoppe, gør vi softwaren fri som open source først. Koden er læsbar (source-available), og ACME er en åben standard (RFC 8555), så et skifte kræver ny konto hos den nye udbyder, validering og nye installationer.	Alt, der kræver Cloud (se listen nedenfor), opdateringer fra FairSSL, fornyelse af licensen og, når licensperioden er udløbet, fornyelse af certifikater.

8. Ekstern kontrol, certificering og forsikring

Udvikling og sårbarheder

- Opdateringer til appliance, service-agenter og deploy-agenter signeres med en hardwarenøgle, og

appliancen installerer kun opdateringer med gyldig signatur.
- Styresystemet under appliancen (Ubuntu LTS) installerer selv Ubuntu's sikkerhedsopdateringer og genstarter ved behov kl. 03:00 UTC.
- En version, der ikke kan verificeres, starter ikke, og den version, der kørte, startes igen. En integration, der ikke kan verificeres, erstatter ikke den installerede.
- I vælger manuel eller automatisk opdatering på appliancen.
- Koden er læsbar (source-available), så I eller en tredjepart kan gennemgå den.
- Sårbarheder meldes til info@fairssl.dk; kontakten står i sslbrain.com/.well-known/security.txt. Sikkerhedssager står på sslbrain.com/sikkerhedsmeddelelser/.
- Vi understøtter den nyeste og den forrige hovedversion og varsler mindst 90 dage, før en version ikke længere får sikkerhedsrettelser.

Certificering og forsikring

- FairSSL har ikke en ISO 27001-certificering. Kontrollerne er kortlagt til ISO/IEC 27001:2022 bilag A og CIS Controls v8.1.
- FairSSL A/S har hos If erhvervsansvars-, produktansvars- og professionel ansvarsforsikring for IT-virksomheder.

9. DORA

DORA og RTS 2024/1774, artikel 7

DORA, forordning (EU) 2022/2554, gælder for finansielle virksomheder og går for dem forud for NIS2 (NIS2 artikel 4). Kommissionens delegerede forordning (EU) 2024/1774 om IKT-risikostyring stiller i artikel 7 krav til krypteringsnøgler og certifikater. Her er de tre stykker, der handler om certifikater, ordret, og hvordan sslbrain dækker dem.

RTS 2024/1774, artikel 7	Sådan dækker sslbrain det
Stk. 1: "Finansielle enheder inkluderer i den politik for forvaltning af krypteringsnøgler, der er omhandlet i artikel 6, stk. 2, litra d), krav om forvaltning af krypteringsnøgler gennem hele deres livscyklus, herunder generering, fornyelse, lagring, sikkerhedskopiering, arkivering, genfinding, overførsel, udrangering, tilbagekaldelse og destruktion af sådanne krypteringsnøgler."	Generering: nøglen laves på appliancen. Fornyelse: hver ny version får som standard en ny nøgle, og en politik kan kræve det. Lagring: krypteret i vaulten. Sikkerhedskopiering: med i appliancens backup. Genfinding: kun de roller, I tillader, kan hente en nøgle. Overførsel: krypteret til service-agenten. Tilbagekaldelse: hos CA'en via ACME eller CA'ens API. Revisionsloggen viser hvert trin. Professional udfylder kryptografipolitikken med jeres indstillinger.
Stk. 4: "Finansielle enheder opretter og vedligeholder et register over alle certifikater og alt udstyr til lagring af certifikater som minimum for IKT-aktiver, der understøtter kritiske eller vigtige funktioner. Finansielle enheder sørger for at ajourføre dette register."	Inventaret er registret: hvert certifikat med CA, nøgletype, udløb og hver server, tjeneste og enhed, det er installeret på. Opdagelse finder certifikater, I ikke kendte, på jeres netværk. Registret holdes ajour ved hver fornyelse og installation.
Stk. 5: "Finansielle enheder sørger for øjeblikkelig fornyelse af certifikater inden de udløber."	Automatisk fornyelse før udløb, på det tidspunkt CA'en anbefaler (ARI, RFC 9773), og den nye version installeres alle steder, certifikatet sidder. Fejler en fornyelse, får I besked.

Stk. 2 og 3 (beskyttelse af nøglerne og udskiftning ved tab eller kompromittering) dækkes af vaulten og af, at et certifikat kan fornyes med ny nøgle og installeres alle steder på én gang.

DORA artikel 28 til 30: hvor svaret står

Afsnitsnumrene er de samme på siden og i PDF'en. Om tjenesten understøtter en kritisk eller vigtig funktion, er jeres vurdering.

DORA	Krav	Svaret
Art. 28, stk. 1 og 2	Styring af IKT-tredjepartsrisiko	Afsnit 5 (leverandørvurdering og nøglen i Cloud) og 11 (rest-risici).
Art. 28, stk. 3	Informationsregister	Afsnit 9 (registret efter ITS 2024/2956).

DORA	Krav	Svaret
Art. 28, stk. 4 og 5	Vurdering før aftale og informationssikkerhed hos leverandøren	Afsnit 4 (FairSSL som leverandør), 6 (kryptografi) og 8 (udvikling og sårbarheder).
Art. 28, stk. 7 og 8	Opsigelse og exitstrategi	Afsnit 4 (hændelser og kontrakt) og 7 (exit).
Art. 29	Koncentrationsrisiko	Afsnit 3 (underleverandører) og 7 (exit og koncentrationsrisiko).
Art. 30	Centrale kontraktbestemmelser	Afsnit 4 (hændelser og kontrakt): vilkårene og databehandleraftalen.

Registret over IKT-leverandører

Oplysningerne til jeres informationsregister efter gennemførelsesforordning (EU) 2024/2956.

Felt	sslbrain
Juridisk navn	FairSSL A/S
Identifikation	CVR-nr. 33075782 (moms-nr. DK33075782). FairSSL har ikke en LEI.
Land	Danmark. Åbrovej 29, 8586 Ørum Djurs.
Type af IKT-tjeneste	Software til certifikathåndtering, der kører hos jer (appliance og service-agenter), og sslbrain Cloud (EU) som tjeneste: licens, udstedelse via CA'er og ACME, AutoDNS og formidling af krypterede beskeder.
Hvor data opbevares	Appliancen: hos jer. sslbrain Cloud (EU): i EU hos underleverandørerne i afsnit 3.
Hvor data behandles	De samme steder.
Underleverandører	UpCloud, OVHcloud, mailbox.org, Microsoft 365, Lettermint. Formål og land i afsnit 3.
Certifikatudstedere (selvstændigt dataansvarlige)	DigiCert, Inc. (USA; DPF) ved certifikater fra DigiCert. Let's Encrypt (Internet Security Research Group, USA) og Google Trust Services (USA) ved gratis certifikater. CA'en følger den certifikatprofil, I vælger.
Kritisk eller vigtig funktion	Jeres vurdering.

10. NIS2 artikel 21, stk. 2, litra a-j

De ti foranstaltninger i artikel 21: hvad produktet hjælper jer med, vores egne kontroller, og hvad I selv gør. NIS2 godkender ikke leverandører; I vurderer dem.

Artikel 21, stk. 2	Produktet hjælper jer med	Vores egne kontroller	I gør selv
a) Risikoanalyse og politikker for informationssikkerhed	Overblik over alle certifikater, hvor de sidder, og hvornår de udløber. Politikker sat ét sted: hvem må hente private nøgler, hvilke domæner der må få certifikater, manuel eller automatisk opdatering. Professional: risikoark udfyldt med jeres indstillinger.	Kontrollerne er kortlagt til ISO/IEC 27001:2022 bilag A og CIS Controls v8.1.	Jeres samlede risikovurdering. Godkend og gennemgå politikkerne.
b) Håndtering af hændelser	Advarsler ved fejl og udløb. En ny version af et certifikat installeres alle steder, det sidder. Revisionsloggen viser forløbet. Professional: hændelsesprocedure med fristerne i artikel 23.	Vi varsler kunden uden unødig forsinkelse og senest inden for 48 timer, hvis en sikkerhedshændelse har påvirket kundens data eller tjenesten.	Vurdér og indberet væsentlige hændelser: tidlig varsling inden 24 timer, underretning inden 72 timer og endelig rapport senest en måned efter.

Artikel 21, stk. 2	Produktet hjælper jer med	Vores egne kontroller	I gør selv
c) Driftskontinuitet, backup og krisestyring	Backup og gendannelse af appliancen. De 12 backup-ord åbner den uden Cloud. Profiler med flere CA'er i rækkefølge. Installerede certifikater virker, selv om Cloud ikke svarer (afsnit 7).	sslbrain Cloud (EU) hostes i EU hos underleverandørerne i afsnit 3. Backup gemmes altid i et eller flere EU-lande, adskilt fra det land, hvor backuppen tages.	Tag backup af appliancen, og opbevar backupfiler og backup-ord uden for den. Øv en gendannelse.
d) Forsyningskædes ikkerhed	Alt, der kører hos jer, er signeret og læsbar kode. Afsnit 5 og 11 siger, hvad FairSSL og Cloud kan og ikke kan.	Underleverandører fra én liste (afsnit 3). I kan gøre indsigelse inden for 30 dage efter varslet.	Vurdér sslbrain og de CA'er, I bruger, som leverandører.
e) Sikkerhed ved anskaffelse, udvikling og vedligeholdelse, herunder sårbarheder	Signerede versioner; en version, der ikke kan verificeres, starter ikke. Manuel eller automatisk opdatering. Sikkerhedsmeddelelser og security.txt.	Opdateringer til appliance, service-agenter og deploy-agenter signeres med en hardwarenøgle. Sikkerhedsopdateringer til systemer og afhængigheder installeres løbende.	Vælg opdateringsform, og installér sikkerhedsopdatering er.
f) Vurdering af foranstaltningerne s effektivitet	Revisionslog med hash-kæde og kædekontrol, eksport for et tidsrum. Professional: NIS2-pakken, signeret af appliancen.	Kontrollerne er kortlagt til ISO/IEC 27001:2022 bilag A og CIS Controls v8.1, og denne dokumentation er versioneret.	Gennemgå dokumentationen med jeres revisor.
g) Cyberhygiejne og uddannelse	Certifikater fornyes automatisk før udløb og efter CA'ens anbefaling (ARI), så kortere levetider (200, 100 og 47 dage) ikke giver manuelt arbejde.	Sikkerhedsopdateringer til systemer og afhængigheder installeres løbende.	Uddan medarbejderne.
h) Kryptografi og kryptering	Private nøgler laves og bliver On-Premise. Vault: XChaCha20-Poly1305 med 256 bit. Beskeder til service-agenter: AES-256-GCM. Versioner: ECDSA P-384. Professional: kryptografipolitik efter forordning 2024/2690, bilagets punkt 9.2, udfyldt med jeres indstillinger.	TLS 1.2 og 1.3 med hybrid post-kvante-nøgleudveksling på Cloud (afsnit 6).	Godkend kryptografipolitikken. Vælg nøgletyper i profilerne.
i) Personalesikkerh ed, adgangsstyring og forvaltning af aktiver	Roller: Free har Owner, Basic Owner og Administrator, Professional og Enterprise alle fire (Owner, Administrator, Operator, Viewer). AD-login fra Professional. Hentning af private nøgler styres pr. rolle og begrænses pr. time. Inventar over servere, tjenester og certifikater.	Administrativ adgang er begrænset til nøglepersoner med rollebaseret adgang (RBAC) og mindst mulige rettigheder.	Tildel roller, og fjern brugere, der stopper.

Artikel 21, stk. 2	Produktet hjælper jer med	Vores egne kontroller	I gør selv
j) Multifaktorautentificering og sikret kommunikation	To-faktor (TOTP) kan slås til pr. bruger ved login gennem sslbrain Cloud. Login med lokal adgangskode eller AD-login på appliancen har ingen to-faktor. Hentning af private nøgler og backup kræver ny bekræftelse af login, gyldig i 5 minutter. Beskeder til service-agenter er krypteret hele vejen.	Beskeder til service-agenter er signeret og krypteret hele vejen; appliance og Cloud taler TLS 1.2 og 1.3.	Slå to-faktor til for hver bruger i Cloud. Kræver I to-faktor, så brug kun Cloud-login på appliancen.

11. Rest-risici og hvad der dæmper dem

Rest-risiko	Hvad der dæmper den
Cloud plus en kopi af datadisken eller en backup åbner de private nøgler, så længe Cloud har den nøgle, der låser kopien.	Beskyt datadisk og backup som private nøgler. Hentede backups er krypteret med jeres adgangskode. Cloud har ikke hovednøglen, og udskiftede nøgler slettes efter 7 dage.
Et snapshot af den kørende virtuelle maskine med hukommelse indeholder den åbne hovednøgle.	Tag snapshots uden hukommelse, og beskyt snapshots som private nøgler. Swap er slået fra på appliancen.
Cloud styrer, om vaulten kan låses op.	De 12 backup-ord åbner altid, også en låsning, uden Cloud.
AutoDNS: den, der styrer Cloud, kan få udstedt certifikater til de navne, der peger på AutoDNS.	CAA-poster med accounturi, overvågning af Certificate Transparency, og AutoDNS kun for de navne, der skal bruge det.
Vælger I at lægge en DNS-API-nøgle i Cloud, kan den, der styrer Cloud, ændre DNS i den zone.	Lad nøglen blive i appliancen, hvor den går gennem dns-proxy.sslbrain.com, uden at Cloud ser den. Brug en nøgle, der kun må skrive _acme-challenge, hvor udbyderen tilbyder det.
Appliancens TLS-nøgle, identitetsnøgle og token til Cloud ligger ukrypteret på datadisken og i hver backup, beskyttet af filrettigheder.	Beskyt datadisken. Hentede backups er krypteret med jeres adgangskode.
Revisionsloggen er hash-kædet, så ændringer kan opdages, men ikke forhindres: den, der har fuld adgang til appliancen, kan skrive den om.	Kædekontrol på appliancen. Fra Professional gemmes kædens seneste hash i Cloud hver time, og hver række sendes til jeres SIEM med syslog over TLS, så en omskrevet log opdages uden for appliancen.
En signeret, men skadelig opdatering.	Signering kræver en fysisk hardware-nøgle. Vælg manuel opdatering, hvis I vil gennemgå hver version først. Koden er læsbar.
Beskeder via Cloud: Cloud ser hvem, hvornår og hvor meget, ikke indholdet.	Forbind service-agenterne direkte til appliancen, hvor netværket tillader det.
Koncentration: Cloud er én leverandør for licens, udstedelse via Cloud og beskeder.	Lokal ACME-kilde, DNS-API-nøgler i appliancen, flere CA'er i rækkefølge og direkte forbundne service-agenter (afsnit 7).

12. Udfyldt leverandørskema

Svar på de spørgsmål, en leverandørvurdering stiller.

Spørgsmål	Svar

Spørgsmål	Svar
Lovgrundlag	NIS2-direktivet (EU) 2022/2555, i Danmark NIS 2-loven (lov nr. 434 af 6. maj 2025). Finansielle virksomheder: DORA (EU) 2022/2554 og RTS (EU) 2024/1774. Persondata: GDPR artikel 28 og 32 i databehandleraftalen.
Leverandør	FairSSL A/S, CVR-nr. 33075782, Danmark. Produkt: sslbrain (appliance On-Premise og sslbrain Cloud (EU)).
Hvor hostes tjenesten, og i hvilket land?	sslbrain Cloud (EU) hostes i EU hos underleverandørerne i afsnit 3. Appliancen kører hos jer.
Hvilke data behandler leverandøren?	I Cloud: konto, licens, nøglen til appliancens vault, konti hos CA'erne, DNS-API-nøgler hvis I vælger det, CSR'er for certifikater fra Cloud, notifikationer sendt gennem Cloud, og antal og versioner fra appliancen. Private nøgler, certifikater, inventar og revisionslog ligger i appliancen (afsnit 2).
Har leverandøren adgang til vores systemer?	Nej. Ingen forbindelser ind i jeres netværk. SSH til FairSSL's support kan kun åbnes fra appliancens lokale konsol, i 24 timer.
Administrativ adgang hos leverandøren	Administrativ adgang er begrænset til nøglepersoner med rollebaseret adgang (RBAC) og mindst mulige rettigheder.
Kryptering af data i hvile	XChaCha20-Poly1305 med 256 bit i appliancens vault; hentede backups krypteret med jeres adgangskode.
Kryptering under transport	HTTPS med TLS 1.2 og 1.3 på appliance og Cloud, TLS 1.3 med X25519MLKEM768 (målt 25-10-2026). Beskeder til service-agenter desuden signeret og krypteret med AES-256-GCM.
Adgangsstyring og MFA	Roller (Owner, Administrator, Operator, Viewer), AD-login fra Professional, to-faktor pr. bruger ved login gennem sslbrain Cloud (ikke ved lokal adgangskode eller AD-login), ny bekræftelse før hentning af private nøgler.
Logning	Hash-kædet revisionslog i appliancen; eksport (CSV, JSON) og SIEM med syslog over TLS fra Professional.
Varsling ved hændelser	Vi varsler kunden uden unødig forsinkelse og senest inden for 48 timer, hvis en sikkerhedshændelse har påvirket kundens data eller tjenesten. Sikkerhedssager på sslbrain.com/sikkerhedsmeddelelser/.
Håndtering af sårbarheder	Meldes til info@fairssl.dk (security.txt). Sikkerhedsopdateringer til systemer og afhængigheder installeres løbende. Ubuntu's sikkerhedsopdateringer installeres automatisk på appliancen.
Ændringshåndtering	Opdateringer til appliance, service-agenter og deploy-agenter signeres med en hardwarenøgle, og appliancen installerer kun opdateringer med gyldig signatur.
Sikker udvikling	Signering med fysisk hardware-nøgle; en version, der ikke kan verificeres, starter ikke; læsbar kode. sslbrain udvikles efter Cyber Resilience Act.
Certificering	FairSSL har ikke en ISO 27001-certificering. Kontrollerne er kortlagt til ISO/IEC 27001:2022 bilag A og CIS Controls v8.1.
Forsikring	FairSSL A/S har hos If erhvervsansvars-, produktansvars- og professionel ansvarsforsikring for IT-virksomheder.
Underleverandører	UpCloud, OVHcloud, mailbox.org, Microsoft 365, Lettermint. Liste: sslbrain.com/nis2/#underleverandoerer. Indsigelse inden for 30 dage efter varslet.
Exit	Nøgler, certifikater og data i appliancen er jeres og bliver hos jer; installerede certifikater virker til udløb. Afsnit 7 beskriver udfald, genstart, udløbet abonnement og en leverandør, der er væk. Personoplysninger i Cloud slettes fra aktive systemer inden for 30 dage.
Databehandleraftale	Laves for jeres konto i sslbrain Cloud.
Kontakt for sikkerhed	info@fairssl.dk

13. Ofte stillede spørgsmål

Er sslbrain en leverandør, vi skal vurdere?

Ja. NIS2-direktivets artikel 21, stk. 2, litra d, og stk. 3 og DORA artikel 28 beder jer vurdere jeres IKT-leverandører. PDF'en har det, I skal bruge: hvad FairSSL og sslbrain Cloud kan og ikke kan, exit, rest-risici, registret og et udfyldt leverandørskema.

Dækker dokumentationen DORA?

Ja. Den citerer RTS 2024/1774 artikel 7, stk. 1, 4 og 5 og viser, hvordan inventar, automatisk fornyelse, vault, ny nøgle ved fornyelse og tilbagekaldelse dækker dem. Den har registret efter ITS 2024/2956 og en tabel over DORA artikel 28 til 30.

Hvad sker der, hvis FairSSL forsvinder?

Nøgler, certifikater og data ligger hos jer, installerede certifikater virker, og appliancen kører videre. Efter en genstart låser de 12 backup-ord op. Afsnit 7 beskriver hver situation og det, der kræver Cloud i dag.

Hvor længe gemmes revisionsloggen?

På appliancen efter plan: Free 30 dage, Basic 90 dage, Professional 2 år og Enterprise 7 år. Skal den gemmes længere, eksporterer I den eller sender den til jeres SIEM.

Hvilke eksportformater findes?

CSV og JSON fra Professional. Hver hændelse har tidspunkt, bruger, handling, objekt, IP-adresse, værdier før og efter og sin plads i hash-kæden.

Kan FairSSL nå vores private nøgler?

Nej. Jeres private nøgler laves og ligger krypteret i jeres egen appliance og dens backup, og sendes end-to-end krypteret til de servere, de installeres på. FairSSL og sslbrain Cloud har ingen kopi af dem. Nøglerne kan kun åbnes med den krypterede data plus enten jeres 12 backup-ord, som kun I kender, eller den roterende nøgle, som sslbrain Cloud udleverer til jeres appliance. Ellers kan de kun hentes ud i appliancen af en bruger med ret til at eksportere nøgler, som først skal bekræfte sin identitet igen.

Har I brug for flere detaljer?

Er I underlagt regler, der kræver mere end denne side og vores udfyldte leverandørskema, kan I søge om adgang til mere detaljeret dokumentation på info@fairssl.dk. Vi vurderer hver ansøgning for sig.

Kontakt

Spørgsmål til dokumentationen sendes til FairSSL A/S på:

info@fairssl.dk