NIS2- och DORA-dokumentation

Det ni behöver om sslbrain för er leverantörsbedömning enligt NIS2 eller DORA, för företag i hela EU. Från Professional skapar appliancen också er egen dokumentation.

sslbrain: dokumentation för er leverantörsbedömning enligt NIS2 och DORA

Version 1.6
Datum 06-11-2026

Stöd för ert arbete med NIS2 och DORA, inte juridisk rådgivning.

Gäller sslbrain på datumet ovan. Den senaste utgåvan finns alltid på sslbrain.com/sv/nis2/.

FairSSL A/S, utgivare av sslbrain

Innehåll

1. Tjänsten och vår roll
2. Data och var de finns
3. Underleverantörer för ert register
4. Drift: ändringar, åtkomst, uppdateringar och incidenter
5. Kontroller i produkten
6. Nycklar och kryptografi
7. Exit och koncentrationsrisk
8. Extern kontroll, certifiering och försäkring
9. DORA
10. NIS2 artikel 21.2 a-j
11. Kvarstående risker och riskbegränsning
12. Ifyllt leverantörsformulär
13. Vanliga frågor

1. Tjänsten och vår roll

Om sslbrain på en sida

Funktion	Hämtar, förnyar och installerar TLS-certifikat på era servrar, lastbalanserare och brandväggar och visar var varje certifikat är installerat och när det löper ut.
Lagring av nycklar och data	On-Premise i er appliance: privata nycklar (skapas på appliancen och lagras krypterade i dess vault), certifikat, installationsplaner, revisionslogg och inställningar.
Innehåll i sslbrain Cloud (EU)	Ert konto och er licens, en nyckel till appliancens vault (avsnitt 5), konton hos certifikatutfärdarna och, om ni väljer det, DNS-API-nycklar. Cloud hostas i EU hos underbiträdena i avsnitt 3.
Utgående trafik	Endast anslutningar som appliancen själv upprättar. Via HTTPS: till cloud.sslbrain.com, acme.sslbrain.com, registry.sslbrain.com och dns-proxy.sslbrain.com samt till de certifikatutfärdare och DNS-leverantörer ni väljer. Dessutom DNS-uppslagningar hos 1.1.1.1, 8.8.8.8 och 9.9.9.9 (port 53 och DNS over HTTPS), Ubuntus säkerhetsuppdateringar från archive.ubuntu.com (port 80) och tidssynkronisering (NTP). Appliancens egen brandvägg tillåter bara dessa. Till Cloud skickas antal och versioner (servrar, certifikat, installationsplaner, serviceagenter, diskanvändning), certifikatbegäranden för certifikat från Cloud och diagnostik bara om ni aktiverar den. Aldrig privata nycklar.
Inkommande trafik	Inga anslutningar utifrån. Appliancens webbgränssnitt svarar bara i ert eget nätverk. Appliancen och service-agenterna upprättar bara utgående anslutningar, och varken FairSSL eller Cloud kan logga in på appliancen.

NIS2, DORA och andra ramverk

- NIS2 är ett EU-direktiv, och varje land har en egen lag. I Sverige är det cybersäkerhetslagen (SFS 2025:1506), som trädde i kraft 15 januari 2026. Artiklarna här är direktivets, så dokumentationen kan användas i hela EU.
- Finansiella företag följer DORA, förordning (EU) 2022/2554, som har företräde framför NIS2 där den täcker samma område (NIS2 artikel 4).
- Kunder som själva är digital infrastruktur eller MSP följer dessutom genomförandeförordning (EU) 2024/2690.
- FairSSL omfattas inte självt av NIS2. Dokumentationen finns för att stödja era skyldigheter i leveranskedjan: NIS2 artikel 21.2 d och 21.3 samt DORA artikel 28 till 30.
- Samma kontroller täcker GDPR artikel 28 och 32 (personuppgiftsbiträdesavtalet och säkerhet i behandlingen).
- FairSSL har ingen ISO 27001-certifiering. Kontrollerna är kartlagda mot ISO/IEC 27001:2022 bilaga A och CIS Controls v8.1.
- sslbrain utvecklas i linje med Cyber Resilience Act, förordning (EU) 2024/2847.

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

2. Data och var de finns

Det mesta är certifikatdata som redan är offentliga i Certificate Transparency-loggar. Personuppgifter gäller bara fakturering, kontaktpersoner och inloggning. Data om er interna miljö stannar hos er. Att Cloud tar emot så lite är en kontroll i sig (uppgiftsminimering, NIS2 artikel 21.2 och GDPR artikel 25 och 32).

Data	Lagringsplats	Klassificering
Privata nycklar	Skapas på appliancen och lagras krypterade i dess vault hos er. Skickas aldrig till Cloud.	Konfidentiellt

Data	Lagringsplats	Klassificering
Åtkomstuppgifter: serverinloggningar, DNS-API-nycklar, CA-konton på appliancen	Krypterade i appliancens vault. En DNS-API-nyckel lagras bara i Cloud om ni själva väljer det för ACME från Cloud.	Konfidentiellt
Interna certifikat, servernamn, IP-adresser och programvara	I appliancens inventering hos er. Bara om ni aktiverar diagnostik skickas utvalda uppgifter (t.ex. servernamn, IP-adress och operativsystem) till FairSSL:s support.	Internt
Antal och versioner	Cloud: antal servrar, certifikat, installationsplaner och service-agenter, versioner och diskanvändning. Används för licens och drift.	Internt
Certifikatbegäranden för certifikat från Cloud	Cloud och den CA ni väljer: namnen i certifikatet och valideringen (AutoDNS eller DNS-API-nyckel).	Offentligt
Aviseringar ni skickar genom Cloud	Cloud och e-posttjänsten Lettermint: ämne och text, som kan nämna servernamn och certifikat. Lettermint raderar meddelandenas innehåll, mottagare och metadata automatiskt 28 dagar efter att de skickats. Aviseringar via er egen SMTP-server eller webhooks går inte genom Cloud.	Internt
Meddelanden till service-agenter via Cloud	Krypterade hela vägen mellan appliance och service-agent. Cloud ser vem, när och hur mycket, inte innehållet.	Konfidentiellt
Revisionslogg	I appliancen. Från Professional sparas kedjans senaste hash i Cloud varje timme.	Internt
Konto, inloggning, kontaktpersoner och fakturering	sslbrain Cloud (EU) och underbiträdena i avsnitt 3.	Personuppgifter

3. Underleverantörer för ert register

- sslbrain Cloud hostas i EU hos underbiträdena i tabellen.
- Certifikatutfärdare (CA): Självständiga personuppgiftsansvariga för utfärdande, validering och Certificate Transparency-loggning av de certifikat kunden beställer. CA:n följer den certifikatprofil kunden väljer.
- Namnen i ett certifikat är offentliga: certifikatutfärdaren skriver dem i Certificate Transparency-loggar.

Leverantör	Ägarskap	Data lagras i	Används till
UpCloud	Finland	EU	Server- och databashosting
OVHcloud	Frankrike	EU	Server- och databashosting
mailbox.org	Tyskland	EU	E-post
Microsoft 365	USA	EU	E-post och kontorssystem
Lettermint	Nederländerna	EU	Systemmejl

Kunden kan invända inom 30 dagar efter aviseringen genom att skriva till info@fairssl.dk.

Ändringslogg

- Inga ändringar ännu.

4. Drift: ändringar, åtkomst, uppdateringar och incidenter

FairSSL som leverantör

- Ändringar: Uppdateringar till appliance, service-agenter och deploy-agenter signeras med en hårdvarunyckel, och appliancen installerar bara uppdateringar med giltig signatur.
- Åtkomst: Administrativ åtkomst är begränsad till nyckelpersoner med rollbaserad åtkomst (RBAC) och minsta möjliga behörigheter.
- Uppdateringar: Säkerhetsuppdateringar till system och beroenden installeras löpande.
- Incidenter: Vi underrättar kunden utan onödigt dröjsmål och senast inom 48 timmar om en säkerhetsincident har påverkat kundens data eller tjänsten. Det står också i villkoren och personuppgiftsbiträdesavtalet. En sårbarhet som har åtgärdats utan att ha påverkat kundens data eller tjänsten är inte en incident (NIS2 artikel 6.6 och 6.15).
- sslbrain utvecklas i linje med Cyber Resilience Act.

Incidenter och avtal

- Vi underrättar kunden utan onödigt dröjsmål och senast inom 48 timmar om en säkerhetsincident har påverkat kundens data eller tjänsten (villkoren, avsnitt 16, och personuppgiftsbiträdesavtalet, avsnitt 8).
- Personuppgiftsincidenter: FairSSL informerar er utan onödigt dröjsmål och senast 48 timmar efter att ha fått kännedom om incidenten (personuppgiftsbiträdesavtalet, avsnitt 8).
- Säkerhetsmeddelanden som kräver att ni agerar skickas via e-post till kontots säkerhetsmottagare, och alla meddelanden finns på sslbrain.com/sv/sakerhetsmeddelanden/.
- Underbiträden: ett nytt eller utbytt underbiträde aviseras per mejl och i ändringsloggen i avsnitt 3. Ni kan invända inom 30 dagar efter aviseringen, och om ingen lösning hittas kan ni säga upp de berörda tjänsterna utan bindningstid.
- Ändringar som kräver att ni agerar meddelas minst 30 dagar i förväg.
- När ni avslutar: abonnemanget löper till slutet av den betalda perioden och övergår sedan till Free. Om Cloud-kontot stängs påverkas inte data som redan finns hos er.
- Personuppgifter som FairSSL behandlar för er raderas eller återlämnas när avtalet upphör. Radering från aktiva system sker inom 30 dagar; säkerhetskopior raderas i den löpande rotationen.
- FairSSL:s sammanlagda skadeståndsansvar är begränsat till vad ni har betalat de senaste 12 månaderna.
- Vår underrättelse ersätter inte era egna tidsfrister för betydande incidenter enligt NIS2 artikel 23 eller DORA artikel 19: enligt NIS2 tidig varning inom 24 timmar, incidentanmälan inom 72 timmar och slutrapport senast en månad efter anmälan.

5. Kontroller i produkten

Er leverantörsbedömning av sslbrain

I NIS2-direktivets artikel 21.2 d och 21.3 och DORA artikel 28 uppmanas ni att bedöma era IKT-leverantörer. Tabellen visar vad FairSSL och sslbrain Cloud kan och inte kan göra i ert nätverk, jämfört med en ACME-klient som använder en offentlig CA.

	sslbrain	**En ACME-klient (t.ex. Certbot med Let's Encrypt)**
Leverantörskod hos er	Appliance, service-agenter och integrationer körs hos er. De är begränsade till det FairSSL har signerat och det ni själva signerar med appliancens nyckel (avsnitt 7), precis som en ACME-klient kör det den är byggd för.	ACME-klienten körs hos er med de behörigheter ni ger den.
Leverantörens styrning	Inga kommandon. Cloud kan inte köra något på appliancen eller service-agenterna. Cloud kan vägra upplåsning och låsa appliancen (avsnitt 5) och erbjuda en ny signerad version som appliancen själv installerar om ni har valt automatisk uppdatering.	Inga kommandon.

	sslbrain	En ACME-klient (t.ex. Certbot med Let's Encrypt)
Uppdateringar	Uppdateringar till appliance, service-agenter och deploy-agenter signeras med en hårdvarunyckel, och appliancen installerar bara uppdateringar med giltig signatur. En version som inte kan verifieras startar inte. Automatisk uppdatering kan stängas av lokalt. Operativsystemet som appliancen körs på (Ubuntu LTS) hämtar bara Ubuntus säkerhetsuppdateringar, signerade av Canonical, och startar om vid behov kl. 03:00 UTC.	Beror på klienten. Certbot uppdaterar sig självt när det installeras enligt rekommendationen.
Utfärdande för era domäner	Utfärdande via Cloud kräver att namnet valideras med AutoDNS (en CNAME per namn) eller med en DNS-API-nyckel som ni har sparat i Cloud. Namn som valideras med en DNS-API-nyckel i appliancen kan Cloud inte utfärda för. Ni väljer per namn. CAA-poster begränsar dessutom vilka certifikatutfärdare och konton som får utfärda.	Den som styr ACME-kontot och valideringen kan få certifikat utfärdade för era namn. CAA-poster begränsar detta på samma sätt.
Avbrutna förnyelser	Om Cloud eller ert abonnemang upphör fungerar de installerade certifikaten tills de löper ut, och data i appliancen är era och stannar hos er. Avsnitt 7 beskriver varje situation.	Om certifikatutfärdaren eller klienten upphör fungerar de installerade certifikaten tills de löper ut.
Åtkomst till ert nätverk	Ingen. Endast den som har tillgång till appliancens lokala konsol kan öppna SSH för FairSSL:s support för felsökning i 24 timmar. Även då krävs åtkomst till appliancen i ert nätverk.	Ingen.
DNS-API-nycklar	Sparas krypterad i appliancens valv, på ett ställe i ert nätverk. Anropen till DNS-leverantören går genom en krypterad anslutning som Cloud inte kan läsa. För ACME från Cloud kan ni välja att spara nyckeln i Cloud.	Sparas på varje server som utfärdar certifikat. certbot, acme.sh och lego sparar den i klartext i en fil eller miljövariabel. win-acme krypterar den som standard med serverns egen Windows-nyckel.

Nyckeln till appliancens vault i sslbrain Cloud

Säkerhetsgranskare frågar först om den. Här står exakt vad den kan och inte kan göra.

- Appliancens vault krypterar privata nycklar med en huvudnyckel på 256 bitar som skapas på appliancen och aldrig skickas till Cloud.
- Huvudnyckeln lagras bara krypterad på datadisken: kopior låsta med nycklar från Cloud (den nuvarande och de senast utbytta) och en kopia låst med de 12 backuporden. Medan appliancen körs finns den okrypterade huvudnyckeln i minnet, inte på disken.
- Cloud skapar en slumpmässig nyckel (32 byte) för varje installation och lagrar den krypterad.
- Nyckeln byts vid varje upplåsning genom Cloud och var 6:e timme.
- Cloud kan inte dekryptera något på egen hand: Cloud har varken huvudnyckeln eller era privata nycklar.
- Cloud tillsammans med en kopia av datadisken eller en säkerhetskopia låser upp nycklarna så länge Cloud fortfarande har nyckeln som låser kopian. Skydda datadisken och säkerhetskopior som privata nycklar.
- Cloud styr tillgängligheten till appliancens vault, inte innehållet: Cloud kan vägra upplåsning eller låsa appliancen. De 12 backuporden låser alltid upp, även en låst appliance, utan Cloud. Appliancen är då upplåst till nästa omstart; det som går genom Cloud står stilla, och nödkontot kan inte hämta privata nycklar eller säkerhetskopior.
- Om Cloud inte svarar fortsätter en upplåst vault att köras. Efter en omstart låser Cloud eller backuporden upp.
- Om två kopior av samma installation körs väljer ni i Cloud vilken som ska fortsätta. FairSSL:s support kan också godkänna ett övertagande från Cloud, och kontots mottagare får ett mejl. Den andra kopian låses.

- Efter återställning från en säkerhetskopia ber Cloud om ert godkännande (eller godkännande från FairSSL:s support) innan den låser upp. De 12 backuporden låser upp direkt. Cloud raderar utbytta nycklar när de är över 7 dagar gamla och inte bland de 10 senaste, så en äldre säkerhetskopia eller diskkopia kan bara låsas upp med backuporden.

NIS2-paketet från er appliance (Professional)

Er egen dokumentation, signerad av appliancen: revisionslogg med kedjekontroll, inventering, förnyelser och fel, policyer för den valda dagen, ifylld kryptografipolicy, riskblad och incidentrutin. Från Professional skapar appliancen NIS2-paketet: en signerad fil för den period ni väljer, klar för revisorn.

- Revisionsloggen med hashvärden och resultatet av kedjekontrollen.
- Certifikatinventering för den valda dagen: namn, CA, nyckeltyp och nyckelstorlek, utgångsdatum och var varje certifikat är installerat.
- Förnyelser och fel under perioden.
- Policyer för den valda dagen: roller och användare, vem som får hämta privata nycklar, domänlås och uppdateringssätt.
- Versioner av appliance och serviceagenter samt om signaturerna är giltiga.
- Kryptografipolicy enligt kommissionens genomförandeförordning (EU) 2024/2690, punkt 9.2 i bilagan, ifylld med era inställningar.
- Riskblad, incidentrutin med tidsfristerna i artikel 23 och ansvarsfördelning mellan er och FairSSL.
- Som PDF och som filer ni kan redigera i Word och kalkylprogram.
- Varje rad i revisionsloggen skickas till ert SIEM med syslog över TLS, och kedjans senaste hash sparas i sslbrain Cloud.

Förordning (EU) 2024/2690 är bara bindande för de entiteter som anges i artikel 1 (t.ex. molntjänster, DNS, MSP, datacenter och tillhandahållare av betrodda tjänster). För andra är den en bra referens.

6. Nycklar och kryptografi

- Data i appliancen: privata nycklar och andra hemligheter krypteras med XChaCha20-Poly1305 och en nyckel på 256 bitar.
- De 12 backuporden: 96 bitar, omvandlade till en nyckel med Argon2id.
- Meddelanden mellan appliance och serviceagenter: signerade med ECDSA (P-384 eller P-256 beroende på serviceagentens nyckel) och krypterade med AES-256-GCM (JWE, ECDH-ES). Det gäller också meddelanden via sslbrain Cloud (EU), som inte kan läsa dem.
- Applianceversioner och integrationer: signerade med ECDSA P-384 och SHA-384.
- Nedladdade säkerhetskopior: krypterade med XChaCha20-Poly1305 och en nyckel som härleds från ert lösenord (Argon2id). Lösenordet är obligatoriskt och ska ha minst 12 tecken.
- Certifikatnycklar: skapas på appliancen, RSA 2048 till 4096 bitar eller ECDSA P-256 och P-384. Certifikatprofilen och de servrar där certifikatet ska installeras bestämmer vilka typer som tillåts. Certifikat som ni själva laddar upp behåller sin nyckel.
- Appliancens webbgränssnitt och Cloud-tjänsterna använder TLS 1.2 och 1.3 och avvisar TLS 1.0 och 1.1 (uppmätt 25-10-2026).

Uppmätt 25-10-2026: TLS 1.3 och hybrid postkvantnyckelutväxling (X25519MLKEM768).

Del	TLS 1.3	X25519MLKEM768
Appliancens webbgränssnitt	Ja	Ja
sslbrain Cloud (cloud.sslbrain.com)	Ja	Ja
acme.sslbrain.com, registry.sslbrain.com, dns-proxy.sslbrain.com	Ja	Ja
Linux-serviceagenten (använder serverns OpenSSL)	Ja	Ja med OpenSSL 3.5 eller senare (t.ex. Debian 13), annars X25519
Windows-serviceagenten (använder Windows egen TLS)	Från Windows Server 2022	Från Windows Server 2025, när Windows har det påslaget

7. Exit och koncentrationsrisk

Vad som händer när sslbrain Cloud eller FairSSL inte finns tillgängligt. Privata nycklar, certifikat och data finns On-Premise hos er i alla fyra situationerna, och installerade certifikat fungerar utan Cloud: de är filer på era servrar som inget i sslbrain tar bort när Cloud inte är tillgängligt.

- Lokal ACME-källa (från Professional): appliancen utfärdar direkt hos certifikatutfärdaren, t.ex. Let's Encrypt eller er egen ACME-CA, utan att gå via Cloud. Validering med AutoDNS eller en DNS-API-nyckel i Cloud kräver fortfarande Cloud; en DNS-API-nyckel i appliancen gör det inte.
- Tillägget Lokal ACME-server (Enterprise) är något annat: en ACME-server på appliancen som era interna ACME-klienter använder och som förmedlar till er egen CA eller en extern ACME-CA.
- Flera certifikatutfärdare i ordning: en profil kan ha flera certifikatkällor, och om den första misslyckas tar nästa över.
- Er egen signeringsnyckel: appliancen har en egen nyckel som skapas på appliancen. Om ni lägger in dess offentliga del lokalt på en server med service-agent kör service-agenten era egna agenter och era egna ändringar av agenter, signerade av appliancen. Nyckeln kan inte godkänna FairSSL:s paket eller uppdateringar.
- Service-agenter kan installeras manuellt på servern från en version ni själva bygger eller får (MSI på Windows, paket eller källkod på Linux). Registreringen sker mot er appliance.
- Om appliancen körs i Docker kan ni själva hämta och uppdatera imagen. Signaturen kan kontrolleras lokalt med sslbrain-sigverify innan imagen startas.
- Som standard låses appliancen upp via Cloud, utan Cloud med de 12 backuporden. Om ni vill vara helt utan Cloud kan ni köpa den 100 % lokala On-Premise-utgåvan (tillägget Offlinedrift).
- Detta kräver Cloud i dag: registrering och aktivering av appliancen, inloggning via Cloud, licensförnyelse, upplåsning efter omstart (annars backuporden), utfärdande via Cloud med AutoDNS, DNS-API-nycklar i Cloud och dns-proxy.sslbrain.com, registrering av service-agenter via Cloud och meddelanden via Cloud, uppdateringar och integrationer från katalogen, aviseringar genom Cloud, revisionsloggens hash i Cloud och koden till konsolens root-shell.

Situation	Det fungerar	Det står stilla
Cloud svarar inte (avbrott)	Appliancen fortsätter att köras med upplåst vault. Användare loggar in med det lösenord appliancen känner till. Med Lokal ACME-källa och DNS-API-nycklar i appliancen förnyas och installeras certifikat direkt hos certifikatutfärdaren. Direktanslutna service-agenter och aviseringar via er egen SMTP-server eller webhooks fungerar.	Utfärdande via Cloud och AutoDNS, meddelanden till service-agenter via Cloud, inloggning via Cloud, uppdateringar, aviseringar genom Cloud och licensförnyelse. Detta återupptas när Cloud svarar igen.
Omstart när Cloud inte är tillgängligt	Som standard låses appliancens vault upp via Cloud. Utan Cloud låser ni upp med de 12 backuporden, och appliancen är upplåst till nästa omstart. Därefter gäller samma sak som vid avbrott.	Samma sak som vid avbrott. Nödkontot kan inte hämta privata nycklar eller säkerhetskopior.
Abonnemanget har löpt ut	Ni får besked senast 28 dagar före utgången. Appliancen fortsätter som Free: de äldsta servrarna upp till gränsen för Free får fortfarande förnyelser och installationer. Övriga servrar finns kvar i inventeringen, behåller sina nycklar och upptäcks fortfarande.	Förnyelse och installation på servrar utöver gränsen för Free samt funktioner och moduler som inte ingår i Free.

Situation	Det fungerar	Det står stilla
FairSSL har upphört permanent	Nycklar, certifikat och inventering är era och stannar hos er. Appliancen fortsätter att köras, och de 12 backuporden låser upp efter omstart. Lokal ACME-källa förnyar direkt hos certifikatutfärdaren tills licensperioden löper ut. Därefter tar appliancen själv bort Professional-modulerna, och Free förnyar via Cloud, så förnyelserna upphör; installerade certifikat fungerar tills de löper ut. Skulle utvecklingen av sslbrain någonsin upphöra, släpper vi först programvaran fri som öppen källkod. Koden är läsbar (source-available), och ACME är en öppen standard (RFC 8555), så ett byte kräver ett nytt konto hos den nya leverantören, validering och nya installationer.	Allt som kräver Cloud (se listan nedan), uppdateringar från FairSSL, förnyelse av licensen och, när licensperioden har löpt ut, förnyelse av certifikat.

8. Extern kontroll, certifiering och försäkring

Utveckling och sårbarheter

- Uppdateringar till appliance, service-agenter och deploy-agenter signeras med en hårdvarunyckel, och appliancen installerar bara uppdateringar med giltig signatur.
- Operativsystemet som appliancen körs på (Ubuntu LTS) installerar automatiskt Ubuntus säkerhetsuppdateringar och startar om vid behov kl. 03:00 UTC.
- En version som inte kan verifieras startar inte, och den version som kördes startas igen. En integration som inte kan verifieras ersätter inte den installerade.
- Ni väljer manuell eller automatisk uppdatering på appliancen.
- Koden är läsbar (source-available), så att ni eller en tredje part kan granska den.
- Sårbarheter rapporteras till info@fairssl.dk; kontakten finns i sslbrain.com/.well-known/security.txt. Säkerhetsmeddelanden finns på sslbrain.com/sv/sakerhetsmeddelanden/.
- Vi stöder den senaste och den föregående huvudversionen och meddelar minst 90 dagar innan en version slutar få säkerhetsrättningar.

Certifiering och försäkring

- FairSSL har ingen ISO 27001-certifiering. Kontrollerna är kartlagda mot ISO/IEC 27001:2022 bilaga A och CIS Controls v8.1.
- FairSSL A/S har hos If allmän ansvarsförsäkring, produktansvarsförsäkring och professionsansvarsförsäkring för IT-företag.

9. DORA

DORA och RTS 2024/1774, artikel 7

DORA, förordning (EU) 2022/2554, gäller för finansiella företag och har för dem företräde framför NIS2 (NIS2 artikel 4). Kommissionens delegerade förordning (EU) 2024/1774 om IKT-riskhantering ställer i artikel 7 krav på kryptografiska nycklar och certifikat. Här återges de tre punkter som handlar om certifikat ordagrant, tillsammans med hur sslbrain uppfyller dem.

RTS 2024/1774, artikel 7	Så uppfyller sslbrain kraven

RTS 2024/1774, artikel 7	Så uppfyller sslbrain kraven
Punkt 1: "Finansiella entiteter ska i den policy för hantering av kryptografiska nycklar som avses i artikel 6.2 d inkludera krav för hantering av kryptografiska nycklar under hela deras livscykel, inbegripet generering, förnyelse, lagring, säkerhetskopiering, arkivering, hämtning, överföring, återkallande, upphävande och förstörelse av dessa kryptografiska nycklar."	Generering: nyckeln skapas på appliancen. Förnyelse: varje ny version får som standard en ny nyckel, och en policy kan kräva det. Lagring: krypterad i appliancens vault. Säkerhetskopiering: ingår i appliancens säkerhetskopia. Hämtning: bara de roller ni tillåter kan hämta en nyckel. Överföring: krypterad till service-agenten. Återkallande: hos certifikatutfärdaren via ACME eller certifikatutfärdarens API. Revisionsloggen visar varje steg. Professional fyller i kryptografipolicyn med era inställningar.
Punkt 4: "Finansiella entiteter ska skapa och upprätthålla ett register över alla certifikat och enheter för lagring av certifikat för åtminstone IKT-tillgångar som stöder kritiska eller viktiga funktioner. Finansiella entiteter ska hålla detta register uppdaterat."	Inventeringen utgör registret: varje certifikat med CA, nyckeltyp, utgångsdatum och varje server, tjänst och enhet där det är installerat. Upptäcktsfunktionen hittar certifikat ni inte kände till i ert nätverk. Registret hålls uppdaterat vid varje förnyelse och installation.
Punkt 5: "Finansiella entiteter ska säkerställa att certifikat snabbt förnyas innan de löper ut."	Automatisk förnyelse före utgång, vid den tidpunkt certifikatutfärdaren rekommenderar (ARI, RFC 9773), och den nya versionen installeras överallt där certifikatet används. Om en förnyelse misslyckas får ni besked.

Punkt 2 och 3 (skydd av nycklarna och byte vid förlust eller kompromettering) täcks av appliancens vault och av att ett certifikat kan förnyas med en ny nyckel och installeras överallt samtidigt.

DORA artikel 28 till 30: här finns svaren

Avsnittsnumren är desamma på sidan och i PDF:en. Ni bedömer om tjänsten stöder en kritisk eller viktig funktion.

DORA	Krav	Svar
Artikel 28.1 och 28.2	Allmänna principer: hantering av IKT-tredjepartsrisk	Avsnitt 5 (leverantörsbedömning och nyckeln i Cloud) och 11 (kvarstående risker).
Artikel 28.3	Informationsregister	Avsnitt 9 (registret enligt ITS 2024/2956).
Artikel 28.4 och 28.5	Bedömning före avtal och informationssäkerhet hos leverantören	Avsnitt 4 (FairSSL som leverantör), 6 (kryptografi) och 8 (utveckling och sårbarheter).
Artikel 28.7 och 28.8	Uppsägning och exitstrategi	Avsnitt 4 (incidenter och avtal) och 7 (exit).
Artikel 29	Preliminär bedömning av IKT-koncentrationsrisker på entitetsnivå	Avsnitt 3 (underleverantörer) och 7 (exit och koncentrationsrisk).
Artikel 30	Viktiga avtalsbestämmelser	Avsnitt 4 (incidenter och avtal): villkoren och personuppgiftsbiträdesavtalet.

Registret över IKT-leverantörer

Uppgifter för ert informationsregister enligt genomförandeförordning (EU) 2024/2956.

Fält	sslbrain
Juridiskt namn	FairSSL A/S
Identifiering	CVR-nr 33075782 (momsregistreringsnummer DK33075782). FairSSL har ingen LEI.
Land	Danmark. Åbrovej 29, 8586 Ørum Djurs.

Fält	sslbrain
Typ av IKT-tjänst	Programvara för certifikathantering som körs hos er (appliance och service-agenter) samt sslbrain Cloud (EU) som tjänst: licens, utfärdande via certifikatutfärdare och ACME, AutoDNS och förmedling av krypterade meddelanden.
Lagringsplats för data	Appliancen: hos er. sslbrain Cloud (EU): i EU hos underbiträdena i avsnitt 3.
Plats för databehandling	Samma platser.
Underbiträden	UpCloud, OVHcloud, mailbox.org, Microsoft 365, Lettermint. Ändamål och land i avsnitt 3.
Certifikatutfärdare (självständigt personuppgiftsansvariga)	DigiCert, Inc. (USA; DPF) för certifikat från DigiCert. Let's Encrypt (Internet Security Research Group, USA) och Google Trust Services (USA) för kostnadsfria certifikat. CA:n följer den certifikatprofil ni väljer.
Kritisk eller viktig funktion	Er bedömning.

10. NIS2 artikel 21.2 a-j

De tio åtgärderna i artikel 21: vad produkten hjälper er med, våra egna kontroller och vad ni själva gör. NIS2 godkänner inte leverantörer; ni bedömer dem.

Artikel 21.2	Produkten hjälper er med	Våra egna kontroller	Ert ansvar
a) Riskanalys och strategier för informationssystemens säkerhet	Översikt över alla certifikat, var de är installerade och när de löper ut. Policyer på ett ställe: vem som får hämta privata nycklar, vilka domäner som får ha certifikat, manuell eller automatisk uppdatering. Professional: riskblad ifyllt med era inställningar.	Kontrollerna är kartlagda mot ISO/IEC 27001:2022 bilaga A och CIS Controls v8.1.	Er samlade riskbedömning. Godkänn och granska policyerna.
b) Incidenthantering	Varningar vid fel och utgång. En ny version av ett certifikat installeras överallt där det används. Revisionsloggen visar förloppet. Professional: incidentrutin med tidsfristerna i artikel 23.	Vi underrättar kunden utan onödigt dröjsmål och senast inom 48 timmar om en säkerhetsincident har påverkat kundens data eller tjänsten.	Bedöm och rapportera betydande incidenter: tidig varning inom 24 timmar, incidentanmälan inom 72 timmar och slutrapport senast en månad därefter.
c) Driftskontinuitet, säkerhetskopiering och krishantering	Säkerhetskopiering och återställning av appliancen. De 12 backuporden låser upp den utan Cloud. Certifikatprofiler med flera certifikatutfärdare i ordning. Installerade certifikat fungerar även om Cloud inte svarar (avsnitt 7).	sslbrain Cloud (EU) hostas i EU hos underbiträdena i avsnitt 3. Säkerhetskopior lagras alltid i ett eller flera EU-länder, åtskilda från det land där säkerhetskopian tas.	Säkerhetskopiera appliancen och förvara säkerhetskopior och backupord utanför den. Öva på återställning.
d) Säkerhet i leveranskedjan	Allt som körs hos er är signerat och har läsbar kod. Avsnitt 5 och 11 beskriver vad FairSSL och Cloud kan och inte kan göra.	Underbiträden från en gemensam lista (avsnitt 3). Ni kan invända inom 30 dagar efter aviseringen.	Bedöm sslbrain och de certifikatutfärdare ni använder som leverantörer.

Artikel 21.2	Produkten hjälper er med	Våra egna kontroller	Ert ansvar
e) Säkerhet vid förvärv, utveckling och underhåll, inbegripet sårbarheter	Signerade versioner; en version som inte kan verifieras startar inte. Manuell eller automatisk uppdatering. Säkerhetsmeddelanden och security.txt.	Uppdateringar till appliance, service-agenter och deploy-agenter signeras med en hårdvarunyckel. Säkerhetsuppdateringar till system och beroenden installeras löpande.	Välj uppdateringssätt och installera säkerhetsuppdateringar.
f) Bedömning av åtgärdernas effektivitet	Revisionslogg med hashkedja och kedjekontroll, export för en vald period. Professional: NIS2-paketet, signerat av appliancen.	Kontrollerna är kartlagda mot ISO/IEC 27001:2022 bilaga A och CIS Controls v8.1, och den här dokumentationen är versionshanterad.	Gå igenom dokumentationen med er revisor.
g) Cyberhygien och utbildning i cybersäkerhet	Certifikat förnyas automatiskt innan de löper ut och enligt certifikatutfärdarens rekommendation (ARI), så att kortare giltighetstider (200, 100 och 47 dagar) inte medför manuellt arbete.	Säkerhetsuppdateringar till system och beroenden installeras löpande.	Utbilda medarbetarna.
h) Kryptografi och kryptering	Privata nycklar skapas och stannar On-Premise. Vault: XChaCha20-Poly1305 med 256 bitar. Meddelanden till service-agenter: AES-256-GCM. Versioner: ECDSA P-384. Professional: kryptografipolicy enligt förordning 2024/2690, punkt 9.2 i bilagan, ifylld med era inställningar.	TLS 1.2 och 1.3 med hybrid postkvantnyckelutväxling på Cloud (avsnitt 6).	Godkänn kryptografipolicyn. Välj nyckeltyper i certifikatprofilerna.
i) Personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning	Roller: Free har Owner, Basic har Owner och Administrator, Professional och Enterprise har alla fyra (Owner, Administrator, Operator, Viewer). AD-inloggning från Professional. Hämtning av privata nycklar styrs per roll och begränsas per timme. Inventering av servrar, tjänster och certifikat.	Administrativ åtkomst är begränsad till nyckelpersoner med rollbaserad åtkomst (RBAC) och minsta möjliga behörigheter.	Tilldela roller och ta bort användare som slutar.
j) Multifaktorsautentisering och säker kommunikation	Tvåfaktorsautentisering (TOTP) kan aktiveras per användare vid inloggning genom sslbrain Cloud. Inloggning med lokalt lösenord eller AD-inloggning på appliancen har ingen tvåfaktorsautentisering. Hämtning av privata nycklar och säkerhetskopior kräver en ny inloggningsbekräftelse som gäller i 5 minuter. Meddelanden till service-agenter är krypterade hela vägen.	Meddelanden till serviceagenter är signerade och krypterade hela vägen; appliancen och Cloud talar TLS 1.2 och 1.3.	Aktivera tvåfaktorsautentisering för varje användare i Cloud. Kräver ni tvåfaktorsautentisering ska ni bara använda Cloud-inloggning på appliancen.

11. Kvarstående risker och riskbegränsning

Kvarstående risk	Riskbegränsning
Cloud tillsammans med en kopia av datadisken eller en säkerhetskopia låser upp de privata nycklarna så länge Cloud har nyckeln som låser kopian.	Skydda datadisken och säkerhetskopior som privata nycklar. Nedladdade säkerhetskopior är krypterade med ert lösenord. Cloud har inte huvudnyckeln, och utbytta nycklar raderas efter 7 dagar.
Ett snapshot av den virtuella maskinen under drift innehåller den okrypterade huvudnyckeln om minnet ingår.	Ta snapshots utan minne och skydda snapshots som privata nycklar. Swap är avstängt på appliancen.
Cloud styr om appliancens vault kan låsas upp.	De 12 backuporden låser alltid upp, även en låst appliance, utan Cloud.
AutoDNS: den som styr Cloud kan få certifikat utfärdade för de namn som pekar på AutoDNS.	CAA-poster med accounturi, övervakning av Certificate Transparency och AutoDNS bara för de namn som behöver det.
Väljer ni att lagra en DNS-API-nyckel i Cloud kan den som styr Cloud ändra DNS i den zonen.	Låt nyckeln stanna i appliancen, där den går genom dns-proxy.sslbrain.com utan att Cloud ser den. Använd en nyckel som bara får skriva _acme-challenge där leverantören erbjuder det.
Appliancens TLS-nyckel, identitetsnyckel och token för Cloud lagras okrypterade på datadisken och i varje säkerhetskopia, skyddade av filbehörigheter.	Skydda datadisken. Nedladdade säkerhetskopior är krypterade med ert lösenord.
Revisionsloggen är hashkedjad, så ändringar kan upptäckas men inte förhindras: den som har full åtkomst till appliancen kan skriva om den.	Kedjekontroll på appliancen. Från Professional sparas kedjans senaste hash i Cloud varje timme, och varje rad skickas till ert SIEM med syslog över TLS, så att en omskriven logg upptäcks utanför appliancen.
En signerad men skadlig uppdatering.	Signering kräver en fysisk hårdvarunyckel. Välj manuell uppdatering om ni vill granska varje version först. Koden är läsbar.
Meddelanden via Cloud: Cloud ser vem, när och hur mycket, inte innehållet.	Anslut serviceagenterna direkt till appliancen där nätverket tillåter det.
Koncentration: Cloud är en enda leverantör för licens, utfärdande via Cloud och meddelanden.	Lokal ACME-källa, DNS-API-nycklar i appliancen, flera certifikatutfärdare i ordning och direktanslutna service-agenter (avsnitt 7).

12. Ifyllt leverantörsformulär

Svar på frågorna i en leverantörsbedömning.

Fråga	Svar
Rättslig grund	NIS2-direktivet (EU) 2022/2555, i Sverige cybersäkerhetslagen (SFS 2025:1506). Finansiella företag: DORA (EU) 2022/2554 och RTS (EU) 2024/1774. Personuppgifter: GDPR artikel 28 och 32 i personuppgiftsbiträdesavtalet.
Leverantör	FairSSL A/S, CVR-nr 33075782, Danmark. Produkt: sslbrain (appliance On-Premise och sslbrain Cloud (EU)).
Var finns tjänstens drift och i vilket land?	sslbrain Cloud (EU) hostas i EU hos underbiträdena i avsnitt 3. Appliancen körs hos er.
Vilka data behandlar leverantören?	I Cloud: konto, licens, nyckeln till appliancens vault, konton hos certifikatutfärdarna, DNS-API-nycklar om ni väljer det, certifikatbegäranden för certifikat från Cloud, aviseringar skickade genom Cloud samt antal och versioner från appliancen. Privata nycklar, certifikat, inventering och revisionslogg lagras i appliancen (avsnitt 2).
Har leverantören åtkomst till era system?	Nej. Inga anslutningar in i ert nätverk. SSH för FairSSL:s support kan bara öppnas från appliancens lokala konsol, i 24 timmar.
Administrativ åtkomst hos leverantören	Administrativ åtkomst är begränsad till nyckelpersoner med rollbaserad åtkomst (RBAC) och minsta möjliga behörigheter.

Fråga	Svar
Kryptering av lagrade data	XChaCha20-Poly1305 med 256 bitar i appliancens vault; nedladdade säkerhetskopior krypterade med ert lösenord.
Kryptering under överföring	HTTPS med TLS 1.2 och 1.3 på appliance och Cloud, TLS 1.3 med X25519MLKEM768 (uppmätt 25-10-2026). Meddelanden till serviceagenter är dessutom signerade och krypterade med AES-256-GCM.
Åtkomstkontroll och MFA	Roller (Owner, Administrator, Operator, Viewer), AD-inloggning från Professional, tvåfaktorsautentisering per användare vid inloggning genom sslbrain Cloud (inte med lokalt lösenord eller AD-inloggning), ny bekräftelse före hämtning av privata nycklar.
Loggning	Revisionslogg med hashkedja i appliancen; export (CSV, JSON) och SIEM med syslog över TLS från Professional.
Underrättelse vid incidenter	Vi underrättar kunden utan onödigt dröjsmål och senast inom 48 timmar om en säkerhetsincident har påverkat kundens data eller tjänsten. Säkerhetsmeddelanden på sslbrain.com/sv/sakerhetsmeddelanden/.
Hantering av sårbarheter	Rapporteras till info@fairssl.dk (security.txt). Säkerhetsuppdateringar till system och beroenden installeras löpande. Ubuntus säkerhetsuppdateringar installeras automatiskt på appliancen.
Ändringshantering	Uppdateringar till appliance, service-agenter och deploy-agenter signeras med en hårdvarunyckel, och appliancen installerar bara uppdateringar med giltig signatur.
Säker utveckling	Signering med fysisk hårdvarunyckel; en version som inte kan verifieras startar inte; läsbar kod. sslbrain utvecklas i linje med Cyber Resilience Act.
Certifiering	FairSSL har ingen ISO 27001-certifiering. Kontrollerna är kartlagda mot ISO/IEC 27001:2022 bilaga A och CIS Controls v8.1.
Försäkring	FairSSL A/S har hos If allmän ansvarsförsäkring, produktansvarsförsäkring och professionsansvarsförsäkring för IT-företag.
Underbiträden	UpCloud, OVHcloud, mailbox.org, Microsoft 365, Lettermint. Lista: sslbrain.com/sv/nis2/#underbitraden. Invändning inom 30 dagar efter aviseringen.
Avslut	Nycklar, certifikat och data i appliancen är era och stannar hos er; installerade certifikat fungerar tills de löper ut. Avsnitt 7 beskriver avbrott, omstart, utgånget abonnemang och en leverantör som inte längre finns. Personuppgifter i Cloud raderas från aktiva system inom 30 dagar.
Personuppgiftsbiträdesavtal	Skapas för ert konto i sslbrain Cloud.
Säkerhetskontakt	info@fairssl.dk

13. Vanliga frågor

Är sslbrain en leverantör ni behöver bedöma?

Ja. I NIS2-direktivets artikel 21.2 d och 21.3 och DORA artikel 28 uppmanas ni att bedöma era IKT-leverantörer. PDF:en har det ni behöver: vad FairSSL och sslbrain Cloud kan och inte kan göra, exit, kvarstående risker, registret och ett ifyllt leverantörsformulär.

Täcker dokumentationen DORA?

Ja. Den citerar RTS 2024/1774 artikel 7.1, 7.4 och 7.5 och visar hur inventering, automatisk förnyelse, vault, ny nyckel vid förnyelse och återkallande uppfyller kraven. Den innehåller registret enligt ITS 2024/2956 och en tabell över DORA artikel 28 till 30.

Vad händer om FairSSL försvinner?

Nycklar, certifikat och data finns hos er, installerade certifikat fungerar och appliancen fortsätter att köras. Efter en omstart låser de 12 backuporden upp. Avsnitt 7 beskriver varje situation och det som kräver Cloud i dag.

Hur länge sparas revisionsloggen?

På appliancen enligt abonnemang: Free 30 dagar, Basic 90 dagar, Professional 2 år och Enterprise 7 år. Behöver ni spara den längre exporterar ni den eller skickar den till ert SIEM.

Vilka exportformat finns?

CSV och JSON från Professional. Varje händelse har tidpunkt, användare, åtgärd, objekt, IP-adress, värden före och efter samt sin plats i hashkedjan.

Kan FairSSL komma åt era privata nycklar?

Nej. Era privata nycklar skapas och lagras krypterade i er egen appliance och dess säkerhetskopia, och skickas end-to-end-krypterade till de servrar där de installeras. FairSSL och sslbrain Cloud har ingen kopia av dem. Nycklarna kan bara öppnas med de krypterade data plus antingen era 12 backupord, som bara ni känner till, eller den roterande nyckel som sslbrain Cloud lämnar ut till er appliance. Annars kan de bara hämtas ut i appliancen av en användare med rätt att exportera nycklar, som först måste bekräfta sin identitet igen.

Behöver ni fler detaljer?

Omfattas ni av regler som kräver mer än den här sidan och vårt ifyllda leverantörsformulär, kan ni ansöka om tillgång till mer detaljerad dokumentation på info@fairssl.dk. Vi bedömer varje ansökan för sig.

Kontakt

Frågor om dokumentationen skickas till FairSSL A/S på:

info@fairssl.dk