NIS2 og DORA: FairSSL ACME og API

Til jeres leverandørvurdering af FairSSL: hvad API'et og ACME-serveren gør, hvor data ligger, hvilke kontroller produktet og vi har, og hvad der er jeres eget ansvar. Siden og PDF'en har samme indhold.

Dokumentation til jeres leverandørvurdering efter NIS2-direktivet og DORA-forordningen

Version 1.5
Dato 01-11-2026

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

Gælder for FairSSL's API og ACME-server på datoen ovenfor. Den nyeste udgave ligger på fairssl.dk/da/nis2-dora/.

FairSSL A/S, CVR-nr. 33075782, Åbrovej 29, 8586 Ørum Djurs, Danmark

Indhold

1. Tjenesten og FairSSL's rolle
2. Data, vi behandler, og hvor de ligger
3. Underleverandører til jeres informationsregister
4. Ændringer, adgang, opdateringer, hændelser og forsikring
5. Kontroller i ACME-serveren og kontrolpanelet
6. Private nøgler
7. Exit og koncentrationsrisiko
8. Ekstern kontrol og sikkerhedskontakt
9. DORA
10. NIS2 artikel 21, stk. 2, litra a-j
11. Udfyldt leverandørskema

1. Tjenesten og FairSSL's rolle

API og kontrolpanel	Bestilling af certifikater fra DigiCert, GlobalSign og Sectigo, overvågning af certifikater og udløb, brugere med rettigheder pr. konto, overvågning af CT-logs for jeres domæner og AutoDNS, som opretter DNS-valideringen hos jeres DNS-udbyder.
ACME-server	En ACME-server efter RFC 8555 på fairssl.dk/acme med External Account Binding (EAB) og ACME Renewal Information (ARI, RFC 9773). Jeres egne ACME-klienter henter og fornyer certifikaterne.
FairSSL's egen status	FairSSL er ikke selv omfattet af NIS2: certifikaterne udstedes af CA'erne, og FairSSL er ikke tillidstjenesteudbyder efter eIDAS. Siden findes for at understøtte jeres forpligtelser i leverandørkæden efter NIS2 artikel 21, stk. 2, litra d, og stk. 3, og DORA artikel 28-30. For finansielle virksomheder går DORA forud for NIS2 (NIS2 artikel 4).
Lovgrundlag	NIS2-direktivet (EU) 2022/2555, i Danmark gennemført ved lov nr. 434 af 6. maj 2025 (NIS2-loven). DORA-forordningen (EU) 2022/2554 med RTS (EU) 2024/1774 og ITS (EU) 2024/2956. For kunder, der er digital infrastruktur eller udbydere af administrerede tjenester: gennemførelsesforordning (EU) 2024/2690.

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

2. Data, vi behandler, og hvor de ligger

Det meste er certifikatdata, som i forvejen bliver offentlige i CT-logs, når certifikatet udstedes. Persondata er kun fakturering, kontaktpersoner, login og ACME-klienternes IP-adresser. Data om jeres interne miljø bliver hos jer, ud over det installationsscriptet melder tilbage.

- Websites, kontrolpanel, API, ACME-server og database kører hos Amazon Web Services EMEA SARL i AWS-regionen eu-central-1 (Frankfurt, Tyskland). Krypterede sikkerhedskopier af databasen ligger i eu-north-1 (Stockholm, Sverige).
- Vi arbejder aktivt på at flytte drifts- og forretningssystemer, der er hostet eller ejet uden for EU, til tjenester, der både er hostet og ejet i EU. Certifikatudstederne (CA'erne) følger det valgte produkt og er ikke en del af flytningen.
- Automatiske system-mails sendes via Lettermint B.V. (Holland), og data behandles og opbevares i EU.
- Datamindskning er en kontrol i sig selv (NIS2 artikel 21, stk. 2, GDPR artikel 25 og 32): ved ACME har FairSSL aldrig jeres private nøgle, og jeres interne miljø ses kun gennem det, installationsscriptet melder tilbage. Det giver en lav risikoprofil for fortrolighed. Kravene til tilgængelighed under DORA ændres ikke af det.

Data	Hvor	Offentligt?
Certifikatdata: domænenavne og, for OV/EV, firmanavn og adresse	FairSSL (AWS Frankfurt) og den CA, der udsteder	Ja, i CT-logs efter udstedelse
Ordre- og valideringsdata for OV/EV: firmaoplysninger og kontaktperson	FairSSL (AWS Frankfurt) og den CA, der validerer	Firmaoplysninger ja, kontaktperson nej
Fakturering, kontaktpersoner og login	FairSSL (AWS Frankfurt); fakturaer i Visma e-conomic	Nej
Servernavn, thumbprint, resultat og fejltekst fra installationen; ACME-klientens IP-adresse og version i hændelsesloggen	FairSSL (AWS Frankfurt), sendt af installationsscriptet i simple-acme-downloaden	Nej

Data	Hvor	Offentligt?
Private nøgler	Ved ACME hos jer. Kun når I lader FairSSL lave nøgle og CSR, opbevares nøglen krypteret hos FairSSL i en begrænset periode (afsnittet om nøgler)	Nej

3. Underleverandører til jeres informationsregister

Til informationsregistret efter DORA artikel 28, stk. 3, og gennemførelsesforordning (EU) 2024/2956. Jeres direkte leverandør er FairSSL A/S, CVR-nr. 33075782, Danmark: forhandler af TLS-certifikater, ACME-server og API til certifikatstyring. Tabellen viser FairSSL's underdatabehandlere, de samme som på listen over underleverandører. Certifikatudstederne DigiCert, GlobalSign og Sectigo er selvstændigt ansvarlige under egne aftaler; de og vores andre leverandører står i privatlivspolitikken. Om tjenesten understøtter en kritisk eller vigtig funktion hos jer, er jeres vurdering.

Leverandør	Tjeneste for FairSSL	Hvor data opbevares og behandles	Overførselsgrundlag
UpCloud Ltd (Finland)	Fra 11. november 2026: hosting af websites, kontrolpanel, API, ACME-server og database	EU (København og Amsterdam)	EU
mailbox.org (Heinlein Hosting GmbH, Tyskland)	Fra 11. november 2026: e-mail	Tyskland	EU
OVHcloud (OVH SAS, Frankrig)	Fra 11. november 2026: låste sikkerhedskopier og håndtering af krypteringsnøgler	Frankrig	EU
Lettermint B.V. (Holland)	Automatiske system-mails	EU	EU
Amazon Web Services EMEA SARL (Luxembourg)	Hosting af websites, kontrolpanel, API, ACME-server og database; AWS WAF; logfiler i Amazon S3	eu-central-1 (Frankfurt); sikkerhedskopier af databasen i eu-north-1 (Stockholm)	EU; DPF og SCC for koncernen i USA
Microsoft 365 og Azure	Kontor- og cloud-infrastruktur	EU (Irland og Holland)	DPF og SCC
Freshdesk (Freshworks Inc., USA)	Helpdesk	AWS Frankfurt	DPF

4. Ændringer, adgang, opdateringer, hændelser og forsikring

- Alle ændringer sker gennem versionsstyring, og hver udrulning til production er sporbar i historikken.
- Administrativ adgang er begrænset til nøglepersoner med rollebaseret adgang (RBAC) og mindst mulige rettigheder.
- Sikkerhedsopdateringer til systemer og afhængigheder installeres løbende.
- Vi varsler kunden uden unødig forsinkelse og senest inden for 48 timer, hvis en sikkerhedshændelse har påvirket kundens data eller tjenesten. Sætningen står også i salgsbetingelserne. En sårbarhed, der lukkes uden at have påvirket data eller tjenesten, er ikke en hændelse i NIS2's forstand (artikel 6, nr. 6 og 15).
- Kunden er ansvarlig for backup af egne systemer og data, også før FairSSL udfører installation eller fjernassistance.
- FairSSL A/S har hos If erhvervsansvars-, produktansvars- og professionel ansvarsforsikring for IT-virksomheder. Forsikringsbevis kan fås på anmodning.
- FairSSL har ikke en ISO 27001-certificering. Kontrollerne er kortlagt til ISO/IEC 27001:2022 bilag A og CIS Controls v8.1. En uafhængig erklæring, fx ISAE 3000, kan indgå i en kundeaftale for kundens regning efter nærmere aftale.

5. Kontroller i ACME-serveren og kontrolpanelet

Kontrollerne, I selv styrer i kontrolpanelet. Standardværdien står i sidste kolonne.

Kontrol	Hvad den gør	Standard
EAB til engangsbrug	En ny ACME-klient skal have en EAB-nøgle. En nøgle til én klient slettes i samme transaktion, som opretter klientens konto, så den ikke kan bruges igen.	Guiden står på "Én klient"; "Flere klienter" vælges aktivt
Lås på navne og wildcard pr. klient	Når låsen er slået til, kan en klient, der har et gyldigt certifikat, kun forny og genudstede de navne, den har, eller færre, og den kan ikke bestille wildcard. Forsøg afvises og logges som hændelse. Første opsætning med EAB må bruge alle navne, kontoen kan validere, så en ny server kommer i gang uden at vente på godkendelse; derefter låser I klienten.	Låst på profilen; slås til pr. klient
Profiler og konti	Klienter samles i profiler med hver sit produkt, låse og notifikationer. Konti hos FairSSL har hver sine AutoDNS-indstillinger, så fx produktion og test kan holdes adskilt.	Efter jeres opsætning
CAA	ACME-serveren tjekker CAA-poster for alle navne mod den CA, der skal udstede, og afviser ordren med en CAA-fejl, når CAA ikke tillader CA'en. Med CAA styrer I selv, hvilke CA'er der må udstede for jeres domæner.	Altid
Notifikationer pr. profil	Mails om hændelser i seks niveauer: kritisk, fejl, advarsler, ordrer, information og fejlsøgning. Hvert niveau omfatter dem under sig.	Ordrer (niveau 200): fejl, advarsler, nye ordrer og nye certifikater
Advarsel, når en klient holder op med ARI	En daglig kontrol advarer, når en klient, der har brugt ARI, ikke har spurgt i 3 dage, og igen efter 7 dage. Det fanger en klient, der er stoppet, før certifikatet udløber.	Altid
Tilbagemelding om installationen	simple-acme fra FairSSL melder efter hver fornyelse tilbage, om certifikatet blev installeret, med servernavn og thumbprint. Resultatet står som hændelse på klienten i kontrolpanelet.	Slået til i simple-acme-downloaden
Monitorerings-API v1	Læseadgang med token til oversigt, certifikater, ACME-klienter og hændelser som JSON, PRTG eller Prometheus, så jeres egen overvågning kan følge certifikaterne.	Token oprettes af jer
To-faktor-login	Kontoen kan kræve to-faktor-login for alle brugere i kontrolpanelet.	To-faktor kan kræves pr. konto

6. Private nøgler

- Ved ACME laver jeres ACME-klient den private nøgle på jeres egen server, og nøglen bliver der. ACME-serveren modtager kun certifikatanmodningen (CSR) og har ingen funktion, der tager imod en privat nøgle.
- Bestiller I et certifikat uden ACME, kan FairSSL's CSR-service lave nøgle og CSR for jer. Nøglen gemmes krypteret med AES-256, med en nøgle afledt af ordren og en adgangskode til download. Adgangskoden opbevares krypteret adskilt fra nøglen, og download kræver både linket og adgangskoden.
- En kørsel hver time sletter nøglen 48 timer efter første download, og senest 60 dage efter den blev lavet (30 dage, hvis ordren annulleres eller certifikatet tilbagekaldes). I kan også selv slette den med linket og adgangskoden. Hver sletning logges på ordren.
- Vil I ikke have, at FairSSL nogensinde har jeres private nøgle, så lav nøglen selv eller brug ACME.

7. Exit og koncentrationsrisiko

- ACME er en åben standard (RFC 8555), som alle større CA'er og ACME-klienter understøtter.
- Et skifte til en anden udbyder kræver en ny konto og EAB hos den nye udbyder, validering af domænerne, eventuelt nye DNS- og CAA-poster og den nye udbyders URL i jeres ACME-klient.
- Installerede certifikater virker til de udløber, også hvis FairSSL ikke længere leverer. Certifikaterne opbevares hos jer og hos den CA, der har udstedt dem.

- Oversigten over jeres certifikater og ACME-klienter kan hentes via monitorerings-API'et, så I har jeres inventar uden for FairSSL.

8. Ekstern kontrol og sikkerhedskontakt

- fairssl.dk og fairssl.se scannes ugentligt af DigiCerts eksterne sårbarhedsscanning uden login. Seneste rapport kan fås på anmodning. ACME-serveren svarer på fairssl.dk/acme på samme servere som fairssl.dk.
- CA'erne revideres årligt efter WebTrust for CAs eller ETSI EN 319 411. Revisionen dækker CA'ernes drift og udstedelse, ikke FairSSL.
- Sikkerhedshenvendelser og sårbarheder sendes til info@fairssl.dk. Kontakten står også i /.well-known/security.txt (RFC 9116) på fairssl.dk og fairssl.se.

Kilder
- RFC 9116 (security.txt): https://www.rfc-editor.org/rfc/rfc9116
- CCADB: CA'ernes revisionsrapporter: https://www.ccadb.org/resources

9. DORA

RTS (EU) 2024/1774 artikel 7 om håndtering af kryptografiske nøgler kræver, at finansielle virksomheder fornyer certifikater før udløb (stk. 5) og fører et register over certifikater og enheder, der opbevarer certifikater (stk. 4).

- Stk. 5: ACME-klienten fornyer automatisk før udløb, og ARI fortæller klienten, hvornår den skal forny. Advarslen om en klient, der er holdt op med ARI, og overvågningen af udløb fanger en fornyelse, der ikke sker.
- Stk. 4, delvist: kontrolpanelet og monitorerings-API'et giver en oversigt over certifikater og ACME-klienter. Enheder, der opbevarer certifikater (servere, HSM'er, load balancere), registrerer I selv.

DORA artikel 28-30 og hvor på siden I finder svaret:

DORA	Emne	Afsnit
Art. 28, stk. 1-2	Jeres politik for IKT-tredjepartsrisiko	Jeres ansvar; siden er input
Art. 28, stk. 3	Informationsregister	Underleverandører
Art. 28, stk. 4-5	Vurdering før aftale	Data, kontroller, nøgler, ekstern kontrol
Art. 28, stk. 8	Exitstrategi	Exit og koncentrationsrisiko
Art. 29	Koncentrationsrisiko og underleverandører	Exit; underleverandører
Art. 30, stk. 2, litra a	Beskrivelse af tjenesten og underleverandører	Tjenesten; underleverandører
Art. 30, stk. 2, litra b	Hvor data behandles og opbevares	Data og placering
Art. 30, stk. 2, litra c	Tilgængelighed, integritet, fortrolighed	Kontroller; nøgler; ændringer og adgang
Art. 30, stk. 2, litra d	Adgang til data ved ophør	Exit (monitorerings-API)
Art. 30, stk. 2, litra e	Serviceniveau	Salgsbetingelserne afsnit 12: ingen SLA
Art. 30, stk. 2, litra f	Bistand ved IKT-hændelser	Hændelser (48 timer)
Art. 30, stk. 2, litra g-i	Samarbejde med myndigheder, opsigelse, uddannelse	Salgsbetingelserne; i øvrigt på forespørgsel
Art. 30, stk. 3	Kritiske eller vigtige funktioner	Den fulde pakke svarer på de punkter, der giver mening; resten på forespørgsel

Kilder
- RTS (EU) 2024/1774: https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj
- ITS (EU) 2024/2956: https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj

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

Tre lag i hver række: hvad produktet hjælper jer med, vores egne kontroller, og hvad der er jeres ansvar.

Litra	Produktet	Vores kontroller	Jeres ansvar
a) Risikoanalyse og politikker	Data- og underleverandørtabellen til jeres risikoanalyse af FairSSL.	Datamindskning; kontroller kortlagt til ISO/IEC 27001:2022 bilag A og CIS Controls v8.1.	Jeres risikoanalyse og politikker.
b) Håndtering af hændelser	Notifikationer om fejl, afviste ordrer og installationer, der fejler.	Varsling senest inden for 48 timer ved hændelser, der påvirker jeres data eller tjenesten.	Jeres hændelsesprocedure og indberetning.
c) Driftskontinuitet og backup	Installerede certifikater virker uden FairSSL; ARI og fornyelse før udløb.	Database i Frankfurt med krypterede sikkerhedskopier i Stockholm.	Backup af egne systemer, også før installation eller fjernassistance.
d) Forsyningskædes ikkerhed	CAA begrænser, hvilke CA'er der må udstede.	Underleverandører med placering og overførselsgrundlag.	Jeres vurdering af FairSSL som leverandør.
e) Sikkerhed ved anskaffelse, udvikling og vedligeholdelse	ACME efter RFC 8555 og ARI efter RFC 9773.	Versionsstyring med sporbar udrulning; løbende sikkerhedsopdateringer; ugentlig ekstern scanning; security.txt.	Opdatering af jeres ACME-klienter og servere.
f) Vurdering af effektivitet	Monitorerings-API'et til jeres egen overvågning af certifikater og klienter.	Scanningsrapport på anmodning.	Jeres egen måling af kontrollerne.
g) Cyberhygiejne og uddannelse	Automatisk fornyelse i stedet for manuelle trin.	Mindst mulige rettigheder for administrativ adgang.	Uddannelse af jeres egne medarbejdere.
h) Kryptografi	Den private nøgle bliver hos jer ved ACME.	CSR-servicens nøgler krypteres med AES-256 og slettes automatisk.	Jeres kryptografipolitik og nøglelængder.
i) Personalesikkerhed, adgangsstyring og aktiver	Brugere med rettigheder pr. konto; EAB til engangsbrug; lås pr. klient; oversigt over certifikater og klienter.	Rollebaseret adgang (RBAC) med mindst mulige rettigheder.	Hvem hos jer har adgang til kontrolpanelet og ACME-klienterne.
j) Multifaktorautentifikation	To-faktor-login, som kontoen kan kræve for alle brugere.	Adgang efter rolle og mindst mulige rettigheder.	At slå kravet om to-faktor til for jeres konto.

11. Udfyldt leverandørskema

De spørgsmål, en leverandørvurdering typisk stiller, med vores svar. Hent det også som CSV.

Spørgsmål	Svar	Afsnit
Leverandørens navn og registreringsnummer	FairSSL A/S, CVR-nr. 33075782, Åbrovej 29, 8586 Ørum Djurs, Danmark	Underleverandører
Hvilken tjeneste leveres?	TLS-certifikater fra DigiCert, GlobalSign og Sectigo, ACME-server og API til certifikatstyring	Tjenesten
Er leverandøren selv omfattet af NIS2?	Nej. CA'erne udsteder, og FairSSL er ikke tillidstjenesteudbyder efter eIDAS	Tjenesten
Hvor opbevares og behandles data?	AWS eu-central-1 (Frankfurt); krypterede sikkerhedskopier af databasen i eu-north-1 (Stockholm); underleverandører som i tabellen	Data og placering

Spørgsmål	Svar	Afsnit
Behandles data uden for EU?	Ja, hos de underleverandører, tabellen nævner, og hos CA'erne DigiCert og Sectigo i USA under DPF	Underleverandører
Har leverandøren adgang til vores private nøgler?	Ikke ved ACME. Ved CSR-servicen krypteret i højst 60 dage	Private nøgler
Hvordan styres ændringer?	Alle ændringer sker gennem versionsstyring, og hver udrulning til production er sporbar i historikken.	Ændringer
Hvordan styres administrativ adgang?	Administrativ adgang er begrænset til nøglepersoner med rollebaseret adgang (RBAC) og mindst mulige rettigheder.	Ændringer
Hvordan holdes systemer opdateret?	Sikkerhedsopdateringer til systemer og afhængigheder installeres løbende.	Ændringer
Hvornår varsles vi om hændelser?	Uden unødig forsinkelse og senest inden for 48 timer, hvis en sikkerhedshændelse har påvirket jeres data eller tjenesten	Hændelser
Har leverandøren en certificering?	Ikke ISO 27001. Kontrollerne er kortlagt til ISO/IEC 27001:2022 bilag A og CIS Controls v8.1; ISAE 3000 efter aftale for kundens regning	Ændringer
Ekstern test?	Ugentlig ekstern sårbarhedsscanning af fairssl.dk og fairssl.se uden login; rapport på anmodning	Ekstern kontrol
Forsikring?	Erhvervsansvars-, produktansvars- og professionel ansvarsforsikring hos If; bevis på anmodning	Forsikring
Kan vi kræve to-faktor-login?	Ja, for alle brugere på kontoen	Kontroller
Exit?	ACME er en åben standard; installerede certifikater virker til udløb	Exit
Tilbyder leverandøren en SLA?	Nej. Se salgsbetingelserne afsnit 12	DORA
Sikkerhedskontakt	info@fairssl.dk og /.well-known/security.txt	Ekstern kontrol

Ofte stillede spørgsmål

Er FairSSL omfattet af NIS2?

Nej. FairSSL forhandler certifikater, som CA'erne udsteder, og er ikke tillidstjenesteudbyder efter eIDAS. Siden findes, fordi I som kunde skal vurdere jeres leverandører efter NIS2 artikel 21, stk. 2, litra d, og stk. 3, eller DORA artikel 28-30.

Skal FairSSL i vores DORA-informationsregister?

Ja, hvis I er en finansiel virksomhed og bruger FairSSL's API eller ACME-server. Afsnittet om underleverandører har de oplysninger, registret beder om. Om tjenesten understøtter en kritisk eller vigtig funktion, vurderer I selv.

Kan FairSSL se vores private nøgler?

Ikke ved ACME: nøglen laves og bliver på jeres server. Kun hvis I bestiller med FairSSL's CSR-service, opbevares nøglen krypteret, indtil den slettes automatisk.

Hvad sker der, hvis FairSSL ikke kan levere?

Installerede certifikater virker til de udløber. I kan skifte til en anden ACME-udbyder med en ny konto, EAB, validering og den nye URL i jeres ACME-klient.

Udfylder I vores leverandørskema?

Vi udfylder ikke kundens eget skema. Leverandørskemaet på siden og den fulde pakke svarer på de spørgsmål, en vurdering typisk stiller.

Den fulde pakke

Skal I bruge dokumentationen til en leverandørvurdering efter NIS2 eller DORA, så skriv til os med virksomhedens navn og hvad vurderingen skal dække. Så sender vi den fulde pakke med scanningsrapport og vores udfyldte leverandørskema.

info@fairssl.dk