

# NIS2 och DORA: FairSSL ACME och API

För er leverantörsbedömning av FairSSL: vad API:et och ACME-servern gör, var data finns, vilka kontroller produkten och vi har och vad ni själva ansvarar för. Sidan och PDF:en har samma innehåll.

Dokumentation för er leverantörsbedömning enligt NIS2-direktivet och DORA-förordningen

Version 1.5

Datum 01-11-2026

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

Gäller för FairSSL:s API och ACME-server på datumet ovan. Den senaste versionen finns på [fairssl.se/sv/nis2-dora/](https://fairssl.se/sv/nis2-dora/).

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

## Innehåll

1. Tjänsten och FairSSL:s roll
2. Data vi behandlar och var de finns
3. Underleverantörer för ert informationsregister
4. Ändringar, åtkomst, uppdateringar, incidenter och försäkring
5. Kontroller i ACME-servern och kontrollpanelen
6. Privata nycklar
7. Exit och koncentrationsrisk
8. Extern kontroll och säkerhetskontakt
9. DORA
10. NIS2 artikel 21.2 a-j
11. Ifyllt leverantörsformulär

# 1. Tjänsten och FairSSL:s roll

|                       |                                                                                                                                                                                                                                                                                                                                             |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| API och kontrollpanel | Beställning av certifikat från DigiCert, GlobalSign och Sectigo, övervakning av certifikat och utgångsdatum, användare med behörigheter per konto, övervakning av CT-loggar för era domäner och AutoDNS, som ställer in DNS-valideringen hos er DNS-leverantör.                                                                             |
| ACME-server           | En ACME-server enligt RFC 8555 på fairssl.dk/acme med External Account Binding (EAB) och ACME Renewal Information (ARI, RFC 9773). Era egna ACME-klienter hämtar och förnyar certifikaten.                                                                                                                                                  |
| FairSSL:s egen status | FairSSL omfattas inte självt av NIS2: certifikaten utfärdas av CA:erna och FairSSL är inte en tillhandahållare av betrodda tjänster enligt eIDAS. Sidan stöder era skyldigheter i leveranskedjan enligt NIS2 artikel 21.2 d och 21.3 och DORA artiklarna 28-30. För finansiella företag har DORA företrädare framför NIS2 (NIS2 artikel 4). |
| Rättslig grund        | NIS2-direktivet (EU) 2022/2555, i Sverige genomfört genom Cybersäkerhetslag (2025:1506). DORA-förordningen (EU) 2022/2554 med RTS (EU) 2024/1774 och ITS (EU) 2024/2956. För kunder inom digital infrastruktur eller som tillhandahåller hanterade tjänster: genomförandeförordning (EU) 2024/2690.                                         |

Källor

- NIS2-direktivet (EU) 2022/2555: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- DORA-förordningen (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 behandlar och var de finns

Det mesta är certifikatdata som blir offentliga i CT-loggar när certifikatet utfärdas. Personuppgifter är begränsade till fakturering, kontaktpersoner, inloggning och ACME-klienternas IP-adresser. Data om er interna miljö stannar hos er, utöver det som installationsskriptet rapporterar tillbaka.

- Webbplatser, kontrollpanel, API, ACME-server och databas körs hos Amazon Web Services EMEA SARL i AWS-regionen eu-central-1 (Frankfurt, Tyskland). Krypterade säkerhetskopior av databasen finns i eu-north-1 (Stockholm, Sverige).
- Vi arbetar aktivt med att flytta drift- och affärssystem som driftas eller ägs utanför EU till tjänster som både driftas och ägs inom EU. Certifikatutfärdarna (CA:erna) beror på den valda produkten och ingår inte i flytten.
- Automatiska systemmejl skickas via Lettermint B.V. (Nederländerna), och data behandlas och lagras inom EU.
- Uppgiftsminimering är en kontroll i sig (NIS2 artikel 21.2, GDPR artiklarna 25 och 32): med ACME har FairSSL aldrig er privata nyckel, och er interna miljö syns bara genom det som installationsskriptet rapporterar tillbaka. Det ger en låg riskprofil för konfidentialitet. Kraven på tillgänglighet enligt DORA ändras inte av detta.

| Data                                                                                                                   | Var                                                                                      | Offentligt?                             |
|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-----------------------------------------|
| Certifikatdata: domännamn och, för OV/EV, företagsnamn och adress                                                      | FairSSL (AWS Frankfurt) och den CA som utfärdar certifikatet                             | Ja, i CT-loggar efter utfärdandet       |
| Order- och valideringsdata för OV/EV: företagsuppgifter och kontaktperson                                              | FairSSL (AWS Frankfurt) och den CA som validerar                                         | Företagsuppgifter ja, kontaktperson nej |
| Fakturering, kontaktpersoner och inloggning                                                                            | FairSSL (AWS Frankfurt); fakturor i Visma e-economic                                     | Nej                                     |
| Servernamn, tumavtryck, resultat och feltext från installationen; ACME-klientens IP-adress och version i händelselogen | FairSSL (AWS Frankfurt), skickat av installationsskriptet i nedladdningen av simple-acme | Nej                                     |

| Data            | Var                                                                                                                                                            | Offentligt? |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| Privata nycklar | Hos er när ni använder ACME. Bara när ni låter FairSSL skapa nyckel och CSR lagras nyckeln krypterad hos FairSSL under en begränsad tid (avsnittet om nycklar) | Nej         |

### 3. Underleverantörer för ert informationsregister

För informationsregistret enligt DORA artikel 28.3 och genomförandeförordning (EU) 2024/2956. Er direkta leverantör är FairSSL A/S, CVR-nr 33075782, ett danskt företag: återförsäljare av TLS-certifikat, ACME-server och API för certifikathantering. Tabellen visar FairSSL:s underbiträden, samma som i förteckningen över underbiträden. Certifikatutfärdarna DigiCert, GlobalSign och Sectigo är självständiga personuppgiftsansvariga enligt egna avtal. De och våra andra leverantörer finns i integritetspolicyn. Ni bedömer själva om tjänsten stöder en kritisk eller viktig funktion hos er.

| Leverantör                                    | Tjänst för FairSSL                                                                                | Var data lagras och behandlas                                                   | Grund för överföring                |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|-------------------------------------|
| UpCloud Ltd (Finland)                         | Från 11 november 2026: drift av webbplatser, kontrollpanel, API, ACME-server och databas          | EU (Köpenhamn och Amsterdam)                                                    | EU                                  |
| mailbox.org (Heinlein Hosting GmbH, Tyskland) | Från 11 november 2026: e-post                                                                     | Tyskland                                                                        | EU                                  |
| OVHcloud (OVH SAS, Frankrike)                 | Från 11 november 2026: låsta säkerhetskopior och hantering av krypteringsnycklar                  | Frankrike                                                                       | EU                                  |
| Lettermint B.V. (Nederländerna)               | Automatiska systemmejl                                                                            | EU                                                                              | EU                                  |
| Amazon Web Services EMEA SARL (Luxemburg)     | Drift av webbplatser, kontrollpanel, API, ACME-server och databas; AWS WAF; loggfiler i Amazon S3 | eu-central-1 (Frankfurt); säkerhetskopior av databasen i eu-north-1 (Stockholm) | EU; DPF och SCC för koncernen i USA |
| Microsoft 365 och Azure                       | Kontors- och molninfrastruktur                                                                    | EU (Irland och Nederländerna)                                                   | DPF och SCC                         |
| Freshdesk (Freshworks Inc., USA)              | Kundsupport                                                                                       | AWS Frankfurt                                                                   | DPF                                 |

### 4. Ändringar, åtkomst, uppdateringar, incidenter och försäkring

- Alla ändringar sker genom versionshantering, och varje driftsättning till production är spårbar i historiken.
- Administrativ åtkomst är begränsad till nyckelpersoner med rollbaserad åtkomstkontroll (RBAC) och minsta möjliga behörighet.
- Säkerhetsuppdateringar för system och beroenden installeras löpande.
- Vi underrättar kunden utan onödigt dröjsmål och senast inom 48 timmar om en säkerhetsincident har påverkat kundens data eller tjänsten. Meningen finns också i försäljningsvillkoren. En sårbarhet som åtgärdas utan att ha påverkat data eller tjänsten är inte en incident i NIS2:s mening (artikel 6.6 och 6.15).
- Kunden ansvarar för säkerhetskopiering av egna system och data, även innan FairSSL utför installation eller fjärrassistans.
- FairSSL A/S har företagsansvars-, produktansvars- och professionsansvarsförsäkring för IT-företag hos If. Försäkringsbevis finns på begäran.
- FairSSL är inte ISO 27001-certifierat. Kontrollerna är kartlagda mot ISO/IEC 27001:2022 bilaga A och CIS Controls v8.1. Ett oberoende bestyrkande, till exempel enligt ISAE 3000, kan ingå i ett kundavtal på kundens bekostnad efter särskild överenskommelse.

### 5. Kontroller i ACME-servern och kontrollpanelen

Kontrollerna ni själva styr i kontrollpanelen. Standardvärdet står i sista kolumnen.

| Kontroll                                 | Vad den gör                                                                                                                                                                                                                                                                                                                                                                                  | Standard                                                                |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| EAB för engångsbruk                      | En ny ACME-klient behöver en EAB-nyckel. En nyckel för en enda klient raderas i samma transaktion som skapar klientens konto, så att den inte kan användas igen.                                                                                                                                                                                                                             | Guiden är inställd på "En klient"; "Flera klienter" måste väljas aktivt |
| Låsning av namn och wildcard per klient  | När låsningen är aktiverad kan en klient med ett giltigt certifikat bara förnya och återutfärda de namn den har, eller färre, och den kan inte beställa wildcard. Försök avvisas och loggas som en händelse. Vid den första konfigurationen med EAB får alla namn som kontot kan validera användas, så att en ny server kommer igång utan att vänta på godkännande; sedan låser ni klienten. | Låst i profilen; aktiveras per klient                                   |
| Profiler och konton                      | Klienter samlas i profiler med varsin produkt, låsningar och aviseringar. Konton hos FairSSL har egna AutoDNS-inställningar, så att till exempel produktion och test kan hållas åtskilda.                                                                                                                                                                                                    | Enligt er konfiguration                                                 |
| CAA                                      | ACME-servern kontrollerar CAA-poster för alla namn mot den CA som ska utfärda certifikatet och avvisar ordern med ett CAA-fel när CAA inte tillåter den CA:n. Med CAA styr ni själva vilka CA:er som får utfärda certifikat för era domäner.                                                                                                                                                 | Alltid                                                                  |
| Aviseringar per profil                   | E-post om händelser på sex nivåer: kritiskt, fel, varningar, order, information och felsökning. Varje nivå omfattar dem under sig.                                                                                                                                                                                                                                                           | Order (nivå 200): fel, varningar, nya order och nya certifikat          |
| Varning när en klient slutar använda ARI | En daglig kontroll varnar när en klient som har använt ARI inte har gjort en förfrågan på 3 dagar, och igen efter 7 dagar. Det upptäcker en klient som har stannat innan certifikatet går ut.                                                                                                                                                                                                | Alltid                                                                  |
| Återkoppling om installationen           | simple-acme från FairSSL rapporterar efter varje förnyelse om certifikatet installerades, med servernamn och tumavtryck. Resultatet visas som en händelse för klienten i kontrollpanelen.                                                                                                                                                                                                    | Aktiverat i nedladdningen av simple-acme                                |
| Övervaknings-API v1                      | Läsåtkomst med token till översikt, certifikat, ACME-klienter och händelser som JSON, PRTG eller Prometheus, så att er egen övervakning kan följa certifikaten.                                                                                                                                                                                                                              | Ni skapar token                                                         |
| Tvåfaktorsinloggning                     | Kontot kan kräva tvåfaktorsinloggning för alla användare i kontrollpanelen.                                                                                                                                                                                                                                                                                                                  | Tvåfaktorsinloggning kan krävas per konto                               |

## 6. Privata nycklar

- Med ACME skapar er ACME-klient den privata nyckeln på er egen server, och nyckeln stannar där. ACME-servern tar bara emot certifikatsigneringsförfrågan (CSR) och har ingen funktion som tar emot en privat nyckel.
- Om ni beställer ett certifikat utan ACME kan CSR-tjänsten hos FairSSL skapa nyckel och CSR åt er. Nyckeln lagras krypterad med AES-256, med en nyckel härledd från ordern och ett lösenord för nedladdning. Lösenordet lagras krypterat separat från nyckeln, och nedladdning kräver både länken och lösenordet.
- En körning varje timme raderar nyckeln 48 timmar efter den första nedladdningen och senast 60 dagar efter att den skapades (30 dagar om ordern annulleras eller certifikatet återkallas). Ni kan också radera den själva med länken och lösenordet. Varje radering loggas på ordern.
- Om ni inte vill att FairSSL någonsin ska ha er privata nyckel, skapa nyckeln själva eller använd ACME.

## 7. Exit och koncentrationsrisk

- ACME är en öppen standard (RFC 8555) som alla större CA:er och ACME-klienter stöder.
- Ett byte till en annan leverantör kräver ett nytt konto och EAB hos den nya leverantören, validering av domänerna, eventuellt nya DNS- och CAA-poster och den nya leverantörens URL i er ACME-klient.
- Installerade certifikat fungerar tills de går ut, även om FairSSL inte längre levererar. Certifikaten lagras hos er och hos den CA som har utfärdat dem.
- Översikten över era certifikat och ACME-klienter kan hämtas via övervaknings-API:et, så att ni har er inventarieförteckning utanför FairSSL.

## 8. Extern kontroll och säkerhetskontakt

- fairssl.dk och fairssl.se skannas varje vecka av DigiCerts externa sårbarhetsskanning utan inloggning. Den senaste rapporten finns på begäran. ACME-servern svarar på fairssl.dk/acme på samma servrar som fairssl.dk.
- CA:erna revideras årligen enligt WebTrust for CAs eller ETSI EN 319 411. Revisionen omfattar CA:ernas drift och utfärdande, inte FairSSL.
- Säkerhetsfrågor och sårbarheter skickas till [info@fairssl.se](mailto:info@fairssl.se). Kontakten finns också i /.well-known/security.txt (RFC 9116) på fairssl.dk och fairssl.se.

### Källor

- RFC 9116 (security.txt): <https://www.rfc-editor.org/rfc/rfc9116>
- CCADB: CA:ernas revisionsrapporter: <https://www.ccadb.org/resources>

## 9. DORA

RTS (EU) 2024/1774 artikel 7 om hantering av kryptografiska nycklar kräver att finansiella företag förnyar certifikat innan de går ut (punkt 5) och för ett register över certifikat och enheter som lagrar certifikat (punkt 4).

- Punkt 5: ACME-klienten förnyar automatiskt innan certifikatet går ut, och ARI talar om för klienten när den ska förnya. Varningen om en klient som har slutat använda ARI och övervakningen av utgångsdatum upptäcker en förnyelse som uteblir.
- Punkt 4, delvis: kontrollpanelen och övervaknings-API:et ger en översikt över certifikat och ACME-klienter. Enheter som lagrar certifikat (servrar, HSM:er, lastbalanserare) registrerar ni själva.

DORA artiklarna 28-30 och var på sidan ni hittar svaret:

| DORA          | Ämne                                              | Avsnitt                                                                         |
|---------------|---------------------------------------------------|---------------------------------------------------------------------------------|
| Art. 28.1-2   | Er policy för IKT-tredjepartsrisk                 | Ert ansvar; sidan ger underlag                                                  |
| Art. 28.3     | Informationsregister                              | Underleverantörer                                                               |
| Art. 28.4-5   | Bedömning före avtal                              | Data, kontroller, nycklar, extern kontroll                                      |
| Art. 28.8     | Exitstrategi                                      | Exit och koncentrationsrisk                                                     |
| Art. 29       | Koncentrationsrisk och underleverantörer          | Exit; underleverantörer                                                         |
| Art. 30.2 a   | Beskrivning av tjänsten och underleverantörer     | Tjänsten; underleverantörer                                                     |
| Art. 30.2 b   | Var data behandlas och lagras                     | Data och lagringsplats                                                          |
| Art. 30.2 c   | Tillgänglighet, integritet, konfidentialitet      | Kontroller; nycklar; ändringar och åtkomst                                      |
| Art. 30.2 d   | Tillgång till data när avtalet upphör             | Exit (övervaknings-API)                                                         |
| Art. 30.2 e   | Servicenivå                                       | Försäljningsvillkoren avsnitt 12: ingen SLA                                     |
| Art. 30.2 f   | Bistånd vid IKT-incidenter                        | Incidenter (48 timmar)                                                          |
| Art. 30.2 g-i | Samarbete med myndigheter, uppsägning, utbildning | Försäljningsvillkoren; övrigt på förfrågan                                      |
| Art. 30.3     | Kritiska eller viktiga funktioner                 | Det fullständiga paketet besvarar de tillämpliga punkterna; resten på förfrågan |

### Källor

- RTS (EU) 2024/1774: [https://eur-lex.europa.eu/eli/reg\\_del/2024/1774/oj](https://eur-lex.europa.eu/eli/reg_del/2024/1774/oj)

## 10. NIS2 artikel 21.2 a-j

Tre lager i varje rad: vad produkten hjälper er med, våra egna kontroller och vad ni ansvarar för.

| Led                                                 | Produkten                                                                                                             | Våra kontroller                                                                                                         | Ert ansvar                                                                      |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| a) Riskanalys och policyer                          | Tabellerna över data och underleverantörer för er riskanalys av FairSSL.                                              | Uppgiftsminimering; kontroller kartlagda mot ISO/IEC 27001:2022 bilaga A och CIS Controls v8.1.                         | Er riskanalys och era policyer.                                                 |
| b) Incidenthantering                                | Aviseringar om fel, avvisade order och misslyckade installationer.                                                    | Underrättelse senast inom 48 timmar vid incidenter som påverkar era data eller tjänsten.                                | Era incidentrutiner och er rapportering.                                        |
| c) Driftskontinuitet och säkerhetskopiering         | Installerade certifikat fungerar utan FairSSL; ARI och förnyelse före utgångsdatum.                                   | Databas i Frankfurt med krypterade säkerhetskopior i Stockholm.                                                         | Säkerhetskopiering av egna system, även före installation eller fjärrassistans. |
| d) Säkerhet i leveranskedjan                        | CAA begränsar vilka CA:er som får utfärda certifikat.                                                                 | Underleverantörer med plats och grund för överföring.                                                                   | Er bedömning av FairSSL som leverantör.                                         |
| e) Säkerhet vid förvärv, utveckling och underhåll   | ACME enligt RFC 8555 och ARI enligt RFC 9773.                                                                         | Versionshantering med spårbar driftsättning; löpande säkerhetsuppdateringar; extern skanning varje vecka; security.txt. | Uppdatering av era ACME-klienter och servrar.                                   |
| f) Bedömning av effektivitet                        | Övervaknings-API:et för er egen övervakning av certifikat och klienter.                                               | Skanningsrapport på begäran.                                                                                            | Er egen mätning av kontrollerna.                                                |
| g) Cyberhygien och utbildning                       | Automatisk förnyelse i stället för manuella steg.                                                                     | Minsta möjliga behörighet för administrativ åtkomst.                                                                    | Utbildning av era egna medarbetare.                                             |
| h) Kryptografi                                      | Den privata nyckeln stannar hos er när ni använder ACME.                                                              | Nycklarna i CSR-tjänsten krypteras med AES-256 och raderas automatiskt.                                                 | Er kryptografipolicy och era nyckellängder.                                     |
| i) Personalsäkerhet, åtkomstkontroll och tillgångar | Användare med behörigheter per konto; EAB för engångsbruk; låsning per klient; översikt över certifikat och klienter. | Rollbaserad åtkomstkontroll (RBAC) med minsta möjliga behörighet.                                                       | Vem hos er som har åtkomst till kontrollpanelen och ACME-klienterna.            |
| j) Multifaktorautentisering                         | Tvåfaktorsinloggning som kontot kan kräva för alla användare.                                                         | Åtkomst efter roll och minsta möjliga behörighet.                                                                       | Att aktivera kravet på tvåfaktorsinloggning för ert konto.                      |

## 11. Ifyllt leverantörsformulär

De frågor en leverantörsbedömning brukar ställa, med våra svar. Hämta det också som CSV.

| Fråga                                      | Svar                                                                                              | Avsnitt           |
|--------------------------------------------|---------------------------------------------------------------------------------------------------|-------------------|
| Leverantörens namn och registreringsnummer | FairSSL A/S, CVR-nr 33075782, Åbrovej 29, 8586 Ørum Djurs, Danmark                                | Underleverantörer |
| Vilken tjänst levereras?                   | TLS-certifikat från DigiCert, GlobalSign och Sectigo, ACME-server och API för certifikathantering | Tjänsten          |

| Fråga                                               | Svar                                                                                                                                                  | Avsnitt                |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Omfattas leverantören själv av NIS2?                | Nej. CA:erna utfärdar certifikaten och FairSSL är inte en tillhandahållare av betrodda tjänster enligt eIDAS                                          | Tjänsten               |
| Var lagras och behandlas data?                      | AWS eu-central-1 (Frankfurt); krypterade säkerhetskopior av databasen i eu-north-1 (Stockholm); underleverantörer enligt tabellen                     | Data och lagringsplats |
| Behandlas data utanför EU?                          | Ja, hos de underbiträden som tabellen nämner och hos CA:erna DigiCert och Sectigo i USA enligt DPF                                                    | Underleverantörer      |
| Har leverantören åtkomst till våra privata nycklar? | Inte med ACME. Med CSR-tjänsten krypterat i högst 60 dagar                                                                                            | Privata nycklar        |
| Hur hanteras ändringar?                             | Alla ändringar sker genom versionshantering, och varje driftsättning till production är spårbar i historiken.                                         | Ändringar              |
| Hur hanteras administrativ åtkomst?                 | Administrativ åtkomst är begränsad till nyckelpersoner med rollbaserad åtkomstkontroll (RBAC) och minsta möjliga behörighet.                          | Ändringar              |
| Hur hålls systemen uppdaterade?                     | Säkerhetsuppdateringar för system och beroenden installeras löpande.                                                                                  | Ändringar              |
| När underrättas vi om incidenter?                   | Utan onödigt dröjsmål och senast inom 48 timmar om en säkerhetsincident har påverkat er data eller tjänsten                                           | Incidenter             |
| Har leverantören en certifiering?                   | Inte ISO 27001. Kontrollerna är kartlagda mot ISO/IEC 27001:2022 bilaga A och CIS Controls v8.1; ISAE 3000 efter överenskommelse på kundens bekostnad | Ändringar              |
| Extern testning?                                    | Extern sårbarhetsskanning av fairssl.dk och fairssl.se varje vecka utan inloggning; rapport på begäran                                                | Extern kontroll        |
| Försäkring?                                         | Företagsansvars-, produktansvars- och professionsansvarsförsäkring hos If; bevis på begäran                                                           | Försäkring             |
| Kan vi kräva tvåfaktorsinloggning?                  | Ja, för alla användare på kontot                                                                                                                      | Kontroller             |
| Exit?                                               | ACME är en öppen standard; installerade certifikat fungerar tills de går ut                                                                           | Exit                   |
| Erbjuder leverantören en SLA?                       | Nej. Se försäljningsvillkoren avsnitt 12                                                                                                              | DORA                   |
| Säkerhetskontakt                                    | info@fairssl.se och /.well-known/security.txt                                                                                                         | Extern kontroll        |

## Vanliga frågor

### Omfattas FairSSL av NIS2?

Nej. FairSSL säljer certifikat som CA:erna utfärdar och är inte en tillhandahållare av betrodda tjänster enligt eIDAS. Sidan finns eftersom ni som kund ska bedöma era leverantörer enligt NIS2 artikel 21.2 d och 21.3 eller DORA artiklarna 28-30.

### Ska FairSSL ingå i vårt DORA-informationsregister?

Ja, om ni är ett finansiellt företag och använder FairSSL:s API eller ACME-server. Avsnittet om underleverantörer innehåller de uppgifter som registret kräver. Ni bedömer själva om tjänsten stöder en kritisk eller viktig funktion.

### Kan FairSSL se våra privata nycklar?

Inte med ACME: nyckeln skapas och stannar på er server. Bara om ni beställer med CSR-tjänsten hos FairSSL lagras nyckeln krypterad tills den raderas automatiskt.

### Vad händer om FairSSL inte kan leverera?

Installerade certifikat fungerar tills de går ut. Ni kan byta till en annan ACME-leverantör med ett nytt konto, EAB, validering och den nya URL:en i er ACME-klient.

### Fyller ni i vårt leverantörsformulär?

Vi fyller inte i kundens eget formulär. Leverantörsformuläret på sidan och det fullständiga paketet besvarar de frågor en bedömning brukar ställa.

## Det fullständiga paketet

Om ni behöver dokumentationen för en leverantörsbedömning enligt NIS2 eller DORA, skriv till oss med företagets namn och vad bedömningen ska omfatta. Då skickar vi det fullständiga paketet med skanningsrapport och vårt ifyllda leverantörsformulär.

[info@fairssl.se](mailto:info@fairssl.se)