StepLock Cloud

Kryptering, sikker kommunikation & serveroversigt

Kryptering og sikker kommunikation

Vi beskytter al kommunikation og lagret information med etablerede og internationalt anerkendte sikkerhedsstandarder. Det betyder, at uvedkommende ikke kan læse, ændre eller manipulere data i systemet.

Hvad betyder det for jer?

- Al trafik mellem enheder og cloud er krypteret.
- Alle lagrede data er krypteret.
- Systemet verificerer altid, at det kommunikerer med den rette part.
- Der forekommer ingen ukrypteret kommunikation.

Sikkerhed i hele kæden

▶ **Cloudplatform**
Al kommunikation sker via en krypteret HTTPS-forbindelse – den samme forbindelse, som anvendes, når du foretager bankforretninger eller handler online. Det sikrer, at data ikke kan aflyttes, og at I kommunikerer med den rigtige server.

▶ **Lagret information**
Alle data i databasen er krypteret – også når de er lagret. Det beskytter informationen, selv hvis nogen skulle få fysisk adgang til serverne.

▶ **Styreenhed og cloud**
Kommunikationen er både krypteret og signeret. Det betyder, at data ikke kan ændres under overførslen.

▶ **Styreenhed og kortlæser**
Vi anvender den åbne og internationale sikkerhedsstandard OSDP Secure Channel. Det forhindrer manipulation eller aflytning mellem kortlæser og styreenhed.

▶ **Mobilåbning**
Al kommunikation mellem mobil og system sker via en krypteret forbindelse med certifikatverifikation.

Teknisk protokolbilag

KOMMUNIKA-TIONSLINK	PROTOKOL	KRYPTERING/ CERTIFIKAT	SIKKERHEDSFUNKTION
Cloudplatform	HTTPS (SSL/TLS)	Offentligt certifikat	Krypteret overførsel og serverautentificering. Offentligt certifikat SHA-256 med RSA-kryptering 2048 bit.
Lagring	-	AES-256	Alle data krypteres i hvile på databaseserveren.
Enhed	HTTPS (SSL/TLS) (HMAC)	Offentligt certifikat AES-256	Krypteret og signeret kommunikation mellem enhed og cloud. Offentligt certifikat SHA-256 med RSA-kryptering 2048 bit.
Enhed ↔ Kortlæser (OSDP)	OSDP SC	AES-128	Krypteret og beskyttet kommunikation mellem styreenhed og kortlæser i henhold til den åbne internationale standard OSDP IEC 60839-11-5.
Mobilåbning	TLS	Offentligt certifikat	Krypteret kommunikation mellem mobilklient og system. Offentligt certifikat SHA-256 med RSA-kryptering 2048 bit.

StepLock Cloud serveroversigt

Denne side beskriver vores serverplaceringer inden for EU med fokus på overholdelse af GDPR, høj tilgængelighed og geografisk redundans for forretningskritiske tjenester. Vores systemer er distribueret i Microsoft Azure for at sikre driftssikkerhed og skalerbarhed.

Oversigt over serverplaceringer

DATACENTER	PLACERING	LEVERANDØR	REDUNDANS	KOMMENTAR
Sweden Central	Sandviken, Sverige	Microsoft Azure	Høj	Primært datacenter
Norway East	Oslo, Norge	Microsoft Azure	Høj	Regionstilpasset telefoni for Norge

Tjenestefordeling

TJENESTETYPE	PLACERING	KOMMENTAR
Webtjenester	Sweden Central	Hostinger hele frontend-løsningen
API	Sweden Central	Alle API-endpoints
App-servere	Sweden Central	Drift af brugerapplikationer
Databaser	Sweden Central	Realtidsdata og brugerinformation
Telefoni (SE/DK)	Sweden Central	SIP/VoIP-funktioner for Sverige og Danmark
Telefoni (NO)	Norway East	SIP/VoIP-funktioner for Norge, lokalt placeret

Platform og infrastruktur

- Cloudplatform: Microsoft Azure
- Datacenterklassificering: Tier III+
- Redundans: LRS (lokalt redundant lagring)

Databeskyttelse

- Data lagres inden for EU
- Kryptering ved lagring og overførsel (TLS 1.2+)
- Backup af servere i henhold til 30-dages politik
- Backup af kundedata i henhold til 10-dages politik

Drift og overvågning

- 24/7 driftovervågning.

Certificeringer og efterlevelse

Alle datacentre opfylder:

- GDPR-kompabilitet
- ISO 27001 – Informationssikkerhed
- ISO 27018 – Beskyttelse af person-oplysninger i cloudmiljøer
- ISO 22301 – Kontinuitetsstyring
- SOC 1/2/3 – Kontrolrapportering
- EN 50600 – Datacenterdesign (Azure tilsvarende niveau)

StepLock Denmark A/S | Fælledvej 17, 7600 Struer, Danmark
+45 53 777 808 | www.steplock.dk | support@steplockaccess.dk