

ABONNENTAVTALENS HOVEDDEL (DEL 1)

1 Innledning

Dette dokumentet (Del 1) utgjør sammen med Bestillingsskjema for SSL-sertifikater (Del 2) og *Certification Practice Statement for Buypass Class 2 SSL certificates* (Del 3) Abonnementavtalen for Buypass Class 2 SSL-sertifikater.

Buypass Class 2 SSL sertifikater inkluderer SSL Domain og SSL Business sertifikater.

For tekniske spesifikasjoner og detaljer rundt SSL-sertifikatets egenskaper henvises det til egne dokumenter. Se mer informasjon på Buypass Web.

Dette dokumentet (Abonnementavtalens hoveddel) utgjør Del 1 av Abonnementavtalen mellom Abonnementen og Buypass.

Vilkårene i dette dokumentet (Del 1) gjelder med mindre det er gjort særskilt unntak i Bestillingsskjema (Del 2) fra ett eller flere av vilkårene.

Abonnementen kan inngå flere avtaler med Buypass om SSL-sertifikater.

Abonnementen kan selv autorisere personer og/eller Partner som på vegne av Abonnementen skal kunne bestille, godkjenne, administrere og benytte SSL-sertifikater. Dette krever at Abonnementen inngår egen avtale med Buypass – se avtalevilkår for Buypass Class 3 SSL-sertifikater.

2 Definisjoner

Begrep	Forkortelse	Beskrivelse
Abonent		Fysisk person eller Virksomhet som har fått utstedt et SSL-sertifikat fra Buypass og som er autorisert til å benytte den private nøkkelen tilhørende SSL-sertifikatet.
Bestillingsskjema (Del 2 av Abonnementavtalen)		Skjema som inneholder nødvendig informasjon for å bestille SSL-sertifikater.
Buypass Web		Buypass' nettsider, www.buypass.no og www.buypass.com .
Certificate Applicant		Se Sertifikatsøker.
Certificate Approver		Se Sertifikatgodkjenner.
Certificate Policy	CP	Et sett med regler som sier hvordan SSL-sertifikater utstedes og behandles.
Certification Practice Statement	CPS	Beskrivelse av hvordan reglene i CP-en blir praktisert. CPS-en utgjør Del 3 av Abonnementavtalen.

Begrep	Forkortelse	Beskrivelse
Certificate Signing Request	CSR	En forespørsel om et digitalt sertifikat. Inneholder bla den offentlige nøkkelen som skal sertifiseres og kan inneholde informasjon om virksomheten og domenet som skal sertifiseres. En CSR er digitalt signert med den korresponderende private nøkkelen og kan dermed benyttes for å dokumentere at avsender har kontroll på denne.
Certificate Transparency	CT	Certificate Transparency handler om åpenhet og innebærer at SSL-sertifikater registreres i åpne og offentlig tilgjengelige logger (CT-logger). Disse CT-loggene gir mulighet for innsyn i og kontroll med alle SSL-sertifikater som er utstedt.
CT-logg		En åpen og offentlig tilgjengelig logg som inneholder sertifikater og som inngår i rammeverket Certificate Transparency.
Enhetsregisteret		Enhetsregisteret inneholder grunndata om enheter som har registreringsplikt i NAV Aa-registeret, Merverdiavgiftsmanntallet, Foretaksregisteret, Statistisk sentralbyrås bedriftsregister, Skattemanntallet for etterskuddspliktige eller Stiftelsesregisteret.
Offentlig nøkkel		Den offentlige nøkkelen i et nøkkelpar som benyttes i asymmetrisk kryptografi. Legges inn i SSL-sertifikatet som dermed knytter bruk av den korresponderende private nøkkelen til Abonnementen og spesifiserte domener.
Privat nøkkel		Den hemmelige nøkkelen i et nøkkelpar som benyttes i asymmetrisk kryptografi. Den private nøkkelen benyttes på servere tilgjengelig på samme domenenavn som i SSL-sertifikatet.
Sertifikatgodkjenner		Person innenfor Abonnementens organisasjon som skal godkjenne sertifikatbestillinger.
Sertifikatsøker		Person innenfor eller utenfor Abonnementens organisasjon som bestiller SSL-sertifikater på vegne av Abonnementen.
Sperring		Tilbakekalling av et sertifikat innenfor sertifikatets levetid, dvs sertifikatet er av en eller annen grunn ikke lenger gyldig og skal ikke lenger brukes.
SSL-sertifikat eller Bypass Class 2 SSL-sertifikat		Et digitalt sertifikat utstedt av Bypass. Sertifikatet benyttes til identifisering av Abonnementen og spesifiserte domener ved kommunikasjon mellom brukere og Abonnement på internett.
Virksomhet		Juridisk enhet som har fått tildelt organisasjonsnummer i Enhetsregisteret i Brønnøysundregistrene, enten disse er aksjeselskap, ansvarlige selskap (ANS), foreninger, enkeltpersonforetak eller andre type enheter.

3 Avtaleprosess

Abonnenter som vil bestille SSL-sertifikater må registrere bestilling på web via Bypass Web.

Bypass vil ved mottak kontakte Sertifikatgodkjenner for å få bekreftet at Sertifikatsøker har myndighet til å bestille SSL-sertifikater. Dette skjer med mindre Sertifikatgodkjenner og/eller Sertifikatsøker er tildelt denne myndigheten som henholdsvis Sertifikatforvalter, Sertifikatbestiller og Sertifikatsøker i forbindelse med avtale om utstedelse av Bypass SSL-sertifikater (Class 3).

Bypass vil videre kontrollere innholdet i Bestillingsskjemaet. Hvilke kontroller som gjennomføres er beskrevet i Del 3 av Abonnementavtalen.

Abonnementen skal informere Sertifikatgodkjenner og Sertifikatsøker om de plikter som påhviler Abonnementen etter Abonnementavtalen.

Bypass registrerer alle SSL-sertifikater i 2 eller 3 CT-logger avhengig av levetid på sertifikatet. Ved å akseptere Abonnementavtalen, gir Abonnementen samtykke til slik registrering av sitt SSL-sertifikat.

4 Abonnementens ansvar og rettigheter

4.1 Innledning

SSL-sertifikater er uløselig knyttet til Virksomheten (Abonnementen) og spesifisert domene. Abonnementen er selv ansvarlig for at SSL-sertifikater ikke misbrukes av Abonnementens brukere. Abonnementen er også ansvarlig for at SSL-sertifikater brukes i hht gjeldende lovverk og vilkårene i dette dokumentet.

Abonnementen er ansvarlig for å bruke SSL-sertifikatet kun for de formål som fremgår av denne avtalen.

4.2 Bestilling av SSL-sertifikater

Før bestilling må Abonnementen ha generert en privat og en offentlig nøkkel. Den offentlige nøkkelen inkluderes i bestillingen. Abonnementen forplikter å oppbevare og beskytte den private nøkkelen på en forsvarlig måte til enhver tid.

Abonnementen forplikter seg til å oppgi korrekt og utfyllende informasjon i bestillingen. Dette gjelder også ved innhenting av informasjon eller dokumentasjon i forbindelse med behandling av bestillingen.

Abonnementen forplikter seg til å informere Bypass omgående hvis oppgitt informasjon ikke lenger er utfyllende eller korrekt.

4.3 Installasjon og bruk av SSL-sertifikater hos Abonnementen

Abonnementen skal kontrollere at innholdet i SSL-sertifikatet er korrekt før det installeres og tas i bruk. Abonnementen må melde fra til Bypass umiddelbart dersom det er feil i innholdet. Ved installasjon aksepteres innholdet i SSL-sertifikatet. Abonnementen må uansett melde fra dersom det avdekkes feil i innholdet etter installasjon.

Bypass anser SSL-sertifikatet som akseptert 14 dager etter utstedelsestidspunktet dersom Abonnementen ikke har meldt fra om feil i innholdet.

SSL-sertifikater som utstedes gjennom denne avtalen kan kun installeres på servere tilgjengelig på samme domenenavn som angitt i SSL-sertifikatet. SSL-sertifikatet bør ikke installeres på utstyr som er utenfor Abonnementens kontroll.

Det er Abonnementen som har det fulle og hele ansvar for at SSL-sertifikatet installeres og beskyttes slik at kun autoriserte brukere hos Abonnementen kan administrere den private nøkkelen og SSL-sertifikatet. Abonnementen skal iverksette rimelig tiltak for å forhindre uautorisert bruk av den private nøkkelen.

4.4 Sperring av SSL-sertifikater

Dersom Abonnementen vet, har grunn til å tro, eller burde ha forstått at uvedkommende har skaffet seg kjennskap til den private nøkkelen, skal Abonnementen straks sørge for å sperre SSL-sertifikatet. SSL-sertifikatet skal sperres ved tap, misbruk eller mistanke om misbruk. Unnlattelse av dette anses som grov uaktsomhet. SSL-sertifikatet skal også sperres dersom informasjon i sertifikatet er uriktig eller unøyaktig.

Dersom SSL-sertifikater sperres av en av årsakene nedenfor (les mer om årsak til sperring på Bypass Web), så skal årsak oppgis ved sperreforespørsel:

- den private nøkkelen er kompromittert, kommet på avveie (keyCompromise #1)
- Abonnementen har skiftet navn eller annen identitetsinformasjon i sertifikatet, for eksempel adresse (affiliationChanged #3)
- sertifikatet er erstattet av et annet sertifikat (superseded #4)
- sertifikatet inneholder domenenavn som ikke lenger brukes (cessationOfOperation #5)

Årsakskode (i parentes) vil bli inkludert på CRL/OSCP og gir informasjon om årsak til sperring til brukere av disse tjenestene. Hvis sertifikatet blir sperret av andre årsaker så skal ingen årsakskode angis.

Sperring av SSL-sertifikater gjøres per telefon til Bypass sperretjeneste eller via sperretjenesten på Bypass Web. Sperring av SSL-sertifikat kan foretas av Kontraktsignerer, eller av de fysiske personer som er tildelt rolle som Sertifikatgodkjenner, Sertifikatsøker eller tildelt roller ved utstedelse av Bypass Class 3 SSL-sertifikater.

Abonnenten forplikter seg til å stoppe bruken av den private nøkkelen umiddelbart når:

- Informasjon i SSL-sertifikatet ikke er korrekt eller gjeldende
- Det er mistanke om misbruk, konstatert misbruk eller kompromittering av den private nøkkelen
- SSL-sertifikatet har blitt sperret

Ved mistanke om misbruk, konstatert misbruk eller kompromittering av den private nøkkelen, forplikter Abonnenten umiddelbart å følge Bypass' instruksjoner mht bruk av privat nøkkel og SSL-sertifikat.

Tap av privat nøkkel medfører at Abonnenten må bestille nytt SSL-sertifikat.

5 Bypass' ansvar og rettigheter

5.1 Behandling av Abonnent- og personopplysninger

5.1.1 Innsamling og lagring

Som et ledd i registrering av informasjon om Abonnenten vil Bypass samle inn og oppbevare personopplysninger knyttet til de enkelte roller hos Abonnenten.

Dersom Bypass på et tidspunkt velger å avslutte tjenesten som omfattes av denne avtalen, kan persondata for de Abonnenter med gyldige sertifikater bli overført til en tredjepart som overtar ansvaret for å videreføre tjenesten inntil sertifikatene utløper. Dersom det skjer så vil Bypass varsle berørte Abonnenter og innhente aksept for å overføre slike data.

5.1.2 Formål

Disse opplysningene vil ikke uten Abonnentens samtykke bli benyttet til annet enn nødvendig kommunikasjon eller produksjon av tjenester under denne Abonnentavtalen. Opplysningene vil bli slettet så fort avtalen ikke lenger er gjeldende, med mindre fortsatt oppbevaring er pålagt gjennom lov.

5.1.3 Samtykke

Ved å akseptere Abonnentavtalen, samtykker Abonnenten til at Bypass kan behandle Abonnent- og personopplysninger som beskrevet i denne avtalen.

5.1.4 Rett til innsyn, endring og sletting

Bypass er behandlingsansvarlig for disse opplysningene og Abonnenten kan rette spørsmål knyttet til behandling av personopplysninger til Bypass Kundeservice.

Abonnenten har også rett til å kreve innsyn i og eventuell retting av personopplysninger som er registrert i tilknytning til Abonnenten.

Abonnenten har også rett til å kreve at personopplysninger om enkelte roller knyttet til Abonnenten blir slettet, med mindre fortsatt oppbevaring er pålagt gjennom lov.

5.1.5 Sikkerhet for opplysningene

Bypass har ansvar for sikkerheten knyttet til personopplysningene og skal gjennom planlagte og systematiske tiltak sørge for at tilfredsstillende informasjonssikkerhet i overensstemmelse med det til enhver tid gjeldende lovverk for dette.

Bypass har taushetsplikt i forhold til personopplysninger som er registrert og vil ikke utlevere disse til tredjeparter, med mindre slik utlevering er påkrevet i henhold til rettskraftig dom, gjeldende lovgivning, eller etter Kundens eget skriftlige ønske eller krav.

5.2 Buypass' erstatningsansvar

Buypass' erstatningsansvar fremkommer av den til enhver tid gjeldende CPS for Buypass SSL Class 2 Certificates (Abonnementavtalen Del 3).

5.3 Sperring av SSL-sertifikat

Buypass kan på eget grunnlag sperre sertifikatet dersom Abonnementen ikke oppfyller vilkårene i denne avtalen eller dersom sertifikatet brukes til ulovlige aktiviteter som phishing eller svindel, eller misbrukes på andre måter.

Buypass kan også sperre SSL-sertifikatet dersom Buypass er blitt gjort oppmerksom på at viktig informasjon i sertifikatet er feil/unøyaktig eller dersom Abonnementen har opphørt.

Dersom sertifikatet er sperret på bakgrunn av en av årsakene oppgitt under, vil årsak til sperring angis ved sperring og inkludert som årsakskode på CRL og OCSP (se også 4.4):

- Buypass mottar bevis for at den private nøkkelen er kompromittert (keyCompromize #1)
- Buypass er gjort kjent med at Abonnementens organisasjonsnavn eller annen identitetsinformasjon i sertifikatet er endret (affiliationChanged #3)
- Buypass finner det nødvendig å sperre sertifikatet fordi det ikke lenger tilfredsstillende gjeldende krav som angitt i CP/CPS (superseded #4)
- Buypass er gjort kjent med at domener i sertifikatet ikke lenger er tillatt brukt (cessationOfOperation #5)
- Buypass mottar bevis for at sertifikatet er blitt misbrukt, eller er kjent med at Abonnementen misligholder sine forpliktelser etter Abonnementavtalen (privilegeWithdrawn #9)

Dersom sertifikatet sperrer av andre årsaker så vil ingen årsakskode inkluderes.

Abonnementen varsles dersom Buypass sperrer et SSL-sertifikat.

6 Varighet av Abonnementavtalen

Abonnementavtalen varer så lenge som SSL-sertifikatene underlagt denne avtalen er gyldig eller til de eventuelt blir sperret. Abonnementen er selv ansvarlig for å bestille nye SSL-sertifikater før de aktive SSL-sertifikatene utløper.

Dersom Abonnementen misligholder sine forpliktelser etter Abonnementavtalen, og ikke retter opp misligholdet innen rimelig frist satt av Buypass, kan Buypass heve Abonnementavtalen med øyeblikkelig virkning. Dersom misligholdet er av en slik art at det ikke lar seg rette opp, kan Buypass heve Abonnementavtalen umiddelbart. Ved en slik heving av Abonnementavtalen vil de SSL-sertifikater underlagt denne avtalen sperrer.

Buypass kan endre innholdet i Abonnementavtalens Del 3 (CPS) ved å publisere en oppdatert CPS på Buypass Web. Den ny CPS gjelder da for bruk av SSL-sertifikatet som finner sted etter at den nye CPS ble publisert.

7 Verneting og lovvalg

Dersom det oppstår en uenighet mellom partene om tolkning eller rettsvirkning av avtalen, skal partene først forsøke å bli enige gjennom forhandlinger og/eller mekling.

Dersom en tvist ikke blir løst ved forhandling eller mekling, kan hver av partene forlange at tvisten bringes inn for Oslo tingrett som eksklusivt verneting.

Forholdet mellom Abonnementen og Buypass reguleres av norsk lov.

8 Force Majeure

Skulle det inntreffe en ekstraordinær situasjon som ligger utenfor partenes kontroll slik at oppfyllelse av denne avtalen er umulig og som etter norsk rett må regnes som Force Majeure, skal motparten varsles om dette så raskt som mulig. Den rammede parts forpliktelser suspenderes så lenge den ekstraordinære situasjonen varer. Den annen parts motytelse suspenderes i samme tidsrom.

9 Kontaktdetaljer Buypass

Buypass AS
Postboks 4364 Nydalen
Nydalsveien 30 A
N-0402 Oslo

Se Buypass Web, e-post: kundeservice@buypass.no

Buypass sperretjeneste:
Se Buypass Web

Kundeservice:
Se Buypass Web, e-post:
kundeservice@buypass.no