Bilag 6 – Specifikation af krav til Brokeren

Version 2.0

Version	Ændringer	Dato

[Broker bedes indsætte virksomhedsnavn]

Indholdsfortegnelse

1 Krav til Brokeren

I henhold til Brokeraftalen påhviler det Brokeren at opfylde en række forpligtelser og krav for at blive Broker og for at vedblive med at være Broker, herunder i forhold til certificering. Disse forpligtelser og krav er nærmere defineret i dette bilag, hvilket omfatter:

- Overordnet om certificering af Brokeren, jf. punkt 2
- Krav til Brokercertificering, der består af to dele:
  - Basiscertificering (første del), jf. punkt 2.2
  - Sikkerhedskrav og UX Scheme (anden del), jf. punkt 2.3
- Krav i relation til revision, jf. punkt 3

Brokeren er forpligtet til at overholde kravene til certificering i hele Brokeraftalens løbetid.

Der henvises i dette bilag til en række dokumenter, herunder dokumenterne "*Basiscertificeringskrav*", "*Security Requirements*" og "*UX Scheme*", hvor kravene er udmøntet og nærmere detaljeret. Disse dokumenter betragtes som en del af Brokeraftalen, jf. Brokeraftalens punkt 1.7.

2 Certificering af og krav til Brokeren

2.1 Generelt

Brokeren skal bidrage til det overordnede sikkerhedsniveau for MitID-infrastrukturen, og Brokeren skal derfor overholde og certificeres i henhold til en række nærmere definerede krav. Broker-certificeringen består af to dele; Basiscertificering (første del), jf. punkt 2.2, og Sikkerhedskrav og UX Scheme (anden del), jf. punkt 2.3.

Basiscertificering og Sikkerhedskrav udgør samlet Kodeks.

Basiscertificeringen finder sted efter indgåelsen af Brokeraftalen og skal sikre, at Brokeren overholder en række krav til Brokeren som virksomhed og Brokerens informationssikkerhedsstyring. Hvis Brokeren ikke opfylder kravene til Basiscertificeringen, afvises Brokeren, og anden del af certificeringen iværksættes ikke.

Efter gennemførelsen af Basiscertificeringen, og når Brokeren har udviklet sin løsning (men inden idriftsættelse af Brokerens løsning), skal Brokeren certificeres i forhold til "*Security Requirements*" og kravene i "*UX Scheme*". Omfanget af certificeringen i relation til "*Security Requirements*" og "*UX Scheme*" er afhængigt af den - eller de - af Brokeren valgte anvendelsesmodeller, jf. punkt **Error! Reference source not found.**.

Certificeringsprocessen forløber på den baggrund overordnet således:

i. Gennemførelse af Basiscertificering, som certificeringspartneren, jf. punkt 2.1.1, skal verificere.

ii. Certificeringspartneren afgiver en rapport til Leverandøren, som enten godkender eller afviser Basiscertificeringen. Hvis Leverandøren afviser Basiscertificeringen, må Brokeren herefter starte Basiscertificeringen igen.

iii. Efter Brokerens udvikling og integration til MitID-løsningen foretages gennemførelse af certificering i forhold til "*Security Requirements*" og "*UX Scheme*", som certificeringspartneren skal verificere. Certificeringspartneren afgiver en rapport til Leverandøren, som enten godkender eller afviser certificeringen.

iv. Leverandøren verificerer og godkender på baggrund af Certificeringspartnerens rapport, at kravene er opfyldt i henhold til Leverandørens evalueringskriterier, hvorefter Brokeren certificeres, og certificeringsattesten udstedes af Leverandøren, jf. punkt 2.1.2. Leverandørens evalueringskriterier fremgår af "*Basecertificering*", "*Security Requirements*" og "*UX Scheme*".

v. Såfremt Leverandøren ikke kan verificere og godkende, at kravene er opfyldt i henhold til Leverandørens evalueringskriterier, som følge af, at Certificeringspartnerens rapport angiver, at Brokeren ikke tilstrækkeligt efterlever kravene i Brokercertificeringen, afvises Brokerens certificeringsansøgning. Brokeren må herefter starte certificeringsprocessen igen. Såfremt Brokeren har bestået Basiscertificeringen allerede, beholder Brokeren denne del af certificeringen.

Certificeringsprocessen er beskrevet yderligere på Broker-sitet.

Brokeren skal svare ærligt og grundigt samt skal være i stand til at demonstrere efterlevelsen af kravene og på anmodning kunne fremlægge dokumentation til certificeringspartneren. Leverandøren er berettiget til vederlag for certificering og re-certificering, jf. Bilag 5, og Brokeren afholder herudover egne omkostninger i relation til certificering og gennemførelsen heraf samt tilhørende aktiviteter, herunder ved anvendelsen af den certificeringspartner, som Leverandøren stiller til rådighed. Hvis Leverandøren afviser Brokerens certificeringsansøgning, skal Brokeren afholde omkostningerne til eventuel ny certificeringsansøgning, hvis afvisningen kræver, at der skal gennemføres en ny fuld certificeringsproces.

Uanset gennemført certificering skal Broker gennemføre certificering på ny såfremt det f.eks. i forbindelse med revisionen konstateres, at kravene til certificering ikke er opfyldt.

2.1.1 Certificeringspartner

Brokeren skal anvende den certificeringspartner, Leverandøren stiller til rådighed, eller egen certificeringspartner, jf. Brokeraftalens punkt 3.2.6.

Brokeren indgår en aftale med certificeringspartneren om gennemførelse af certificering.

Det er certificeringspartneren, der verificerer, at Brokeren har besvaret og dokumenteret opfyldelse af kravene tilstrækkeligt. Certificeringspartneren indstiller til Leverandøren, om Brokeren kan opfylde kravene og kan gennemføre brokercertificeringen. Det er Leverandøren, der afslutningsvist udsteder en certificeringsattest, jf. nedenfor.

2.1.2 Certificeringsattest

Den endelige certificeringsattest skal indeholde følgende:

- En attest om Brokerens overholdelse af kravene til certificering, der er udstedt af Leverandøren.
- En underskrevet ledelseserklæring afgivet af Brokerens ledelse, hvor ledelsen erklærer, at Brokeren har svaret sandfærdigt på kravene og efter bedste overbevisning, samt at Brokerens ledelse ikke er bekendt med, at der er nogen forhold hos Brokeren, som gør Brokeren uegnet til at blive Broker.
- En rapport udarbejdet af certificeringspartneren om Brokerens efterlevelse af kravene indeholdt i Broker-certificeringen. Konklusionen skal godkendes af Leverandøren.

2.1.3 Re-certificering

2.1.3.1 Generelt

Når Brokeren er certificeret, skal Brokeren kun re-certificeres i tilfælde af ændringer i Brokerens løsning, som nærmere defineret i punkt 2.2, eller i tilfælde af ændringer i certificeringskravene, der er indeholdt i dette bilag.

I tilfælde af ændringer i Brokerens løsning, der har betydning for løsningens sikkerhed, skal Brokeren inden idriftsættelse notificere Leverandøren herom. Leverandøren afgør, om Brokerens ændringer kræver re-certificering. Re-certificering skal være opnået inden idriftsættelse af ændringerne i Brokerens løsning.

Ændringer foretaget af Leverandøren kan kræve re-certificering i forhold til overholdelse af "*Security Requirements*" og "*UX Scheme*".

Leverandøren sikrer, at Brokeren får et rimeligt varsel til at gennemføre re-certificeringen.

Brokeren skal selv afholde omkostninger til re-certificeringen.

2.1.3.2 Krav til re-certificering

Re-certificering kan ske som en fuldstændig re-certificering eller som en delvis re-certificering, hvilket er nærmere beskrevet i det følgende:

En fuldstændig re-certificering, der omfatter basiscertificering og certificering i forhold til "*Security Requirements*" og "*UX Scheme*", er påkrævet i følgende tilfælde:

- Såfremt Brokeren ikke er i stand til at aflevere en årlig revisionserklæring i henhold til Brokeraftalens Bilag 6.
- Såfremt den årlige revisionserklæring, jf. punkt 3, indeholder kritiske bemærkninger vedrørende Brokerens overholdelse af Kodeks og "*UX Scheme*" på kritiske områder.
- Såfremt Leverandøren vurderer, at kravene til certificering skal opdateres og ændres i et omfang, der kræver re-certificering.

En delvis re-certificering, der alene omfatter de relevante dele af certificeringen, er påkrævet i følgende tilfælde:

- Væsentlige ændringer i relation til Brokerens centrale komponenter, der anvendes i henhold til MitID-løsningen, herunder i henhold til integrations- og anvendelsesmodellerne, og som har indflydelse på overholdelsen af "*Security Requirements*" og "*UX Scheme*". Dette omfatter:
    - Såfremt Brokeren ønsker at anvende andre anvendelsesmodeller, der omfatter flere "*Security Requirements*" og "*UX Scheme*"-krav, skal Brokeren certificeres i forhold til de relevante dele af "*Security Requirements*" og "*UX Scheme*", der ikke allerede er dækket.
    - Såfremt ændringerne påvirker kode i Brokerens komponenter, der er implementeret specifikt i forhold til overholdelsen af "*Security Requirements*" og "*UX Scheme*", er certificering af de relevante dele af "*Security Requirements*" og "*UX Scheme*" nødvendig, før de pågældende komponenter kan idriftsættes.
    - Såfremt ændringer alene påvirker en eller flere komponenter, skal der kun ske re-certificering af de individuelle komponenter af de relevante dele af "*Security Requirements*" og "*UX Scheme*". Det er Brokerens ansvar at påvise, at det kun er nødvendigt at re-certificere en individuel komponent.

Såfremt Brokeren er i tvivl om, hvorvidt re-certificering er nødvendig, er det Brokerens ansvar at foretage en vurdering af, hvorfor en ændring ikke nødvendiggør en re-certificering, samt at ændringerne ikke vil påvirke opfyldelsen af kravene. Denne vurdering skal afleveres via Broker Management (BMPS) og skal godkendes af Leverandøren, før re-certificering kan undlades.

2.1.3.3 Ikke omfattet af re-certificering

En re-certificering er ikke påkrævet i følgende tilfælde:

- Såfremt Brokeren forbedrer eller opdaterer Brokerens informationssikkerhedsstyringssystem, som er grundlaget for basiscertificeringen, og ændringerne ikke medfører, at kravene til basiscertificering ikke længere overholdes.

Forbedringer vil blive dokumenteret i den årlige revisionserklæring, hvilket anses for tilstrækkeligt. Et informationssikkerhedsstyringssystem er et system, som naturligt forbedres løbende. Dette indebærer, at ændringer i følgende områder ikke medfører krav om re-certificering, hvis kravene er opfyldt:

  - Intern organisering
  - Personalesikkerhed
  - Styring af informationsaktiver
  - Adgangsstyring
  - Kryptering
  - Fysiske sikkerhedsforanstaltninger
  - Driftssikkerhed
  - Kommunikationssikkerhed
  - Sikkerhedskrav i forbindelse med udvikling og vedligeholdelse, herunder sikkerhedsudviklingsmetoder og databeskyttelse gennem design og standardindstillinger
  - Leverandørstyring
  - Styring af sikkerhedshændelser
  - Styring af beredskab
  - Styring af efterlevelse (Compliance) af lovgivning, kontrakter, sikkerhedskrav

- Såfremt Brokeren opdaterer og forbedrer de tekniske sikkerhedskontroller på baggrund af deres egne sikkerhedsstyringsprocesser, dog under forudsætning af, at Basiscertificeringskravene, "*Security Requirements*" og "*UX Scheme*" stadig overholdes – f.eks. opdatering af transportsikkerhed eller sikkerhedshærdning af komponenter. Dette vil ikke medføre krav om re-certificering, så længe de påkrævede sikkerhedstests udføres.
- Ændringerne må ikke ændre autentifikations-flowet og medføre overtrædelser af Kodeks og "*UX Scheme*", hvilket vil blive betragtet som ikke-overholdelse af Kodeks og "*UX Scheme*".

2.2 Basiscertificering

Kravet om basiscertificering er relateret til Brokerens informationssikkerhedsstyringssystem og skal omfatte den del af Brokerens organisation, hvor Brokerens løsning udvikles, driftes og administreres. Brokeren skal kunne dokumentere, at denne har et effektivt ledelsessystem for informationssikkerhed.

Brokerens gennemførelse af basiscertificering skal godkendes af Leverandøren, jf. punkt 2.1.

For at gennemføre basiscertificering skal Brokeren udfylde et kravskema ("*Base Certification Requirements Form*") for basiscertificering ved at besvare kravene og vedlægge relevant dokumentation for opfyldelse heraf, herunder at Brokeren har tilstrækkelige kontroller implementeret. Det er en forudsætning, at omfanget af Brokerens ledelsessystem for informationssikkerhed omfatter Brokerens løsning og ydelser og de krævede kontroller. Krav inden for følgende kontrolområder indgår i basiscertificering:

- Intern organisering
- Personalesikkerhed
- Styring af informationsaktiver

- Adgangsstyring
- Kryptering
- Fysiske sikkerhedsforanstaltninger
- Driftssikkerhed
- Kommunikationssikkerhed
- Sikkerhedskrav i forbindelse med udvikling og vedligeholdelse, herunder sikkerhedsudviklingsmetoder og databeskyttelse gennem design og standardindstillinger
- Leverandørstyring
- Styring af sikkerhedshændelser
- Styring af beredskab
- Styring af efterlevelse (compliance) af lovgivning, revision, kontrakter og sikkerhedskrav

Leverandøren godkender Brokerens basiscertificering, såfremt at denne er fyldestgørende og opfylder de angivne krav.

2.3 "*Security Requirements*" og "*UX Scheme*"

2.3.1 Anvendelsesmodeller i forhold til "*Security Requirements*"

Certificeringen og de hertil hørende "*Security Requirements*" varierer i forhold til, hvilke(n) anvendelsesmodel(ler), som Brokeren vælger, jf. det detaljerede dokument "*Security Requirements*". Anvendelsesmodellerne er nærmere beskrevet i bilag 3.

Brokeren kan kombinere anvendelsesmodellerne, og Brokeren skal opfylde alle de "*Security Requirements*", der skal opfyldes i relation til de valgte (og kombinerede) anvendelsesmodeller.

2.3.2 "*Security Requirements*"

Brokeren skal overholde en række nærmere definerede "*Security Requirements*" for at kunne gennemføre certificering og for at fortsætte med at være Broker. De relevante Sikkerhedskrav, som Brokeren skal certificeres efter, er beskrevet i det detaljerede dokument "*Security Requirements*", som er tilgængeligt i brokerpakken.

De enkelte "*Security Requirements*" er fordelt inden for følgende områder:

- Integrationskrav til Kernen
    - Transportsikkerhed og integritet, herunder:
        - Krav til brug af kryptografisk hardware (HSM) som er [FIPS 140-2] level 3 eller højere.
    - Adgang til Control API og Broker Management API
    - Generelle implementerings- og integrationskrav
- Krav til komponenter og flow
    - Generelle krav til implementer af komponenter og flows
    - Risk Data, herunder:
        - Krav om, at Brokeren indsamler risk data fra Slutbrugeren og videregiver risk data til MitID-løsningen ved anvendelse af standardmodellen eller fleksibilitetsmodellen. Kravene til indsamling af risk data er yderligere specificeret i "*Security Requirements*".

- Klient
- Klient Backend
- Embedded Authentication Frontends
- Sikkerhedshærdning af Klient og mitigering mod kendte trusler, herunder:
  - Obfuskerende og run-time integritetsbeskyttende tiltag, der tilføjes JavaScript kode, der eksekveres i Slutbrugerens browser. Brokeren kan her vælge at en kommerciel løsning eller egen udvikling og brug af Open Source tools.
- PSD2
- Single Sign-on (SSO)

- S-SDLC Requirements
  - Krav til kontinuerlig sikkerhedsevaluering, herunder:
    - Krav om penetrationstest og code review foretaget af uafhængig part, samt udbedring af observationer i henhold til angivne acceptkriterier.
- Support af User Agent
- Generiske sikkerhedskrav

2.3.3 Overholdelse af "*UX Scheme*"

Overholdelse af "*UX Scheme*" er en central del af broker-certificeringen for at sikre genkendelighed og tryghed i Slutbrugerens anvendelse af MitID. "*UX Scheme*" er uafhængig af den eller de valgte anvendelsesmodeller. De relevante "*UX Scheme*"-krav, som Brokeren skal certificeres efter, er beskrevet i det detaljerede kravdokument "*Kravskema for UX Scheme*", som er tilgængelig i brokerpakken.

De enkelte krav er fordelt indenfor følgende områder:

- Slutbruger-centreret autentifikation-flows i genkendeligt og konsekvent grafisk indtryk ved brug af grafiske elementer og symboler herunder bl.a. font, ikoner, knapper fra MitID-designsystem
- Tydelige fejlmeddelelser og adgang til hjælp
- Tilbyde alle tilgængelige Identifikationsmidler i MitID-løsningen
- Responsivt design
- Understøttelse af tilgængelighed ved overholdelse af Webtilgængelighedsloven (WCAG 2.1 level A og AA eller lignende)
- Understøttelse af mobiltilgængelighed (guidelines for WAI eller lignende)
- Understøttelse af de tre sprog; dansk, engelsk og grønlandsk

For at gennemføre certificering for overholdelse af "*UX Scheme*", skal Brokeren for hvert krav i "*Kravskema for UX Scheme*" angive, at Brokeren opfylder kravet og hvor påkrævet dokumentere opfyldelse af kravene inden for den valgte anvendelsesmodel. Brokerens certificeringspartner skal herefter gennemgå denne dokumentation og verificere, at Brokeren har dokumenteret tilstrækkeligt, at "*UX Scheme*"-et er overholdt. Certificeringspartneren skal i den sammenhæng have adgang til relevant dokumentation hos Brokeren.

3 Årlig revision

Brokeren skal levere en specifik ISAE 3000 type 2-revisionserklæring til Leverandøren på årlig basis, hvor Brokeren dokumenterer overholdelse af Kodeks og "*UX Scheme*", samt Underdatabehandleraftalens forpligtelser. Såfremt at Brokerens certificering er blevet godkendt med observationer, der kræver afhjælpning, skal disse indgå i revisionen med henblik på at dokumentere, at disse er udbedret til et acceptabelt niveau.

Brokerens revisionserklæring skal ikke basere sig på en revisionserklæring fra Leverandøren.

Revisionserklæringen skal baseres på Leverandørens revisionsinstruks. Der vil være en revisionsinstruks pr. anvendelsesmodel.

Revisionserklæringen skal udstedes af en ekstern statsautoriseret revisor.

Revisionsperioden vil være 1. november til 31. oktober. Brokeren skal levere den endelige revisionsrapport til Leverandøren senest den 31. december hvert år.

Hvis Brokeren er certificeret i perioden 1. november til 31. juli, skal Brokeren levere en ISAE 3000 type 2-revisionserklæring for perioden fra certificering til 1. november ved første afgivelse af en revisionserklæring. I andre tilfælde, hvor Brokeren ikke er certificeret i førnævnte periode, skal Brokeren først levere en ISAE 3000 type 2-revisionserklæring for førstkommende erklæringsperiode.

Såfremt Brokeren ikke er i stand til at levere en årlig revisionserklæring i henhold til Brokeraftalens Bilag 6, kan Leverandøren spærre Brokerens tilslutning til MitID-infrastrukturen, herunder annullere Brokerens certificering, og en re-certificering vil være påkrævet, jf. punkt 2.1.3.