

Underbilag 04.a Teknik og sikkerhed

Tilslutningsaftale for kommercielle visningsklienter

December 2024

VERSIONSHISTORIK

Version	Titel	Ændring	Ansvarlig	Dato
1.0	Teknik og sikkerhed	Første version	DIGST	Februar 2021
2.0	Teknik og sikkerhed	K-2, K-15 og K-16 udgår Korrekturlæst og konsekvensrettet K-1 er opdateret Krav om Autentifikation er opdateret K-24 er opdateret	DIGST	Juli 2021
3.0	Teknik og sikkerhed	Der er foretaget en række ændringer i krav og formuleringer Korrekturlæst	DIGST	December 2024

[Vejledning til Udbyder:

Udbyder bedes besvare de i dette Bilag 4.a (Teknik og sikkerhed) angivne krav i Underbilag 04.a.i (Løsningsbeskrivelse) med Udbyders egen løsning på kravene.

Udbyder skal ikke ændre i bilaget, medmindre dette specifikt er angivet.]

INDHOLDSFORTEGNELSE

Indledning	5
Tekniske krav	5
Sikkerhedskrav	6

UNDERBILAG

Underbilag 04.a.i Løsningsbeskrivelse (Teknik og sikkerhed)

Indledning

Dette bilag indeholder tekniske krav og krav til sikkerhed.

Løsningsbeskrivelsen, under overholdelses af kravene i dette bilag, fremgår af Underbilag 04.a.i (Løsningsbeskrivelse). Løsningen i Underbilag 04.a.i skal ligge inden for rammerne af Basisgodkendelsen, herunder Bilag 04 (Teknologi, drift og sikkerhed).

Tekniske krav

I dette afsnit er anført de tekniske krav til Udbyders Visningsklient.

04.a K-1 Autentifikation

Autentifikation af Slutbruger skal foregå via en MitID-certificeret Broker eller subbroker, som er NSIS-anmeldt på niveau 'Betydelig' eller højere.

Såfremt Visningsklienten benytter Digital Post til autentifikation af Slutbruger, skal Visningsklienten overholde de til enhver tid gældende krav til Visningsklienten, der følger af Regler og vilkår for Tjenesteudbyderes brug af NemLog-in Services på tu.nemlog-in.dk, samt OIO OIDC eller tilsvarende standarder.

04.a K-2 Opbevaring af Slutbrugers data i cache

Caching af en Meddelelse må kun forekomme i en igangværende Session og have til formål at optimere den samlede brugeroplevelse. Ved afslutning af en Session skal cache altid tømmes.

04.a K-3 Afslutning af en Session

Ved log-out eller udløb på en Slutbrugers autorisation skal en Session ophøre, og der skal foretages ny autentifikation, hvis Slutbruger ønsker at fortsætte sessionen. Slutbrugers Session skal ophøre senest efter 20 minutters inaktivitet.

04.a K-4 Aktivering af eksterne links

Visningsklienten skal understøtte, at eksterne links i Meddelelser kan aktiveres, og at det samtidig er tydeligt for Slutbruger, at denne forlader Visningsklienten og Digital Post-løsningen.

04.a K-5 Automatisk kopiering af Slutbrugers Meddelelser

Udbyder skal sikre, at det ikke er muligt at foretage en automatisk kopiering af Slutbrugers Meddelelser, uden at dette er under Slutbrugers fulde kontrol og eksplicite samtykke, herunder med ledsaget information om sikkerhedshensyn.

04.a K-6 Opbevaring og kopiering af metadata

Der må alene ske midlertidig opbevaring eller kopiering af MeMo Metadata og Digital post specifikke metadata i det omfang, dette er nødvendigt for at understøtte den almindelige posthåndtering i overensstemmelse med kravene i Tilslutningsaftalen.

04.a K-7 Sletning af metadata

MeMo Metadata og Digital post specifikke metadata skal slettes efter, at Slutbruger har afsluttet sin Session.

04.a K-8 Visningsklientens opdatering af metadata

Visningsklienten skal via Digital Post-løsningen sikre, at Digital post specifikke metadata i Meddelelser opdateres på baggrund af Slutbrugers interaktion.

Sikkerhedskrav

Dette afsnit indeholder sikkerhedskravene til Udbyders Visningsklient og til organiseringen af Udbyder.

04.a K-9 Overensstemmelse med ISO 27001

Udbyder skal tilrettelægge sikkerhedsarbejdet vedrørende Visningsklienter i overensstemmelse med ISO 27001.

04.a K-10 Opbevaring af data fra Digital Post-løsningen

Visningsklienter må ikke opbevare nogen former for data fra Digital Post-løsningen.

04.a K-11 Sikring af Slutbrugers data

Udbyder skal sikre, at Slutbrugers data er beskyttede, når de formidles via Visningsklienten, både i forbindelse med Slutbrugers inddatering og anden håndtering af data.

04.a K-12 Sikring af Visningsklienten

Udbyder skal beskytte Visningsklienten samt integrationer til Digital Post-løsningen mod udefrakommende angreb samt angreb fra Udbyders ansatte og brugere af Visningsklienten og dens Repræsentationer. Dette skal ske med et højt sikkerhedsniveau igennem

anvendelse af en kombination af tidssvarende beskyttelsesmekanismer, fx firewalls, IDS, IPS og antivirus.

04.a K-13 Sikring af Visningsklienten

Visningsklienten skal til stadighed sikres mod hacking og cracking og skal kontinuerligt detektere og imødegå kendte og nye opståede trusler samt angreb, herunder bl.a.:

- URL injection, cookie injection og lignende angreb
- Cross site scripting (XSS) og lignende angreb
- Sql-interception
- DDOS, Flooding og lignende angreb
- Horizontal samt Vertical Privilege escalation
- Password Sniffing og lignende angreb

04.a K-14 OWASP

App-løsninger og webapplikationer skal implementeres under hensyntagen til de guidelines, der følger af henholdsvis OWASP Top 10 Mobile Threats og OWASP Top 10 Most Critical Web Application Security Risks, samt fremtidige revisioner af disse eller tilsvarende bredt anerkendte oversigter.

04.a K-15 Anvendelse af SSL-certifikat og DNSSEC

Det website, REST API eller lign., som Visningsklienten afvikles fra eller benytter sig af, skal tilknyttes et gyldigt SSL-certifikat. Domæner skal sikres med DNSSEC.

04.a K-16 Sikring af Slutbrugers bevis

Udbyder skal sikre, at der sker den registrering, som er nødvendig for, at Slutbruger i relevante situationer kan føre bevis for dennes handlinger i forbindelse med Visningsklienten, såfremt registreringen af handlingen ikke varetages i Digital Post-løsningen.

04.a K-17 Slutbrugers adgang til registreringer

Udbyder skal sikre, at Slutbruger har adgang til registreringerne i overensstemmelse med 04.a K-16.

04.a K-18 Udlevering af data i forbindelse med tilsyn

Udbyder skal senest fem hverdage efter Digitaliseringsstyrelsens anmodning herom udlevere data vedr. drift, sikkerhed og anvendelse af Visningsklienten. Data skal udleveres til Digitaliseringsstyrelsen i søgbar elektronisk form, som aftales med Digitaliseringsstyrelsen.

04.a K-19 Indberetning af sikkerhedshændelser

Enhver sikkerhedshændelse vedrørende Visningsklienten skal uden ubegrundet ophold indberettes til Digitaliseringsstyrelsen.

04.a K-20 Indberetning af sikkerhedshændelser til Datatilsynet

Såfremt sikkerhedshændelser relaterer sig til persondata, er Udbyder særskilt forpligtet til at handle i overensstemmelse med databeskyttelsesreglerne, herunder indberetning til Datatilsynet. Udbyder er forpligtet til samtidig at orientere Digitaliseringsstyrelsen om al sådan kommunikation med Datatilsynet.

04.a K-21 Udbyder skal bidrage til fejlsøgning og håndtering

I forbindelse med generelle trusler eller angreb mod Digital Post-løsningen og/eller én eller flere visningsklienter, er Udbyder forpligtet til i rimeligt omfang at bidrage til fejlsøgning og håndtering, også selv om Udbyders egen Visningsklient ikke er omfattet af den pågældende trussel eller et konkret angreb.

Underbilag 04.a.i Løsningsbeskrivelse

Tilslutningsaftale for kommercielle visningsklienter.

December 2024

[Vejledning til Udbyder:

Her bedes Udbyder beskrive den tekniske og sikkerhedsmæssige løsning i forbindelse med Udbyders Visningsklient. Beskrivelsen udarbejdes i overensstemmelse med kravene i Underbilag 04.a (Teknik og sikkerhed) og Udbyders løsningsbeskrivelse i Underbilag 04.i (Løsningsbeskrivelse).]