Sikker adgang til personfølsomme data i Aula

Version 1.0

26. februar 2019

TEL
+45 35 36 95 05
+46 8 669 75 75

SALES
orders@liga.com

WWW
liga.com

TWITTER
@ligainsights

VAT
DK31938260
SE556597-2253

Forord

Når en bruger har adgang til personfølsomme data i Aula skal der være sikkerhed for, at brugerens identitet er på niveau "betydelig" i overensstemmelse med Digitaliseringsstyrelsens NSIS-standard version 2.0

En del af den tilgængelige dokumentation om emnet tager i skrivende stund (februar 2019) ikke højde for den seneste version 2.0 af NSIS-standarden[1].

Liga har derfor udarbejdet dette whitepaper for at beskrive, hvorledes kommuner og institutioner kan opnå sikker adgang til AULA i overensstemmelse med Digitaliseringsstyrelsens vejledning[2] til overholdelse af kravene. Beskrivelsen er tænkt som en hjælp til IT-afdelinger og IT-ansvarlige i kommuner og institutioner.

Overordnet arkitektur

Login til Aula sker via en af de tre mulige "Identity Providers":

- UNI-Login
- Context Handler (Kombit)
- Kommunens egen Identity Provider

De tekniske krav til login er beskrevet i Aula-dokumentationen fra Netcompany[3]

I forbindelse med login oplyser myndighedens Identity Provider hvilket sikkerhedsniveau brugeridentiteten har opnået som defineret i NSIS standarden. Der findes tre niveauer:

- Lav
- Betydelig
- Høj

(De tre niveauer afløser den tidligere NSIS-standards sikringsniveauer 1-4)

Adgang i Aula til personfølsomme data kræver som ovenfor nævnt, at brugeridentiteten er verificeret på niveau "betydelig". Dette stiller krav til ikke alene login-proceduren, men også udstedelsesprocessen omkring den elektroniske identitet. Det er den enkelte kommunes eller institutions ansvar at sikre, at reglerne overholdes.

Hvad kræves?

For at en brugeridentitet kan opnå niveau "betydelig" kræves der multifaktor-autentifikation. Ordet "to-faktor" anvendes i daglig tale om mange forskellige løsninger, men i forhold til NSIS er der en meget præcis beskrivelse i vejledningen. Der skal anvendes faktorer fra mindst to ud af tre mulige kategorier:

- En unik, fysisk enhed, som personen er i besiddelse af ("Indehaverbaseret autentifikationsfaktor" – f.eks. et chipkort)
- Noget personen ved ("Vidensbaseret autentifikationsfaktor" – f.eks. et password)
- Noget personen er ('Iboende autentifikationsfaktor" – f.eks. biometri)

To forskellige passwords vil eksempelvis ikke leve op til kravene om multifaktor.

[1] Digitaliseringsstyrelsen (05.10.2018), *National Standard for Identiteters Sikringsniveauer (NSIS) Version 2.0*, tilgængelig på /https://digst.dk/media/18271/national-standard-for-identiteters-sikringsniveauer-nsis-version-20-endelig.pdf

[2] Digitaliseringsstyrelsen (02.11.2018), *Vejledning til National Standard for Identiteters Sikringsniveauer (NSIS), version 2.0,* tilgængelig på https://digst.dk/media/18660/vejledning-til-national-standard-for-identiteters-sikringsniveauer-nsis-version-20.pdf (herefter refereret til som "NSIS-vejl 2.0"

[3] Netcompany (2018), *T0150 – Login og Step-up*, version 1.0, tilgængelig på https://Aulainfo.dk/wp-content/uploads/Sikkerhedsnotat-Login-og-Step-up-Aula.pdf

Logon til en computer eller en smartphone kan i sig selv ikke kan regnes som en faktor, idet oplåsning skal være en specifik handling der er knyttet til selve autentifikationen. En nøglefil vil som udgangspunkt heller ikke kunne regnes som en faktor[1].

En "unik, fysisk enhed, som personen er i besiddelse af" vil i praksis være et chipkort indeholdende brugerens digitale identitet (f.eks. NemID Medarbejdersignatur) eller en anden form for hardware token som er uløseligt knyttet til personen.

En arbejdscomputer kan ikke udfylde funktionen som "unik, fysisk enhed". Hvis en bruger autentificerer til computeren med brugernavn/password kan computeren ikke efterfølgende anvendes som faktor i en anden kategori. Det samme gør sig gældende med tablets og mobiltelefoner.[2]

Step-up

Hvis brugeren er logget på via UNI-Login er brugeridentiteten som udgangspunkt på niveau "Lav". UNI-Login tilbyder at brugeren kan foretage "step-up" med privat NemID eller NemID Medarbejdersignatur.

Hvis brugeren er logget på via Context Handler er det i skrivende stund planlagt at tilbyde en SAML-baseret step-up. Hvis brugeren er logget på via kommunens egen Identity Provider understøttes allerede nu SAML-baseret steup-up.

De to sidstnævnte løsninger er interessante, idet Aula er tilfreds med en SAML-forespørgsel, hvori der står at brugeridentiteten er på niveau "betydelig". Det er med andre ord alene afsenderens (og som indledningsvis nævnt, kommunens eller institutionens) ansvar at sikre, at dette også er tilfældet.

Fra et brugermæssigt synspunkt vil det simpleste være, at brugeren blot skal logge på én gang. Dette kan opnås ved at vælge en brugerautentifikation, som fra starten er på NSIS niveau "betydelig" for brugere, som skal have adgang til personfølsomme data.

Revisionskrav

Identity Providere er underlagt revisionskrav i henhold til NSIS 2.0.[3]

I forhold til Aula betyder dette, at Identity Providere som giver adgang med NSIS sikringsniveau "betydelig" er underlagt revision og skal afgive en årlig erklæring vedrørende proces og anvendelse af elektroniske identiteter.

Anvendes en løsning, som baserer sig på NemID Medarbejdersignatur identiteter vil selve brugeridentiteten være fritaget for ovennævnte revision. Derimod vil en løsning, som baserer sig på en intern brugerdatabase være underlagt revision.

Fra revisionsvejledningen:
"Ved anmeldelse på niveau Betydelig anvendes selvdeklarering suppleret med en revisionserklæring fra en uafhængig statsautoriseret revisor eller et overensstemmelsesvurderingsorgan (jf. eIDAS artikel 3, stk. 1, nr. 18), som bekræfter, at løsningens tekniske og sikkerhedsmæssige udformning er gennemgået, at kravene i denne standard er overholdt af løsningen på det angivne Sikringsniveau, og at der er implementeret processer for løbende at sikre, at det angivne Sikringsniveau opretholdes. Anmeldelsen suppleres med en ledelseserklæring underskrevet af en tegningsberettiget, hvoraf det

[1] NSIS-vejl 2.0 side 12 pkt. 3
[2] Ibid
[3] Digitaliseringsstyrelsen (18.01.2019), *Revisionsvejledning til National Standard for Identiteters Sikringsniveauer*, tilgængelig på https://digst.dk/media/19016/nsis-revisionsvejledning-version-20.pdf

fremgår, at alle relevante krav er opfyldt og fornødne processer for opretholdelse er implementeret. Der skal årligt indsendes en ny revisionserklæring, som bekræfter, at kravene til stadighed opfyldes."[1]

Sammenligning af løsninger

Nedenstående skema er en oversigt over de mest almindelige løsninger til brugerautentifikation. Det er vigtigt at notere sig, at samtlige løsninger som involverer brugernavn/password kræver, at oprettelsen af brugeren sker i en proces i overensstemmelse med NSIS niveau "betydelig" hvis brugeridentiteten skal kunne anvendes på samme niveau.[2] Det er ikke tilstrækkeligt at en kommune f.eks. blot opretter brugeren i sin lokale brugerdatabase.

Løsning	Beskrivelse	Fordele	Ulemper	NSIS niveau
PIN-kode beskyttet chipkort med kvalificeret digitalt certifikat	Nøglepar genereret i chipkort. Verifikation mod CA	Højeste sikkerhed.. Let at implementere mod eksisterende infrastruktur. Revisionsmæssigt compliant.	Kræver proces for udstedelse af kvalificerede certifikater	Høj
PIN-kode beskyttet chipkort med NemID Medarbejdersignatur	Verifikation mod NemID (Nets DanID CA)	Høj sikkerhed. Let at implementere mod eksisterende infrastruktur. Revisionsmæssigt compliant.	Kræver proces for udstedelse af NemID Medarbejdersignatur certifikater	Betydelig
PIN-kode beskyttet chipkort med eget-udstedt certifikat	Verifikation mod egen CA	Høj sikkerhed. Overkommelig integration mod eksisterende infrastruktur.	Kræver proces for håndtering af egen CA og udstedelse af certifikater. Kræver årlig revisionserklæring	Betydelig
Brugernavn / password + NemID login i browser	Verifikation mod directory med supplerende NemID Medarbejdersignatur login	Veldokumenteret løsning	Kræver proces for udstedelse af NemID Medarbejdersignatur certifikater. Dårlig brugeroplevelse.	Betydelig
Brugernavn / password + Token	Verifikation mod Directory med supplerende hardware token	God brugeroplevelse	Kan være tungt at implementere. Token bør være beskyttet mod tyveri. Økonomi kan blive udfordring	Betydelig
Brugernavn / password / bekræftelse fra app	Verifikation mod directory suppleret med kode fra smartphone app	Let at implementere mod eksisterende infrastruktur	Sikker registrering af smartphone til brugeren er vanskelig at opnå og skal dokumenteres revisionsmæssigt årligt	Betydelig
Brugernavn / password	Verifikation mod directory	Let at implementere mod eksisterende infrastruktur	Ingen to-faktor	Lav
Brugernavn / password / SMS	Verifikation mod directory suppleret med SMS-kode	Let at implementere mod eksisterende infrastruktur	SMS er vanskeligt at beskytte, kan læses på stjålne devices, kan medføre krav om	Lav

[1] Digitaliseringsstyrelsen (05.10.2018), *National Standard for Identiteters Sikringsniveauer (NSIS) Version 2.0*, tilgængelig på /https://digst.dk/media/18271/national-standard-for-identiteters-sikringsniveauer-nsis-version-20-endelig.pdf s. 24 pkt. 4

[2] NSIS-vejl. Side 8 pkt. 6

			arbejdsmobiler	
Brugernavn / password til aktivering af centralt opbevaret medarbejdersignatur	Almindelig løsning i mange kommuner	Forefindes i flere kommuner	Ingen to-faktor	Lav
Brugernavn / password fra personligt registreret computer	Verifikation mod directory fra kendt device	Brugerautentificering allerede på plads	Computeren kan ikke benyttes som faktor i en anden kategori, når brugeren har anvendt den sammen med brugernavn/password. Ingen to-faktor	Lav

Ligas anbefaling

Liga anbefaler at basere brugerens login på en identitet, som allerede er på NSIS sikringsniveau ”betydelig”. Dermed elimineres behovet for step-up både i forhold til Aula og til andre IT systemer med tilsvarende compliance krav.

Ved at anvende NemID Medarbejdersignatur som identitet er udstedelsesproces og anvendelse velbeskrevet og certificeret. Dermed minimeres revisionsomfanget.

Ved at anvende selvsamme bruger login til arbejdscomputeren kan identiteten benyttes til login til andre løsninger (single sign-on) på NSIS sikringsniveau ”betydelig”.

For yderligere information, kontakt:

Liga ApS
Center Boulevard 5
2300 København S
Tel +45 35 36 95 06

Bjarke Alling
Tel +45 40 13 91 05
ba@liga.com

Jens Nielsen
Tel +45 26 20 95 06
jn@liga.com