|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Notat

|  |  |
| --- | --- |
| Vedrørende: | Handlingsplan - IT-arkitektur review Nyt Unilogin  |
| Skrevet af: | STIL |
| Version: | 0.2  |
| Fordeling: | Digitaliseringsstyrelsen, KL |

 |

# Handlingsplan for: 7.5 Sikre ID-Løsninger for børn og unge

Indholdsfortegnelse

[Handlingsplan for: 7.5 Sikre ID-Løsninger for børn og unge 1](#_Toc4355915)

[1 Bemærkninger til indstilling fra review-rapport 2](#_Toc4355916)

[2 Handlingsplan for anbefalinger til projektet 2](#_Toc4355917)

[2.1 Anbefalinger 3](#_Toc4355918)

[2.2 Opsummering på handlingsplan 7](#_Toc4355919)

[3 Øvrige bemærkninger til arkitektur-reviewet 7](#_Toc4355920)

# Bemærkninger til indstilling fra review-rapport

I aftalen om kommunernes økonomi for 2019, er regeringen og KL blevet enige om at udvikle en mere sikker ID- og loginløsning målrettet skolebørn, der kan supplere det nuværende Unilogin. Analyser i regi af Fællesoffentlig digitaliseringsstrategi (initiativ 7.5) har forud herfor vist et behov for:

* Øget sikkerhed når børn logger ind i den digitale skole
* Sikkert to-faktor login til børn
* Mulighed for at kommuner selv udvikler Identity Providers (IdP)

Der er nedsat et fællesoffentligt projekt med deltagelse af STIL, KL og Digitaliseringsstyrelsen. STIL står for den tekniske udvikling af et nyt Unilogin, som vil bestå af følgende produkter:

* Videreudviklet Unilogin-IdP, så slutbrugerne oplever et nyt loginbillede, ny adgangskode og passwordpolitik for Unilogin.
* Udvikling af en ny tofaktor løsning til børn baseret på øget sikkerhed via en lærer eller en kontaktperson til barnet.
* Unilogin-broker, der understøtter en fødereret sikkerhedsmodel, hvor forskellige IdP’er kan tilkobles – eksempelvis en kommunes egen IdP. Tilkoblingen sker på en måde, så udbydere af skole-løsninger alene skal koble deres løsning til brokeren og ikke til mange forskellige IdP’er.

Den 26. feb. gennemgik det fællesoffentlige projekt et IT-arkitektur review. Denne handlingsplan er projektets imødegåelse af de anbefalinger, som er modtaget efter review’et.

I opsamlingen over hvilke principper, der er opfyldt, noterer projektet sig at applikation og infrastruktur er fuldt opfyldt, hvorimod øvrige principper kun er delvist opfyldt. Principper vedr. opgaver vurderer IT-arkitekturrådet ikke er opfyldt, dog mangler der en redegørelse for, hvorfor dette ikke er tilfældet.

Projektgruppen vurderer overordet, at de syv anbefalinger samt den tværgående anbefaling er relevante for projektet. De syv projektanbefalinger er mulige at indarbejde i projektets indhold og tidsplan.

Projektgruppen er enig i, at der forestår en omfattende kommunikation om den nye løsning. Kommunikationsplan aftales med de fællesoffentlige parter, og har ikke været genstand for reviewet.

# Handlingsplan for anbefalinger til projektet

Nedenfor følger projektets handlingsplan baseret på de anbefalinger, som følger af arkitektur reviewet, sammenfattet i den fremsendte review rapport. Det understreges, at nærværende handlingsplan og angivne konsekvenser for scope, tid og økonomi er projektets estimat, godkendt af projektejer, men endnu ikke behandlet i projektets styregruppe.

Projektet vil indarbejde justeringer som følge af anbefalingerne i projekternes tidsplan og produktoversigt. Det er samlet set vurderingen, at anbefalingerne ikke ændrer på projektenes samlede tidsplaner.

Den præcise idriftsættelsesdato for ny Unilogin Idp, Idp broker og to-faktor login til børn er ikke besluttet endnu, idet projekterne afventer en yderligere dialog med KL om det rigtige tidspunkt ifht. Aula udrulningen til skoler og dagtilbud

## Anbefalinger

Her følger redegørelse for, hvorledes projekterne vil søge at tage højde for de syv projektanbefalinger.

**1. Det anbefales, at projektet kommunikerer dets scope, forretningsmæssigt behov, afgrænsninger og snitflader – med fokus på hvordan det indgår i det samlede billede af autorisation og autentifikation på skoleområdet.**

Projektgruppen er enig i, at der er behov for kommunikation om projekternes indhold. Der er udarbejdet en kommunikationsplan med fokus på alle relevante målgrupper, herunder såvel slutbrugere, leverandører samt uddannelsesinstitutioner. Centralt i kommunikationen vil indgå, hvilken forandring, uddannelsesinstitutionerne og brugerne vil opleve. Heri vil også indgå det forretningsmæssige behov, som den øgede sikkerhed i det nye Unilogin understøtter. Bl.a. vil der blive lagt vægt på børn dannelse i forhold til at forstå behovet for øget sikkerhed, fx at adgangskoder er private og ikke skal deles. Kommunikations- og implementeringsplan forelægges den fællesoffentlige arbejdsgruppe.

Kommunikationen vil i vid udstrækning fokusere på autentifikationsdelen, idet projekterne udvikler en ny autentifikationsløsning. Autorisationsdelen håndteres i de enkelte applikationer samt i produktet, Skolegrunddata, som blev beskrevet for it-arkitektur reviewet i den fremsendte produktbeskrivelse. Skolegrunddata baserer sig på import af data om brugere og relationer, hvilket nyt Unilogin trækker på. Registreringspraksis vedr. importdata i Skolegrunddata projektet anses for at være udenfor dette projektets scope, men er beskrevet i et roadmap for skolegrunddata-programmet.

I kommunikationen vil afgrænsningen til Skolegrunddata, samt afgrænsningen til applikationerne, som anvender det nye Unilogin blive beskrevet på passende niveau afhængig af målgruppen.

Der vil derudover blive taget initiativ til – med udgangspunkt i den fællesoffentlige arkitektur for brugerstyring som projektet baserer sig på – at beskrive, hvorledes føderede sikkerhedsløsninger og trustfællesskaber skal forstås. Det vurderes, at der i den kommunale sektor er et stort behov for at forstå denne sammenhæng på overordnet niveau mhp. at forstå, hvorledes lokale IdP’er eksempelvis kan indgå i den nye føderationsløsning. Dette vil indgå i kommunikationsplanen.

**2. Det anbefales, at projektet laver et roadmap for hvilke elementer og komponenter der leveres hvornår. Det roadmap skal kunne understøtte den samlede fortælling for økosystemet.**

Der vil blive udarbejdet et roadmap for det samlede økosystem, som offentliggøres på viden.stil.dk. Roadmap vil forinden blive forelagt styregruppen. Formålet med roadmappet vil være at beskrive på et overordnet niveau, hvilke forandringer STIL forventer at levere frem mod 2021, herunder både fællesoffentlige initiativer samt STIL initiativer.

Projektgruppen vil også sikre kommunikation af målarkitekturen for det samlede økosystem for at understøtte de udarbejdede roadmaps.

For så vidt angår spørgsmålet om, hvornår tjenesteudbyderne kan ibrugtage den nye Unilogin løsning og IdP fordeler, så er kommunikation herom en del af selve kommunikationsplanen.

Vedr. ibrugtagning af egne IdP’er, f.eks. som følge af, at der med det nye Unilogin ikke længere vil være en mulighed for at synkronisere passwords på tværs af den nationale IdP og lokale AD’er, er der igangsat en særskilt proces herom. Denne proces skal tilvejebringe anbefalinger for løsningsscenarier i kommunerne, når Unisync lukker. Dette anses for at være udenfor projekterne.

**3. Det anbefales, at projektet udarbejder en implementeringsplan, der tydeliggøre hvilke forandringer de tilknyttede tjenester og brugere kan forvente.**

Projektgruppen forelægger udkast til overordnet implementeringsplan og kommunikationsplan for den fællesoffentlige styregruppe.

I implementeringsplanen vil det være tydeliggjort at tjenesteudbyderne, der i dag anvender Unilogin, ikke i første omgang vil opleve forandringer i den tekniske løsning, idet arkitekturen for IdP broker sikrer bagudkompabilitet med fortsat udstilling af det nuværende Unilogin id sammen med et broker id. På sigt vil tjenesteudbyderne forventeligt opleve et pseudonymiseret id. Dette vil fremgå af roadmap.

Fsva. tilrettelæggelse af kommunernes lokale Id håndtering, er der aftalt en særskilt proces. Det skal bemærkes, at udfasning af password-synkronisering ikke er en del af projekterne og vil blive gennemført uafhængigt af disse. Idet indførelsen af en ny passwordpolitik introduceres med idriftsættelsen af nyt Unilogin, vil en fortsat usikker udveksling af passwords sænke sikkerheden for det nye Unilogin. Derfor har STIL besluttet at koordinere hhv. idriftsættelse af nyt Unilogin med udfasning af password synkronisering. Kommunikation herom til kommuner udarbejdes derfor som led i en særskilt proces med KL.

**4. Det anbefales, at projektet træffer en beslutning om, hvordan det vil forholde sig til manglen på et passende NSIS sikkerhedsniveau for børn, der er blevet genkendt af en relevant anden bruger, indenfor tidsrammen af projektet.**

Projektet anerkender, at der fra fællesoffentlig side ikke kan leveres et bud på NSIS subprofilering tidsnok til idriftsættelsen af ny Unilogin IdP og IdP broker.

Projektet vil derfor forelægge et forslag til en subprofilering af NSIS for børn for Digitaliseringsstyrelsen på særskilt møde i marts/april mhp. en drøftelse forud for en teknisk implementering.

Forslag til konkret opmærkning af sikkerhedsniveau for børn, som øger sikkerheden fra ’Lav’, fremsendes således til Digitaliseringsstyrelsen. Det forudsættes at STIL alene vil fortage en subprofilering af NSIS for børn, som ’steppes up’ i sikkerhed via den step up løsning, som STIL udvikler i projektet for to-faktor login til børn.

**5. Det anbefales, at projektet tydeliggør hvilke data der bevæger sig internt i projektet og mellem projektets komponenter og identificerede snitflader til eksterne afhængigheder og tjenesteudbydere, hvordan det transporteres og hvordan sikkerheden understøttes.**

Projektet vil som del af den kommunikation, der offentliggøres på viden.stil.dk levere beskrivelser, der adresserer hvordan data bevæger sig mellem komponenterne mhp. at identificere en bruger op i mod en tjenesteudbyder. Beskrivelserne vil også tage højde for de data, som projektet modtager fra Elevregisteret, som er en komponent udenfor projektet. Elevregisteret leverer data om nye elever til brug for oprettelse af et Id i Unilogins Idp.

Processerne er overordnede som følger:

1. Udbyderen viderestiller brugeren til brokeren med angivelse af krævet sikringsniveau. På brokeren ledes brugeren til den ønskede IdP, der kan opfylde det krævede sikringsniveau.
2. IdP’en autentificerer personen og fastlægger, hvilket sikkerhedsniveau brugeren er logget ind med.
3. Brokeren kobler personen med de aktørtyper, roller og relationer[[1]](#footnote-1), der er registreret for personen i Skolegrunddata på baggrund af import af data fra institutionerne administrative systemer.
4. Brugeren sendes tilbage til udbyderen med en billet, som angiver sikringsniveau, aktørtype, rolle og relationer, så udbyderen kan give personen adgang til det, som vedkommende må få adgang til.

Der er således både afhængigheder til udbydere i forhold til det krævede sikringsniveau og de krævede aktørtyper, roller og relationer, til institutionerne i forhold til registreringerne i Skolegrunddata og til kvaliteten af evt. lokale IdP-løsninger. Beskrivelser af overordnede dataflow vil fremgå af viden.stil.dk.

Projektet er i gang med at afklare med Digitaliseringsstyrelsen, hvorledes sikringsniveauer kan håndteres på tværs af infrastrukturen. Når dette er klarlagt, vil dette også indgå i beskrivelserne af infrastrukturen, der bliver lagt på viden.stil.dk.

**6. Det anbefales, at projektet tilstræber at step-up komponenten er tilstrækkeligt løst koblet til UNI-login til at den kan genbruges af andre IDP’er.**

Projektet har med det forelagte udkast til arkitektur for to-faktor step up af børn lagt op til, at step up i sikkerhed alene kunne foretages på Unilogin IdP’en.

På baggrund af IT-arkitekturrådets anbefaling er projektet i gang med at afdække muligheden for at dekoble step up funktionaliten fra Unilogin IdP’en og i stedet placere funktionaliten om del af brokerens funktionalitet.

Afdækningen gennemføres i løbet af marts og primo april mhp. en justering af arkitekturen, som kan forelægges den fælleoffentlige arbejdsgruppe samt projektets styregruppe. Det er forventningen, at det teknisk er muligt at placere step up funktionaliteten i brokeren og gøre den uafhængig af Unilogin IdP’en. Det introducerer dog en række udfordringer. En afklaring af de tekniske udfordringer skal derfor gennemføres, inden endelig beslutning kan foretages.

**7. (AR. 1.3 og AR. 6.2) Projektet bør udarbejde komplette komponent-, begrebs- og aktørlister. Disse kan yderligere med fordel sættes op som komponent-, begrebs- og aktørmodeller der viser relationerne mellem dem.**

Projektet vurderer, at der er udarbejdet en komponentmodel, som også er fremsendt til arkitektur reviewet. Projektet er dog samtidig enig i, at der er behov for entydige benævnelser af begreber, aktører og komponenter særligt i forbindelse med kommunikationen om projektet til målgrupperne.

Projektet vil derfor udvide den allerede udarbejdede begrebsliste for at sikre, at alle relevante begreber indgår i listen.

På viden.stil.dk, hvor dokumentation rettet mod hhv. skoler, kommuner og leverandører vil fremgå, vil begrebslisten også indgå i materialet. Dokumentation på viden.stil.dk leveres som del af implementeringsplanen.

Vedr. aktørmodeller inddrager projektet aktører (elever) fra et elevregister, som leveres af Skolegrunddata produktet. Projektet udvides med en model for elevdata modtaget fra elevregisteret.

## Opsummering på handlingsplan

Nedenfor fremgår opsummering samt tidsplan for implementering af anbefalingerne samt vurdering af evt. økonomiske konsekvenser.

|  |  |  |
| --- | --- | --- |
| **Anbefaling** | **Tid** | **Vurdering af projektøkonomi** |
| 1 | April. Kommunikationsplan forventes fulgt frem mod idriftsættelsestidspunkt | Ingen effekt på projektøkonomi |
| 2 | Maj. Roadmap offentliggøres på viden.stil.dk | Ingen effekt på projektøkonomi |
| 3 | April. Implementeringsplan forelægges i marts mhp. igangsætning i april. | Ingen effekt på projektøkonomi |
| 4 | April. Forslag til subprofilering fastlægges i projektet og vedtages efterfølgende i arbejdsgruppe samt forelægges styregruppe. | Ingen effekt på projektøkonomi |
| 5 | Maj.Projektet vil levere beskrivelser af dataflow og håndtering af sikringsniveau mellem IdP, broker og tjenesteudbyder | Ingen effekt på projektøkonomi |
| 6 | April. Justering af arkitekturen for step up skal gennemføres i marts mhp. vedtagelse ultimo marts. | Afklare som del af fastlæggelsen af arkitekturen for step up. |
| 7 | Maj. Modeller for komponenter, begrebsliste og aktørmodeller offentliggøres på viden.stil.dk som del af kommunikation rettet mod leverandører og kommuner. | Ingen effekt på projektøkonomi |

# Øvrige bemærkninger til arkitektur-reviewet

Det bemærke, at der i tilbagemeldingerne er sket en vis sammenblanding af hhv. produktet Skolelogin, som dækker over Unilogin IdP og IdP broker og Skolegrunddata, som dækker over data fra kommunerne om relationer til brug for elevregistret. Der er en kobling mellem de to produkter, idet nye brugere oprettet i Skolegrundata overføres til Unilogin IdP’en mhp. at der kan oprettes en bruger som har tilknyttet et Unilogin ID. Dette sikrer bagudkompabilitet i forhold til leverandørerne systemer.

STIL har derudover noteret, at reviewet alene er foretaget af hhv. KL og Digitaliseringsstyrelsen. Dette har betydet, at andre domæner, ikke har kunne bidrage med nye vinkler på projektet. KL har i arbejdsgruppens behandling af handlingsplanen opfordret til, at projektet beder om yderligere eksterne review, i det omgang det kan bidrage til yderligere kvalitet i projektet.

Projektet havde bl.a. ønsket input i forhold til subprofilering af NSIS rettet mod børn, hvilket it-arkitektur review’et ikke kunne levere. Projektet har efterfølgende taget kontakt til Digitaliseringsstyrelsen mhp. et sparringsmøde herom.

Projektet vil gerne inddrages i det tværgående arbejde med NSIS jf. den tværgående anbefaling.

1. Defineret i KL’s rollekatalog: https://www.kl.dk/media/11557/rollekatalog-for-bpi-brugeraktrer-og-brugerroller.pdf. [↑](#footnote-ref-1)