# ***Styregruppen for data og arkitektur***

# **Reviewrapport for: Initiativ 7.5 Sikre ID-løsninger til børn og unge**

26. februar 2019

**Indhold**

[***Styregruppen for data og arkitektur*** 1](#_Toc2342787)

[**Reviewrapport for: Initiativ 7.5 Sikre ID-løsninger til børn og unge** 1](#_Toc2342788)

[Initiativ 7.5 Sikre ID-løsninger til børn og unge 2](#_Toc2342789)

[Reviewgrundlag 2](#_Toc2342790)

[Projektresume 3](#_Toc2342791)

[Indstilling 3](#_Toc2342792)

[Anbefalinger 4](#_Toc2342793)

[Anbefalinger til det nuværende projekt 4](#_Toc2342794)

[Tværgående Anbefalinger 5](#_Toc2342795)

# Initiativ 7.5 Sikre ID-løsninger til børn og unge

Reviewet af Initiativ 7.5 Sikre ID-løsninger til børn og unge er udført 20. februar til 5. marts 2019 på baggrund af projektets fremsendte materialer:

1. PID Børnelogin en-faktor og IDP fordeler
2. PID børnelogin to-faktor
3. Produktfortælling for skolelogin og skolegrunddata
4. Processer understøttet af nyt UNIlogin - Børnelogin
5. Wireframe til ny unilogin
6. SkoleLogin – Komponentdiagram
7. Rådgivende risikovurdering børnelogin jan 2019
8. Bilag 3.a Hele brugerrejsen
9. A0100 – Analyserapport – Skolelogin\_1.0
10. A0100 – Analyserapport – Skolelogin\_tillæg 1.1
11. A0100 – Skolelogin – Proof of concept afrapportering
12. D0130 – Logisk datamodel – Skolelogin
13. D180 – Integrationsdesign - Skolelogin

Reviewet er udført i overensstemmelse med retningslinjer for arkitekturreviews, godkendt af styregruppen for data og arkitektur maj 2017. Reviewboardet og deltagere er listet i nedenstående tabel:

|  |  |
| --- | --- |
| **Reviewboard:** | Gerner Zinglersen, KL |
|  | Thomas Pedersen, Digitaliseringsstyrelsen |
|  | Gitte Stoltenberg, KL |
| **Sekretariat for 8.1:** | Adam Arndt, Digitaliseringsstyrelsen - CTD |
|  | Asbjørn Flyger Lauwersen, Digitaliseringsstyrelsen - CTD |
| **Projektdeltagere:** | Katja Prause, Styrelsen for IT og Læring |
|  | Steen Lindén, Styrelsen for IT og Læring |
|  | Lars Johansen, Netcompany |
| **Observatører:** | Ewa Gottwald, Digitaliseringsstyrelsen |
|  | Charlotte Birkeholm, KL |

# Reviewgrundlag

Udgangspunktet for reviewet udgøres af hvidbog om fællesoffentlig digital arkitektur. Principper fra hvidbogen er gengivet nedenfor:

*1. Arkitektur styres på rette niveau efter fælles rammer (styring)*

*2. Arkitektur fremmer sammenhæng, innovation og effektivitet (strategi)*

*3. Arkitektur og regulering understøtter hinanden (jura)*

*4. Sikkerhed, privatliv og tillid sikres (sikkerhed)*

*5. Processer optimeres på tværs (opgaver)*

*6. Gode data deles og genbruges (information)*

*7. It-løsninger samarbejder effektivt (applikation)*

*8. Data og services leveres driftssikkert (infrastruktur)*

# Projektresume

På baggrund af initiativ 7.5 Sikre ID-løsninger for børn og unge, er dette projekt oprettet med midler fra Økonomiaftalen 2019 til at forbedre login-funktionaliteten for børn i det nuværende UNI-Login, for at øge informationssikkerheden for børn i skolerne. Indeholdt i projektet er der et rent didaktisk mål om at børn vænnes til at have et kodeord som er hemmeligt og ikke må deles, og at der på samme vis findes følsom information der skal passes bedre på end anden information. Derudover skal projektet etablere følgende:

En (1) identitetsprovider (*Autentifikationstjeneste*) med (2) en tilhørende step-up funktionalitet, der øger sikkerheden for korrekt identifikation af brugeren igennem verifikation fra anden person (*2-faktor login akkreditiv*). (3) En IdP-fordeler (*Login-tjeneste / identitetsbroker*) samt (4) differentieret passwordpolitik for børn 6 – 12 fra år.

I det nuværende UNI-login finder man, ud over den loginfunktionalitet der her bliver udskiftet, en række andre funktioner og databaser, som den nye IDP-setup vil trække på. Disse andre funktionaliteter står til udskiftning over tid, som en del af en samlet opdeling og opdatering af det eksisterende UNI-login.

# Indstilling

*Det vurderes, at Initiativ 7.5 Sikre ID-løsninger til børn og unge er delvist i overensstemmelse med principper og regler for den fællesoffentlige arkitektur, som fremstillet i hvidbog om fællesoffentlig digital arkitektur. Under forudsætning af at den nuværende løsning UNI-loginløsning videreføres sideløbende i en overgangsperiode der tillader tjenesteudbyderne at tage højde for forandringerne i systemet.*

Samtalen ved reviewet afspejler en stor bevidsthed om hvordan projektet kan bygges rent teknisk, og der ligeledes er gjort en del tanker om hvordan løsningen skal passe ind i det samlede system. Projektet står nu overfor udfordringen med at kommunikere disse tanker og løsningens konsekvenser til tjenesteudbyderne og andre parter der bliver påvirket af forandringen, for at sikre at implementeringen kan forløbe planmæssigt og løsningen kan indfri mest muligt af sit potentiale. Dette afspejles i vurderingerne og anbefalingerne, der i høj grad relaterer sig til at tydeliggøre projektets scope og konsekvenser for tjenesteudbyderene.

Reviewboardet finder at niveauerne applikation og infrastruktur er fuldt opfyldt, niveauet opgaver er ikke opfyldt og resten er delvist opfyldt. Reviewboardet har udarbejdet 7 anbefalinger til det nuværende projekt, som relatere sig til de fortsatte overvejelser og beslutninger projektet bør forholde sig til, for at leve fuldt op til FDA.

|  |  |  |
| --- | --- | --- |
| **Niveau** | **Vurdering**  Reviewboardet har udarbejdet **8** anbefalinger, givet i denne review-rapport. **7** anbefalinger til det nuværende projekt og **1** tværgående anbefaling.  Projektet anmodes om at tage stilling til anbefalingerne til det nuværende projekt i en handlingsplan. Sekretariatet tager gerne imod forslag til håndteringen af tværgående anbefalinger. | |
| **Styring** | Delvist opfyldt |  |
| **Strategi** | Delvist opfyldt |  |
| **Jura** | Delvist opfyldt |  |
| **Sikkerhed** | Delvist opfyldt |  |
| **Opgaver** | Ikke opfyldt |  |
| **Information** | Delvist opfyldt |  |
| **Applikation** | Delvist opfyldt |  |
| **Infrastruktur** | Delvist opfyldt |  |

# Anbefalinger

Reviewet af Initiativ 7.5 Sikre ID-løsninger til børn og unge har identificeret en række anbefalinger, der fremstår i to kategorier:

1. Anbefalinger til det nuværende projekt: Herunder fremstår anbefalinger til projektet i dets nuværende og kommende faser, som det er præsenteret for reviewboardet.
2. Tværgående anbefalinger: Disse anbefalinger identificeres af reviewboardet som centrale og relevante for projektets fremtidige succes, men samtidig af en sådan karakter, at disse udfordringer ikke kan løses af projektet isoleret set.

For så vidt angår anbefalinger til det nuværende projekt anmodes projektet om at imødegå disse ud fra følg-eller-forklar princippet i deres bemærkninger til reviewrapporten samlet i en handlingsplan. For tværgående anbefalinger, udarbejder sekretariatet for initiativ 8.1 beslutningsoplæg. Disse beslutningsoplæg indgår ligeledes i styregruppen for data og arkitekturs behandling af reviewet.

## Anbefalinger til det nuværende projekt

**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.**

Reviewboardet finder det væsentligt at projektet beskriver hvordan det relatere sig til det samlede landskab af autorisation og autentifikation som tidligere har været berørt af UNI-login, og som nu skal overtages af det nye UNI-login. Det bør tydeliggøres hvilke forretningsbehov der bliver dækket af det nuværende projekt og tydeliggøre afgrænsningen til andre funktioner, systemer og komponenter. Beskrivelsen af disse grænser kan med fordel inddrage brugerrejser på tværs af afgræsningerne som dokumentationsværktøj.

**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.**

For at sikre forståelse for processen for udskiftningen af funktionaliteten fra det gamle UNI-login til det nye UNI-Login hos aftagere af løsningen, bør et tydeligt roadmap udarbejdes. Dette roadmap bør vise hvornår tjenesteudbyderne kan begynde at tage den nye løsning i brug, og hvornår det ikke længere er muligt at bruge den gamle løsning, så de kan nå at planlægge en hensigtsmæssig migration eller finde en alternativ løsning.

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

Ligesom i anbefaling 2 bør implementeringsplanen have fokus på hvordan projektet påvirker omverdenen, de tjenesteudbydere der er i målgruppen og selve brugerne. Det er væsentligt at projektets aftagere tydeligt forstår hvordan deres situation ændre sig fra den nuværende situation når det nye UNI-login bliver tilgængeligt. Herunder om andre tjenester bliver taget ud af drift, som konsekvens af det nye UNI-Login.

**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.**

Det er usandsynligt at de ansvarlige for NSIS standarden kan nå at lave en opdatering der tager højde for projektets behov for et NSIS niveau mellem ”Lav” og ”Betydelig”. Derfor bør projektet på egen hånd træffe beslutning om hvordan det givne sikkerhedsniveau skal opmærkes til tjenesteudbyderne, så de kan tage højde for det i implementeringen af det nye UNI-Login.

**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.**

Det var ikke umiddelbart tydeligt for reviewboardet, hvordan data bevæger sig i systemet, og hvordan det bliver omformet eller mappet undervejs, ud fra reviewmaterialet. Det har skabt forvirring om hvem der får adgang til data om børns relationer og klassetrin og skole, og hvordan de kanaler der transportere den data beskyttes.

**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.**

Muligheden for at bruge en 3. person som identifikation, giver mulighed for at myndighedspersoner, forældre og værger kan understøtte en mere sikker login proces for en lang række brugere der endnu ikke er eller aldrig bliver it-kyndige nok til at kunne anvende NemID. Derfor har Step-up funktionaliteten potentiale som en fællesoffentlig byggeblok. For at understøtte at dette potentiale kan indfries bør projektet bygge step-up komponenten så løst koblet fra resten af systemet at den, med relativt lidt arbejde, kan kobles på andre IDP’er.

**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 har mange forskellige interessenter, med meget på spil, og det er vigtigt at projektet kan kommunikere effektivt og ensartet både internt og eksternt. Det kræver ensartethed i navngivning på tværs af dokumentationen i projektet, og tydelige forklaringer af hvor mange komponenter og aktører der er indtænkt i projektet, hvad de gør og hvad de relaterer sig til.

## Tværgående Anbefalinger

**8.** **Der bør etableres en NSIS-standard, der kan kommunikere et sikkerheds-niveau der er ophøjet af en anden part.**

I forbindelse med reviewet af opdateringen af UNI-login, er det blevet tydeligt at de forskellige niveauer ikke er finkornede nok til at håndtere den forskel i sikkerhed der opstår når et barn identificeres af 3. part, som ophøjelse af autentifikationen. Den næste version af NSIS bør tage højde for den type nuancer.