Konceptnotat vedr. sikkerhedsmodel for Samarbejdsplatformen

Dette notat beskriver et koncept for en sikkerhedsmodel til Samarbejdsplatformen. Formålet er at give introduktion til de identificerede forretningsmæssige behov samt præsentere hovedlinjerne i en sikkerhedsmodel, der kan opfylde disse behov. Dette arbejde ligger forud for kravspecifikationen af sikkerhedsløsningen herunder formulering af de endelige sikkerhedskrav, der kan opfattes som slutproduktet. Konceptnotatet giver således en sammenhængende beskrivelse på overordnet niveau samtidig med en motivering for de trufne designvalg.

Hovedfokus i notatet er på de funktionelle sikkerhedsaspekter herunder styring af brugernes adgange til funktioner og data, mens mere driftsorienterede- og organisatoriske sikkerhedsaspekter afklares senere.

1. Forretningsmæssige behov

I dette afsnit beskrives de væsentligste forretningsbehov, der er identificeret inden for sikkerhedsområdet. Hovedvægten er lagt på de specielle udfordringer i Samarbejdsplatformen, mens helt sædvanlige forhold ikke er beskrevet (fx fysisk sikkerhed i driftsmiljøer). De forretningsmæssige behov kan opfattes som pejlemærker for udarbejdelsen af sikkerhedsmodellen og er udslagsgivende for valg af arkitekturmønstre, standarder, teknologier, rettighedsmodeller etc.

1. **Understøtte behandling af følsomme personoplysninger**
   Under det indledende analysearbejde er det klarlagt, at Samarbejdsplatformen vil skulle behandle følsomme personoplysninger samt give brugerne adgang til disse efter nøje fastsatte regler. Et eksempel kan være i beskedmodulet, hvor forældre, lærere eller andet fagpersonale skal kunne kommunikere om elevers trivsel, herunder sociale forhold, diagnoser mv.

2. **Overholdelse af lovgivning (persondataregulering)**
   Det er naturligvis en klar forudsætning for Samarbejdsplatformen, at den foretagne behandling af personoplysninger er lovmedholdelig. Da der som tidligere nævnt behandles følsomme personoplysninger, er kravene skærpede. Undervejs i Samarbejdsplatformens levetid (maj 2018) vil den nye Databeskyttelsesforordning fra EU træde i kraft, og løsningen bør derfor være forberedt for de nye krav i denne.

3. **Brugervenlighed (step-up model)**
   Samarbejdsplatformen skal understøtte en smidig hverdag i skolen og i

dagtilbud, og derfor er der et ønske om at sikkerhedsløsningen ikke skal være en unødig blokering for brugerne. Særligt er der fokus på, at fx brug af NemID nøglekort kun skal afkræves af brugerne, når der specifikt tilgås følsomme data, mens almindelige/ufølsomme data kan tilgås med letvægtsmekanismer som UNILogin etc. Med andre ord skal sikringsniveauet kunne tilpasses følsomhedsniveauet, hvilket naturligt medfører en step-up model (detaljeres senere).

4. **Understøttelse af Widgets**
   Samarbejdsplatformen skal udgøre en fleksibel og dynamisk ramme, hvor funktioner og data fra eksterne leverandører kan indlejres i Samarbejdsplatformen gennem såkaldte *widgets*. Denne dynamik skal understøttes af sikkerhedsmodellen, så brugeroplevelse og sikkerhedsniveauer er konsistente på tværs af platform og widgets. Dette afføder et behov for at kunne overføre sikkerhedskontekst til widgets.

5. **Understøttelse af Apps**
   Samarbejdsplatformen skal ikke alene understøtte web applikationer men også "native apps", som installeres på mobile enheder. Dette stiller særlige krav til sikkerhedsmodellen, som bør indtænkes fra begyndelsen.

6. **Genbruge eksisterende autentifikationskomponenter (UNILogin, NemID)**
   Samarbejdsplatformen lever ikke et vakuum men skal indgå i et digitalt økosystem, hvor der allerede findes en række løsninger, og hvor nye kommer til i løsningens levetid. Det fremgår således i aftalen om konkretisering af det fælles brugerportalinitiativ for folkeskolen, at Samarbejdsplatformen skal benytte allerede eksisterende infrastruktur i form af Uni-login.

   Undervejs i Samarbejdsplatformens levetid udrulles næste generation af NemID og NemLog-in, og da eID området i det hele taget er i stor bevægelse i disse år, er det vigtigt at fleksibelt i løsningens levetid kan integreres med nye løsninger. I Digitaliseringsstrategiens initiativ 7.5 er der endvidere fokus på nye og sikre ID-løsninger til børn og unge, hvilket ligeledes vil påvirke løsningslandskabet.

2. Sikkerhedsmodellens hovedtræk

I dette afsnit gennemgås de vigtigste hovedtræk i den sikkerhedsmodel, der foreslås til Samarbejdsplatformen.

2.1 Dataklassifikation

Datamodellen i Samarbejdsplatformen skal understøtte opmærkning af alle data efter en følsomhedsklassifikation (fx som den KOMBIT benytter til støttesystemerne). Dataklassifikationen er et fundamentalt værktøj til at sikre, at automatiseret logik i platformen kan håndtere data korrekt i forbindelse med brugerautentifikation, adgangskontrol, logning, videregivelse etc.

Som et konkret eksempel skal dataobjekters følsomhed kunne indgå som en attribut (fx et tal i intervallet 1-4)[1], der benyttes i afgørelser vedr. adgangskontrol. Dette kunne fx være regler i stil med flg.:

- *Hvis følsomhed(dataobjekt) >= følsom_personoplysning gives kun adgang, hvis autentifikationsniveau(bruger) >= 3 og roller(bruger) indeholder "kontaktlærer".*

I forbindelse med kravspecifikationsarbejdet, foretages der en systematisk gennemgang af informationsmodellen for Samarbejdsplatformen, hvor alle data/attributter kortlægges og klassificeres. I den forbindelse vil nogle dataobjekter (fx beskeder) både kunne være ufølsomme og følsomme, afhængigt af konteksten (indholdet af beskeden). Det er ligeledes relevant at se på, hvordan data fødes, hvordan det flyder i systemet og hvornår de slettes – med andre ord hele livscyklus for data.

Da meget indhold er brugergenereret, vil det være nødvendigt med brugerinddragelse til at sikre en korrekt klassificering af data, herunder at brugerne via brugerfladen har værktøjer til at markere et objekt som følsomt. Det er derfor kravstillet, at en bruger (f.eks. en lærer) kan markere beskeder som indeholdende følsom information. Brugerinddragelse fordrer igen en bevidsthed og oplæring af relevante brugergrupper

[1] Den detaljerede klassifikation anvendes internt i løsningen. I brugergrænsefladen kan der anvendes en mere simpel model, så brugere fx blot markerer en kommunikation som "følsom", hvorefter dette internt mappes til det rette niveau.

(fx lærere) i forhold til at identificere og agere korrekt på følsomt indhold, så den organisatoriske implementering kan gå hånd i hånd med værktøjerne i platformen.

Opsummeret skal Samarbejdsplatformen altså sikre flg. til understøttelse af sikkerhedsmodellen:

a. Alle dataobjekter klassificeres i henhold til en følsomhedsklassifikation (fx 1-4).
b. Det aktuelle følsomhedsniveau er til rådighed som en attribut ved beslutninger om adgange.
c. De nødvendige værktøjer i brugerfladen skal eksistere til at muliggøre en korrekt opmærkning af fx brugergenereret indhold, hvor følsomhed ikke er givet a priori. Eksempelvis skal både en forælder og lærer kunne markere, at en given kommunikationstråd indeholder følsomme oplysninger, hvorefter al adgang til den herefter tager højde for det ekstra beskyttelsesniveau. Dette er derfor kravsat i kravspecifikationen.

2.2 Brugerautentifikation

Autentificering af brugere vil være en vigtig kapabilitet i Samarbejdsplatformen og et vigtigt fundament for sikkerhedsmodellen. Det fremgår i aftalen om konkretisering af det fælles brugerportalinitiativ for folkeskolen, at Samarbejdsplatformen skal benytte allerede eksisterende infrastruktur i form af Uni-login for så vidt angår forældre og elever.

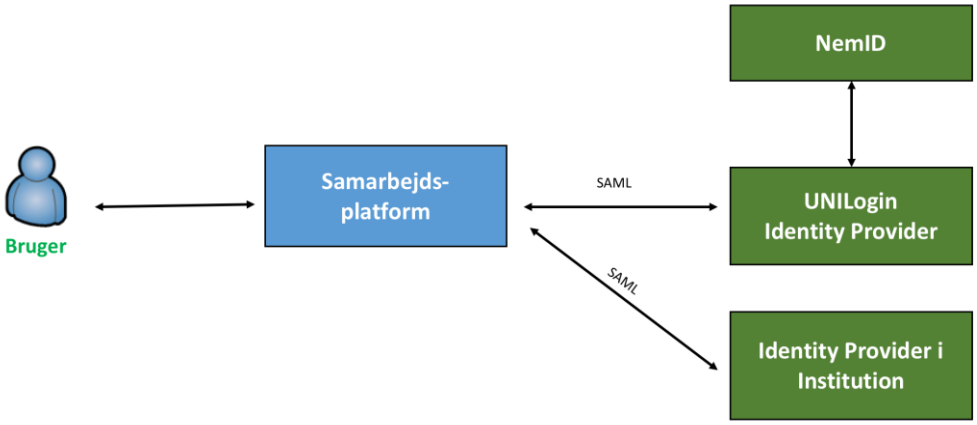
Her er det værd at bemærke, at både NemID, NemLog-in og UNILogin videreudvikles i løsningens levetid, hvilket der bør tages højde for i løsningsdesignet. I den fællesoffentlige digitaliseringsstrategi for 2016-2020 findes eksempelvis initiativer omhandlende sikre ID-løsninger til børn og unge, der må forventes at skulle kunne finde anvendelse i Samarbejdsplatformen, når de er færdigudviklede.

For at sikre en fleksibel autentifikation baseres brugerautentifikationen på flg. principper:

- Samarbejdsplatformen forestår ikke selv brugerautentifikation men delegerer til (eksterne) Identity Providers, som der er et tillidsforhold til. Dette kan fx være UNILog-in eller kommunale Identity Providers[2], som videreformidler et domænebaseret log-in for kommunale brugere (fx lærere tilknyttet et AD på en skole eller i en kommune).

[2] I praksis vil man nok integrere til en kommunal "broker"-løsning som Støttesystem ContextHandler, der så viderestiller til en bagvedliggende kommunal Identity Provider. Det er dog samme integrationsmønstre og protokoller (SAML 2.0), der her anvendes.

- Integrationen til den eksterne Identity Provider sker via SAML 2 protokollen for at sikre en stabil snitflade og løs kobling kobling udadtil.
- Det skal være muligt gennem konfiguration i Samarbejdsplatformen at tilføje nye Identity Providers, når nye udbydere bliver tilgængelige i løsningens levetid (fx næste generationer af NemID).
- I forbindelse med autentifikation fra en ekstern Identity Provider tilknyttes et sikringsniveau (level of assurance) til den aktuelle brugersession, som udgør et mål for tillid til brugerens identitet (fx 1-4). Dette niveau bruges som en attribut i forbindelse med adgangskontrolbeslutninger, og baseres på NSIS[3] rammeværket (National Standard for Identiteters Sikringsniveauer), der definerer kravene til det enkelte niveau.
- Hvis brugeren er autentificeret på ét niveau (fx niveau 2="Lav" via UNILogin) men ønsker adgang til data, som er klassificeret til et højere niveau (fx 3 = "Betydelig"), skal Samarbejdsplatformen kunne trigge *step-up authentication* dvs. bede brugeren om at re-autentificere sig på et højere niveau (via en passende Identity Provider).



Figur 1: Delegeret autentifikation

Ved at opfylde disse principper opnås en fleksibel og løst-koblet arkitektur, hvor Samarbejdsplatformen ikke er bundet til bestemte udbydere af eID. Samtidig opnås single sign-on inden for et givet sikringsniveau.

Der er i brugerportalsinitiativet truffet beslutning om, at UNILogin videreudvikles med sikker step-up autentifikation med NemID, som giver mulighed for at tilgå følsomme personoplysninger. Denne model for autentifikation vil derfor være den primære, som kravspecificeres for Samarbejdsplatformen, men ved at basere løsningsarkitekturen på ovennævnte designprincipper, vil det være let at tilpasse løsningen, hvis virkeligheden ændrer/udvikler sig. Som eksempel kan nævnes, at forbindelser til nye SAML Identity

[3] https://hoeringsportalen.dk/Hearing/Details/59539

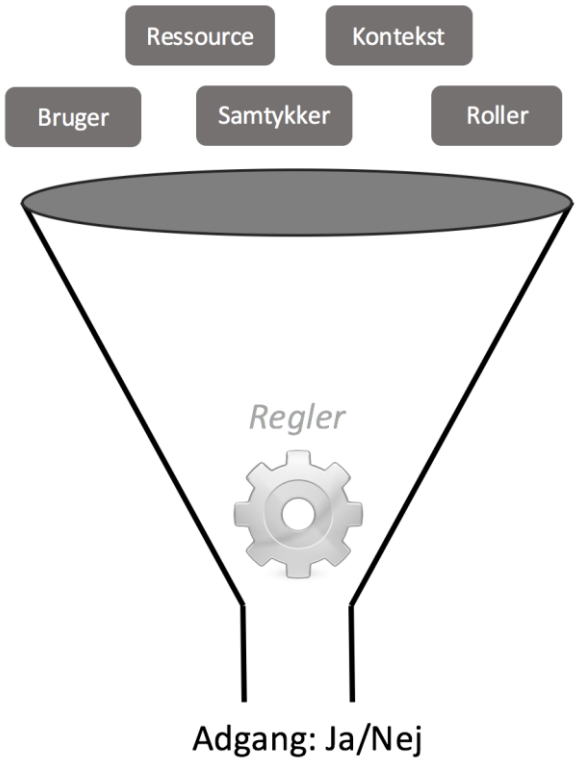
Providers ideelt set bør kunne oprettes som konfiguration og ikke gennem udvikling af ny kode.

2.3 Rettighedsmodel og adgangskontrol

I Samarbejdsplatformen er der identificeret behov for at kunne styre brugeres adgange ud fra regler, der trækker på en række forskellige attributter som beslutningsgrundlag:

- Følsomheden og ejerskabet (fx elev) af det dataobjekt, der tilgås (ud fra følsomhedsklassifikationen).
- Den operation, der ønskes udført (fx identificeret ved en handling i en use case).
- Brugerens identitet og relation til datasubjektet – herunder fx forældre-barn relationer, lærer-elev relationer etc.
- Roller tildelt brugeren af en administrator sammen med evt. dataafgrænsninger på disse (fx ”kontaktlærer for 1.A.”, eller ”administrator for Moseskolen”).
- Autentifikationsstyrken (Level of Assurance) for den aktuelle brugersession.
- Indhold af evt. samtykker fra Datasubjektet til behandling af oplysninger.

Ovenstående behov leder naturligt frem til en rettighedsmodel, som implementeres som en hybrid mellem traditionel RBAC (rollebaseret adgangskontrol) og ABAC (attributbaseret adgangskontrol). Ved at kominere disse modeller kan man opnå det bedste fra begge paradigmer, herunder en fleksibel og finkornet model, som samtidig giver sporbarhed og er auditérbar. Samme type hybrid er i øvrigt valgt for den fælleskommunale rammearkitektur.



Figur 2: Håndhævelse af adgang

I forbindelse med udarbejdelsen af use cases er der identificeret en række rolle/rettighedsmatricer, som viser relationer mellem funktioner/handliner i use cases og overordnede roller. I sikkerhedsmodellen vil hver distinkt handling i en use case blive opmærket med et særskilt rettigheds-ID, som repræsenterer rettigheden. I et administrativt interface skal disse rettigheder kunne samles til logiske roller, der ved tildeling til brugere kobles med dataafgrænsninger, som kan afgrænse en rolle i forhold til et individ, en gruppe (fx en klasse), en organisation (fx en skole) eller en kommune. Herved er det en ren konfiguration at ændre eksisterende roller eller skabe nye roller efterhånden som behovene ændrer sig.

Samarbejdsplatformen forventes at operere med sit eget lokale brugerkatalog, hvor tildelte roller og dataafgrænsninger kan gemmes per bruger, og hvor man for hver brugerkonto gemmer relationen mellem NemID og UNILogin. Gennem et administrativt interface (samt evt. udstillede web services) kan den enkelte institution- eller kommuneadministrator tildele rollerne til brugerne gennem en decentralt administrationsmodel efter samme overordnede principper, som i dag anvendes i SkoleIntra.

Det antages, at forældre-barn samt lærer-elev relationer kan hentes pålideligt ud fra UNILogins infotjenester[4]. Dette er dog et af de emner, der skal yderligere afklares i den videre proces.

2.4 Samtykkemodul

Der er i forbindelse med analysen af sikkerhedsmodellen identificeret et behov for at kunne indhente samtykker fra brugerne – både direkte samtykker og forældresamtykker på deres børns vegne.

Samtykkemodulet kan forretningsmæssigt gøre det muligt at foretage behandling af personoplysninger (herunder videresendelser af personoplysninger), som der ikke er en direkte lovhjemmel til, og samtidig kan samtykker give brugerne indsigt og handlemuligheder i forbindelse med behandlingen af personoplysninger.

Den videre juridiske analyse vil klarlægge, hvor og i hvilke situationer, der er lovhjemmel til behandling af personoplysninger, og hvor der er behov for et samtykke. I kravspecifikationen vil der blive stillet krav til et generisk samtykkemodul, som kan løfte de samtykkebehov, som den juridiske analyse identificerer. For dette modul er det vigtigt, at alle relevante regler til samtykker i lovgivningen honoreres (specifikt, frivilligt, informeret, utvetydig viljestilkendegivelse osv.), og at det skal kunne trækkes tilbage lige så let som det skal kunne afgives.

I selve håndhævelsen af adgange, skal eksistensen af et samtykke kunne spille ind i regler, der afgør, om der gives adgang eller ej. Dette kan konkret ske ved, at samtykkemodulet kan returnere et attributsæt vedr. brugerens aktive samtykker, og at disse attributter herefter kan indgå som værdier i forretningsregler, der afgør adgange. Heri ligger også, at samtykker ikke bør indeholde fritekst, men bør opmærkes på en måde, så de let kan behandles maskinelt.

Et relateret aspekt er 'tilladelser', der er sprogligt er en variant af samtykke, men som teknisk formentlig kan håndteres på samme måde i platformen. Begrebet 'samtykke' brugeres således ofte i kontekst af persondatareguleringen ("jeg giver samtykke til at skolepsykologen inddrages i kommunikationen om mit barns trivsel"), mens tilladelser kan dække andre ting ("jeg giver tilladelse til, at min barn må hentes af sine bedsteforældre").

[4] Der er planer om at videreudvikle UNILogins WS10 tjeneste, således at det kan fremgå, om en lokal skoleadministrator har overskrevet forældre-barn relationer i forhold til de autoritative data fra CPR registret. I givet fald bør der kunne tages højde for dette i Samarbejdsplatformen, således at adgang til følsomme data ikke gives på baggrund af usikre data.

2.5 Integration af widgets

Som tidligere nævnt skal Samarbejdsplatformen udgøre en fleksibel og dynamisk ramme, hvor funktioner og data fra eksterne leverandører kan indlejres i Samarbejdsplatformen gennem såkaldte *widgets*. Denne dynamik skal understøttes af sikkerhedsmodellen, så brugeroplevelse og sikkerhedsniveauer er konsistente på tværs af Samarbejdsplatform og widgets.

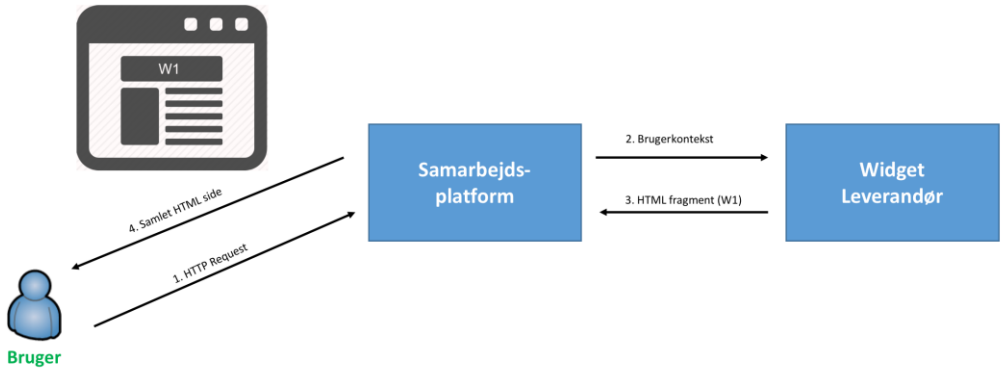
Det forventes, at Leverandøren af Samarbejdsplatformen kommer til at definere et fast API mod eksterne leverandører af widgets. Samarbejdsplatformen forventes via dette at overføre en række informationer om den aktuelle brugerkontekst (herunder hvem brugeren er, tildelte roller, aktuelt assurancelevel etc.).

Der er overvejet flere integrationsmodeler for widgets, og der er ikke truffet endelig beslutning om disse. Nedenfor gennemgås modellerne overordnet.

2.5.1 Server-side integration

Én model består i, at widget-leverandøren returnerer et HTML fragment til Samarbejdsplatformen, som indlejrer dette centralt, inden den samlede side sendes til browseren. I modellen er der altså pt. lagt op til en server-side integration frem for klient-side integration, som er udbredt i glaspladeportaler som Borger.dk og Virk.dk. Hermed er det kun Samarbejdsplatformen, som har en session med brugerens browser. Widget-leverandøren forventes at kunne foretage sin egen brugerstyring ud fra den overførte brugerkontekst.

En server-side integrationsmodel for widgets er illustreret på nedenstående figur:



Figur 3: Widgets integreret server-side

Bemærk at integrationsmodellen skal sikre kommunikationen mellem Samarbejdsplatformen og widget leverandøren (trin 2 og 3 på figuren) fx ved brug af to-vejs TLS med stærk kryptering og gensidig autentifikation baseret på FOCES/VOCES certifikater.

Hvis man går videre med server-side modellen, skal i det videre forløb afklares, om en widget skal kunne kommunikere ønske om step-up authentication til platformen, eller om en widget altid opererer under et fast sikringsniveau (som arves fra Samarbejdsplatformens aktuelle brugerkontekst). Det skal i afklaringsfasen fastlægges, hvilken brugerkontekst (herunder brugerattributter) Samarbejdsplatformen videreformidler til widgets samt hvordan snitfladen mellem disse skal indrettes.

2.5.2 Client-side integration

En anden tilgang er at integrere widgets client-side ved brug af HTML5, CSS, Javascript. Afhængigt af valgte teknologi forventes den enkelte widget at have sin egen session med browseren, og at der ved opstart af en widget foregår et SAML Web SSO forløb i den enkelte widget, hvor brugeren autentificeres af Identity Provideren og sessionen skabes. Dette betyder, at behovet for overførsel af brugerkontekst mellem Samarbejdsplatform og widget bliver mindre.

2.6 Håndtering af Apps

I ovenstående beskrivelse er der overvejende taget udgangspunkt i et scenarie, hvor samarbejdsplatformen udgør en web-applikation, der tilgås via en browser (enten på en PC eller mobil enhed) – i kravspecifikationen omtalt som ”browserløsningen”.

Imidlertid skal Samarbejdsplatformen også understøtte udvikling af Apps på mobile enheder. Ved en ”App” forstås her en applikation, som installeres på enheden fra en App store (fx Google Play eller Apples App Store), og som underliggende kan være baseret på forskellige slags teknologier (fx Native Apps eller ”Wrapper Apps” der underliggende er baseret på en browser).

For Apps er en række forskellige sikkerhedsmodeller overvejet, som beskrives herunder. Det endelige valg af App-teknologi og sikkerhedsmodel vil ske i dialog med markedet og den kommende leverandør. Derfor vil kravspecifikationen på dette område operere med en række optioner og fokus på teknologi-neutral kravssætning, som kan give den fornødne fleksibilitet. Uanset hvad er det givet, at der stadig findes et forretningsbehov for sikker adgang til følsomme personoplysninger samt single sign-on fra Samarbejdsplatformens App til en widget leveret af en tredjepart.

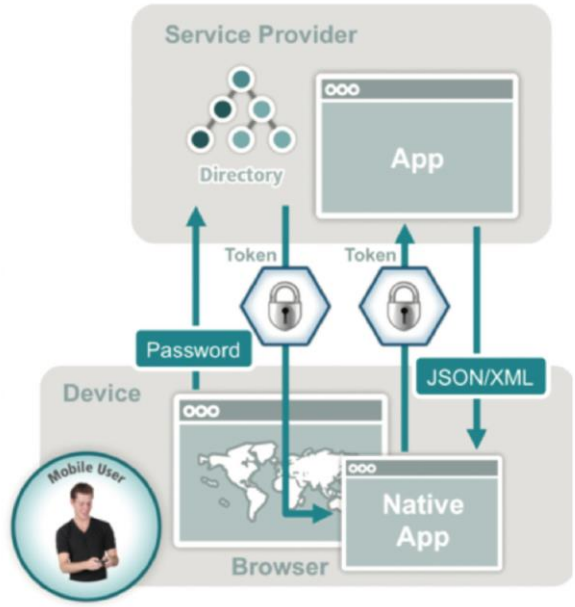
Én model kunne være, at UNILog-ins "APP Auth" løsning vil kunne finde anvendelse[5] evt. i en videreudviklet udgave. Den nuværende løsning fungerer ved, at brugeren indtaster sit UNILog-in brugerid og password i App'ens brugergrænseflade, som herefter valideres mod en back-end tjeneste. Hvis App'en har lov til at spørge, og brugeren har abonnement på App'en, kommer der et svar tilbage om, hvorvidt kombinationen af brugerid og password er korrekt. Det er dog pt. ikke afklaret, om UNILog-ins "App Auth" løsning også vil blive udbygget med step-up autentificering samt en evt. fremtidig sikker ID til børn og unge, eller om der skal findes andre løsninger på stærk autentifikation i Apps.

En anden ofte set model, som kan være relevant her er, at brugeren installerer en App på et personligt, mobilt device, og herefter første gang personaliserer App'en ved foretage en indrullering via en PC fx med brug af NemID. Her kunne en professionel (fx en lærer) evt. spille en rolle ved at bekræfte en elevs identitet med sit eget NemID under den initielle indrullering. Slutresultatet af denne indrullering er, at der i App'en bliver genereret en personlig nøgle, som entydigt er koblet til brugeren, og som centralt er registreret som tilhørende brugeren i Samarbejdsplatformen. Med denne nøgle kan App'en autentificere sig over for back end tjenester på brugerens vegne og dermed tilgå brugerens data, profil osv. Brugerens nøgle er beskyttet dels af enheden og dels af fx en personlig PIN-kode, brug af touch ID eller lignende på brugerens enhed som det fx kendes fra U2F og UAF protokollerne fra FIDO alliance[6].

En tredje variant kunne være, at App'en under den initielle personaliseringsproces starter en mobil browser og iværksætter et SAML log-in i denne, hvorefter browseren lukkes og brugerens SAML token overføres til App'en, der herefter personaliseres ud fra dette. Herved kan en eksisterende web-baseret SAML 2.0 Identity Provider genbruges i mobilkontekst. Modellen er illustreret på nedenstående figur:

[5] http://www.stil.dk/It-og-administration/Brugere-og-adgangsstyring/Udbyder-UNILogin/Apps

[6] https://fidoalliance.org



Figur 4: Omveksling fra browser log-in til brugerkontekst i App[7]

[7] Fra "A Standards-based Mobile Application IdM Architecture" af Ping Identity.