skolfederation.se
info@skolfederation.se

Tillit och användbarhet med Skolfederation

Skolfederation – för enkel och säker tillgång till tjänster

Undervisningen i den svenska skolan är på väg in i en digitaliserad värld. För att lättare ta tillvara möjligheterna med digitala tjänster krävs att en väl fungerande inloggningslösning finns för elever och personal. Lösningen måste vara enkel, säker, kostnadseffektiv, lättadministrerad och utvecklingsbar samtidigt som den värnar den personliga integriteten. Med en väl fungerande inloggningslösning på plats för elever och personal kan mer fokus ägnas åt pedagogiken och de digitala tjänster som skolan vill använda.

Skolfederation har som sitt syfte att:

Underlätta svensk utbildningssektors användning av digitala tjänster i utbildningen

Tillhandahålla en gemensam identitets- och behörighetsfederation, som gör tjänster enkelt åtkomliga för elever och lärare i landets skolor

Värna användarnas personliga integritet och samtidigt erbjuda en säker tjänst för medlemmarna

Skolfederation har växt fram ur dialoger och samverkan inom utbildningssektorn kring användning av digitala tjänster i skolan. Under 2011 drevs arbete inom SIS projekt - IT standarder för lärande för att starta Skolfederation. En förebild för och bakgrund till bildandet av en identitetsfederation är identitetsfederationen Swamid inom universitets och högskolevärlden.
Skolfederation har likt andra federativa initiativ ambitionen att följa Svensk e-legitimation. Skolfederation togs fram under ledning av SIS, och drivs nu av .SE (Stiftelsen för Internetinfrastruktur).

Aktörer
Under 2012 samverkade berörda aktörer för att skapa en tjänst som motsvarar medlemmarnas behov. Inriktningen klarnade och under 2013 började anslutning av medlemmar och produktion av tjänsten stabiliseras. Nu är ett hundratal aktörer engagerade i arbetet med Skolfederation, som intresserade eller medlemmar. Många tjänsteleverantörer som huvudmän efterfrågar är med och många huvudmän är på väg. Tjänsteleverantörerna ser att om tre år kommer digitala resurser användas parallellt 50/50 med traditionella läromedel och en gemensam inloggningstjänst anses viktig eller av avgörande betydelse för användningen av digitala tjänster i utbildningen.

Samverkan och utveckling
Samverkan sker för att öka förståelsen och underlätta medlemmarnas arbete genom erfarenhetsutbyten, möjligheter att visa tjänster och användning i demoskolor, samt lyfta fram olika goda exempel.
Utifrån medlemmarnas önskemål pågår utveckling för att hantera högre säkerhet med en utökad tillitsnivå mellan skolhuvudmän och e-tjänster. Utveckling görs också för att underlätta administration av medlemmarnas metadata.

Bakgrund i SIS-projektet – IT-standarder för lärande

Att Skolfederation har skapats är resultatet av ett större projekt, IT-standarder för lärande, som drivs av SIS (Swedish Standards Institute) i SIS TK 450, med syfte att göra det lättare för skolan att använda digitala tjänster och digitalt innehåll med hjälp av gemensamma standarder.

Gemensamma öppna standarder
SIS-projektet strävar inte efter att skapa några nya standarder, eftersom det redan finns lämpliga sådana. I stället är målet att skapa gemensamma riktlinjer, vägledning och praxis för hur de ska tillämpas, samt sprida kunskapen och medvetandet om hur de ska användas.
Om leverantörer och kommuner inte behöver skapa egna lösningar för integrationen av innehåll, utan kan arbeta med lösningar baserade på gemensamma och öppna standarder, förbättras förutsättningarna för skolans användning av digitala resurser.

SIS-projektet sätter upp ett antal effektmål:
• Att användningen av digitala lärresurser ökar i skolarbetet.
• Att en ökad användning av digitala resurser ska ge eleverna möjligheter att förbättra sina resultat.
•Att såväl kommunala skolor som friskolor använder framtagna riktlinjer vid beställning av digitala resurser.
•Att leverantörer använder riktlinjerna vid produktionen av digitala lärresurser och tjänster.
•Att nya leverantörer etablerar sig och marknaden expanderar, såväl inom som utanför Sverige.

Tjänsten Skolfederation

Skolfederation är en samverkan mellan skolhuvudmän och e-tjänsteleverantörer. Tjänsten riktar sig till skolhuvudmän och leverantörer av e-tjänster som kan bli medlemmar. Skolfederation är en identitetsfederation där medlemmarna litar på varandras användaridentifiering.

Skolfederation tillhandaåller en infrastruktur för inloggning som underlättar tillgång till digitala resurser, värnar användarnas personliga integritet och erbjuder en säker tjänst för medlemmarna. Grundläggande är att den identifiering som görs hos skolhuvudmännen och används i skolan även kan användas för inloggning hos andra tjänsteleverantörer.

Avtal och regler
För att medlemmarna ska kunna använda och lita på varandras identiteter och användaruppgifter, krävs att alla medlemmar följer Skolfederations regelverk.
Förvaltningen av Skolfederation och även den löpande verksamheten sköts av federationsoperatören (.SE, Stiftelsen för Internetinfrastruktur) och omfattar medlemshantering, metadatahantering, drift och utveckling av den gemensamma infrastrukturen, förvaltning av avtal och

Tillägstjänst för tillgång till trådlösa nät
Genom ett samarbete mellan Skolfederation och Sunet får elever och lärare i svenska skolan, via eduroam, möjlighet till wifi på ca 7000 platser, varav fler än 500 i Sverige. Wifin finns på lärosätena, men även på stationer, restauranger, kaféer etc. Eduroam har tidigare bara funnits tillgängligt för universitet och högskolor, men finns nu även för grund- och gymnasieskolor som en del inom Skolfederation.

Samtrafikavtal
Eduroam (education roaming), som finns i 54 länder, är ett samarbete inom forsknings- och utbildningsvärlden för att kunna utnyttja varandras wifi. Skolfederation och Sunet, som är ansvarig för den svenska anslutningen till eduroam, har ett samtrafikavtal som möjliggör för skolhuvudmän som är medlemmar i Skolfederation att även bli medlemmar i det globala eduroamsamarbetet.

Medlemmar i Skolfederation

Tjänsten riktar sig till huvudmän och tjänsteleverantörer inom utbildningssektorn. Förutsättningarna inom utbildningssektorn sätter ramarna för tjänsten, såsom aktörer av huvudmän och tjänsteleverantörer, lagkrav, kommersiella behov, marknadsutveckling med mera.

Följande aktörer kan vara medlemmar i Skolfederation;

- En skolhuvudman för någon av de skolformer som uppräknas i Skollagen (2010:800) och som antingen genom det allmänna eller privata anordnar utbildning. Det går bra att ha separata avtal för olika skolenheter.
- En svensk myndighet som arbetar med skolan.
- En leverantör av e-tjänster som har rekommenderats av en skolhuvudman

Läromedel och administration
Skolhuvudmän, är Sveriges kommuner och friskolor. Tjänsteleverantörer är exempelvis digitala läromedel, olika media, lärplattformar och administrativa tjänster som schema, elevregister, planering, uppföljning, text, tal, bild och filmbehandlingstjänster, publicering och lagring.

Andra aktörer som berörs och behöver ge stöd för användning av Skolfederation är leverantörer till skolhuvudmän och tjänsteleverantörer, såsom produktleverantörer, systemintegratörer och konsulter.

Federationsregister
För att bli medlem kan en aktör börja med en intresseanmälan. Därefter gör de en medlemsansökan genom att teckna avtal, sedan görs metadataregistrering, där medlemmen lämnar metadata som kontrolleras och laddas i federationsregistret. Medlemsavtalen för Skolfederation finns i två varianter, ett för huvudmän samt ett för tjänsteleverantörer. De består av ett huvudavtal för medlemskap med bilagor för tekniska krav, säkerhetsföreskrifter, attribut, priser och ordlista. För att främja användningen har tjänsten en enkel och förutsägbar prissättning, med en fast volymberoende årlig medlemsavgift.

Nytta för medlemmarna

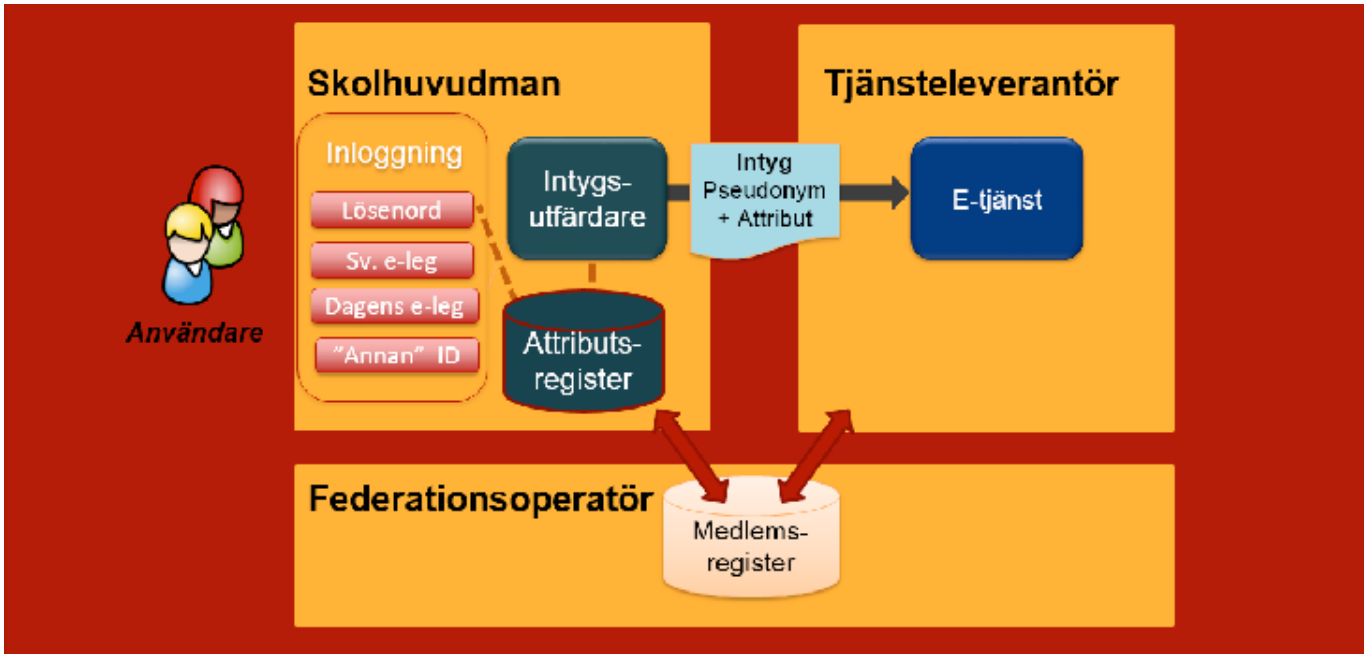
En enda inloggning till skolan för tillgång till både interna och externa tjänster minskar tidskrävande administration av konton och lösenord till många tjänster.
Skolorna kan tryggare ge tillgång till olika tjänster när användningen av känsliga uppgifter kan begränsas och endast nödvändiga uppgifter för tillgång till tjänsten behöver lämnas.

Minskat behov av integrationer gör det lättare att ansluta fler tjänster för att använda i skolan. När en skola väl är ansluten till Skolfederation, behövs ingen ytterligare teknisk integration med nya tjänsteleverantörer (som också är anslutna till Skolfederation).

Standardiserat gränssnitt
Inloggningsmetoder kan förändras utan att anslutna tjänster påverkas. Skolfederation ger ett standardiserat gränssnitt för informationsutbyte mellan huvudmän och tjänsteleverantörer. Den ordinarie inloggningen till skolan sker i ett första steg, innan information lämnas till tjänsteleverantören. På så sätt kan metoder för inloggning förändras utan att gränssnitt mot tjänsteleverantörer påverkas.

Sänkta integrationskostnader
De som erbjuder nätbaserade tjänster till skolan får med Skolfederation tillgång till en säker, standardiserad inloggningstjänst som alla anslutna skolor kan använda.
Leverantörernas integrationskostnader kan sänkas när de bara behöver anpassa sina system en gång för att fungera i federationen. De slipper på så sätt administrera ett eget användarregister. Tjänsteleverantörer kan därmed lättare göra sina tjänster tillgängliga för skola, lärare och elever, vilket underlättar tillgång till fler tjänster, uppkomst av nya tjänster och kombinationer av innehåll.

Federationens uppbyggnad



Skolfederation är en identitetsfederation vilket innebär att en sammanslutning av organisationer kommit överens om att lita på varandras elektroniska identiteter i sina IT-system.

Skolhuvudman
Den grundläggande idén för en identitetsfederation är att autentiseringen av användare sker så nära källan som möjligt, lämpligen när eleven eller läraren loggar in på skolans interna nätverk.
Som medlem blir huvudmannen en identitetsutfärdare i Skolfederation. När en användare har autentiserat sig genom att logga in i skolans interna IT-system utfärdas ett elektroniskt identitetsintyg om att användaren är känd och accepterad av skolan som godkänns av samtliga medlemmar i federationen. Intyget kan kompletteras med attribut av olika slag, till exempel vilken klass och skola en elev går i.

Personuppgifter
Identitetsintyget behöver inte innehålla några personuppgifter. Det skickas sedan till den tjänst som användaren vill logga in till, utan ytterligare inloggning.
För många skolor är det enkelt att ansluta sig till Skolfederation. De har redan den tekniska miljö som krävs och behöver bara aktivera funktionen.

Tjänsteleverantör
En e-tjänsteleverantör som blir medlem behöver bara integrera sitt inloggningssystem med identitetsfederationen en gång men måste fortfarande sluta avtal med varje skola för tillgång till tjänster. Tjänsteleverantörer får genom Skolfederation tillgång till en säker, standardiserad inloggningstjänst som alla anslutna skolor kan använda.

Opartisk verifiering – Federationsoperatör
Skolfederation har också en federationsoperatör som godkänner och dokumenterar alla medlemmar, samordnar deras användning och tillämpning av standarder samt tillhandahåller grundläggande tjänster åt dem. Det är .SE (Stiftelsen för Internetinfrastruktur) som har denna uppgift. Federationsoperatörens viktigaste funktion är att ansvara för ett register över alla medlemmar genom vilket identitetsintygen verifieras opartiskt och säkert.

Tillit
Tilliten till de identiteter och attribut som används inom Skolfederation är av stor betydelse. Om en part missköter sin hantering kan det leda till att tilliten till alla medlemmars identiteter och attribut försämras. För att säkerställa en hög tillit till identiteter och attribut inom Skolfederation måste därför alla medlemmar följa de säkerhetsföreskrifter som specificeras i medlemsavtalet.

Vikten av den personliga integriteten

Att kunna identifiera en person är en viktig funktion, men det är även viktigt att hänsyn tas till den personliga integriteten. Därför ska bara nödvändig information skickas till e-tjänsteleverantörer anslutna till Skolfederation.

Ett grundläggande krav i Skolfederationen är att alla parter följer personuppgiftslagen (1998:204). Det är medlemmen i Skolfederation som ska se till att kraven som ställs i personuppgiftslagen uppfylls och följs.
Medlemmarna ska endast behandla de personuppgifter som är nödvändiga för tjänsten.

Pseudonymer för ökad personlig integritet
Då Skolfederation värnar om den personliga integriteten, eftersträvar vi att användare identifieras med ”pseudonymer” i stället för personnummer. Det gör att användarens verkliga identitet normalt inte visas för e-tjänsteleverantören, men att användarens rätta identitet vid behov kan spåras, exempelvis vid missbruk.

Nya pseudonymer
Det finns två typer av pseudonymer, beständiga (eng. persistent) och tillfälliga (eng. transient) pseudonymer.

- Med beständiga pseudonymer tilldelas en användare en och samma pseudonym för en e-tjänst, men olika pseudonymer används för olika e-tjänster.
- Med tillfälliga pseudonymer ges en användare aldrig samma pseudonym, utan användaren får en ny pseudonym vid varje nytt tillfälle de använder en e-tjänst.

Attribut

Grunden i identitetssystem är att det kan avgöras om en person verkligen är den han eller hon utger sig för att vara. Men när det handlar om att ge åtkomst till digitala läromedel är det av integritetsskäl en fördel om behörighet baseras på attribut som skola, årskurs och så vidare, snarare än på användarens personnummer.

Eftersom Skolfederation värnar den personliga integriteten är målsättningen att en användare i varje given situation endast ska behöva dela med sig av just den information som är nödvändig.
Ska du som användare till exempel boka en biljett med studentrabatt på en webbplats, så behöver företaget som säljer biljetten inte få reda på ditt personnummer. Det ska räcka med att du loggar in i Skolfederation och att din skola intygar att du är student, utan att sända ditt personnummer.

Lokalt underhåll
Ansvaret för att underhålla dessa användaruppgifter (attribut) åligger respektive skolhuvudman. De förväntas uppdatera när till exempel elever byter skola eller personal slutar eller får nya arbetsuppgifter. Attributen förväntas därför hämtas från den primära källa i kommunen eller friskolan, som kan vara en katalog (AD, eDirectory) eller en databas.

Attribut för Skolfederation
En viktig uppgift för Skolfederation är att verka för enighet kring ett antal gemensamma attribut för landets skolor. Attributen är uppdelade i tre grupper för att förenkla för skolhuvudmän att välja attribut för olika ändamål. För tillgång till attribut gäller en minimalistisk princip.

Basattribut är den minsta attributmängd som kan användas och utgör normalt ingen risk för integriteten. Basattribut kan ingå i alla intyg, vilka varje intygsutfärdare (IdP) ska kunna leverera.

Standardattribut är en utökad attributmängd som vid behov kan ingå i intyget till tjänsteleverantören efter överenskommelse med skolhuvudmannen. Dessa bör varje intygsutfärdare (IdP) kunna leverera.

Utökade attribut kan innehålla uppgifter av känsligare art, och bör inte användas utan en noggrann prövning av säkerhet och personuppgiftshantering. Vid prövningen är det viktigt att en samlad bedömning görs av det som tillgängliggörs.

Teknik

Den tekniska infrastrukturen för Skolfederation har byggts upp med samma standarder som redan används för den svenska universitets- och högskolefederationen SWAMID. Skolfederation har likt andra federativa initiativ (som exempelvis Svensk e-legitimation) ambitionen att använda följande SAMLv2-profiler:

- Implementationsprofilen eGov2 (beskriver vilka SAML-förmågor som erfordras).
- Deploymentprofilen saml2int (beskriver hur SAML-förmågorna ska användas).

Aktörskrav

Tjänsteleverantör (SP, service providers), Skolfederations tjänsteleverantörer ska ha förmågan att konsumera intyg.

Huvudman (IdP, identity providers), Skolfederations huvudmän ska ha förmågan att identifiera och autentisera användare, exempelvis elever, och som ett resultat av detta ställa ut ett intyg.

Federationsoperatör, Federationsoperatören ska tillhandahålla digitalt signerat aggregerat SAML-metadata vilket kan anses vara Skolfederationens kärna, den grundläggande tilliten.

Övergripande teknisk infrastruktur

SAML-metadata (MD, metadata)
För att aktörerna i Skolfederation ska kunna lita på varandras intyg krävs ett utbyte av de publika nycklarna i varje aktörs nyckelpar och därigenom kan intygets signatur verifieras. Utbytet sker genom att lokalt SAML-metadata, vilket beskriver en aktörs egenskaper, förmågor och publika nycklar, aggregeras till federationsoperatören som digitalt signerar och publicerar det aggregerade SAML-metadatat, vilket således innehåller federationens samtliga aktörers egenskaper, förmågor och publika nycklar.
I saml2int beskrivs hur SAML-metadata skall presenteras. Utformningen av SAML-metadata regleras i OASIS SAML V2.0 metadata specification [SAML2Meta] och hantering av SAML-metadata regleras i OASIS Metadata Interoperability Profile [MetaIOP]. Samtliga ingående aktörer i Skolfederation skall stödja dessa.

Validering av metadata
Innan aktören skickar in metadata till federationen kan de själva validera den mot Skolfederation. Det kan göras genom att ladda upp en fil eller att ange URL på följande plats: http://validator.skolfederation.se.

Publicering av metadata
Skolfederations aggregerade och signerade metadata publiceras här:
https://meta01.skolfederation.se/skolfederation-2_0.xml
Federationsoperatörens publika nyckel för verifiering av metadata återfinns här:
https://meta01.skolfederation.se/skolfederation-2_0.crt
Varje ingående aktör ska signaturverifiera SAML-metadata vid varje förändring mot minst en nyckelkälla.

Autentiseringsförfrågan
I grundscenariot där en användare, exempelvis elev, önskar använda en tjänst, men är oidentifierad blir denne ombedd att autentisera sig. Den förfrågan som tjänsten skapar i detta scenario är en autentiseringsförfrågan vilken användaren tar med sig till intygsutfärdaren (IdP).
Skolfederationen har valt att använda saml2int som deploymentprofil vilken tydligt beskriver hur SAML V2.0 Web Browser SSO Profile [SAML2Prof] ska användas, vilket i sin tur återspeglar sig på autentiseringsförfrågan. Autentiseringssvaret kan vara en följd av en autentiseringsförfrågan, men det kan också vara ett autentiseringssvar utan någon föregående autentiseringsförfråga.

Pseudonymer
Skolfederation värnar om den personliga integriteten. Därför är det av vikt att samtliga ingående parter kan hantera pseudonymer som identifieringsbegrepp (subjekt). Följande två format som är en del av SAML2Core5 ska stödjas:
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
urn:oasis:names:tc:SAML:2.0:nameid-format:transient
Persistenta pseudonymer har egenskapen att de alltid mappar en användare till samma pseudonym per tjänst. Det vill säga att olika tjänster ger olika pseudonymer.
Transienta pseudonymer mappar aldrig en användare till samma pseudonym, utan användaren får en ny pseudonym vid varje nytt tillfälle och för varje tjänst.

Anvisningstjänst (DS, Discovery Service)
I grundscenariot där en användare, exempelvis elev, önskar använda en tjänst, men är oidentifierad så blir denne ombedd att autentisera sig. I en tvåpartsrelation vet tjänsten vilken intygsutfärdare (IdP) som denne ska anvisa användaren till. I en federation likt Skolfederation med 100-talet intygsutfärdare krävs därför en funktion för att anvisa användaren till ”sin” intygsutfärdare. Funktionen benämns anvisningstjänst (discovery services).
Det bör poängteras att en central anvisningstjänst inte är en nödvändighet utan tjänsteleverantören kan själv välja att implementera en funktion för lokal anvisning baserat på SAML-metadata.
Det bör också poängteras att det finns möjlighet till ett scenario med o-ombedda intyg (unsolicited respons). Där ansluter användaren först till sin intygsutfärdare (IdP) med en parameter i anropet som sedan används för att anvisa användaren till rätt tjänst (SP).
Hantering av anvisning regleras av OASIS Identity Provider Discovery Service Protocol Profile [IdPDisco]. Samtliga ingående aktörer i Skolfederationen skall stödja detta.

Skolfederations anvisningsttjänst återfinns här:
https://ds.skolfederation.se/

Single logout
Skolfederation har inledningsvis inget krav på att ingående aktörer ska stödja single-logout. Skolfederation sätter dock inte några infrastrukturella hinder att implementera single-logout.

Attributstjänst (AA, Attribute Authority)
Skolfederations intressenter har inte inledningsvis pekat på några för federationen gemensamma attributstjänster (AA, Attribute Authority). Skolfederation sätter dock inte några infrastrukturella hinder att implementera attributstjänster.

Samverkan – kring utveckling och möjligheter

Skolfederation har växt fram tack vare ett gott samarbete mellan skolhuvudmän och tjänsteleverantörer. Grundläggande är samverkan kring utvecklingen av Skolfederation som en gemensam inloggningstjänst för utbildningssektorn så den motsvarar medlemmarnas behov och underlättar tillgång till digitala tjänster i skolan.

Inom ramen för Skolfederation ges också utrymme för dialog och utbyte av erfarenheter och behov kring utvecklingen av användningen av digitala tjänster i skolan, en utveckling som Skolfederation öppnar möjligheter för.
Det ges möjlighet att i ”demoskolor” med inloggning visa konkreta tjänster i praktikten hos några av federationens tjänsteleverantörer. Där visas även andra funktioner och mer skollika exempel.
Skolfederation har en referensgrupp som är rådgivande i policyfrågor rörande verksamheten, som är öppen för alla som kan bli medlemmar; skolhuvudmän, tjänsteleverantörer och myndigheter.

Grundläggande förutsättning
Skolfederation är en grundläggande förutsättning för tillgång till digitala tjänster i skolan. Med en väl fungerande inloggningslösning på plats för elever och personal kan mer fokus ägnas åt pedagogiken och de digitala tjänster som skolan vill använda.