

Ordlista

Detta är en ordlista att använda som stöd enbart vid konferensen Tekniksnack om digitalisering av nationella prov den 11 mars 2020. Den ska inte användas vid andra tillfällen.

Förkortningar

| Förkortning | Beskrivning |
|-------------|--|
| API | Förkortning av engelska termen <i>Application Programming Interface</i> . I denna kontext avser vara ett tekniskt gränssnitt och en specifikation, vilka tillhandahålls över en nätverkstjänst. API erbjuds för att olika applikationer och system ska kunna kommunicera med en specifik programvara eller webbtjänst. |
| EPPN | Attribut i standarden SS 12000, som avses vara användaridentifieraren i identitetsfederationen. Formatet liknar en e-postadress, men är inte användaren e-postadress. EPPN skapas med hjälp av en lokalt unik användaridentifierare (t ex ett lokalt user-id), ett '@' och en säkerhets-domän (exempelvis user-id@subdomän.kommun.se). På så sätt avser EPPN representera en spårbar och globalt unik sträng som är beständig över tid för varje användare. |
| DNP | Skolverkets webbtjänst för digitala nationella prov |
| FIDUS | Federationsförbund för IDentitetshantering, Utbildning och Skola är en interfederation som drivs från Skolverket. Se <i>interfederation</i> |
| IdP | Förkortning av engelska termen <i>Identity Provider</i> (se nedan) |
| LoA | Förkortning av engelska termen <i>Level of Assurance</i> , se <i>tillitsnivåer</i> |
| MFA | Multifaktorsautentisering (se nedan) |
| SAML | Förkortning av engelska termen <i>Security Assertion Markup Language</i> , som är en biljettbaserad säkerhetsmetod för hantering av inloggnings-information mellan internetbaserade tjänster i en federation. |
| SP | Förkortning av engelska termen <i>Service Provider</i> , se <i>tjänsteleverantör</i> |
| SSO | Förkortning av engelska termen <i>Single Sign-On</i> (se nedan) |
| SS 12000 | Svensk standard för informationsutbyte mellan verksamhetsprocesser i skolan. |
| SUNET | Swedish University computer NETwork är en avdelning på Vetenskapsrådet. |
| TLS/SSL | TLS är en förkortning av engelska termen <i>Transport Layer Security</i> . TLS är ett protokoll för säker dataöverföring på webben. Protokollet är designat för att en dag ersätta SSL, som är en förkortning av engelska termen <i>Secure Sockets Layer</i> . SSL är ett Internetprotokoll som utvecklades av Netscape för att kryptera den data som skickas mellan en webbläsare och en server (och vice versa). SSL stöds idag av alla populära webbläsare. Webbläsaren indikerar en SSL-skyddad session genom att ändra http till https samt visa upp ett litet hänglås. Hemsidans besökare kan klicka på hänglåset för att se SSL-certifikatet. |

Termer

| Term | Förklaring |
|---------------|---|
| Attribut | Variabel som ingår i en persons eller ett objekts digitala representation. Exempel på de attribut som representerar en person i ett digitalt system är förnamn, efternamn, personnummer, osv. |
| Autentisering | Kontroll (verifiering) av uppgiven identitet vid exempelvis åtkomst till en applikation eller webbtjänst. |

| Term | Förklaring |
|-------------------------------|--|
| Autentiseringsmetoder | Det finns flera metoder för identifiering av användare. Den enklaste formen av autentisering sker genom att användaren uppger (loggar in med) sitt användarnamn och ett personligt lösenord. Autentisering över Internet brukar också, men behöver inte, omfatta användning av så kallade elektroniska certifikat. Se även multifaktorsautentisering. |
| Certifikat | Elektroniskt certifikat, även kallad e-certifikat eller digitalt certifikat är ett elektroniskt intyg som styrker att en elektronisk identitetshandling eller e-legitimation är korrekt och giltig. Certifikat som används på en klient kallas för klientcertifikat och certifikat som används på en server kallas för servercertifikat. |
| Edu-ID | Idag är eduID ett studentkonto, som kan användas för att logga in på Antagning.se eller för att aktivera och hantera studentkonton hos lärosätena i Sverige. Skolverket i samarbete med Sunet utvecklar nu utökade funktioner för att eduID också ska kunna användas inom skolan för inloggning till DNP. |
| Federation | En överenskommelse mellan två eller flera parter (organisationer) där man inom federationen har överenskomna gemensamma regler och att parterna litar på varandra att upprätthålla dessa regler. |
| Federerad TLS autentisering | En typ av autentiseringsmetod som använder säkerhetsprotokollet Transport Layer Security (TLS). Metoden tillämpas för autentisering i samband med provisionering. Eftersom Internet är ett offentligt nätverk, används TLS-protokollet för att säkra autentiseringen genom datakryptering. |
| Federation för provisionering | För provisionering (se nedan) till Skolverkets tjänster används en särskild federation som kräver en ömsesidig TLS-autentisering. Autentiseringen görs då genom att begära ett klientcertifikat och validera certifikatet när klientbegäran sker över TLS/SSL. Inom FIDUS är Skolfederation Kontosynk exempel på en sådan federation. |
| Identitetsfederation | Även kallad federation. Inom identitets- och åtkomsthantering avses oftast en identitets- och behörighetsfederation. |
| Identity provider | Part inom en identitetsfederation, som inom ramen för federationen, ansvarar för identifiering av användare och inhämtning av attribut. Denna part ställer ut de identitetsintyg som är avsedda för tjänsteleverantörernas e-tjänster. |
| Interfederation | Överenskommelse mellan två eller flera federationsoperatörer som ingår i ett förbund för att sammansluta federationerna. Interfederation äger rum när en användare från en federation får åtkomst till en tjänst som är registrerad i en annan federation. Även kallad federationsförbund. Skolverket har tagit fram interfederationen FIDUS, som i nuläget ansluter Skolfederation och SWAMID. Fler federationer kan anslutas i framtiden. |
| Metadata | I detta sammanhang avser metadata teknisk information som krävs för samverkan mellan federationens medlemmar. Dessa hanteras i olika register i form av medlemsmetadata och federationsmetadata. |
| Multifaktorsautentisering | En nivå av säkerhet som är starkare än autentisering med endast användarnamn och lösenord. Metoden ställer krav på att identitetskontrollen verifieras med flera former av oberoende faktorer som bevisar identiteten. Man kan till exempel kombinera lösenord med engångslösenord via SMS, säkra kort och dosor av olika slag, mobila certifikat (som exempelvis Freja eID+ och Mobil Bank-ID) och biometrisk identifiering (t ex fingeravtryck och ansiktigenkänning). Även kallad flerfaktorsautentisering eller stark autentisering. |

| Term | Förklaring |
|-------------------------|--|
| Provisionering | Dataöverföring av personuppgifter och undervisningsinformation till Skolverkets webbtjänst |
| Publik nyckel | Inom kryptering används så kallade krypteringsnycklar tillsammans med en krypteringsalgoritm. Moderna kryptosystem använder asymmetrisk kryptering där avsändare och mottagare använder olika krypteringsnycklar. Den som vill kunna ta emot krypterade meddelanden måste ha två nycklar, en publik nyckel som sprids öppet till alla som önskar skicka krypterade meddelanden till användaren, och en privat nyckel som används för dekryptering, och som måste hållas hemligt. Den publika nyckeln går inte att använda för att dekryptera ett krypterat meddelande. En fördel med denna ordning är att sändare och mottagare inte behöver träffas för överlämning av nycklar. |
| Service provider | Se <i>tjänsteleverantör</i> (nedan) |
| Single sign-on | Samlad inloggningsprocedur med autentisering som gäller för en användares tillgång till flera olika digitala tjänster. I praktiken innebär det att en användare behöver endast logga in en gång för att nå de system som är anpassade till tjänsten. |
| Skolenhetskod | Varje skolenhet som följer skollagen (2010:800) har en skolenhetskod i Skolverkets skolenhetsregister. Koden är nationell identifierare för skolenheten och ska inte blandas ihop med andra lokala koder som representerar skolenheten hos huvudmannen, t ex kostnadsställe (konto i ett ekonomisystem) eller organisationskod i ett HR-system. |
| Skolfederation | Skolfederationen är en identitetsfederation som drivs av Internetstiftelsen, i syfte att skapa enklare och säkrare åtkomst till skolans digitala resurser. Skolfederation ingår i FIDUS. |
| SWAMID | SWAMID är en identitetsfederation som omfattar de flesta lärosäten, forskningsinstitut och andra myndigheter som är relaterade till svensk forsknings- och utbildningssektor. SWAMID drivs av SUNET. SWAMID ingår i FIDUS. |
| Tillitsnivåer | Tillförlitligheten av hur en organisation hanterar sina identiteter i enlighet med skyddsklassning som har definieras i ett tillitsramverk. Målet är att man ska utifrån de säkerhetskrav som ställs på tjänsten kunna veta vilken person som faktiskt sitter vid skärmen vid inloggning på ett konto, och att personen är en betrodd användare med aktuell behörighet. |
| Tjänsteleverantör | Part inom en identitetsfederation, som inom ramen för federationen, tillhandahåller en eller flera e-tjänster. Även kallad förlitande part. Engelska: <i>Service Provider</i> |
| Tvåfaktorsautentisering | En typ av multifaktorautentisering, som ställer krav på att identitetskontrollen verifieras genom kombination av två olika faktorer. Även känd som 2FA. Se <i>multifaktorsautentisering</i> |