Signalering av tillitsnivå vid inloggning

Skolon Support - 2024-09-26 - Digitala Nationella Prov

Observera att denna artikel endast riktar sig till de skolhuvudmän som utfärdar e-leg i sin egna IDP. Skolhuvudmän som använder Skolons integration med Freja organisationsID kan alltså bortse från denna artikel.

När en användare loggar in till DNP genom Skolon kommer Skolon kontrollera om användaren har rollen personal. Eftersom Skolverket kräver att personal autentiserar sig med en giltig e-legitimation till Skolverkets provplattform kommer Skolon att kontrollera tillitsnivån (LoA); om användaren inte uppnår minsta krav kommer Skolon att initiera en så kallad step-up verifiering

Step-up verifieringen kan antingen hanteras av Skolon genom Freja eID eller genom en e-legitimation från huvudmannens egna IDP. I praktiken innebär detta att de huvudmän som vill använda e-legitimationen via sin egna IDP har två olika val:

1. Att personal alltid autentiserar sig med e-legitimation när de loggar in till Skolon
2. Att personal inte loggar in med e-legitimation till Skolon, men att step-up verifiering initieras när användaren försöker logga in till Skolverkets provplattform via Skolon

Oavsett om ni väljer alternativ 1 eller 2 måste er egna IDP ha stöd för att signalera en godkänd tillitsnivå i SAML-intyget som utfärdats. Detta görs med SAML-standarden och attributet AuthnContext

Om ni väljer alternativ 2 kommer Skolon i samband med step-up verifieringen att begära en ny autentisering från huvudmannens IdP med krav på den tillitsnivån som Skolverket beslutat. Det görs med hjälp av SAML2-protokollet genom AuthnRequest.

Alternativ 1 - IDP utfärdar alltid godkänd tillitsnivå i SAML-intyget
För att inte trigga en step-up verifikation när personal ska logga in till Skolverkets provplattform via Skolon kan ni konfigurera er IDP att alltid skicka med ett *AuthnContext* med *AuthnContextClassRef* som uppfyller en enligt DIGG godkänd tillitsnivå för e-leg.

Se tabellen nedna för vilka tillitsnivåer som accepteras. Notera att det är DIGG och Skolverket som satt dessa krav, inte vi på Skolon.

Alternativ 2 - Step-up verifikation vid inloggning till Skolverketsprovplattform
Om SAML-intyget från er IDP inte innehåller en godkänd tillitsnivå, och en användare försöker logga in till Skolverkets provplattform via Skolon kommer Skolon att initiera en

step-up verifikation från er IDP genom ett *AuthnRequest.*

Skolon förväntar sig då som svar, ett SAML2 Response innehållande *AuthnContext* med *AuthnContextClassRef* som uppfyller begäran enligt nedan.

Exempel på AuthnRequest innehållande RequestedAuthnContext med AuthnContextClassRef

```
<samlp:AuthnRequest ... >
        ...
                <samlp:RequestedAuthnContext>
<saml:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/loa2</sam
l:AuthnContextClassRef>
<saml:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/loa3</sam
l:AuthnContextClassRef>
<saml:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/loa4</sam
l:AuthnContextClassRef>
<saml:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/uncerti
fied-loa2</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/uncerti
fied-loa3</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/loa2-no
nresident</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/loa3-no
nresident</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>http://id.swedenconnect.se/loa/1.0/loa4-no
nresident</saml:AuthnContextClassRef>
<saml:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/nf-low</s
aml:AuthnContextClassRef>
<saml:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/nf-sub</s
aml:AuthnContextClassRef>
<saml:AuthnContextClassRef>http://id.elegnamnden.se/loa/1.0/nf-high</
saml:AuthnContextClassRef>
        </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Exempel på Response från er IDP innehållande AuthnContext

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" ...
>
        ...
                <saml:Assertion ... >
                        ...
```

```
                                <saml:AuthnStatement ... >
                                <saml:AuthnContext>
                                        <saml:AuthnContextClassRef>
http://id.swedenconnect.se/loa/1.0/uncertified-loa2
                                        </saml:AuthnContextClassRef>
                                </saml:AuthnContext>
                        </saml:AuthnStatement>
        </saml:Assertion>
</samlp:Response>
```

Testa inloggningen

När ni konfigurerat ovan är ni redo att testa inloggningen. Vi har samlat information om testinloggning till Skolverkets provplattform via Skolon på supportartikeln Testa inloggning till Skolverkets provplattform.

Tillitsnivåer som accepteras

Tillitsnivåerna som Skolon accepterar kommer att vara samma som de som angivits som godkända av Skolverket och DIGG. I tabellen nedan finns den signalering som Skolverkets provtjänst litar på.

URI	Tillitsnivå för DIGG-godkände-legitimation eller eIDAS tillitsnivå	DIGG godkänd IdP
http://id.swedenconnect.se/loa/1.0/uncertified-loa2	2	NEJ
http://id.swedenconnect.se/loa/1.0/uncertified-loa3	3	NEJ
http://id.swedenconnect.se/loa/1.0/uncertified-loa4	4	NEJ
http://id.swedenconnect.se/loa/1.0/uncertified-eidas-low	Låg	NEJ
http://id.swedenconnect.se/loa/1.0/uncertified-eidas-sub	Väsentlig	NEJ
http://id.swedenconnect.se/loa/1.0/uncertified-eidas-high	Hög	NEJ
http://id.elegnamnden.se/loa/1.0/loa2	2	JA
http://id.elegnamnden.se/loa/1.0/loa3	3	JA
http://id.elegnamnden.se/loa/1.0/loa4	4	JA
http://id.swedenconnect.se/loa/1.0/loa2-nonresident	2	JA
http://id.swedenconnect.se/loa/1.0/loa3-nonresident	3	JA
http://id.swedenconnect.se/loa/1.0/loa4-nonresident	4	JA

Värdet i tabellen ovan är hämtat från en Bilaga till SKR's Vägledning för skolhuvudmän – Tekniska förutsättningar för digitala nationella prov (DNP)