Beställning av federation till VGR AD (AD FS) – SAML  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Rekommenderade länkar att läsa igenom innan beställning läggs.

* Inera: [Referensarkitektur för Identitet & åtkomst](https://rivta.se/documents/ARK_0046/Referensarkitektur-Identitetochatkomst-RevA.pdf).
* VGRs riktlinje för MFA krav: [download.do (vgregion.se)](https://hittaidiariet.vgregion.se/download.do?id=2585059&filename=PM+g%C3%A4llande+krav+p%C3%A5+flerfaktorsautentisering)

Instruktioner:

1. Lägg beställningsärende (RITM) i Plexus till Identitet & åtkomst.

Rubrik på ärendet i Plexus ska vara ”VGR AD (AD FS): Beställning av federation för *<applikation>*”.

Ex: ”VGR AD (AD FS): Beställning av federation för Heroma (VGR)”.

Detta ärende innehåller fyra aktiviteter:

* 1. 45 minuter konsultation innan konfiguration.
  2. Konfiguration av federeringen.
  3. Dokumentation av federeringen.
  4. 30 minuter konsultation efter konfiguration.

Om det finns önskemål om mer tid så beställs det via gängse processer för resurser till projekt/uppdrag, med syfte att ta fram information för att kunna lägga en beställning på federation.

1. Fyll i informationen nedan och bifoga detta dokument i ärendet.  
   Säkerställ att alla obligatoriska fält är ifyllda, samt att all grå text är ersatt.
2. Om det finns ett godkänt undantag på kravet på flerfaktorsautentisering från Digitaliseringesdirektören och/eller ESB så ska detta bifogas i ärendet, som länk till Diariet.

|  |  |  |
| --- | --- | --- |
| **Övergripande** | |  |
| OBLIGATORISKT |  | |
| VALFRITT  Objekt  (skall finnas med i BIT-filen) | Exempel  92102 Personal / HR | |
| VALFRITT  Frikod 2  (skall finnas med i BIT-filen) | Exempel  50020 | |
| VALFRITT  Tjänst  (skall finnas med i BIT-filen) | Exempel  Heroma HR | |
| VALFRITT  Leverantörens produktinformation  (länk) | Exempel  [Heroma: Personal- och löneadministrativt system](https://www.cgi.com/se/sv/business-process-services/hr-and-payroll/heroma) | |
| VALFRITT  Leverantörens systemdokumentation för konfiguration av AD FS federation.  (länk) | Exempel | |
| VALFRITT  Befintlig systemdokumentation  (länk) | Exempel  G:\RS.VGRIT.Systemdokumentation\Heroma | |
| VALFRITT  Arkitekturbeskrivning (ADD)  (länk) | Exempel  [Word - Heroma Infraskalning ADD (vgregion.se)](http://iserver.vgregion.se/#/document/viewer/bb434d0b-edd3-43b3-b85e-b9f25e11c5fe?library=5979f3ae-dffb-4c42-af33-e3874d59ed5f) | |

|  |  |
| --- | --- |
| **Applikationsdata** | |
| OBLIGATORISKT  Applikationens namn |  |
| OBLIGATORISKT Beskrivning av applikationen  (max 100 tecken) |  |
| OBLIGATORISKT Vilken miljö ska applikationen sättas upp i?   * AD FS PreProduktion (Test) * AD FS Produktion * AD FS Produktion E-tjänstekort * AD FS Produktion Sjunet   (Välj en per beställning. VGRs rutin är att en ny applikation först sätts upp i AD FS Test. När testerna fungerar som förväntat så ska en **ny beställning** läggas för uppsättning i AD FS Produktion.) | Exempel |
| OBLIGATORISKT  Är applikationen Claims baserad?   * Claims aware application * Non Claims aware applikation | Exempel |
| OBLIGATORISKT Bifoga URL eller fil till applikationens metadata.  Alternativt ange manuell information för applikationen.  (Vid manuell information gå vidare med nedanstående frågor) |  |
| VALFRITT Applikationens Autentiserings uppgifter mot AD FS.   * Certifikat   Bifoga det certifikat ni ev vill använda i AD FS federationen. |  |
| OBLIGATORISKT Vilket protokoll ska användas? Ange URL.   * WS federation Passive protocol * SAML 2.0 Web SSO protocol   (Support för WS-Trust protocol är alltid aktiverat för en federationsuppsättning.) |  |
| OBLIGATORISKT  Trust identifier  (Måste var en unik identifier för applikationen.) |  |
| OBLIGATORISKT Finns det ett godkänt undantag från kravet på flerfaktorsautentisering från VGRnet?   * JA * NEJ   (Om JA, bifoga beslutet som länk till Diariet) |  |
| VALFRITT Claims - Issuance Transform Rules  Vilka Claim ska vi skicka med och hur? | Exempel Send LDAP attribut as Claims: E-mail Address Name Name ID Windows Account Name  User Principal Name |

# AD FS Data:

|  |  |
| --- | --- |
| AD FS Data |  |
| Federation Service Identifier(Stage)  Federation Service Identifier(Production)    Federation Metadata URL SAML/WS- Fed (Stage)  Federation Metadata URL SAML/WS-Fed (Production)     OpenID Connect Discovery (Stage)   OpenID Connect Discovery (Stage) | <http://adfs-test.vgregion.se/adfs/services/trust>  <http://adfs.vgregion.se/adfs/services/trust>    <https://adfs-test.vgregion.se/federationmetadata/2007-06/federationmetadata.xml>  <https://adfs.vgregion.se/federationmetadata/2007-06/federationmetadata.xml>    <https://adfs-test.vgregion.se/adfs/.well-known/openid-configuration>  <https://adfs.vgregion.se/adfs/.well-known/openid-configuration> |
| WS-Fed Sign-On Endpoint (Stage)  WS-Fed Sign-On Endpoint (Production) | <https://adfs-test.vgregion.se/adfs/ls/>  https://adfs.vgregion.se/adfs/ls/ |
| SAML-P Sign-On Endpoint (Stage)  SAML-P Sign-On Endpoint (Production) | <https://adfs-test.vgregion.se/adfs/ls/>  https://adfs.vgregion.se/adfs/ls/ |
| OAuth 2.0 token endpoint (Stage)  OAuth 2.0 token endpoint (Production) | <https://adfs-test.vgregion.se/adfs/oauth2/>  <https://adfs.vgregion.se/adfs/oauth2/> |
| OAuth 2.0 authorization endpoint (Stage)  OAuth 2.0 authorization endpoint (Production) | <https://adfs-test.vgregion.se/adfs/oauth2/>  <https://adfs.vgregion.se/adfs/oauth2/> |