TrustedDialog – funktionsbrevlådor

Innehållsförteckning

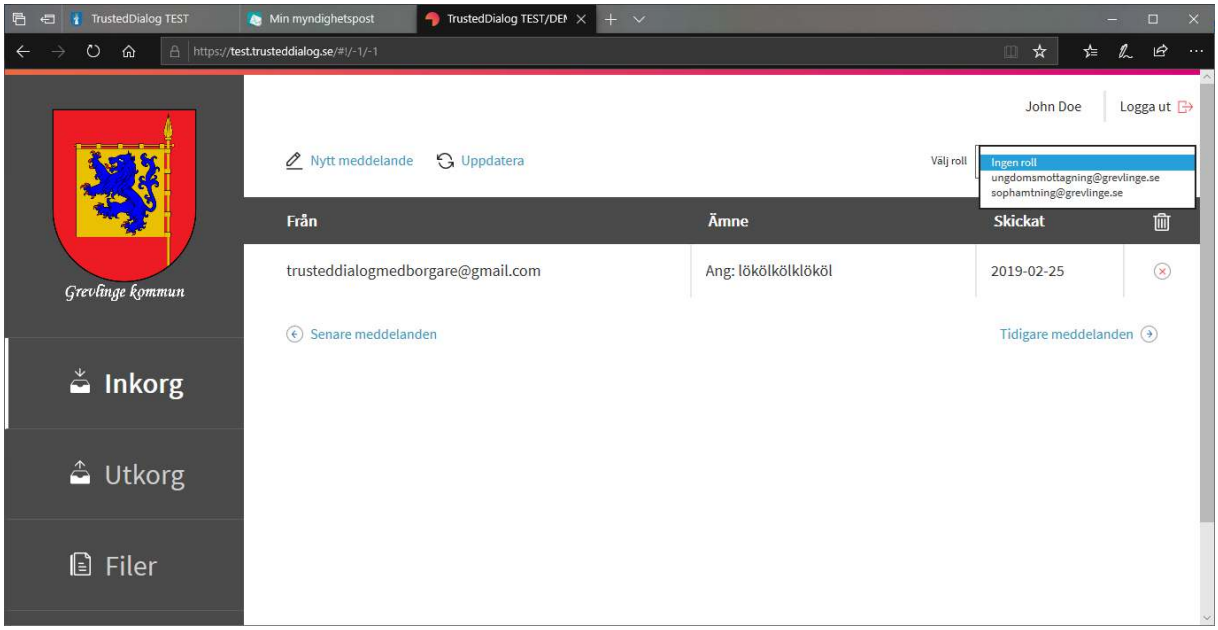
1. Inledning

Detta dokument syftar till att ge all nödvändig information om TrustedDialog funktionsbrevlådor, alltifrån tanken med dem till hur de används och hur de konfigureras.

2. Syfte

Syftet med funktionsbrevlådor är att flera TrustedDialog-användare ska kunna använda samma brevlåda, att externa aktörer ska kunna adressera funktioner snarare än individer och att vid behov dölja personinformation om enskilda individer (socialtjänsthandläggare etc) för omgivningen.

3. Användning



Efter inloggning kan användare som har åtkomst till funktionsbrevlådor välja dessa i dropdownen överst till höger (notera att även användare som denna användare är ombud för kommer upp här). När användaren valt en funktionbrevlåda agerar användaren som denna funktion. Inkorgen, utkorgen och filerna som visas är funktionens, tills användaren väljer en annan funktion eller att vara sin egen individuella användare igen.

För att adressera en funktionsbrevlåda loggar användaren in i TrustedDialog och anger funktionsbrevlådans e-postadress. Då skickas ett notifieringsmeddelande med vanlig e-post till funktionsbrevlådans e-postadress, och de som har behörighet till funktionsbrevlådan kan logga in och se meddelandet. I avsnitt 4 beskrivs både konfigurationen för att ge behörighet att ta emot meddelandet och hur man ser till att e-postnotifieringen går till rätt personer.

Observera att all kommunikation i TrustedDialog sker inom TrustedDialog! Vi får många frågor om hur funktionsbrevlådor ska kunna adresseras via vanlig e-post men hela syftet med TrustedDialog är ju att informationen ska finnas inuti den digitala brevlådan, för både avsändare och mottagare, eftersom det typiskt är känslig information.

För mer detaljerad information om användande hänvisas till TrustedDialogs användardokumentation.

4. Konfiguration

Konfigurationen av funktionsbrevlådor består av tre delar: TrustedDialog, katalogtjänsten (Active Directory etc) samt e-posthanteringen. TrustedDialogs grundtanke är att så mycket som möjligt av behörighetskonfigurationen ska ligga i katalogtjänsten, man ska inte behöva sätta behörigheter i TrustedDialog. Konfigurationen handlar istället om hur TrustedDialog ska plocka upp behörighetskonfigurationen från katalogtjänsten/IDP:n

4.1. TrustedDialog

```
server.auth.userRolesAttribute=urn:oid:1.3.6.1.4.1.5923.1.1.1.7
```

Ovan exempel är default i TrustedDialog. Det innebär att TrustedDialog förväntar sig ett attribut med namnet urn:oid:1.3.6.1.4.1.5923.1.1.1.7 (SAML v2-format på attribut) som ska uttrycka vilka funktionsbrevlådor användaren har tillgång till. Nedan beskrivs hur en sådan konfiguration ser ut i en IDP.

4.2. IDP

IDP:ns ansvar i detta fall är att ge TrustedDialog den attributsinformation som krävs för att ge behörigheter till funktionsbrevlådor. Om TrustedDialog är konfigurerad enligt defaultuppsättningen så behöver IDP:n kunna släppa ifrån sig ett attribut med värde enligt:

```
urn:oid:1.3.6.1.4.1.5923.1.1.1.7=socialtjanst@grevlinge.se;sophamtning@grevlinge.se
```

Med SAML-format ser det ut enligt:

```
<saml2:Attribute FriendlyName="eduPersonEntitlement"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.7"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" >
   <saml2:AttributeValue>ungdomsmottagning@grevlinge.se;socialtjanst@grevlinge.se
   </saml2:AttributeValue>
 </saml2:Attribute>
```

Hur görs denna konfiguration i IDP? Det beror på IDP och är utanför scopet av detta TrustedDialog-dokument. Men, man kan säga något om de tre för TrustedDialog vanligaste IDP:erna och hur det konfigureras där

Nexus HAG

Certezza har mycket bra kompetens på Nexus HAG och kan hjälpa till om så krävs. Förslagsvis konfigureras en attributgrupp i Nexus HAG och man kan då bestämma vilka attribut från katalogtjänsten som ska skickas med SAML-biljetten och vad de ska tas ifrån i katalogtjänsten. För mer information hänvisas till Certezza och/eller Nexus dokumentation.

Nexus HAG har tyvärr inte funktionalitet för att kunna översätta ett gruppmedlemsskap i katalogen till ett SAML-attribut, så om Nexus HAG används så krävs ett attribut i katalogen innehållande funktionsbrevlådeinformationen, dvs ungdomsmottagning@grevlinge.se;sophamtning@grevlinge.se eller motsvarande.

PhenixID PAS

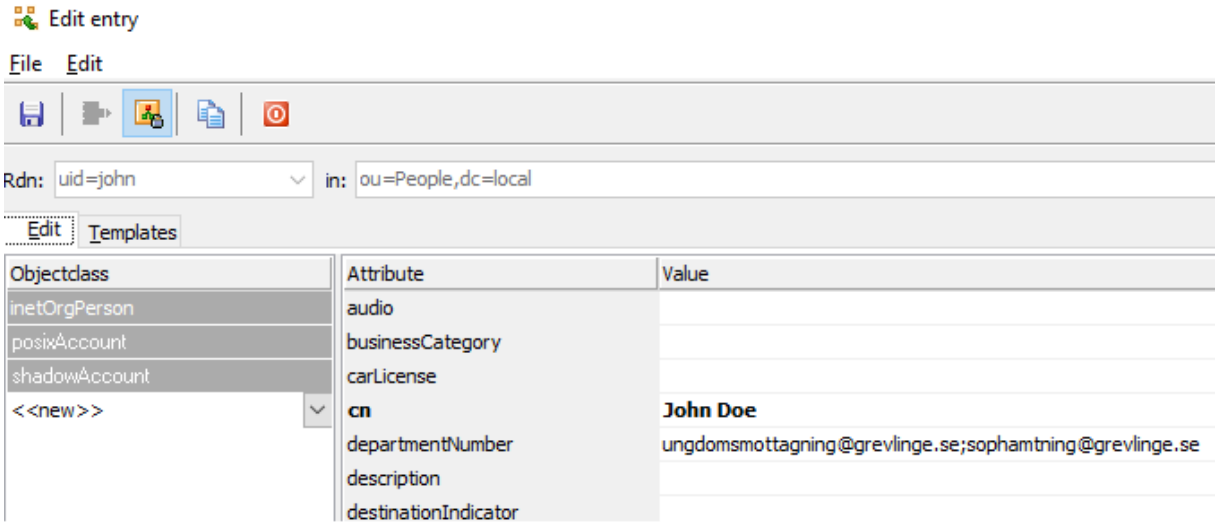
Även i PAS anges vilken information som ska tas från katalogtjänsten och skickas in i SAML-biljetten. PAS har möjlighet att ta gruppmedlemsskap i katalogen och översätta till SAML-attribut. För mer information hänvisas till PhenixID-dokumentation.

Microsoft ADFS

I Microsoftvärlden kallas attribut för claims och man får konfigurera claims för varje attribut som ska skickas. ADFS kan ta gruppmedlemsskap från AD:t och ange som claims (dvs SAML-attribut) i biljetten, för mer info hänvisas till Microsofts dokumentation.

4.3. Katalogtjänst

Grundinformationen för tillgång till funktionsbrevlådorna måste finnas i katalogtjänsten. Om PAS eller ADFS används som IDP så kan detta vara gruppmedlemskap, annars måste det vara ett faktiskt katalogattribut.



I exemplet ovan ser vi katalogattributet departmentNumber innehållande två funktionsbrevlådor. En motsvarande konfiguration behövs för Nexus HAG, medan man för PAS eller ADFS kan använda grupptillhörighet istället. Hur informationen kommer in i detta attribut ligger utanför detta dokument, men man kan ju tänka sig att man vill använda en IDM-lösning, eller scripts eller liknande för att åstadkomma det.

4.4. E-posthantering

Konfigurationsbeskrivningen ovan beskriver hur en användare får åtkomst till en funktionsbrevlåda i TrustedDialog, här beskrivs hur vi ser till att e-postnotifieringen går till rätt personer.

Som beskrivs i avsnitt 3 så resulterar ett säkert meddelande till en funktionsbrevlåda dels i att ett meddelande skapas i TrustedDialog och dels att en e-postnotifiering skickas till den adress man angett (sophamtning@grevlinge.se eller motsvarande). För att se till att e-postmeddelandet till sophamtning@grevlinge.se går till rätt personer måste vi alltså konfigurera e-postsystemet (Exchange eller motsvarande) så att berörda personer antingen har åtkomst till e-postbrevlådan sophamtning@grevlinge.se eller att det ligger en forward så att inkommande meddelanden till sophamtning@grevlinge.se går ut till rätt personer. Dessa personer är rimligen antingen alla som kommer åt TrustedDialog-brevlådan sophamtning@grevlinge.se eller vissa av dem, men det finns

ingen rimlig anledning att notifieringarna ska gå ut till fler personer än som faktiskt kan komma åt information.

TrustedDialog har ingen koppling till Exchange eller annat e-postsystem för att ta adresser från det och skapa behörigheter.

5. Spårbarhet

När en användare skickar ett meddelande med en funktionsbrevlåda så loggas att det skett och vilken inloggad användare som gjort det. Det personliga ansvaret och spårbarheten finns alltså där även om adressen för mottagaren är en funktionsbrevlådas.

6. Relevanta angränsande funktioner

6.1. Ombudshantering

I TrustedDialog 3.5 kommer funktionen att en användare kan agera ombud för en annan användare. Det fungerar på motsvarande sätt som funktionsbrevlådor, i att en användare kan agera i en annan brevlådas namn.