RIV Teknisk Anvisning Basic Profile
Med intygspropagering 2.0

Arkitekturledningens tekniska expertgrupp
Kontaktperson: Forum på http://rivta.forge.osor.eu samt t-grupp@arkitekturledningen.se
2010-02-03

Sveriges Kommuner och Landsting
Arkitekturledning

Innehållsförteckning

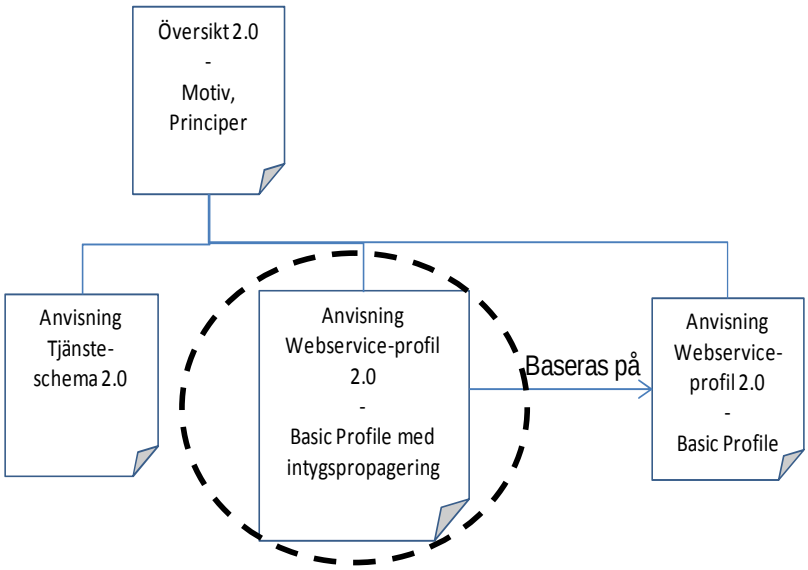
Versionshantering för framtagande av detta dokument

Revision	Datum	Vem	Kommentar
PA1	2010-02-01	Johan.Eltes@callistaenterprise.se	Utkast för diskussion med NPÖ-projektet och T-gruppen. Återstår: - Exempel-WSDL - Verifiering genom RIVTA-refappen - Spec av SOAP-faults för auktorisationsfel
PA2	2010-02-02	Johan.Eltes@callistaenterprise.se	Uppdaterad efter avstämning med T-gruppen. Återstår: - Exempel-WSDL - Verifiering genom RIVTA-refappen Spec av SOAP-faults för auktorisationsfel
PA3	2010-02-02	Johan.Eltes@callistaenterprise.se	Justerat flera skrivfel i stycket för regel #2.

RIV TA Basic Profile 2.0

1 Inledning

Detta dokument beskriver regelverket för RIV Tekniska Anvisningar Basic Profile 2.0 med intygspropagering. Det är en påbyggnad på Profile 2.0 för att möjliggöra överföring av slutanvändarens SAML2-intyg i syfte att utföra BIF åtkomstkontroll baserad på slutanvändarens identitet och beskrivande egenskaper.



1.1 Målgrupp

Denna anvisning riktar sig till dem som ska specificera WSDL för en nationell tjänsteinteraktion i enlighet den tekniska RIV-profil som benämns ”Basic Profile med intygspropagering”. Anvisningen innehåller endast regeluppsättningen som definierar profilens avvikelser från ”Basic Profile”. För bakgrund, motiv, krav samt de principer som ligger till grund för utvecklingen av profilen hänvisas till Översikt RIV Tekniska Anvisningar 2.0 [R2].

1.2 Syfte

Syftet med denna anvisning är att beskriva en utökning av basprofilen som ger möjlighet att föra över ett SAML-intyg som representerar en starkt autentiserad slutanvändare.

1.3 Tillgänglighet

1.4 Referenser

Ref	Dokument	Beskrivning och ev. webbadress	Ansvarig
[R1]	T-Boken	VIT-bokens tekniska arkitektur. Principer för uppbyggnad av den nationella arkitekturen i form av en teknisk referensarkitektur samt användningsfall med ett tekniskt perspektiv på realisering. Webblänk till PDF för REV A: http://www.arkitekturledningen.se/undermappar/Dokument/T%20boken%20-%20REV%20A.pdf	Arkitekturledningens tekniska expertgrupp, SKL
[R2]	Översikt RIV Tekniska Anvisningar 2.0	Bakgrund, motiv, krav samt de principer som ligger till grund för utvecklingen av denna anvisning. Webblänk till PDF för översikten: http://rivta.forge.osor.eu/specs/RIV_TA_OVERSIKT_2.0.pdf	Arkitekturledningens tekniska expertgrupp, SKL
[R3]	RIV Teknisk Anvisning Tjänsteschema 2.0	Anvisning för att specificera ett XML-schema (tjänsteschema) för ett tjänstekontrakt. Definierar elementen för WSDL-filens meddelanden. Webblänk till PDF för anvisningen: http://rivta.forge.osor.eu/specs/RIV_TA_TJANSTESCHEMA_2.0.pdf	Arkitekturledningens tekniska expertgrupp, SKL
[R4]	RIV Teknisk Anvisning Basic profile 2.0	Basprofilen för denna profil. Webblänk till PDF för anvisningen: http://rivta.forge.osor.eu/specs/RIV_TA_BASICPROFILE_2.0.pdf	The Web Services Interoperability Organization och ISO
[R5]	WS-I Simple Soap Binding Profile	" Defines the WS-I Simple SOAP Binding Profile 1.0, consisting of a set of non-proprietary Web services specifications, along with clarifications and amendments to those specifications which promote interoperability" Weblänk till profilen : http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html	The Web Services Interoperability Organization
[R6]	SAML Core 2.0	Definierar format för den biljett som i denna profil binds till soap-headern. Webbänk till specifikationens hemsida: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf	Oasis
[R7]	Exempel - Tjänsteinteraktion	All fragment av WSDL och XML-scheman som finns i detta dokument härrör ur den tjänsteinteraktion som ligger till grund för exempelapplikationerna för Java och .Net. Webblänk till tjänsteinteraktionens WSDL och XML-scheman: https://svn.forge.osor.eu/svn/rivta/src/bp20/refapp/trunk/java/cxf/rivta-bp20-refapp-schemas/src/main/resources/schemas/business/JournalinfoApoteketRIV/	Arkitekturledningens tekniska expertgrupp, SKL
[R8]	Exempel – konsument och producent i Java och .Net	Referensapplikationerna syftar till att vara ett generellt underlag för den utvecklare som ska utveckla en tjänstekonsument eller en tjänsteproducent för en tjänsteinteraktion som följer denna profil. Det är en målsättning att detta ska avlasta nationella projekt från att ta fram projektspecifika kodexempel för varje nationell tjänsteinteraktion som specificeras enligt denna profil. Webblänk till hemsida för exempelapplikationer: https://forge.osor.eu/plugins/wiki/index.php?RivTaBp2.0-RefApp&id=111&type=g	Arkitekturledningens tekniska expertgrupp, SKL

1 Beskrivning av namnregler

Denna profils namn är ”RIV Tekniska Anvisningar – Basic Profile med intygspropagering 2.0” och refereras **${profil}**

Denna profils kortnamn är ”rivtabpip20” och refereras **${profilKortnamn}**

2 Följsamhet mot externa regelverk

Här definieras de externa regelverk (t.ex. profiler) som utgör regelbas för denna profil. Det är en målsättning att denna profil ska kunna läsas uppifrån och ner utan detaljerad kunskap om externa regelverk. För regler som inte lyfts fram i denna profil (av förbiseende eller för att de inte bedömts viktiga) hänvisas till de externa regelverk som redovisas här.

Regel #1, Följsamhet mot RIV TA BP 2.0

Utformning av WSDL *skall* följa RIV TA BP 2.0, med tillägg av de regler som definieras i denna profil.

Motiv: Interoperabilitet

3 Detaljerade regler

Regel #2: Propagering av intyg

Elementet Assertion från SAML 2.0 Core skall användas för att i soap-header specificera intyg för den medarbetare vars åtkomsträttigheter ska verifieras.

- WSDL *skall* importera (xsd:import) följande schema för namnrymd "urn:oasis:names:tc:SAML:2.0:assertion" som *bör* ges namnrymdsalias "saml".
- Det andra wsdl:Part-elementet i varje wsdl:Message som definierar ett request-meddelande *skall* ha namnet Assertion och värdet "saml:Assertion" för attributet "element".
- Varje Assertion-part enligt ovan *skall* bindas till soap:header under wsdl:binding / wsdl:operation / wsdl:input.
- Tjänstekonsumenten *skall* det SAML-assertion som representerar slutanvändarens biljett och som tjänsteproducenten kan använda för att med hjälp av BIF Authorization utföra åtkomstkontroll.

Motiv: För att tjänsteproducent ska kunna utföra åtkomstkontroll avseende medarbetarens rättigheter utföra begärd tjänst (i första hand att fråga efter den vårddokumentation som uttrycks i fråge-meddelandet), krävs att tjänsteproducenten har tillgång till en SAML-biljett som representerar medarbetaren med hennes identitet och egenskaper. SAML-biljetten måste vara kompatibel och accepterad av BIF åtkomstkontroll.

Exempel: Se …