

RIV TA Basic Profile 2.1 med intygsspropagering

RIV Tekniska Anvisningar

Utgåva B
2012-01-03

Utgåvehistorik

<i>Utgåva</i>	<i>Revision Datum</i>	<i>Beskrivning</i>	<i>Ändringarna gjorda av</i>	<i>Definitiv revision fastställd av</i>
PA1	2010-02-01	Utkast för diskussion med NPÖ-projektet och T-gruppen. Återstår: <ul style="list-style-type: none">• Exempel-WSDL• Verifiering genom RIVTA-refappen• Spec av SOAP-faults för auktorisationsfel	Johan.Eltes@callistaenterprise.se	
PA2	2010-02-02	Uppdaterad efter avstämning med T-gruppen. Återstår: <ul style="list-style-type: none">• Exempel-WSDL• Verifiering genom RIVTA-refappen• Spec av SOAP-faults för auktorisationsfel	Johan.Eltes@callistaenterprise.se	
PA3	2010-02-02	Justerat flera skrivfel i stycket för regel #2.	Johan.Eltes@callistaenterprise.se	
PA4	2010-02-09	Verifierad med refapp, dock utan att testa mot BIF ÅKT eller annan tjänst som behöver intyget.	Johan.Eltes@callistaenterprise.se	
PA5	2011-06-27	Uppdaterat för RIVTA 2.1	Marcus.krantz@callistaenterprise.se	
A	2011-10-19	Revision fastställd		Arkitekturledningens Tekniska Expertgrupp, Center för eHälsa i samverkan
PB1	2011-12-14	Uppdaterat dokumentet i och med byte av projektplats från Osor till Google code. Enbart ändringar under rubriken Referenser och länk till referensapplikation.	hans.thunberg@callistaenterprise.se	
B	2012-01-03	Revision fastställd		Arkitekturledningens Tekniska Expertgrupp, Center för eHälsa i samverkan

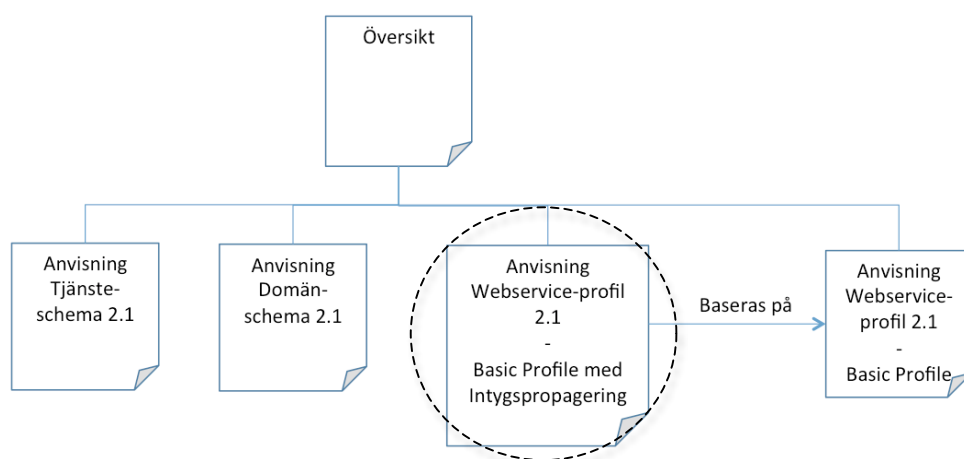
INNEHÅLLSFÖRTECKNING

1. INLEDNING	4
1.1. MÅLGRUPP	4
1.2. SYFTE	4
1.3. TILLGÄNGLIGHET	4
1.4. REFERENSER	4
1 BESKRIVNING AV NAMNREGLER	7
2 FÖLJSAMHET MOT EXTERNA REGELVERK	7
REGEL #1, FÖLJSAMHET MOT RIV TA BP 2.1	7
3 DETALJERADE REGLER	7
REGEL #2: PROPAGERING AV INTYG	7

RIV TA Basic Profile 2.1

1. Inledning

Detta dokument beskriver regelverket för RIV Tekniska Anvisningar Basic Profile 2.1 med intygspropagering. Det är en påbyggnad på Profile 2.1 för att möjliggöra överföring av slutanvändarens SAML2-intyg för en slutanvändares identitet.



1.1. Målgrupp

Denna anvisning riktar sig till dem som ska specificera WSDL för en nationell tjänsteinteraktion i enlighet med 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 2.1 [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 (invånare eller medarbetare).

1.3. Tillgänglighet

Detta dokument är publicerade under licensen Creative Commons CC-BY-SA (<http://creativecommons.org/licenses/by-sa/2.5/se/>). Det betyder att du fritt får kopiera, distribuera och skapa bearbetningar av anvisningarna, under förutsättning att upphovsmannen (Sveriges Kommuner och Landsting) anges (men inte på ett sätt som antyder att de godkännt eller rekommenderar din användning av verket).

Denna profil är verifierad genom exempelapplikationer. Källkoden [R10] för dessa distribueras under öppen-källkodsliscensen Apache License, Version 2.0 (<http://www.apache.org/licenses/LICENSE-2.0>)

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:	Arkitekturledningens tekniska expertgrupp, Center för eHälsa i samverkan



Ref	Dokument	Beskrivning och ev. webbadress	Ansvarig
		http://www.cehis.se/images/uploads/dokumentarkiv/Referensarkitektur_vard_omsorg_VIT-bokens_tekniska_arkitektur_Rapport_110314_REV_B.pdf	
[R2]	Översikt RIV Tekniska Anvisningar REV B	Bakgrund, motiv, krav samt de principer som ligger till grund för utvecklingen av denna anvisning. Webblänk till PDF för översikten: http://code.google.com/p/rivta/source/browse/wiki/specs/RIV_Tekniska_Anvisningar_Oversikt_REV_B.pdf	Arkitekturledningens tekniska expertgrupp, Center för eHälsa i samverkan
[R3]	RIV Teknisk Anvisning Tjänsteschema 2.1	Anvisning för att specificera ett XML-schema (tjänsteschema) för ett tjänstekontrakt. Definierar elementen för WSDL-filens meddelanden. Webblänk till PDF för anvisningen: http://code.google.com/p/rivta/source/browse/wiki/specs/RIV_Tekniska_Anvisningar_Tjansteschema_2.1.pdf	Arkitekturledningens tekniska expertgrupp, Center för eHälsa i samverkan
[R4]	WS-I Basic Profile	” Defines the WS-I Basic Profile 1.1, consisting of a set of non-proprietary Web services specifications, along with clarifications, refinements, interpretations and amplifications of those specifications which promote interoperability ” Webblänk till WS-I Basic Profile: http://www.ws-i.org/Profiles/BasicProfile-1.1.html	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” Webblänk till profilen : http://www.ws-i.org/Profiles/SimpleSoapBindingProfile-1.0.html	The Web Services Interoperability Organization
[R6]	HCC spec.	SITHS HCC: Certifikat för svensk vård och omsorg. Webblänk till PDF för REV 2.34: http://www.inera.se/VirtDocRoot/Tj%C3%A4nster/SITHS/Visasp%C3%A5_bolagswebb/04.St%C3%B6djande_dokument/HCC_specifikation.pdf	Inera AB
[R7]	SOAP 1.1 spec	Definierar ett XML-baserat protokoll för utbyte av information. Är grunden för den standardisering som går under benämningen ”web services”. Webblänk till specifikationens hemsida: http://www.w3.org/TR/2000/NOTE-SOAP-20000508/	W3C
[R8]	WSDL 1.1 spec	Beskrivningsspråk för web-services. Syftar till att stödja utvecklingsverktyg i design-time och web-service-konsumenterna i run-time. Webblänk till specifikationens hemsida: http://www.w3.org/TR/wsdl	W3C
[R9]	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:	Arkitekturledningens tekniska expertgrupp, Center för eHälsa i samverkan



Ref	Dokument	Beskrivning och ev. webbadress	Ansvarig
		http://code.google.com/p/rivta/source/browse/RefApp/rivta-bp-21/java/cxf/trunk/rivta-bp21-refapp-schemas/src/main/resources/schemas	
[R10]	Exempel – konsument och producent i Java och .Net	<p>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.</p> <p>Webblänk till hemsida för exempelapplikationer: http://code.google.com/p/rivta/wiki/Bp21ReferenceApplication</p>	Arkitekturledningens tekniska expertgrupp, Center för eHälsa i samverkan

1 Beskrivning av namnregler

Denna profils namn är "RIV Tekniska Anvisningar – Basic Profile med intygspagering 2.1" och refereras **`{profil}`**.
Denna profils kortnamn är "rivtabpip21" 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 2.1

Utformning av WSDL *skall* följa RIV TA BP 2.1, 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 eller invånare vars identitet ska intygas.

- 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: Vissa externa parter till vård och omsorg kräver SAML-intyg som bärare av aktörens identitet.

Exempel: Se WSDL för profilens referensapplikation, t.ex.

http://rivta.googlecode.com/svn/RefApp/rivta-bpip-21/java/cxf/trunk/rivta-bp21-refapp-schemas/src/main/resources/schemas/interactions/MakeBookingInteraction_1.0_rivtabpip21.wsdl