

Diameter ABFAB Application

Thursday, March 31, 2011

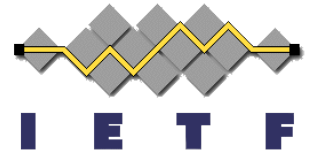
draft-jones-diameter-abfab

Mark Jones

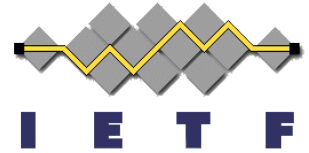
Hannes Tschofenig

IETF 80

Prague, Czech Republic



I-D in a nutshell

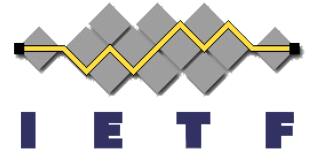


- Specifies a new Diameter application that extends the Diameter EAP application with new AVPs.

AVP Name	+-----+	
	Command-Code	
	-----+-----+	
	DER	DEA
-----	-----+-----+	
SAML-Assertion	0	1
SAML-AuthnRequest	1	0
SAML-AuthnResponse	0	1
	+-----+-----+	

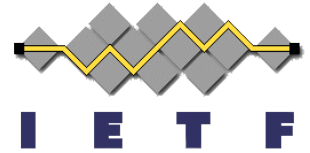
- Diameter server may maintain state or may be stateless (indicated by the Auth-Session-State AVP)
- Diameter client MUST support the Authorization Session State Machine defined in RFC3588.

DER command



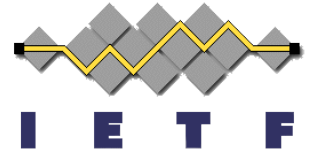
- New SAML-AuthnRequest AVP:
 - UTF8String encoded SAML AuthnRequest message.
 - Only included in the first DER message sent by the Diameter client.
- SAML Authorization happens immediately after the EAP authentication procedure has been completed.
- Auth-Request-Type AVP MUST be set to the value AUTHORIZE_AUTHENTICATE.

DEA command



- Contains one of two new AVPs which are included in the final DEA command of the EAP exchanges.
- SAML-AuthnResponse AVP:
 - UTF8String encoded SAML AuthnResponse message.
- SAML-Assertion AVP:
 - UTF8String encoded SAML assertion.

Next Steps



- Open issues:
 - Multiple assertion AVPs per response?
 - Encrypt XML payloads?
 - Allow Authorize-Only exchanges post-authentication to retrieve more SAML attributes?
 - Lots more to study but hey, it is -00. ☺
- Adopt as ABFAB WG document?

Feedback?

