Enterprise Rights Management

Annex B – Cross-Enterprise-ID – Technical Recommendation

Version 0.9, 04.09.2009

Status: Draft

© ProSTEP iViP Association, 2009

Abstract

This document is Annex B of ProSTEP iViP Recommendation PSI 7, which provides recommendations for the adoption of ERM technology for the implementation of secure data exchange processes. The present document reviews existing standards and recommendations for Single Sign-On and provides a technical recommendation for the implementation of the Federated Identity Management scenario.

© ProSTEP iViP e.V. All rights reserved

Disclaimer

ProSTEP iViP Recommendations (PSI Recommendations) are recommendations that are available for general use. Anyone using these recommendations is responsible for ensuring that they are used correctly. This PSI Recommendation gives due consideration to the prevailing state-of-the-art at the time of publication. Anyone using PSI Recommendations must assume responsibility for his or her actions and acts at their own risk. The ProSTEP iViP Association and the parties involved in drawing up the PSI Recommendation assume no liability whatsoever. We request that anyone encountering an error or the possibility of an incorrect interpretation when using the PSI Recommendation should contact the ProSTEP iViP Association (psi-issues@prostep.com) immediately so that any errors can be rectified.

Copyright

I. All rights to this PSI Recommendation, in particular the copyright rights of use, and sale such as the right to duplicate, distribute or publish the recommendation, remain exclusively with the ProSTEP iViP Association and its members.
II. This PSI Recommendation may be duplicated and distributed unchanged, for instance for use in the context of creating software or services.
III. It is not permitted to change or edit this PSI Recommendation.
IV. A suitable notice indicating the copyright owner and the restrictions on use must always appear.

© ProSTEP iViP e.V. All rights reserved

Contents

Abstract ii

Disclaimer iii

Copyright iii

List of Figures v

Chapter 1. Introduction 1

Chapter 2. Existing Single Sign-On standards and recommendations 3

2.1. An abstract model for Single Sign-On . . . 3

2.2. Single Sign-On based on SAML . . . 5
2.2.1. Overview of SAML . . . 5
2.2.2. Standardized SSO-profiles for SAML . . . 7
2.2.2.1. Web Browser SSO Profile . . . 7
2.2.2.2. Enhanced Client or Proxy (ECP) Profile . . . 8
2.2.2.3. Holder-of-Key Web Browser SSO Profile . . . 9
2.2.3. Security aspects of SAML-based Single Sign-On . . . 9

2.3. Single Sign-On based on WS-* / CardSpace . . . 10
2.3.1. Overview of WS-* . . . 10
2.3.1.1. WS-Security . . . 10
2.3.1.2. WS-Trust . . . 11
2.3.1.3. WS-Policy . . . 12
2.3.1.4. WS-SecurityPolicy . . . 12
2.3.1.5. WS-Federation . . . 12
2.3.1.6. Role of other WS-* specifications in the SSO-context . . . 13
2.3.2. Standardized SSO-profiles for WS-* . . . 13
2.3.3. Relying Party is a conventional Web Server . . . 15
2.3.4. Relying Party provides a Security Token Server (STS) . . . 17

2.4. ODETTE's SESAM recommendation . . . 19

Chapter 3. Cross-Enterprise-ID-Recommendation 21

3.1. Single supplier tier . . . 21

3.2. Multiple supplier tiers . . . 22

Bibliography 25

© ProSTEP iViP e.V. All rights reserved

List of Figures

1 Abstract system architecture with ERM and IdM 1
2 An abstract model for Single Sign-On 4
3 Single Sign-On based on SAML 6
4 CardSpace Screenshot 14
5 Relying Party is conventional Web Server 16
6 Relying Party with Security Token Service 18
7 Cross-Enterprise-ID for a single supplier tier 21
8 Cross-Enterprise-ID for multiple supplier tiers 23

© ProSTEP iViP e.V. All rights reserved