Singapore Standards Council

TR 29 : 2012

(ICS 35.100.70; 35.240)

TECHNICAL REFERENCE

National authentication framework – Authentication operator interface messages

Incorporating Amendment No. 1, No. 2 and Corrigendum No. 1

Published by

Enterprise Singapore

TR 29 : 2012
(ICS 35.100.70; 35.240)

TECHNICAL REFERENCE

National authentication framework – Authentication operator interface messages

ISBN 978-981-4353-23-6

First published, 2012

NOTE

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

Contents

Foreword

This Technical Reference (TR) was prepared by the National Authentication Framework Interface Specifications Working Group (NAFISWG) of the Security and Privacy Standards Technical Committee (SPSTC) under the direction of the Information Technology Standards Committee (ITSC). The ITSC endorsed the Technical Reference on 29 February 2012.

The National Authentication Framework (NAF), a key programme under the Infocomm Development Authority's iN2015 Masterplan, aims to deploy a nationwide platform for strong authentication for end-users accessing key online services.

The strategic objectives of the NAF are to provide a trusted and cost-effective strong authentication platform for government e-services and businesses, thereby promoting the pervasive use of strong authentication and enhancing Singapore's standing as a secure and trusted e-commerce hub.

The primary focus of this TR is to standardise the technical communications between the authentication operators and service providers in the NAF, thereby providing the flexibility for new authentication operators to come on board the NAF and ease of switching by service providers to different operators.

This Technical Reference is not to be regarded as a Singapore Standard. This Technical Reference is made available for provisional application over a period of two years, but does not have the status of a Singapore Standard. The aim is to use the experience gained to modify the Technical Reference so that it can be adopted as a Singapore Standard. Users of the Technical Reference are invited to comment on its technical content, ease of use and any ambiguities or anomalies. These comments can be submitted using the feedback form provided at the end of the Technical Reference and will be taken into account in the review of the publication. At the end of the two years, the Technical Reference will be reviewed by the WG to discuss the comments received and to determine its suitability as a Singapore Standard. Submission for approval by the Standards Council as a Singapore Standard will be carried out only upon agreement after review.

Attention is drawn to the possibility that some of the elements of this Technical Reference may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

Technical Reference for national authentication framework – Authentication operator interface messages

Section One – General

0 Introduction

This Technical Reference (TR) defines the technical communications between Service Providers (SPs) and Authentication Operators (AOs) and caters for both the single NAF AO and the multiple NAF AOs scenario.

This TR is based on a "SP Proxy" architecture model as shown in Figure 1, where the service provider (SP) takes the 2-Factor Authentication (2FA) data from the end-user and sends them to the NAF AO for authentication. The NAF AO's authentication service is not accessible on the Internet hence end-users do not interface with the NAF AO directly for authentication. The SP that subscribes to NAF connects to the NAF AO using a private network. A step-by-step illustration showing the information flow in the single NAF AO and the multiple NAF AOs scenario is provided in Annex A.

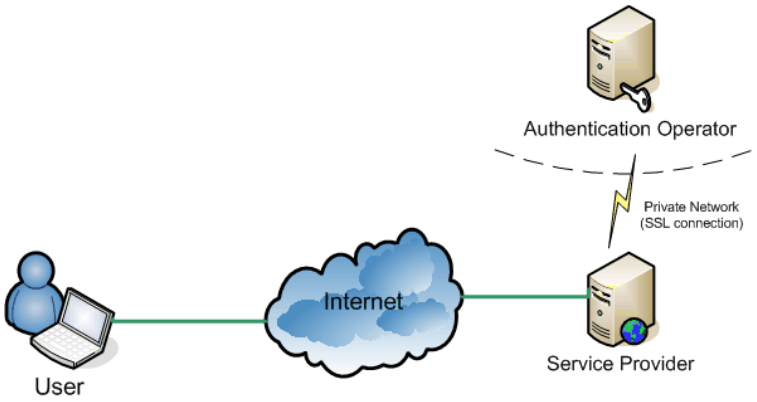

Figure 1 – NAF "SP proxy" architecture

Any AO or SP joining NAF shall ensure that their applications communicate with the other entity using the protocol message format defined in the TR. The communication (or interface) between SP and the NAF AO (as well as between NAF AOs) is based on Web Services such as SOAP version 1.1 and XML 1.0. Throughout the entire specification, SOAP version 1.1 and XML 1.0 are only used in the write-up as a possible option for Web Services

1 Scope

This TR defines the protocol messages that shall be used in the deployment of NAF to communicate information between the SP and the NAF AO (as well as between NAF AOs). All messages are communicated via SOAP protocol and are synchronous (i.e. a request message will be followed by a response message). The Web Service end-points and SOAP message format are defined by the Web Service Definition Language (WSDL).

NAF enables SPs to use additional 2nd authentication factor besides the existing one to authenticate end users. This form of authentication is known as 2FA and generally delivers a higher level of authentication assurance.

The TR also defines the following protocols used in authentication and transaction signing processes:

- Authentication;
- Obtain challenge;
- Out of band (for SMS OTP);
- Transaction signing;
- Authentication for biometric challenge-response.

It further defines the following protocols used in 2FA device management processes:

- Register for an NAF 2FA device via an SP;
- Link an NAF 2FA device to an SP;
- SP to use the end-user's preference of 2FA device stored at the NAF AO;
- SP to check status of end-user's NAF account;
- SP to check status of end-user's NAF 2FA device;
- SP to issue 2FA device;
- NAF AO to issue 2FA device;
- Suspension;
- Reactivation;
- Synchronisation;
- Revocation.

The 2FA and 2FA device management message flow can be found in Annex B.

2 Normative references

The following referenced document is indispensable for the application of this standard. The latest edition of the referenced document (including any amendments) applies.

National Institute of Standards and Technology (NIST)	Recommendation for Key Management – Part 1: General (Revised), May 2006