This is a free page sample. Access the full version online.

Miscellaneous Publication

Strategies for the implementation of a Public Key Authentication Framework (PKAF) in Australia

SAA MP75—1996

This is a free page sample. Access the full version online.

STRATEGIES FOR THE IMPLEMENTATION OF A PUBLIC KEY AUTHENTICATION FRAMEWORK (PKAF) IN AUSTRALIA

SAA MP75—1996

PUBLISHED BY STANDARDS AUSTRALIA

(STANDARDS ASSOCIATION OF AUSTRALIA)
1 THE CRESCENT, HOMEBUSH, NSW 2140

ISBN 0 7337 0802 1

This is a free page sample. Access the full version online.

ABSTRACT

As electronic commerce becomes commonplace, there is a growing need for users to ensure that electronic transactions can be validated. Compatible national and international systems of 'digital signatures' are necessary for the introduction of secure electronic commerce.

Standards Australia formed the Public Key Authentication Framework (PKAF) Task Group to examine all options for operating a national system for the creation and management of digital signatures as well as being compatible with systems in other countries.

This strategy report describes issues and recommendations relevant to Australia's businesses and government operations, and also addresses compatibility issues between organizations and private citizens (both locally and internationally).

Policy and legal issues are also canvassed.

© Copyright – STANDARDS AUSTRALIA

Users of Standards are reminded that copyright subsists in all Standards Australia publications and software. Except where the Copyright Act allows and except where provided for below no publications or software produced by Standards Australia may be reproduced, stored in a retrieval system in any form or transmitted by any means without prior permission in writing from Standards Australia. Permission may be conditional on an appropriate royalty payment. Requests for permission and information on commercial software royalties should be directed to the head office of Standards Australia.

Standards Australia will permit up to 10 percent of the technical content pages of a Standard to be copied for use exclusively in-house by purchasers of the Standard without payment of a royalty or advice to Standards Australia.

Standards Australia will also permit the inclusion of its copyright material in computer software programs for no royalty payment provided such programs are used exclusively in-house by the creators of the programs.

Care should be taken to ensure that material used is from the current edition of the Standard and that it is updated whenever the Standard is amended or revised. The number and date of the Standard should therefore be clearly identified.

The use of material in print form or in computer software programs to be used commercially, with or without payment, or in commercial contracts is subject to the payment of a royalty. This policy may be varied by Standards Australia at any time.

This is a free page sample. Access the full version online.

TABLE OF CONTENTS

1 INTRODUCTION 12

1.1 Background 12

1.2 Purpose of a Public Key Authentication Framework 12

1.3 Scope of the Public Key Authentication Framework (PKAF) 13

1.4 Standards 13

2 TERMINOLOGY 15

2.1 Certificate 15

2.2 Certification Authority (CA) 15

2.3 Certification Block 15

2.4 Digital Signature 16

2.5 Digitized Signature 16

2.6 Distinguished Name 16

2.7 Intermediate Certification Authority (ICA) 16

2.8 Organizational Registration Authority (ORA) 16

2.9 Policy and Root Registration Authority (PARRA) 16

2.10 Public Key Authentication Framework (PKAF) 17

2.11 PKAF Infrastructure 17

2.12 Revocation of Certificate 17

2.13 Trusted 17

2.14 Trustedness 17

2.15 Valid Certificate 18

3 PKAF REQUIREMENTS 19

3.1 Summary of Key PKAF Requirements 19

3.1.1 User Authentication 19

3.1.2 Certification Policies 19

This is a free page sample. Access the full version online.

3.1.3 Certification Practice Statements 19

3.1.4 Trusted Certification Authority 19

3.1.5 Multiple Certificates 20

3.1.6 Certificate Revocation Lists 20

3.1.7 Services of CA 21

3.2 General Infrastructure Requirements 21

3.2.1 Trust 21

3.2.2 Interoperability 22

3.2.3 Naming Convention 22

3.2.4 Scalability 22

3.2.5 Flexibility 23

3.2.6 Archiving 23

3.3 Key Generation and Management 23

3.3.1 Certified Key Generation 24

3.3.2 Secure Key Generation and Key Management 25

3.3.3 Key Backup 25

3.3.4 Initiating Revocation 25

3.3.5 Notice of Revocation 25

3.3.6 Presumptions in Adjudications 25

3.4 Certification Authority (CA) Requirements (applicable to PARRA, ICA, ORA) 26

3.4.1 Level of Trust 26

3.4.2 Availability 26

3.4.3 Services and Functions 26

3.4.3.1 User Authentication 27

3.4.3.2 Certificate Generation 27

3.4.3.3 Certificate Distribution 27

3.4.3.4 Certificate Storage and Retrieval 28

SAI GLOBAL

This is a free preview. Purchase the entire publication at the link below:

Product Page

Looking for additional Standards? Visit Intertek Inform Infostore

Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation