ISO/IEC 9594-4:2005-12 (E)

Information technology - Open Systems Interconnection - The Directory: Procedures for distributed operation

Contents

Page

Reference number INTERNATIONAL STANDARD 9594-4 Fifth edition 2005-12-15 Information technology -- Open Systems Interconnection -- The Directory: Procedures for distributed operation Technologies de l'information -- Interconnexion de systèmes ouverts (OSI) -- L'annuaire: Procédures pour le fonctionnement réparti PDF disclaimer This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area. Adobe is a trademark of Adobe Systems Incorporated. Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below. electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester. ISO copyright office Case postale 56 · CH-1211 Geneva 20 Tel. + 41 22 749 01 11 Fax + 41 22 749 09 47 E-mail copyright@iso.org Web www.iso.org Published by ISO in 2006 Published in Switzerland CONTENTS 1 Scope 1

2 Normative references 1
2.1 Identical Recommendations ..... International Standards| 1
2.2 Other references 2

3 Definitions 2
3.1 Communication Model Definitions 2
3.2 Basic Directory Definitions 2
3.3 Directory Model Definitions 2
3.4 DSA Information Model definitions 2
3.5 Abstract Service definitions 3
3.6 Directory replication definitions 3
3.7 Distributed operation definitions 3

4 Abbreviations 5

5 Conventions 5

6 Overview 6

7 Distributed Directory System Model 7

8 DSA Interactions Model 7
8.1 Decomposition of a request 8
8.1.1 NSSR decomposition 8
8.1.2 Request decomposition 8
8.2 Uni-chaining 8
8.3 Multi-chaining 9
8.3.1 Parallel multi-chaining 9
8.3.2 Sequential multi-chaining 9
8.4 Referral 10
8.5 Mode determination 10

9 Overview of DSA Abstract Service 11

10 Information types 11
10.1 Introduction 11
10.2 Information types defined elsewhere 11
10.3 Chaining Arguments 12
10.4 Chaining Results 15
10.5 Operation Progress 15
10.6 Trace Information 16
10.7 Reference Type 16
10.8 Access point information 16
10.9 DIT Bridge knowledge 17
10.10 Exclusions 17
10.11 Continuation Reference 18

11 Bind and Unbind 19
11.1 DSA Bind 19
11.2 DSA Unbind 20

12 Chained operations 20
12.1 Chained operations 20
12.2 Chained Abandon operation 21
12.3 Chained operations and protocol version 21

13 Chained errors 21
13.1 Introduction 21
13.2 DSA Referral 21

14 Introduction 23
14.1 Scope and Limits 23
14.2 Conformance 23
14.2.1 Interaction involving a first edition DSA 23
14.3 Conceptual model 23
14.4 Individual and cooperative operation of DSAs 23
14.5 Cooperative agreements between DSAs 24

15 Distributed Directory behaviour 24
15.1 Cooperative fulfilment of operations 24
15.2 Phases of operation processing 24
15.2.1 Name Resolution phase 24
15.2.2 Evaluation phase 25
15.2.3 Results Merging phase 25
15.3 Managing Distributed Operations 25
15.3.1 Request decomposition 25
15.3.2 DSA as Request Responder 25
15.3.3 Completion of Operations 26
15.4 Loop handling 26
15.4.1 Loop detection 26
15.4.2 Loop avoidance 26
15.5 Other considerations for distributed operation 26
15.5.1 Service controls 26
15.5.2 Extensions 27
15.5.3 Alias dereferencing 27
15.5.4 Resolving context-variant names 27
15.5.5 Paged results 27
15.6 Authentication of Distributed Operations 28

16 The Operation Dispatcher 28
16.1 General Concepts 28
16.1.1 Procedures 28
16.1.2 Use of common data structures 28

16.1.3 Errors 30
16.1.4 Asynchronous events 30
16.2 Procedures of the Operation Dispatcher 32
16.3 Overview of procedures 33
16.3.1 Request Validation procedure 33
16.3.2 Abandon procedure 33
16.3.3 Find DSE procedure 33
16.3.4 Single entry interrogation procedure 34
16.3.5 Modification procedures 34
16.3.6 Multiple entry interrogation procedures 34
16.3.7 Name Resolution Continuation Reference procedure 34
16.3.8 List and Search Continuation Reference procedure 34
16.3.9 Result Merging procedure 34

17 Request Validation procedure 34
17.1 Introduction 34
17.2 Procedure parameters 35
17.2.1 Arguments 35
17.2.2 Results 35
17.3 Procedure definition 36
17.3.1 Abandon processing 36
17.3.2 Security checks 36
17.3.3 Input preparation 36
17.3.4 Validity assertion 37
17.3.5 Loop detection 37
17.3.6 Unable or unwilling to perform 37
17.3.7 Output processing 38

18 Name Resolution procedure 38
18.1 Introduction 38
18.2 Find DSE procedure parameters 38
18.2.1 Arguments 38
18.2.2 Results 38
18.2.3 Errors 39
18.2.4 Global variables 39
18.2.5 Local and shared variables 39
18.3 Procedures 39
18.3.1 Find DSE procedure 40
18.3.2 Target Not Found sub-procedure 43
18.3.3 Target Found sub-procedure 45
18.3.4 Check Suitability procedure 46

19 Operation evaluation 49
19.1 Modification procedure 49
19.1.1 Add Entry Operation 49
19.1.2 Remove Entry Operation 50
19.1.3 Modify Entry Operation 51
19.1.4 Modify DN operation 52
19.1.5 Modify operations and Non-Specific Subordinate References 54
19.2 Single entry interrogation procedure 55
19.3 Multiple entry interrogation procedure 55
19.3.1 List procedures 55
19.3.2 Search procedures 58

20 Continuation Reference procedures 68
20.1 Chaining strategy in the presence of shadowing 68
20.1.1 Master only strategy 70
20.1.2 Parallel strategy 70
20.1.3 Sequential strategy 70
20.2 Issuing chained subrequests to a remote DSA 70
20.3 Procedures' parameters 70
20.3.1 Arguments 70

20.3.2 Results ... 71
20.3.3 Errors ... 71
20.4 Definition of the procedures ... 71
20.4.1 Name Resolution Continuation Reference procedure ... 71
20.4.2 List Continuation Reference procedure ... 73
20.4.3 Search Continuation Reference procedure ... 75
20.4.4 APInfo procedure ... 76
20.5 Abandon procedure ... 79

21 Results Merging procedure ... 80

22 Procedures for distributed authentication ... 81
22.1 Originator authentication ... 82
22.1.1 Identity-based authentication ... 82
22.1.2 Signature-based originator authentication ... 82
22.2 Results authentication ... 82

23 Knowledge administration overview ... 83
23.1 Maintenance of knowledge references ... 83
23.1.1 Maintenance of consumer knowledge by supplier and master DSAs ... 83
23.1.2 Maintenance of subordinate and immediate superior knowledge in master DSAs ... 84
23.1.3 Maintenance of subordinate and immediate superior knowledge in consumer DSAs ... 84
23.2 Requesting cross reference ... 84
23.3 Knowledge inconsistencies ... 85
23.3.1 Detection of knowledge inconsistencies ... 85
23.3.2 Reporting of knowledge inconsistencies ... 85
23.3.3 Treatment of inconsistent knowledge references ... 85
23.4 Knowledge references and contexts ... 85

24 Hierarchical operational bindings ... 86
24.1 Operational binding type characteristics ... 86
24.1.1 Symmetry and roles ... 86
24.1.2 Agreement ... 86
24.1.3 Initiator ... 86
24.1.4 Establishment parameters ... 87
24.1.5 Modification parameters ... 88
24.1.6 Termination parameters ... 88
24.1.7 Type identification ... 88
24.2 Operational binding information object Class definition ... 88
24.3 DSA procedures for hierarchical operational binding management ... 89
24.3.1 Establishment procedure ... 89
24.3.2 Modification procedure ... 90
24.3.3 Termination procedure ... 91
24.4 Procedures for operations ... 92
24.5 Use of application contexts ... 92

25 Non-specific hierarchical operational binding ... 92
25.1 Operational binding type characteristics ... 93
25.1.1 Symmetry and roles ... 93
25.1.2 Agreement ... 93
25.1.3 Initiator ... 93
25.1.4 Establishment parameters ... 93
25.1.5 Modification parameters ... 94
25.1.6 Termination parameters ... 94
25.1.7 Type identification ... 94
25.2 Operational binding information object class definition ... 94
25.3 DSA procedures for non-specific hierarchical operational binding management ... 94
25.3.1 Establishment procedure ... 94
25.3.2 Modification procedure ... 95
25.3.3 Termination procedure ... 95
25.4 Procedures for operations ... 96
25.5 Use of application contexts ... 96

Annex A - ASN.1 for Distributed Operations 97

Annex B - Example of distributed name resolution 101

Annex C - Distributed use of authentication 103

C.1 Summary 103
C.2 Distributed protection model 103
C.2.1 Quality of protection 103
C.3 Signed chained operations 103
C.3.1 Chained signed arguments 104
C.3.2 Chained signed results 104
C.3.3 Merging of Signed List or Search Results 104
C.3.4 Multi-chaining Request 105
C.4 Encrypted chained operations 105
C.4.1 Point-to-point (DUA->DSA or DSA->DSA) encryption on request 105
C.4.2 Point-to-point (DUA<-DSA or DSA<-DSA) encryption on result 105
C.4.3 End-to-end encryption on DAP Result and point-to-point encryption on DSP Chaining Result 106
C.4.4 Merging of List/Search Results (merging with re-encryption by DSA 1) 106
C.4.5 Merging-not-allowed for List/Search Results 107
C.4.6 Multi-chaining a DAP Request using an Encryption-Key (net-key) 107
C.5 Signed and encrypted distributed operations 108
C.5.1 End-to-end signatures, with point-to-point encryption 108
C.5.2 End-to-End Signature and Encryption on DAP Result, Point-to-Point Signature and Encryption on DSP 108
C.5.3 End-to-End Signature on DAP, Point-to-Point Encryption on DSP and DAP Result 109

Annex D - Specification of hierarchical and non-specific hierarchical perational binding types 110

Annex E - Knowledge maintenance example 112

Annex F - Amendments and corrigenda 115