

Contents

1. Introduction	1
1.1 Nature and Intent of the Reference Model	1
1.2 Scope of the Reference Model	2
1.2.1 Users and Systems	2
1.2.2 Commands and Responses	2
1.2.3 Customisation and Help	3
1.2.4 Invocation of System Services	3
1.2.5 Sharing of System Services	3
1.2.6 Concurrent Usage	4
1.3 The Object Concept	4
1.4 Notation	6
2. Overview of the Reference Model	8
2.1 Systems, Access Points and Networks	8
2.2 CRL Processors, Transmitters and Contexts	8
2.3 UserManager and KnownUsers	10
2.4 Customisers, Commands and Responses	11
2.5 Helpers and Histories	11
2.6 Concurrency	12
2.7 Name Managers and Directories	12
2.8 Protectors and the Bonded Store	13
2.9 Constraints on the Initial State	13
3. Application of the Reference Model	14
3.1 Method	14
3.2 Example: Login Command	15
3.3 Example: Copy Command	17
4. Users	20
4.1 Functional Requirements	20
4.2 Overview	21
4.3 Object Type: Transmitter	23
4.4 Object Type: Message	23

4.5 Object Type: CRLProcessor	23
4.6 Object Type: Command	24
4.7 Object Type: Response	25
4.8 Object Type: User Manager	25
4.9 Object Type: Known User	26
4.10 Object Type: User Profile	27
4.11 Object Type: User Identification	27
4.12 Object Type: User Pass	27
4.13 Object Type: User Verification Criteria	27
5. Contexts	28
5.1 Functional Requirements	28
5.2 Overview	29
5.3 Object Type: Elementary Context	33
5.4 Object Type: Context	33
5.5 Object Type: ContextTree	34
5.6 Examples and Extensions	35
5.6.1 The Current Context	35
5.6.2 Particular Contexts	35
5.6.3 Searching	35
5.7 Formal Interface Definitions	36
5.7.1 Context Operation: GetNameManager	37
5.7.2 ContextTree Operation: GetContextTree	37
5.7.3 ContextTree Operation: GetContext	38
5.7.4 ContextTree Operation: InsertContextTree	39
5.7.5 ContextTree Operation: RemoveContextTree	40
5.7.6 ContextTree Operation: ExpandContextName	41
6. Customisation	42
6.1 Functional Requirements	42
6.2 Overview	43
6.3 Object Type: Customiser	44
7. Help	46
7.1 Functional Requirements	46
7.2 Overview	48
7.3 Object Type: Helper	48
8. History	51
8.1 Functional Requirements	51
8.2 Overview	52
8.3 Object Type: History	53
8.4 Object Type: SingleEvent	54
8.5 Object Type: TimeStamp	54

9. Concurrency	55
9.1 Functional Requirements	55
9.2 Overview	56
9.3 Object Types for Synchronisation and Scheduling	57
9.4 Object Types for Resource Sharing	57
9.5 Object Types for Processes	58
9.6 Object Types for Transaction Processing	58
10. CRL Object Management	59
10.1 Functional Requirements	59
10.2 Overview	59
10.2.1 CRL and Model Types	59
10.2.2 Registered Holder	61
10.2.3 Checking of Commands	61
10.3 Object Type: CRL Type	63
10.3.1 Functional Requirements	63
10.3.2 Overview	64
10.4 CRL Objects	67
10.5 CRL Operations	67
10.6 Object Type: ObjectReference	68
10.7 Formal Interface Definitions	68
10.7.1 Wellformedness Condition for CRL Type	69
10.7.2 CRLType Operation: IncludeNewOperation	69
10.7.3 CRLType Operation: IncludeNewAccessRight	69
10.7.4 CRLType Operation: RemoveOperation	70
10.7.5 CRLType Operation: RemoveAccessRight	70
10.7.6 Wellformedness Condition for ObjectReference	70
10.7.7 ObjectReference Operation: GetType	71
11. Naming	72
11.1 Functional Requirements	72
11.2 Overview	72
11.3 Object Type: Name	74
11.4 Object Type: SimpleName	74
11.5 Object Type: NameManager	74
11.6 Object Type: Directory	75
11.7 Example	76
11.8 Formal Interface Definitions	77
11.8.1 NameManager Operation: ResolveName	78
11.8.2 NameManager Operation: ListReferences	79
11.8.3 Directory Operation: FindObjectRef	79
11.8.4 Directory Operation: InsertEntry	80

11.8.5 Directory Operation: RemoveEntry	81
11.8.6 Directory Operation: GetSimpleNames	81
11.8.7 Directory Operation: GetNames	82
12. Protection	83
12.1 Functional Requirements	83
12.2 Overview	84
12.3 Object Type: Protector	84
12.4 Object Type : ProtectionDomain	86
12.5 Object Type : Protection	87
12.6 Object Type: Permission	88
12.7 Object Type: Access Right	89
12.8 Object Type: Control Expression	90
12.9 Formal Interface Definitions	90
12.9.1 Wellformedness Condition for Protector	90
12.9.2 Protector Operation: Access	91
12.9.3 Protector Operation: AddProtectionDomain	91
12.9.4 Protector Operation: RemoveProtectionDomain	91
12.9.5 Wellformedness Condition for ProtectionDomains	92
12.9.6 ProtectionDomain Operation: AddProtectedObject	92
12.9.7 ProtectionDomain Operation: RemoveProtectedObject	92
12.9.8 ProtectionDomain Operation: Allow	92
12.9.9 ProtectionDomain Operation: Disallow	93
12.9.10 ProtectionDomain Operation: RetrieveProtection	93
12.9.11 Wellformedness Condition for Protection	93
12.9.12 Protection Operation: IsAllowedUse	94
12.9.13 Wellformedness Condition for Permission	94
12.9.14 Permission Operation: EvaluatePermission	94
13. Shared Storage	95
13.1 Functional Requirements	95
13.2 Overview	95
13.3 Object Type : Bonded Store	96
13.4 Formal Interface Definitions	97
13.4.1 BondedStore Operation: RetrieveObject	97
13.4.2 BondedStore Operation : StoreObject	98
References	99
Appendix A. Notation	100
Appendix B. The VDM Metalanguage	104
Index of Terms	116