

Digital Signature Manager

Contents

About Digital Signatures	6-3
Cryptography and Digital Signatures	6-4
Components of a Full Signature	6-5
The Digital Signature	6-5
The Certificate Set	6-6
Creating and Verifying Signatures	6-8
About Public-Key Certificates	6-8
Using the Digital Signature Manager	6-11
Determining the Version Number of the Digital Signature Manager	6-11
Using a Context	6-12
Creating a Full Signature	6-14
Verifying a Full Signature	6-16
Creating a Simple (Unencrypted) Digest	6-19
Getting Information From a Signature or Certificate	6-19
Dealing With Standard Signatures in Files	6-22
Digital Signature Manager Reference	6-23
Constants and Data Types	6-23
Signer Information Structure	6-23
Certificate Information Structure	6-25
Standard Signature Icon Suite	6-26
Name Attribute Information Structure	6-26
Digital Signature Manager Functions	6-27
Assembly-Language Interface	6-27
Creating and Disposing of a Context	6-28
Processing Data to Generate a Digest	6-30
Creating a Signature	6-31
Verifying a Signature	6-38
Creating a Digest	6-43
Getting Information From a Signature or Certificate	6-45
Application-Defined Function	6-54

Summary of the Digital Signature Manager	6-56
C Summary	6-56
Constants and Data Types	6-56
Digital Signature Manager Functions	6-58
Pascal Summary	6-60
Constants and Data Types	6-60
Digital Signature Manager Functions	6-62
Assembly-Language Summary	6-63
Result Codes	6-64