

Contents

1.	Introduction	1-1
1.1	Definitions	1-2
1.2	Background	1-2
1.3	Related Documents	1-7
1.4	Notation	1-7
1.5	Scope	1-7
2.	Guidelines for the Basic Data Encryption Capability	2-1
2.1	Data Transmission Protocol	2-1
2.1.1	About the Layer 1 Protocol	2-1
2.1.2	About the Layer 2 Protocol	2-1
2.1.3	About the Layer 3 Protocol and ADSI Parameters	2-3
2.2	Minimizing the Setup Delay Over Multiple Sessions	2-5
2.2.1	DES Challenge and Response Protocol	2-8
2.3	ADSI Authentication and DES Session Key Exchange	2-10
2.3.1	Basic Beller-Yacobi Authentication and Key Agreement Procedure and Data Exchanges	2-14
2.4	Change Key Capability	2-18
3.	Guidelines for the Advanced Data Encryption Capability	3-1
3.1	Data Transmission Protocol	3-1
3.1.1	About the Layer 1 Protocol	3-1
3.1.2	About the Layer 2 Protocol	3-2
3.1.3	About the Layer 3 Protocol and ADSI Parameters	3-4
3.1.3.1	Data from the Server to the CPE/Peripheral	3-4
3.1.3.2	Data from the CPE/Peripheral to the Server	3-6
3.2	Minimizing the Setup Delay Over Multiple Sessions	3-9
3.2.1	DES Challenge and Response Protocol	3-12
3.3	ASDI Authentication and DES Session Key Exchange	3-15
3.3.1	Full Beller-Yacobi Authentication and Key Agreement Procedure and Data Exchanges	3-20
3.4	Change Key Capability	3-24
4.	Automatic Procedure To Engage Available Basic or Advanced Encryption	4-1
4.1	If the Server Supports Only the Basic Encryption Capability	4-1
4.2	If the Server Supports the Advanced Encryption Capability	4-2
5.	Miscellaneous Capabilities of the Advanced Encryption Peripheral	5-1
5.1	Query for Optional Capabilities of the Peripheral	5-1
5.2	Invoking an Optional Advanced Peripheral Capability	5-3
5.3	Transmission of Data Messages	5-5
6.	Recommendations	6-1
7.	Summary of Timers	7-1
	References	References-1

Glossary Glossary-1

List of Figures

Figure 1-1.	Functional View of an ADSI CPE Port to an Encryption Peripheral	1-6
-------------	--	-----