TM Vendor Name

TM Module Name

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 – General

1.1 Overview

<Text>

1.2 Security Levels

Section	Security Level
1	2
2	2
3	2
4	2
5	0
6	2
7	0
8	2
9	2
10	2
11	2
12	2

Table 1: Security Levels

1.3 Additional Information [O]

<Text>

2 – Cryptographic Module Specification

2.1 Description

Purpose and Use:

<Text>

Module Type: Hardware

Module Embodiment: SingleChip

Module Characteristics: SubChip

Cryptographic Boundary:

<Text>

Tested Operational Environment's Physical Perimeter (TOEPP) [O]:

<Text>

<Other Diagrams, Photographs and Descriptive Text>

<Picture or Block Diagram>
Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
T1 Model	T1 Hardware ver	T1 Firmware V	T1 Processor	T1 NSR Features

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.3 Excluded Components

<Excluded components statements or table>

2.4 Modes of Operation

Modes List and Description:

Table Name	Description	Type	Status Indicator
T5 Name	T5 Descrip	Approved	T5 Status

Table 3: Modes List and Description

<Text>

Mode Change Instructions and Status [O]:

<Text>

Degraded Mode Description [O]:

<Text>

2.5 Algorithms

Approved Algorithms:

ApprovedAlgorithmTable From Web Cryptik ApprovedAlgorithmTable

<Text>

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
T6 Algo Name	T6 Algo Prop Name: T6 Algo Prop Value	UltraLock Cryptographic Module	T6 Ref

Table 4: Vendor-Affirmed Algorithms

<Text>

Non-Approved, Allowed Algorithms:

Name	Properties	Implementation	Reference
T7 Algo Name	T7 Algo Prop Name: T7 Algo Prop Value	UltraLock Cryptographic Module	T7 Ref

Table 5: Non-Approved, Allowed Algorithms

<Text>

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
T8 Algo Name	T8 Caveat	T8 Use

Table 6: Non-Approved, Allowed Algorithms with No Security Claimed

<Text>

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
T9 Algo	T9 Use

Table 7: Non-Approved, Not Allowed Algorithms

<Text>

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
T10 Name	AsymKeyPair-KeyGen	T10 Descrip	T10 SF Cap: T10 SF Value	DES CBC AES-CBC

Table 8: Security Function Implementations

<Text>

2.7 Algorithm Specific Information

<Text>

2.8 RBG and Entropy

Cert Number	Vendor Name
E2	microsoft

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
T12 Name	Non-Physical	T12 OE	T12 Sample Size	T12 Ent Per Sample	T12 Cond Comp

Table 10: Entropy Sources

<Text>

2.9 Key Generation

N/A for this module.

<Text>

2.10 Key Establishment

N/A for this module.

<Text>

N/A for this module.

<Text>

2.11 Industry Protocols

<Text>

2.12 Additional Information [O]

<Text>

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
T13 Phy Port	Data Input Data Output Control Input Control Output Status Output	T13 Data Passes

Table 11: Ports and Interfaces

<Text>

3.2 Trusted Channel Specification [O]

<Text>

3.3 Control Interface Not Inhibited [O]

<Text>

3.4 Additional Information [O]

<Text>

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
T14 Name	T14 Descrip	T14 Mech Other	T14 Strength Each	T14 Strength Min

Table 12: Authentication Methods

<Text>

4.2 Roles

Name	Type	Operator Type	Authentication Methods
T15 Name	Identity	T15 Op Type	T14 Name

Table 13: Roles

<Text>

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
T16 Name	T16 Descrip	T16 Indicator	T16 Inputs	T16 Outputs	T10 Name	T15 Name - T24 Name: G,W,Z

Table 14: Approved Services

<Text>

4.4 Non-Approved Services

Name	Description	Algorithms	Role
T17 Name	T17 Descrip	T9 Algo	T17 Role

Table 15: Non-Approved Services

<Text>

4.5 External Software/Firmware Loaded

<Text>

4.6 Bypass Actions and Status [O]

<Text>

4.7 Cryptographic Output Actions and Status [O]

<Text>

4.8 Additional Information [O]

<Text>

5 Software/Firmware Security

5.1 Integrity Techniques

<Text>

5.2 Initiate on Demand

<Text>

5.3 Open-Source Parameters [O]

<Text>

5.4 Additional Information [O]

<Text>

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

How Requirements are Satisfied [O]:

<Text>

6.2 Configuration Settings and Restrictions [O]

<Text>

6.3 Additional Information [O]

<Text>

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
T18 Mech	T18 Frequency	T18 Guidance

Table 16: Mechanisms and Actions Required

<Text and Photos>

7.2 User Placed Tamper Seals [O]

Number:

Placement:

Surface Preparation:

Operator Responsible for Securing Unused Seals:

Part Numbers:

<Text and Pictures>

7.3 Filler Panels [O]

<Text and Pictures>

7.4 Fault Induction Mitigation [O]

<Text>

7.5 EFP/EFT Information [O]

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature			
HighTemperature			
LowVoltage			
HighVoltage			

Table 17: EFP/EFT Information

<Text>

7.6 Hardness Testing Temperature Ranges [O]

Temperature Type	Temperature
LowTemperature	
HighTemperature	

Table 18: Hardness Testing Temperatures

<Text>

7.7 Additional Information [O]

<Text>

8 Non-Invasive Security

8.1 Mitigation Techniques [O]

<Text>

8.2 Effectiveness [O]

<Text>

8.3 Additional Information [O]

<Text>

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
T21 Name	T21 Descrip	Dynamic

Table 19: Storage Areas

<Text>

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
T22 Name	T21 Name	External	Encrypted	Automated	Direct	AES-CBC

Table 20: SSP Input-Output Methods

<Text>

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
T23 Name	T23 Descrip	T23 Rationale	T23 Op Initiation

Table 21: SSP Zeroization Methods

<Text>

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
T24 Name	T24 Descrip	T24 Size - T24 Strength	T24 Types - PSP	DES CBC	T10 Name	TDES-CBC

Table 22: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
T24 Name	T22 Name	T21 Name: Encrypted	T24 Duration	T23 Name	

Table 23: SSP Table 2

<Text>

9.5 Transitions [O]

<Text>

9.6 Additional Information [O]

<Text>

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
DES CBC	T25 Prop	T25 Methd	Bypass	T25 Indicator	T25 Details

Table 24: Pre-Operational Self-Tests

<Text>

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
DSA KeyGen (FIPS186-2)	T26 Prop	T26 Method	CAST	T26 Indicator	T26 Details	T26 Condition

Table 25: Conditional Self-Tests

<Text>

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
DES CBC	T25 Methd	Bypass	T25 Period	T25 Period Method

Table 26: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
DSA KeyGen (FIPS186-2)	T26 Method	CAST	T26 Period	T26 Period Method

Table 27: Conditional Periodic Information

<Text>

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
T28 State Name	T28 Descrip	T27 Condition 1	T27 Recovery	T27 Indicator

Table 28: Error States

<Text>

10.5 Operator Initiation of Self-Tests [O]

<Text>

10.6 Additional Information [O]

<Text>

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

<Text>

11.2 Administrator Guidance

<Text>

11.3 Non-Administrator Guidance

<Text>

11.4 Design and Rules [O]

<Text>

11.5 Maintenance Requirements [O]

<Text>

11.6 End of Life [O]

<Text>

11.7 Additional Information [O]

<Text>

12 Mitigation of Other Attacks

12.1 Attack List [O]

<Text>

12.2 Mitigation Effectiveness [O]

<Text>

12.3 Guidance and Constraints [O]

<Text>

12.4 Additional Information [O]

<Text>