

Trusted Platform Module (TPM) SECURITY POLICY VERSION 0.45

**Copyright © 2000 Compaq Computer Corporation, Hewlett-Packard Company, IBM Corporation,
Intel Corporation, Microsoft Corporation**

All rights reserved.

DISCLAIMERS:

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE.

NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED OR INTENDED HEREBY.

COMPAQ, HP, IBM, INTEL, AND MICROSOFT, DISCLAIM ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF PROPRIETARY RIGHTS, RELATING TO THE USE OF THE INFORMATION IN THIS SPECIFICATION AND TO THE IMPLEMENTATION OF INFORMATION IN THIS SPECIFICATION. COMPAQ, HP, IBM, INTEL, AND MICROSOFT, DO NOT WARRANT OR REPRESENT THAT SUCH IMPLEMENTATION(S) WILL NOT INFRINGE SUCH RIGHTS.

WITHOUT LIMITATION, COMPAQ, HP, IBM, INTEL, AND MICROSOFT DISCLAIM ALL LIABILITY FOR COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOST PROFITS, LOSS OF USE, LOSS OF DATA OR ANY INCIDENTAL, CONSEQUENTIAL, DIRECT, INDIRECT, OR SPECIAL DAMAGES, WHETHER UNDER CONTRACT, TORT, WARRANTY OR OTHERWISE, ARISING IN ANY WAY OUT OF USE OR RELIANCE UPON THIS SPECIFICATION OR ANY INFORMATION HEREIN.

All product names are trademarks, registered trademarks, or service marks of their respective owners.

TABLE OF CONTENTS

SECTION	PAGE
1 INTRODUCTION	1
1.1 PURPOSE AND SCOPE	1
1.2 DOCUMENT OUTLINE.....	1
1.3 REFERENCES	1
2 OVERVIEW OF THE TPM	2
3 IDENTIFICATION AND AUTHENTICATION POLICY	3
3.1 ADMINISTRATOR IDENTIFICATION AND AUTHENTICATION POLICY	3
3.2 ENTITY OWNER IDENTIFICATION AND AUTHENTICATION POLICY	4
3.3 ENTITY USER IDENTIFICATION AND AUTHENTICATION POLICY	4
4 ACCESS CONTROL POLICY	5
4.1 ROLES AND SERVICES	5
4.2 CRITICAL SECURITY PARAMETERS	5
4.3 MODES OF ACCESS	7
5 PHYSICAL SECURITY POLICY.....	8
5.1 ORGANIZATIONAL SECURITY POLICIES.....	8
5.2 STATIC SECURITY FEATURES.....	8
6 OPERATIONAL SECURITY POLICY.....	9
6.1 SYSTEM INITIALIZATION.....	9
6.2 CRYPTOGRAPHIC OPERATION	9
7 ELECTROMAGNETIC EMANATIONS POLICY	11

1 INTRODUCTION

1.1 Purpose and Scope

This document is the statement of Security Policy for the Trusted Platform Module (TPM). The Security Policy is a requirement of the ISO 15408 Common Criteria evaluation. In this context, the Target of Evaluation (TOE) covered by this policy is the TPM device itself. The definition of the TPM comes from the TCPA specification version 1.0. This policy document is a precise specification of the security rules under which the TOE operates. The achievement of these policies is through a combination of assumed organizational security policies, assumptions related to physical and procedural measures, and IT functional requirements.

1.2 Document Outline

This Security Policy is system-specific; therefore, it first sets the context in Section 2 by providing an overview of the TPM functionality. The remaining sections include: identification and authentication policy in Section 3, access control policy in Section 4, physical security policy in Section 5, operational security policy in Section 6, and electromagnetic emanations policy in Section 7.

1.3 References

TCPA Specification Version 1.0
IEEE P1363

2 OVERVIEW OF THE TPM

The TPM is a product that consists of hardware and software components to provide increased trust in a platform. The TPM sub-system provides a reporting root of trust, RNG, integrity metric storage, a protected storage mechanism and the ability to create anonymous identities. The TOE is the TPM and the ISO 15408 evaluation level is EAL3.

The TPM implements functionality in building blocks. Table 1 lists the building blocks that are in the TOE.

Table 1 – TPM Building Blocks

Building Block	TOE	Additive
Protected functions	X	
Shielded locations	X	
TCPA TPM API	X	
Random Number Generator (RNG)	X	
Protected storage	X	
Integrity metric storage	X	
Identity creation	X	
Audit event creation	X	
Audit Log		X

TODO Need discussion of TOE and TPM here.

3 IDENTIFICATION AND AUTHENTICATION POLICY

There are three operational roles defined for the TPM. They are:

- Administrator, also known as TPM owner
- Entity owner
- Entity user

An administrator or user shall access all protected functionality and shielded locations only through the authentication mechanism, i.e., by supplying the appropriate authentication token. There are three types of authentication tokens:

- The TPM ownership token provides proof of TPM ownership. The creation of the token occurs when the owner completes the ownership protocol. The value is stored in a shielded location inside of the TPM. The administrator provides this token to access administrator functionality, including system configuration.
- The entity ownership token provides proof of entity ownership. The creation of the token occurs during the entity creation process. The entity owner must present this token for the TPM to load the entity. The token must be available when the owner attempts to load the entity into the TPM.
- The entity use token provides proof of the right to use the entity. The creation of the token occurs during the entity creation process. After a successful load of the entity into the TPM, the user must supply the token for each operation that uses the loaded entity.

The TPM requires authentication before it performs any protected function. All TPM configuration functions require the proper validation of the ownership token. Loading an entity requires two authorizations; the owner's execution authentication and the entities load authorization.

The TOE detects unsuccessful authentication attempts and invalidates the entity load buffer when the number of attempts exceeds the attempt trigger. The trigger value is a configurable value that the TPM owner may set.

The description of the administrator and user/operator roles and their authentication policies are in the subsections below.

All authentications use the same mechanism, the TCPA authorization protocol. This protocol uses the HMAC construct to prove knowledge of the token without passing the actual token value. Checking the authentication token for validity involves performing the TCPA authorization protocol and comparing the results of the protocol.

3.1 Administrator Identification and Authentication Policy

The protection of the TPM ownership token is internal to the TPM. Access to TPM protected functions and TPM configuration functions require knowledge of the TPM ownership token. Only individuals or applications authorized to perform the Administrator role have knowledge of the TPM authentication token.

Those persons who have the Administrator role shall:

- Agree to protect keys and data access

- Agree to report loss of keys or perceived compromise to security
- Agree not to collude.

The organization shall be responsible for Administrator agreement with these policies.

3.2 Entity Owner Identification and Authentication Policy

Entity owner authentication, i.e., verification of knowledge of the entity owner token, is required as a condition of loading an entity into the TPM. This functionality is inherent within the TPM.

An entity owner wishing to load an entity into a TPM must supply the entity ownership token using the mechanism defined by the TCPA specification. The TPM validates the supplied token using the authentication protocol and if successful allows the loading of the entity. Failure to provide the correct token results in a failure to load the entity. A successful load results in the decryption of the entity from a wrapped state and loading into a proper-shielded location of the TPM.

The load process does not automatically allow the use of the entity; the entity user must provide the entity use token (see next section).

Entity owners shall be responsible to ensure that all ownership tokens have protection. The creation of the ownership token is a responsibility of the entity owner and can use any mechanism. The storage of ownership tokens outside of the TPM requires cryptographic protections.

The entity owners' organization shall be responsible to ensure that:

- Entity owners agree to protect ownership tokens
- Entity owners agree to report loss of ownership tokens or perceived compromise to security
- Entity owners agree not to collude.

3.3 Entity User Identification and Authentication Policy

Entity user authentication, i.e., verification of knowledge of the entity user token, is required as a condition of using a loaded entity. This functionality is inherent within the TPM.

An entity user wishing to use a loaded entity in the TPM must supply the entity use token using the mechanism defined by the TCPA specification. The TPM validates the supplied token using the authentication protocol and if successful allows the use of the entity. Failure to provide the correct token results in a failure to execute the function. A successful authentication results in the execution of the requested function.

Entity users shall be responsible to ensure that all use tokens have protection. The creation of the use token is a responsibility of the entity owner and can use any mechanism. The storage of use tokens outside of the TPM requires cryptographic protections.

The entity use organization shall be responsible to ensure that:

- Entity users agree to protect ownership tokens
- Entity users agree to report loss of ownership tokens or perceived compromise to security
- Entity users agree not to collude.

4 ACCESS CONTROL POLICY

The TPM enforces user access to cryptographic IT assets in accordance with the specified access control policy. These include:

- Roles and services that can be accessed by those roles
- Critical security parameters such as authentication tokens and cryptographic keys
- Modes of access (read, write, execute, and delete) to services and cryptographic security parameters

4.1 Roles and Services

4.1.1 Administrator Roles and Services

To perform any command related to system configuration the administrator must supply the TPM ownership token. The TPM System configuration commands available only to the administrator include:

- Setting the TPM ownership authentication token
- Set configuration status

In the case of a TPM ownership token compromise, the administrator shall be responsible for following manufacturer guidance in resetting the TPM ownership token.

The administrator shall be responsible for changing the TPM ownership token periodically, as defined by the organization, to ensure its security.

4.1.2 Entity Owner Roles and Services

Entity owners load their entities into the TPM using the entity ownership token associated with the entity. Loading of an entity does not include the usage of the loaded entity. If the entity owner believes that the ownership token is compromised the entity owner is responsible for reporting the compromise to the administrator and/or resetting the ownership token on the affected entity.

4.1.3 Entity User Roles and Services

Entity users use loaded entities on the TPM using the entity use token associated with the entity. If the entity owner believes that the use token is compromised the entity user is responsible for reporting the compromise to the administrator and the entity owner.

4.2 Critical Security Parameters

4.2.1 Authentication Tokens

The TPM uses the TCPA authentication protocol to validate authorization to perform operations. The authorization token is a 20-byte blob of data. The TPM only has permanent storage for the TPM ownership token.

For entity authentication tokens, token storage is part of the entity. The TPM after loading an entity maintains the use token in a shielded location. When the TPM unloads the entity, it ensures the proper destruction of the user token area.

The TPM must ensure that no functions can access the TPM ownership token in a manner inconsistent with use of the TPM ownership token to prove TPM ownership.

4.2.2 Endorsement Key

The TPM endorsement key provides evidence to trusted third parties that the TPM is a unique device and that the TPM was properly constructed. See the TCPA specification for additional information.

The TPM endorsement key is a 2048 RSA key pair generated by the TPM in response to the TPM ownership protocol. The private key remains on the TPM in a shielded location and never leaves the TPM. The TOE manufacturer endorses the public key. The endorsement key shall only be in use for two operations TPM ownership and identity creation.

4.2.3 Storage Root Key

The storage root key (SRK) provides the mechanism to migrate information from one TPM to another. The SRK, as any other entity, can have authorization tokens, however the default is for the SRK to have a “null” authorization token. Having a null value is only a convenience for users of the TPM. At any time, the TPM owner can reset the authorization value for the SRK to a true authentication token.

The SRK is a 2048 RSA key pair generated by the TPM in response to the TPM ownership protocol. The private key remains on the TPM in a shielded location and never leaves the TPM.

4.2.4 Entities

The TOE design allows for the creation, storage, use and destruction of entity keys. Entities can be identities, storage keys and signature keys. The creation of entities uses the internal processing of the TPM and the TPM RNG. The TPM must create and operate with RSA key sizes of 512, 768, 1024 and 2048. All operations with entities use the protected capabilities of the TPM. The loading of entities

4.2.5 Key Destruction

The TPM is required to provide a means to securely overwrite keys, thereby destroying them, in accordance with FIPS 140-1 standards.

The TPM destroys all values in shielded locations by setting the shielded location to all zeros. For all non-volatile entities, (identities, storage keys etc.) the destruction occurs either when the TPM evicts the entity or the TPM goes through an initialization cycle.

The TPM destroys the TPM ownership token when the TPM owner establishes a new ownership token.

4.2.6 Cryptographic Operations

The design of the TOE allows for the usage of various keys. Only TPM protected functions can operate with the private portion of an RSA key pair. All TPM protected functions must be internal to the TOE and protection provided to avoid modification or exposure.

The TPM shall provide an API set that matches the TCPA specification. Additional entry points into the TPM which are not TCPA specific are possible as long as these functions do not access or manipulate TCPA protected functions or shielded locations.

All operations in the TPM that use the private key of a RSA key pair must be done by TPM protected function.

4.3 Modes of Access

The TOE shall implement the following modes of access:

Information/Function	Mode of Access	Role
GetCapability	Read only	All users
GetCapabilitySigned	Read only	All users - requires entity authorization
TPM firmware	Read only	All users
TPM firmware	Read/Write	Administrator
Entity load	Read only	All users
Entity use	Read only	All users
Take Ownership	Read/Write	Administrator
Set Configuration Information		Administrator

5 PHYSICAL SECURITY POLICY

The TPM is an enhanced subsystem version of a standard PC client. The use of the TOE does not guarantee the security of the overall system. The responsible authority in each agency or department shall assure that the agency or department's computer or telecommunication systems provide an acceptable level of security for the given application and environment.

5.1 Organizational Security Policies

The organization shall enforce standard security measures for PC Clients. The TOE relies on the organization to provide a physically secure environment. Many implementations of the TOE will not be in areas that provide no physical security and are hostile (i.e. mobile platforms in a hotel room). The organization must provide physical security to the TOE and methods for detecting attacks on the TOE.

Physical measures that an organization could employ to protect the TOE include:

- Chassis cover sensor
- Alert on LAN
- Chassis bolt down hole
- Tamper evident tape on chassis or TPM

5.2 Static Security Features

The TPM must ensure that all shielded locations are only accessible and useable by TPM protected functions. The TPM shall ensure that unintended exposure of shielded locations does not occur. Unintended exposure for example would not include the use of the GetRandom instruction to obtain a random number and then passing the resulting random number outside the TPM.

The TPM always sets volatile registers and buffers to zero on power-up or in response to an INIT command.

The TPM maintains some information in shielded locations that is non-volatile and available across power cycles. This information includes the endorsement key and the SRK. The TPM shall ensure that these non-volatile areas are only accessible by TPM protected functions.

The TPM shall ensure that an audit event generates for each event. The administrator can select which events generate an audit event. The TPM does not have an audit log just the ability to generate the audit event. The trusted platform sub-system is responsible for reading the audit event register, creating and maintaining the audit log.

6 OPERATIONAL SECURITY POLICY

6.1 System Initialization

The Administrator is responsible for initializing the TPM. Initialization includes:

- Setting the TPM ownership token
- Creating the SRK

6.2 Cryptographic Operation

6.2.1 Key Generation

The TPM generates RSA keys in sizes 512, 768, 1024 and 2048 bits. The source of randomness shall be the TPM RNG. The generation of the key shall use the mathematics and protocols from P1363.

6.2.2 Digital Signatures

The TPM creates digital signatures with RSA key sizes of 512, 768, 1024 and 2048 bits. The TPM shall use P1363 for the mechanisms and structures to create the digital signature. The TPM shall use the TPM RNG as the source for any randomness that the process may require. The TPM may either perform the hash operation on the actual data or receive the hash directly.

The TPM shall only perform a digital signature when the private key is in a shielded location. It is the responsibility of the requestor to ensure that the private key is available in the location.

The TPM shall only perform the operation after the TPM verifies that the authentication token presented as part of the signature request properly validates the function. The TPM shall include in the header all security attributes of the signing key (internal/external, migration etc.). The TPM shall include in the header all security attributes regarding the signature value (internal/external etc.)

The limitation of the amount of data that a signature can sign comes from the RSA modulus size and the amount of header and padding in the signature block. P1363 specifies the amount for each key size.

The TPM validates a digital signature performing the decryption on a submitted signature and comparing the resulting hash value. The TPM does not perform any form of message recovery and only reports the success or failure of the signature verification.

The TPM shall only use a key with a security attribute of signing for signature operations and may never use the key for an encryption or decryption operation.

6.2.3 Encryption

The TPM encrypts and decrypts values with RSA key sizes of 512, 768, 1024 and 2048 bits. The TPM shall use P1363 for the mechanisms and structures to encrypt and decrypt the values. The TPM may use the same internal functions to perform encryption and signatures but the TPM must ensure that encryption keys only perform encryptions and signature keys only perform signatures.

The TPM shall only perform encryption or decryption operations with a key that is in a shielded location. It is the responsibility of the requestor to ensure that the key is available in the location.

The TPM shall only perform the operation after the TPM verifies that the authentication token presented as part of the encryption/decryption request properly validates the function. The TPM shall include in the header all security attributes of the encryption key (internal/external, migration etc.). The TPM shall include in the header all security attributes regarding the encrypted value (internal/external etc.).

The TPM when decrypting a value shall enforce the security attributes found in the encryption header. This includes if the decrypted value can migrate from a shielded location.

7 ELECTROMAGNETIC EMANATIONS POLICY

A TOE security policy must specifically limit the electromagnetic radiation emanated by the TOE and the procedural and physical measures required to prevent the disclosure of cryptography-related IT assets to unauthorized individuals or users.