National Institute of Standards and
Technology

Derived Test Requirements for FIPS PUB 140-1 Appendix A, *A Cryptographic Module Security Policy*

February 1, 1997
Draft

William N. Havener
Roberta J. Medlock
Lisa D. Mitchell
Robert J. Walcott

Draft Appendix A: A Cryptographic Module Security Policy

February 1, 1997

The following paragraphs provide a general discussion of the security policy that should be included in the documentation the vendor provides to the Cryptographic Module Testing (CMT) laboratory. Such a policy must be provided so that the CMT laboratory can perform test TE01.07.01.

A.1 Definition of Cryptographic Module Security Policy

Cryptographic Security Policy is defined in FIPS PUB 140-1 as:

> A precise specification of the security rules under which a cryptographic module must operate, including the security rules derived from the requirements of this standard and the additional security rules imposed by the manufacturer. [FIPS PUB 140-1]

In this document, the test for this security policy, TE01.07.01, states:

> The specification should be complete, and detailed enough to be able to answer the following question: "What access does operator X, performing service Y while in role Z have to security-relevant data item K?" for every role, service, and security-relevant data item contained in the cryptographic module.

In other words, the security policy specifies the rules of operation of the cryptographic module that define within which role(s), and under what circumstances (when performing which services), an operator is allowed to maintain or disclose each security relevant data item of the cryptographic module.

A.2 Purpose of Cryptographic Module Security Policy

There are three major reasons for developing and following a precise cryptographic module security policy:

- To induce the cryptographic module vendor to think carefully and precisely about who he wants to access the cryptographic module, the way different system elements can be accessed, and which system elements to protect.

- To provide a precise specification of the cryptographic security to allow individuals and organizations (e.g., validators) to determine whether the cryptographic module, as implemented, does obey (satisfy) a stated security policy.

- To describe to the cryptographic module user (organization, or individual operator) the capabilities, protections, and access rights they will have when using the cryptographic module.

A.3 Specification of a Cryptographic Module Security Policy

A.3.1 General

A cryptographic module security policy should be expressed in terms of roles, services, cryptographic keys and other critical security parameters. It should address, at a minimum, an identification and authentication (I&A) policy and an access control policy. An I&A policy specifies whether a cryptographic module operator is required to identify himself to the system, and, if so, what information is required and how it should be presented to the system in order for the operator to prove her identity to the system (i.e., authenticate herself). Information required to be presented to the system might be passwords or individually unique biometric data. Once an operator can perform services using the cryptographic module, an access control policy specifies what mode(s) of access she has to each security-relevant data item while performing a given service.

A.3.2 Identification and Authentication (I&A) Policy

Each cryptographic module should have an authentication component within its security policy. It may be one of the following types:

- No Authentication - Neither users nor cryptographic officers need to perform any authentication function in order to use the cryptographic module. This type is only acceptable at security level 1.

- Role-Based Authentication - Every individual who is permitted to perform the services in a given role performs the same authentication sequence, using the same authentication data (e.g., specifying the role name and role password). In this case of role-based authentication, every individual who is permitted to perform the services in a given role would type in the same role password during the authentication process. Role-based authentication is acceptable at security levels 1 and 2.

- Identity-Based Authentication - Every operator who is allowed to use the cryptographic module, whether that operator is a user or cryptographic officer, must perform an authentication sequence using information unique to that operator (e.g., individual passwords or biometric data) to perform any services using the cryptographic module. Identity-based authentication is acceptable at all security levels, but is required at levels 3 and 4.

- Identity- and Role-Based Authentication - Every operator who is allowed to use the cryptographic module must perform an initial authentication sequence using information unique to that operator to perform any services using the cryptographic module. Then, in order to perform the services in a given role, the operator must perform another authentication sequence with information specific to that role, to be able to perform any of the services in that role.

Note: *FIPS PUB 140-1 does not require an authentication policy at security level 1.*

A.3.3 Access Control Policy

The access control policy enforced by the cryptographic module must be sufficiently precise, and of sufficient detail to allow the operator and testers to know what security-relevant data items the operator has access to while performing a service, and the modes of access the operator has to these data items. Also, the testers and operator must be able to know if and how the kinds of accessible data items change when the service is invoked from each role.

A.3.3.1 Identify Elements of the Access Control Policy

1. All roles,
2. All services,
3. All security-relevant data items:
   a. Cryptographic keys - both plaintext and encrypted keys,
   b. Other critical security parameters (e.g., authentication data (passwords)), and
4. The system's modes of access (e.g., read, write, execute, delete).

A.3.3.2 Define the Access Control Policy

1. Assumptions (examples):

   a. An operator who can perform a given role can perform all services within that role.

   b. Each operator performing a service within a given role will have the same access to the system's security-relevant data items (including NO ACCESS) as any other operator performing the same service within the same role.

   c. The same operator may have different access to the same security-relevant data items while performing different services within a given role.

   d. The same operator may have different access to the same security-relevant data items while performing the *same* service from *different* roles (e.g., An operator, acting in the crypto officer role, may be able to modify a security-relevant data item that that operator could only view while in the user role).

   e. An operator can perform no cryptographic services, functions, or operations unless he or she is acting within one of the roles defined for the cryptographic module.

f. An operator can perform no cryptographic functions or operations, unless he or she is performing/requesting one of the cryptographic services specified for the cryptographic module.

g. An operator has no access to a cryptographic key or key components, authentication data, or other security relevant data items except through the invocation of a service within a defined cryptographic role.

Note: *If the system, of which the cryptographic module is a part, allows operations to be performed other than those defined within cryptographic services (e.g., system administrator operations in a multi-processing system), and, it is possible to access any of the security-relevant data items defined in part 3 of section A.3.3.1 above while performing these operations, the vendor must provide a security policy specifying who, and during which operations, the security-relevant data items can be accessed, including the allowable mode(s) of access in each case.*

2. Statement of the Access Control Policy

a. For each role, the vendor shall define (specify) what services an operator may perform while in that role.

b. For each such service within each role, the vendor shall specify what access an operator performing that service within that role has to be a security-relevant data item identified in part 3 of section A.3.3.1 above.

Note: *The vendor may make a general statement such as "For all security-relevant data items not included within the list for a given service within a given role, the operator performing that service in that role has no access."*