Requirements from the

Crypto Catalog

Version: 1.0

2017-04-19

National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2017-04-19	Initial Catalog

Introduction

Purpose. This document presents the functional and assurance requirements found in the *Crypto Catalog*. Common Criteria evaluation, facilitated in the U.S. by the National Information Assurance Partnership (NIAP), is required for IA and IA-enabled products in National Security Systems according to CNSS Policy #11.

Using this document. This representation of the Protection Profile includes:

- *Security Functional Requirements* for use in evaluation. These are featured without the formal Assurance Activities specified in the Protection Profile, to assist the reader who is interested only in the requirements.

  It also includes, in tables shown later, particular types of security functional requirements that are not strictly required in all cases. These are:

  - *Selection-based Security Functional Requirements* which become required when certain selections are made inside the regular Security Functionality Requirements (as indicated by the **[selection:]** construct).
  - *Objective Security Functional Requirements* which are highly desired but not yet widely-available in commercial technology.
  - *Optional Security Functional Requirements* which are available for evaluation and which some customers may insist upon.

- *Security Assurance Requirements* which relate to developer support for the product under evaluation, development processes, and other non-functionality security relevant requirements.

Security Functional Requirements

Cryptographic Operation - User Data Encryption

FCS_COP.1.1(1) The TSF shall perform user data encryption/decryption in accordance with a specified cryptographic algorithm [**selection**: *cryptographic algorithm*] and cryptographic key sizes [**selection**: *key sizes*] that meet the following [**selection**: *list of standards*] .

The following table provides the allowed choices for completion of the selection operations of FCS_COP.1/UDE:

Application Note: There is app note here. What we really want is a nice table of the catalog options. And also, we would like the aactivity to be eactivity.

Security Assurance Requirements

Selection-Based Security Functional Requirements

Objective Security Functional Requirements

Optional Security Functional Requirements