



Real Privacy Management™ (RPM™) Protecting Sensitive Compartmented Information within Information Systems

Version 1.3

Table of Contents

- 1: Abstract:
- 1: Overview
- 2: DCID 6/3 Level-of-Concern
- 2: Confidentiality
- 3: Integrity
- 5: Availability
- 5: Conclusion
- 6: RPM Mapping

ABSTRACT:

This paper provides an overview of how RPM maps to the DCID 6/3 SCI security policies.

Overview

This overview is intended to give the reader an introduction to Relevant Security's Real Privacy Management™ (RPM) technology and its relevance to the Director of Central Intelligence Directive (DCID 6/3) and protecting sensitive compartmented information within information systems.

“RPM is one such security feature, and this white paper will map the how and why relevance to DCID 6/3”

DCID 6/3 establishes the security policies and procedures for storing, processing, and communicating classified intelligence information in information systems. Information from the intelligence community constitutes an asset vital to the effective performance of national security roles.

RPM is a secret-key, key generation and key management method for performing continuous authentication and security of electronic communications. It provides a control mechanism for verifying keys and identities with a message key for securing each communication that is owned and identified by each participant. RPM performs encryption of communications between participants using standard ciphers.

DCID 6/3 notes that intelligence information must be properly managed, and that its confidentiality, integrity, and availability be ensured. DCID 6/3 promotes the use

of efficient procedures and cost-effective, computer-based security features and assurances.

DCID 6/3 Level-of-Concern

Within DCID 6/3 the Level-of-Concern is a rating assigned to an information system. A separate Level-of-Concern is assigned to each information system based on confidentiality, integrity, and availability. The Level-of-Concern for confidentiality, integrity, and availability can be Basic, Medium, or High.

Protection Level 4 is where a user cleared at the secret level sits at a top secret terminal.

Protection level 5 is where a user cleared at the unclassified level sits at a top secret terminal

- The Level-of-Concern assigned to an information system for confidentiality is based on the sensitivity of the information it maintains, processes, and transmits.
- The Level-of-Concern assigned to an information system for integrity is based on the degree of resistance to unauthorized modifications.
- The Level-of-Concern assigned to an information system for availability is based on the needed availability of the information maintained, processed and transmitted by the system for mission accomplishment, and how much tolerance for delay is allowed.

Confidentiality

Each information system that processes intelligence information shall incorporate Confidentiality Requirements. These security features will control the release of information commensurate with the sensitivity level of the information being processed, as well as the clearance, formal access approval, and need-to-know of the users as determined by the assigned protection level. Confidentiality requirements are broken into 5 different protection levels (PL1, PL2, PL3, PL4, and PL5).

As the intelligence community builds platforms and systems at the Confidentiality Protection Level 4 (PL4) and Protection Level 5 (PL5) requirements. Specific Requirements need to be met.

DCID 6/3 Section 4.B.4.a(14) Identification & Authentication I&A6 states the following security requirement as noted in the following Table 1:

Table 1: I&A 4.B.4.a(14) I&A6

If there is communications between two or more systems, then bi-directional authentication between the two systems is required.

RPM provides bi-directional, mutual authentication and data security that is capable of continuous transaction security. For example, in a client-server environment, Bi-Directional **Mutual Authentication** is a security feature in which a *client* process **must** prove its identity to a *server*, and the *server* **must** prove its identity to the *client* before any application traffic is sent to the client-to-server connection. RPM facilitates a bi-directional authentication handshake that proves the identity of both parties via RPM mutual authentication. The authentication handshake will be performed prior to any application message communication, thereby meeting the bi-directional mutual authentication requirement, as well as the requirement that authentication be established prior to any communications of application data.

In fact, RPM can be placed at any level within the Open System Interconnection (OSI) Reference Model. The capability of embedding RPM at the lower OSI levels improves the performance and gives the dependent applications native functions to call; providing a greater range of flexibility.

The RPM basic components and processing methodology is outlined in the following Table 2:

Table 2: Basic RPM components

Initial generation, pairing, and distribution of participant keys.
Maintenance and validation of participant authentication for any given communication.
Maintenance and validation of message keys for encrypting any given communication.

Integrity

Each system that processes intelligence information shall implement security features that will ensure the degree of resistance to unauthorized modification of the information that is commensurate with its determined integrity Level-of-Concern (See Table 3: Integrity Level of Concern).

Table 3: Integrity Level of Concern

Level of Concern	Integrity Factors
Basic	Reasonable degree of resistance required against unauthorized modification, or loss of integrity will have an adverse effect.
Medium	High degree of resistance required against unauthorized modification, but no absolute, or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organization-level interests.
High	Very high degree of resistance required against unauthorized modification, or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests, or loss of integrity will have an adverse effect on confidentiality.

DCID 6/3 notes that a system operating at the Medium and High Level-of-Concern for integrity shall implement the following features (see Table 4: DCID 6/3 Section 5.B.3.a(7) Integrity2 and Table 5: DCID 6/3 Section 5.B.3.a(8) Integrity3).

Table 4: DCID 6/3 Section 5.B.3.a(7) Integrity2

Data and software storage integrity protection, including strong integrity mechanisms (e.g., encryption).

RPM in and of itself does not encrypt messages. RPM does however manage the message key to be used by a cipher to encrypt the message. RPM derives a unique message key for each message and then calls a cipher to encrypt the message using the message key. RPM is “cipher agnostic”, meaning that it can work with any standard cipher. The most popular cipher being used is the Advanced Encryption Standard (AES). RPM works with published security policies for FIPS 140-2 validated cryptographic modules.

Table 5: DCID 6/3 Section 5.B.3.a(8) Integrity3

The implementation of specific non repudiation capabilities.

RPM does utilize a mathematical function that yields a guarantee of authenticity of the owner of the RPM key. RPM can also provide an integrity guarantee around a transmitted message by using a message authentication code (MAC) algorithm.

Utilizing RPM MAC can be used to guarantee the authenticity of the RPM exchange as well as a providing for the integrity of the cipher text generated by the message key encrypted content.

Availability

Each system that processes intelligence information shall implement security features that will ensure information is available for use when, where, and in the form required, commensurate with its determined Availability Level-of-Concern (See Table 6: Availability Level of Concern).

Table 6: Availability Level of Concern

Level of Concern	Integrity Factors
Basic	Information must be available with flexible tolerance for delay or loss of availability will have an adverse effect.
Medium	Information must be readily available with minimum tolerance for delay or bodily injury might result from loss of availability or loss of availability will have an adverse effect on organizational-level interests.
High	Information must always be available upon request, with no tolerance for delay; or loss of life might result from loss of availability; or loss of availability will have an adverse effect on national-level interests; or loss of availability will have an adverse effect on confidentiality.

The RPM method is very fast, very small, and efficient; allowing it to be available in a myriad of systems and scenarios, where inserting alternative methods may hinder availability at the Medium and High Levels-of-Concern.

The RPM algorithm is implemented as using simple mathematics of register-based modular arithmetic. This allows RPM to be implemented using a basic CPU of any computing device. It does not need a math coprocessor or accelerators. The use of basic register-based mathematics of a CPU is what gives RPM the performance and efficiency required for continuous transaction authentication and security. An entire RPM mutual authentication, encryption and message exchange process is completed as a single asymmetric transmission.

Conclusion

The intelligence community is responsible for safeguarding its information at all times. Safeguards should be applied such that appropriate security measures are implemented to ensure the confidentiality, integrity, and availability of its information. The mix of security safeguards selected for systems that process

intelligence information shall ensure that the system meets the policy requirements that are set forth in DCID 6/3.

As this white paper details, RPM is a security method that meets **Confidentiality**, **Integrity**, and **Availability** specifics. As a secret-key authentication and security solution RPM provides end-to-end security. With RPM you get mutual authentication for every transmission – a fully encrypted message for every transmission; and unique authentication and encryption of every transmission.

Requirement	Definition	RPM Mapping
Confidentiality	The assurance that information is not disclosed to unauthorized entities or processes.	<ul style="list-style-type: none"> RPM provides bi-directional, mutual authentication and data security that is capable of continuous transaction security. The authentication handshake can be performed prior to any application message communication, thereby meeting the bi-directional mutual authentication requirement, as well as the requirement that authentication be established prior to any communications of application data. RPM can be placed at any level within the Open System Interconnection (OSI) Reference Model.
Integrity	The protection against unauthorized modification or destruction of information.	<ul style="list-style-type: none"> RPM manages the message key to be used by a cipher to encrypt the message. RPM is “cipher agnostic”, meaning that it can work with any standard cipher. RPM works with published security policies for FIPS 140-2 validated cryptographic modules. Utilizing MAC with RPM can guarantee the authenticity of the RPM exchange as well as a providing for the integrity of the cipher text generated as encrypted content.
Availability	The timely, reliable access to data and information services for authorized users.	<ul style="list-style-type: none"> The RPM method is very fast, very small, and efficient; allowing it to be available in a myriad of systems and scenarios An entire RPM mutual authentication, encryption and message exchange process is completed as a single asymmetric transmission.

Programming libraries for the RPM method are available in Software Developer Kits (SDK) for C, C++, and Java. RPM is provided as a license for use of the patented intellectual property of Relevant Security.



Relevant Security Corp.
 990 South Broadway, Suite 400
 Denver, CO 80209
 Toll Free: +1-877-576-9665
 Phone: +1-720-836-7350
 www.rscorp.com

For more information

Protecting SCI: www.rscorp.com/library/whitepapers/sci.html

RPM™ details: www.rscorp.com/rpm