Security Assessment
January 14, 2011 – Extended Summary

RS Corp

Cryptography Assessment of RS Corp's Real Privacy Management^{TM} (RPM) System

Extended Summary

Extended Summary – January 14, 2011

Prepared by:

Giovanni Di Crescenzo
Senior Scientist
732-699-2108
giovanni@research.telcordia.com

For further information regarding the findings in this report, please contact:

Russ Silva
Principal Consultant
401-333-4502
rsilva@telcordia.com

Document Revision History:

Description – 10GRSC Cryptographic Assessment	**Date**
Draft Detailed Report delivered to RS Corp	14 January 2011

Limitations on Disclosure and Use of This Report

This report may contain information concerning potential vulnerabilities of RS Corp's software products and methods of exploiting them. Telcordia Technologies, Inc. ("Telcordia") recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein.

It is important to note that there is no such thing as absolute information security. All information systems, which are by their nature dependent on human beings, are vulnerable. Telcordia considers the major cryptographic vulnerabilities of the analyzed systems and applications to be identified. However, Telcordia cannot guarantee that RS Corp's systems are immune from attacks or misuse.

This report may recommend that RS Corp use certain software or hardware products manufactured or maintained by other vendors. Telcordia bases these recommendations on prior experience with the capabilities of those products. Nonetheless, Telcordia does not and cannot warrant that a particular product will work as advertised by the vendor, or that it will operate in the manner intended.

List of Acronyms

AES	Advanced Encryption Standard
PDAF	Position Digit Algebra Function
OWC	One-Way Cut

Executive Summary

RS Corp contracted with Telcordia Technologies, Inc. ("Telcordia") to conduct a cryptographic assessment of RS Corp's RPM product. This is Telcordia's first assessment of RS Corp's RPM product.

Telcordia characterizes RS Corp's RPM product as the composition of *technology* (a short term to denote a collection of cryptographic and security methods and techniques) and *system* (a short term to denote a possibly distributed architecture that integrates the technology components so to provide end-to-end functionalities to all entities having access to the architecture).

Within this cryptographic assessment, Telcordia has performed a *high-level cryptography, security and performance analysis* of RS Corp's RPM technology and system design to assess the strengths and identify weaknesses in the design's approaches.

During this analysis, Telcordia:

- Reviewed any specified relevant cryptography, security and performance requirements;
- Identified the cryptographic or security assumptions; and
- Assessed whether the relevant cryptography, security and performance requirements are reasonably attained by the high-level cryptography design, key management, and associated system security mechanisms and operations processing, in the context of the present conditional access architecture, user behavior deemed "realistic" by Telcordia, and industry "best practices" selected by Telcordia.

Telcordia considered the following:

- The system's architectural design from the viewpoint of what needs to be protected and from whom;
- The designers' specified requirements and assumptions;
- Additional cryptography, security and performance requirements based on knowledge of the state of the art;
- Matching the system's architecture requirements against methods that malicious users may employ to prevent attainment of the requirements;
- Performing a high-level analysis of the present cryptographic and security mechanisms, to determine whether the present system architecture attains selected "best practices" in cryptography and security; and
- An analysis of the present and planned system to determine whether the system's methodologies "fit together seamlessly" from a cryptographic viewpoint.

A cryptographic assessment of RS Corp's RPM technology and system was performed. Resources used to produce the assessment included:

- Phone and e-mail communication;
- Computer emulation of RPM technology;
- Reviewing 20+ technical documents provided by RS Corp.

Telcordia's assessment included several stages. First, a detailed specification of the goals and functionalities of RS Corp's RPM technology and system was made. Telcordia then analyzed the potential threats against this technology and system, given their functionalities. Telcordia then formulated a comprehensive list of cryptographic, security and performance requirements for generic technology and system with similar functionalities in a mathematically modeled environment. Finally, Telcordia performed the core of the cryptographic, security and performance analysis by inspecting the extent to which the proposed RPM technology and system meet these requirements. This resulted in a number of findings that can be characterized as follows:

1) Valid cryptographic, security and performance properties of RS Corp's RPM technology and system,
2) Findings of any gaps between RS Corp's RPM technology and system, and "generically ideal" technology and system meeting the described cryptographic, security and performance requirements
3) Recommendations on how to fill these gaps using modifications to the design or presentation of RS Corp's RPM technology and system or to the algorithms used in it.

With respect to this technology and system, in this assessment Telcordia does the following:

a. Lists its main findings during the above cryptography, security and performance analysis, paying special attention to the requirements that RS Corp's RPM technology and system should satisfy.
b. Exposes any obvious or potential gaps in the current version of RS Corp's RPM technology and system.
c. Recommends modifications or additional operations that are necessary to close such gaps.

Each Telcordia finding is categorized as being an ***Exposure***, a ***Concern***, an ***Informational*** or an ***Observation***:

<u>Exposures</u> are the most critical findings, posing an immediate risk to the security of the system, application and/or network, and need to be addressed in as timely a manner as possible.

<u>Concerns</u> are findings that pose some risk to the security, but need not be addressed at the same priority as *Exposures*.

<u>Informational</u> are security issues that need to be noted, but do not necessarily pose a real risk to the system at this time.

<u>Observations</u> do not necessarily pose a security risk, but are usually items of interest. They can indicate a "good" finding to show that the proper security measures have been applied in specific areas that were tested.

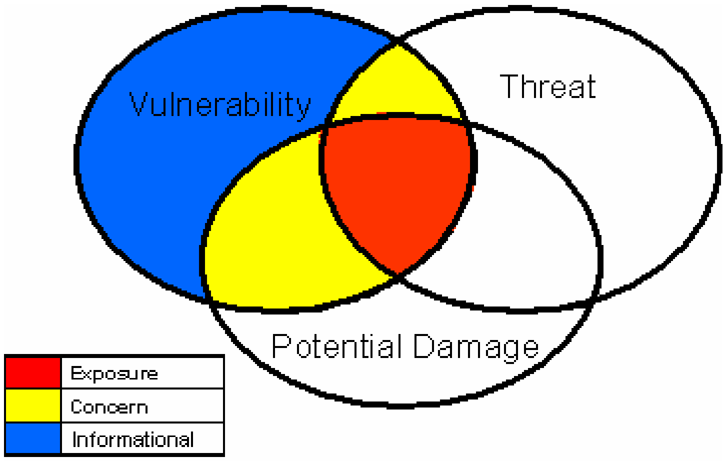

Figure 1: How Telcordia Categorizes Vulnerabilities

While findings, gaps and recommendations will be detailed in the complete version of this document, below is a summary of some of the significant findings related to RS Corp's technology and system. Telcordia's findings in this area consist of:

- *Zero (0) Exposures*[1],
- *One (1) Concern*[2] and
- *Nine (9) Informational*[3] issues.

RS Corp's RPM technology includes the following:

1) A method to generate a stream of pseudo-random values via efficient functions such as Position Digit Algebra Functions and a One-Way Cut function
2) A method to schedule multiple one-time usable block cipher keys
3) A method to encrypt data via one-time keys
4) A method to authenticate sender and receiver during an encryption session
5) A method to protect stored data or cryptographic keys
6) A method to provide communication security between any two parties.

RS Corp's RPM system includes the following:

1) An architecture to provide end-to-end security guarantees, including entity authentication, security for data at rest and security for data in transit, in a scenario with a very general trust model and adversary model assumptions.
2) Variations of this architecture that provide end-to-end security guarantees, including entity authentication, security for data at rest and security for data in transit, in many other scenarios with different trust models and adversary model assumptions.

[1] *Exposures are the most critical findings, posing an immediate risk to the security of the system, application and/or network, and need to be addressed in as timely a manner as possible.*

[2] *Concerns are findings that pose some risk to the security, but need not be addressed at the same priority as Exposures.*

[3] *Informational are security issues that need to be noted, but do not necessarily pose a real risk to the system at this time.*

A list of Telcordia findings with respect to the above main approaches and techniques in RS Corp's RPM technology and system can be found in the following table.

Issue on Approach or Techniques	Telcordia finding
Enhancing documented cryptographic requirements	Informational
Cryptography and performance requirements for RPM	Informational
Preliminaries – Adversary model assumptions	Informational
Approach – Key scheduling algorithms	Informational
Technique – Analysis of Position Digit Algebra Function	Informational
Technique – Analysis of One-Way Cut	Informational
Technique – Randomness of one-time keys	Informational
Technique – Backward invertibility of one-time keys	Informational
Technique – Entropy of one-time keys	Informational
Comparable Techniques	Concern

Table 1: Telcordia Findings on Main Approaches and Techniques

Telcordia believes that the combination of all these paradigms and solutions in RS Corp's RPM technology and system is a top-level, state-of-the-art, solution to the problem of designing an end-to-end multi-party security system. Overall, RS Corp's RPM technology and system can certainly be considered as the result of sound, ingenious and novel thinking, targeting the most appropriate goals for the security properties of any system of this kind. More specifically, RS Corp has addressed essentially all major cryptographic and security attacks known in the related literature, and used essentially all necessary state-of-the-art cryptographic and security algorithms, protocols and techniques that are applicable to systems of this type. Additionally, RS Corp has proposed novel technology to solve the following problems: generation of a stream of pseudo-random values with special security guarantees, efficiently and securely encrypting data, continuously authenticating sender and receiver during an encryption session, protecting stored data or cryptographic keys, and providing communication security between any two parties.

The RPM end-to-end security system reaches a level of content security that is comparable to the state of the art in this research direction, and, in fact, surpasses the state of the art by novel paradigms and solutions; most notably, the continuous refreshing of encryption keys via a stream of pseudo-random values with special security guarantees, such as backward one-way computability. This, in turns, provides a novel combination of security guarantees for the resulting 2-party communication protocol, including continuous entity authentication during the encryption session, backward communication confidentiality, resistance to intrusion attacks. While some of the techniques in RS Corp's RPM system have been used, with variants and modifications, in other designed methods for end-to-end security architectures, Telcordia believes that the previously mentioned novel combination of security guarantees for the 2-party communication protocol resulting from the RPM technology is likely to have been previously unachieved in any end-to-end security product. As it is always the case in the cryptography and security areas, improved security guarantees come at some cost, typically with respect to other security guarantees or performance guarantees. Telcordia tested both cases and reports that

1) the performance guarantees offered by the RPM technology and system are comparable to the state of the art;
2) the guarantees offered in other security aspects are very slightly weakened, but in a way that remains negligible with respect to all potential scenarios, users and applications.

As it is always the case in the cryptography and security areas, novel paradigms and solutions do not exist in the vacuum, and are related to previously invented paradigms and solutions. In particular, when novel security guarantees are achieved via novel paradigms and solutions, it is legitimate to ask whether these novel guarantees were already achieved or easily achievable via previously invented paradigms and solutions. Telcordia tested both cases and reports that

1) the novel security guarantees offered by the RPM technology and system were seemingly not achieved by previous solutions;
2) a limited version of the novel security guarantees offered by the RPM technology and system might be achievable by conventional or suitable extensions of previous solutions.

With respect to this latter point, Telcordia generates a deployment concern and believes that more work is required to assess the extent to which the limited version of these security guarantees suffices for applications of end-to-end security systems or the full guarantees offered by RPM technology is indeed required.

Telcordia's analysis further tested whether RS Corp's conditional access architecture contained any security concerns (denoting an area in which the architecture might become vulnerable to an attack as a result of a significant investment of financial, software and hardware resources combined with a significant amount of hacking intelligence). With respect to this analysis, Telcordia reports that it found no security concerns. The latter finding gives further evidence towards the quality of this product.

Furthermore, Telcordia's analysis tested whether RS Corp's RPM technology and system contained any security high risks or exposures (denoting areas in which the technology and system are substandard and vulnerable to a known or currently feasible attack). With respect to this analysis, Telcordia reports to have found no security high risks or exposures. This latter finding is a clear sign that this architecture is the result of a significant amount of thoughtful and sound design approaches and obfuscation, security and cryptography techniques.

Telcordia's overall cryptographic assessment of RS Corp's RPM technology and system is positive and is accompanied with recommendations to demonstrate the soundness of the technology design and the verifiability of the architecture's security properties in future releases. These recommendations contain, in turn, analysis action items that certainly fall within RS Corp's set of skills in the area.

Telcordia's analysis further tested whether improvements to RS Corp's technology and system**,** based on state-of-the-art security and cryptographic design and analysis techniques are possible. With respect to this analysis, Telcordia reports to have determined that improvements are possible, and strongly recommends RS Corp to implement these improvements to their technology and system (even though the lack of implementation of such improvements will not result in any specific security vulnerability). The main areas suitable for improvements are certainly expected to be within RS Corp's set of skills, and are summarized as follows:

- To achieve backward communication confidentiality and increased security against intrusion attacks, suitable and timely techniques to delete temporary cryptographic keys in RPM technology are recommended.
- Mathematical arguments are recommended to support properties of the RPM technology building blocks and the resulting security guarantees of the overall RPM technology and system.
- Mathematical, simulation, emulation arguments are recommended to support any claims that the novel security guarantees offered by the RPM technology and system might not be achievable by conventional or suitable extensions of previous solutions.

Telcordia's analysis further tested whether RS Corp's RPM technology and system satisfies a suitable and intentionally not exhaustive list of crucial security requirements, categorized as cryptography requirements (in Figure 2) and performance requirements (in Figure 3).

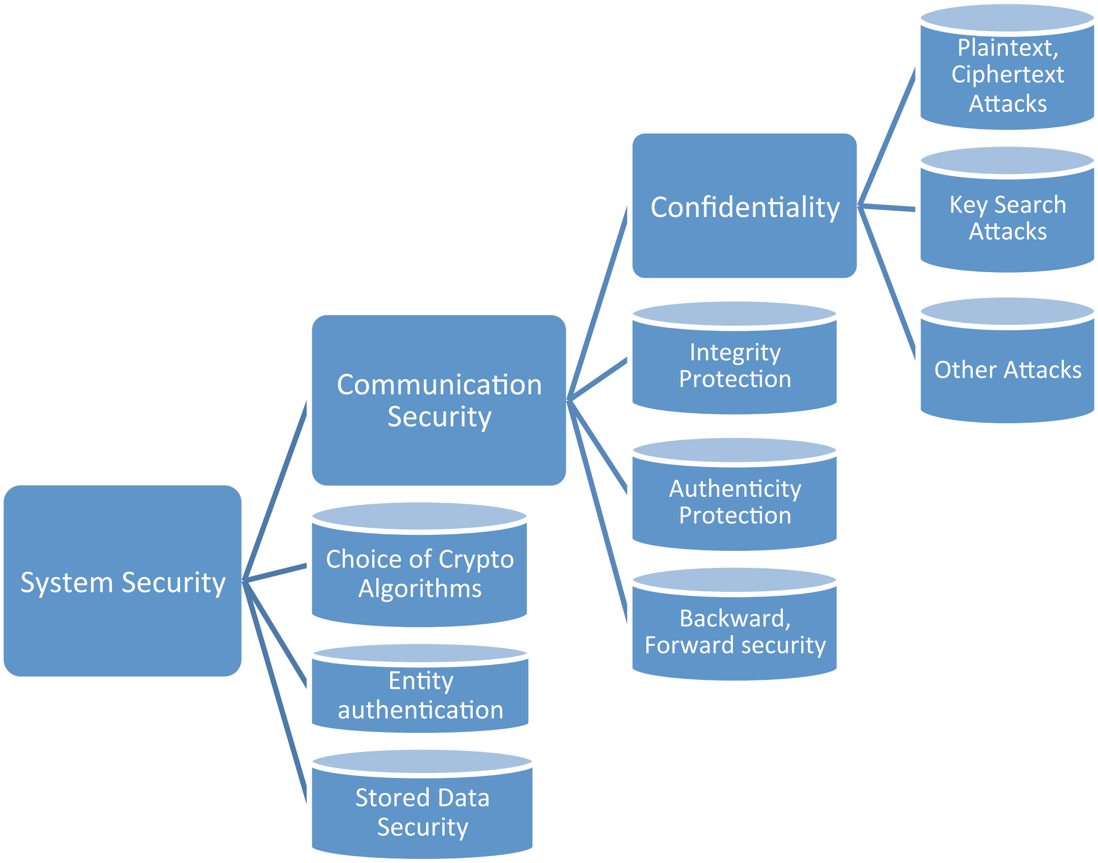

Figure 2: Cryptographic and security requirements

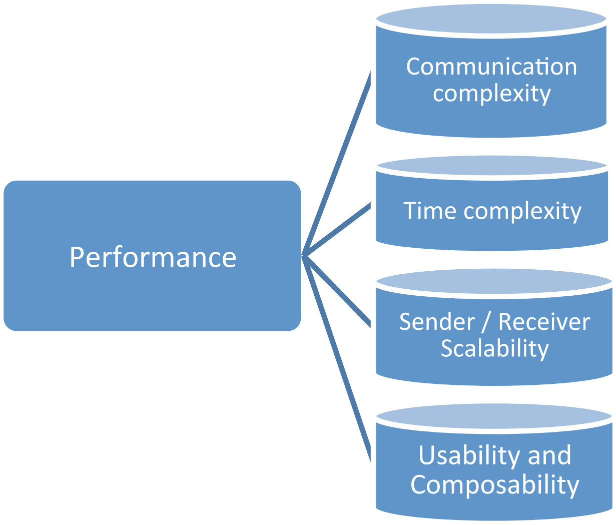

Figure 3: Performance requirements

With respect to this analysis, Telcordia reports to have determined that RS Corp's conditional access architecture satisfies all security requirements and satisfies all performance requirements. Details on how such requirements are satisfied, along with a Telcordia score, and an explanation of the score meaning, is be provided in the following two tables.

Requirement Class	Requirement	Telcordia score
Cryptography	Confidentiality against plaintext/ciphertext attacks	8
Cryptography	Confidentiality against key search attacks	8
Cryptography	Confidentiality against other attacks	9
Cryptography	Integrity protection	8
Cryptography	Authenticity protection	8
Cryptography	Backward/forward security	9
Cryptography	Choice of cryptographic algorithms	8
Cryptography	Entity authentication	9

Performance	Communication complexity	7
Performance	Time complexity	8
Performance	Sender/receiver scalability	9
Performance	Usability and composability	9

Table 2: Telcordia's Scorecard on Cryptographic Requirements

Requirement score	Explanation of score meaning
10	Product perfectly satisfies this security requirement. Moreover, the requirement will be satisfied well beyond our lifetime's attacking or hacking capabilities. Because of intrinsic product space features, Telcordia expects to only very rarely (if at all) assign this score.
9	Product very strongly satisfies this security requirement. No enhancements or very few enhancements of limited relevance seem to be applicable, given current state of the art, to improve the product's security with respect to this requirement.
8	Product strongly satisfies this security requirement. Some enhancements of significant relevance may be applicable from current state of the art to improve the product's security with respect to this requirement.
7	Product satisfies this security requirement. The specific solution can be significantly improved but choosing not to implement these improvements would not result in any vulnerability.
6	Product satisfies this security requirement or will satisfy it after some minimal amount of work that can be easily carried out by the product designer.
5	Product does not completely satisfy this security requirement, in that it may contain some non-trivial technical gaps, possibly leading to product vulnerabilities. Some modest amount of work may be required to fill these gaps and fix these vulnerabilities.
4	Product only partially satisfies this security requirement. There are serious gaps, leading to product vulnerabilities. Filling these gaps or fixing these vulnerabilities would require major re-design of the product's architecture.
3	Product is far from meeting this security requirement. It is unclear whether re-designing efforts could possibly lead to a product meeting this requirement.
2	It is expected that no practical product can possibly meet this security requirement.
1	It can be proved that no practical product can possibly meet this security requirement.
0	It can be proved that no product will ever meet this security requirement.
N/A	Not applicable. Either requirement is not well defined or not enough information was obtained to evaluate whether the product satisfies this requirement.

Table 3: Telcordia's Explanation of Score Meaning