The RPM Authentication System

Relevant Security's Real Privacy Management™ (RPM) technology is a mutual authentication and data security method that provides continuous transaction security. RPM is a lightweight, fast method that performs in real-time, enabling strong security for software, firmware and hardware applications.

RPM is a secret-key method for performing continuous, mutual authentication and security of electronic communications and data. RPM security provides:

- A unique set of secret keys that are owned by and identify each participant
- A control mechanism for verifying keys and identities – mutually authenticating the parties
- A message key for securing each communication
- Encryption of communication between participants using standard ciphers

The basic RPM components and processing:

- Generating, pairing, and distributing participant keys
- Validating participant keys for any given communication
- Maintaining participant keys (revoking, updating, etc.)
- Exchange of secure communications between participants using an agreed upon cipher and message encryption key

Where does RPM apply?
In general, security is needed in a wide variety of electronic applications. RPM can be placed at any level within the Open System Interconnection (OSI) Reference Model. If an application is open or has not yet been built, the lower the level at which security techniques can be placed, the better. Embedding RPM at lower OSI levels improves the performance and gives the dependent applications native functions to call.

The most obvious applications are where secure communications are desired or required – military operations, financial transactions, health care, enterprise security, etc. The true realization of the RPM method is where it makes secure communication possible in areas that lack security today, such as embedded systems. The flexibility, features and fundamental architecture of RPM provide the necessary security and privacy aspects required for communications platforms today and in the future.

RPM cryptographic strengths
Quite obviously, any new method for secure communications should be an improvement over current solutions. Relevant Security's RPM method does so in several ways:

- **RPM uses simple math** – no exponentiation, Montgomery division, long multiplication, etc. Just register-optimized Add-without-Carry as the core mathematical function.
  - This provides for the fastest and most efficient security in any current or envisioned computing environment, simply requiring a core CPU and no additional math co-processors or accelerators.
- **RPM math is provable**, today and forever – RPM is based on an underdetermined system of equations, which is a provably unsolvable theorem of algebra.
  - RPM uses a provable system of equations that is future assured. Most other methods use a system of equations that is "thought to be" unsolvable. such as theoretical mathematical equations.
- **RPM supports Future Secrecy -** a cryptographic capability such that even if a message is broken through a singular, brute-force attack where the cipher itself has been compromised, RPM does not reveal the user credentials – they are still protected. This is because RPM presents a Binomial Probability problem in determining key pair digits traversing the system's equations from the broken message key used by the cipher to the upper level user credentials.
  - RPM Future Secrecy means there is still entropy in the system so that participant and owner network security is retained even if a message were to be broken. No other available security method offers this level of strength.

990 S. Broadway, Suite 300
Denver, CO USA 80209

RPM Business strengths

The cryptographic strengths combined with the technical superiority leads to a security solution that meets and exceeds the needs of the business owners.

Features

- **Mutual and constant authentication** of all network access and control points for every transaction; for both sender and recipient
- **Continuous key management** that secures every transmission with a fresh key
- **Single transmission operation** for total asynchronous security
- **Minimal code space in multiple platforms** C, C++ and Java
- **Flexible Trust Model** supports federated trust as well as hierarchical control and peer-to-peer models for integration into any network or data model
- **Total data security** from end to end
- **Endlessly scalable key management**, data model driven
- **Provable algorithm mathematics** for future assurance
- **End user simplicity** for easy adoption
- **Fast integration and implementation** and for any data communications process
- **Simple expandability,** operation and system maintenance

Benefits

- **More Secure** – mutual authentication for every transmission
- **Faster and More Efficient** – 5 microseconds in software, near line speed in hardware, allowing continuous use
- **Smaller** - the code base is small enough to fit on any embedded device
- **Flexible** – works with any trust model - allowing for easy integration into any business data model
- **Future-Assured** - underdetermined system of equations – based on sound mathematics
- **Scalable** - allows for millions of users
- **Maintainable** – no requirement to integrate with third parties to revoke or manage access
- **Interoperable** – works with existing cryptography and PKI
- **Simpler** - easy expansion, operation, implementation, system maintenance
- **Less Expensive** - in integration time, maintenance and expertise required

Conclusion

Authentication and data security methods are required in order to build and provide confidence that existing, new, classified and global communications networks offer real security and privacy for the owners and participants. RPM has the cryptographic, technical and business strengths that improve upon or replace existing methods while meeting every network security requirement.

990 S. Broadway, Suite 300
Denver, CO USA 80209