RELEVANT SECURITY
CONTINUOUS AUTHENTICATION

Real Privacy Management

In Plain English

Athenticating and encrypting every transmission, every time, on any device, on any network

Relevant Security Introduces RPM^{TM}

TODAY, AS NEVER BEFORE, NETWORK CONVERGENCE IS DRIVING THE INCREASE IN NEW CONSUMER AND BUSINESS APPLICATIONS ACROSS DIVERSE PLATFORMS TO BILLIONS OF END-USER DEVICES. WHETHER THE NETWORK SUPPORTS WIRELESS VOICE, WIRELESS DATA, MOBILE COMPUTING, WIRELESS TO WIRED CONNECTIVITY, NEAR FIELD COMMUNICATIONS OR EMBEDDED SYSTEMS, THE MISSING INGREDIENT FOR MAKING THESE NETWORK SUCCESSFUL TO THE END-USER IS SECURITY. THESE NETWORKS REQUIRE SECURITY THAT WORKS EVERYWHERE AND SCALES TO MILLIONS OF USERS.

New applications that depend on converging networks require better authentication and data security. Whether the application is for electronic payments, email, digital rights management voice over IP, mobile messaging or enterprise business applications, require a more secure method of protecting users and their information. Current solutions are too big, too slow, too weak, too hard to implement and too susceptible to fraud. Real Privacy Management™ (RPM™) from Relevant Security is the only solution that authenticates and encrypts every transmission, every time, on any device, on any network.

7

SECURITY LOGIC WITH RPM:

CONTINUOUS AUTHENTICATION

1 **EASY TO IMPLEMENT**
small SDK, simple key management

2 **WORKS EVERYWHERE**
In any application, device, platform, network

3 **FASTER MORE EFFICIENT**
it is 8 to 50 times faster than other toolkits.

The average user assumes they are already secure today. They are surprised to find that other security toolkits that attempt to offer “safe” communications sessions are not safe.

RPM Addresses Security Concerns

The common session-based security solution uses one time authentication, only authenticates one party (typically the server) and has a number of problems. A typical PKI security solutions that is used for SSL only authenticates the parties at the start of a session and provides encryption with a long lived key; one that is valid for the entire session or longer. This allows third parties to break into a communication through many means, including spoofing a server, hijacking a session from the user and piggybacking on a user communication with a secondary set of transmissions. These methods leave the user and service provider vulnerable to many types of fraud, including identity theft and financial fraud.

There are a number of additional problems with traditional security methods. They have performance issues, being slow and taking up too many resources to utilize. This prevents them from being used effectively in embedded systems and small packet networks.

Public-key security techniques requires the use of certificates. Certificates are usually long-lived credentials and once they are compromised can be exploited for a lengthy time.

Certificates also require third parties for creation and authentication. This limits the type of network configuration that may be used and requires that third parties be involved in the network transaction. Being required to use third parties also limits the type of trust network that can be used, requires trust to be hierarchical, resolving to a root authority. True peer-to-peer networks cannot be created if third parties are required. Third party certificate authorities also complicate key management since public keys must be acquired from an authority before they are distributed to a user requiring authentication. There is also a problem with being able to provide services for the future since the mathematics of public-key systems is theoretical and thus cannot be guaranteed to be assured in the future.

RPM is faster, more efficient and more secure than the typical public-key security. If one were to provide mutual authentication of users in public-key SSL it would take 13 transmissions to complete the handshake. In RPM a handshake can be completed in a single transmission. An entire RPM private and secure message can be performed in less time than it takes to perform a full PKI handshake and the PKI handshake does not even include any content encryption.

CONTINUED ON PAGE 3

The Method
Real Privacy Management In Action

72% of companies say they are more vulnerable to security breaches since there are more ways to attack corporate networks including wireless

The RPM method provides the safe security experience that users expect to get. RPM does this by being a secret-key authentication and security solution that provides end-to- end security. With RPM you get; mutual authentication for every transmission; a fully encrypted message for every transmission; fresh authentication and encryption keys for every transmission. RPM does this through its method of using secret keys where each party is able to compute the next expected secret key of the other party, compare this key to to the key being provided and determine that it is the proper key before continuing with the communication. RPM provides a number of fundamental cryptographic functions as part of the core API. The method described in this paper uses PDAF and OWC.

4 SMALL AND SCALABLE
Small enough to fit on a chip or embedded system for use by millions.

5 SECURE
The only solution that authenticates and encrypts every single transmission, using a fresh key

6 FUTURED-ASSURED
Underdetermined system of equations is provably secure

7 USES NO THIRD-PARTY INTEGRATION
No digital certificates required.

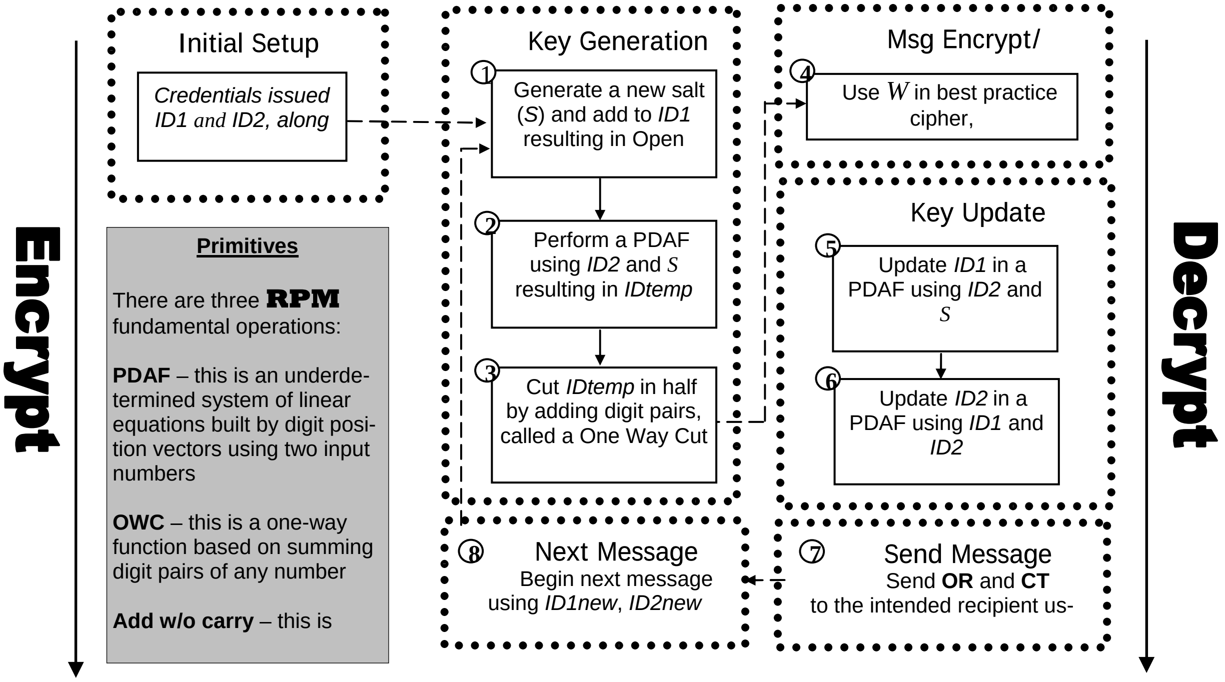
CONTINUED FROM PAGE 2

Further complicating the use of PKI is the size of the software libraries that are required to implement security. A typical PKI Java code library is 65KB. The RPM Java libraries are less than 10KB, leaving more space for applications on smaller devices.

Part of the problem with security is to be able to address the concern that more powerful computing can be used by malicious users to break the security method. In PKI systems, today's key size should be a 1024 bit key. Already, the National Institute of Standards and Technology (NIST) in the U.S. and other standards bodies are recommending that 2048 bit keys be used to maintain security. The future will require even larger keys. Going to 2048 bit keys using PKI means that significantly more computing resources will be required for applications to maintain the same level of security than what is currently required for1024 bit keys.

While PKI may lack scalability, RPM is scalable. The requirement of third party certificate authorities in PKI makes scaling trust unmanageable. If you were to take a network and dynamically add new nodes and new users and do this as the network of services increases and end users increase there would be too many processes, too many components and too many third parties to effectively grow. RPM has a trust model that allows it to grow dynamically and to do so within the topology of the network.

The RPM Authentication and Key Management Method



Encrypt

Initial Setup

Credentials issued ID1 and ID2, along

Primitives

There are three **RPM** fundamental operations:

PDAF – this is an underdetermined system of linear equations built by digit position vectors using two input numbers

OWC – this is a one-way function based on summing digit pairs of any number

Add w/o carry – this is

Key Generation

1 Generate a new salt (*S*) and add to *ID1* resulting in Open

2 Perform a PDAF using *ID2* and *S* resulting in *IDtemp*

3 Cut *IDtemp* in half by adding digit pairs, called a One Way Cut

Msg Encrypt/

4 Use *W* in best practice cipher,

Key Update

5 Update *ID1* in a PDAF using *ID2* and *S*

6 Update *ID2* in a PDAF using *ID1* and *ID2*

8 Next Message
Begin next message using *ID1new*, *ID2new*

7 Send Message
Send **OR** and **CT** to the intended recipient us-

Decrypt

The RPM technique is a secret-key based authentication and key management method. The participants are provided a set of keys that are initially known by both parties. When one participant wants to send a secure communication to the other party the RPM method is used to generate a new set of keys, one for authentication and a second for encrypting the message, and the encrypted message associated with the communication. The means by which RPM creates the new keys for authenticating the sender and encrypting the message is the patented technology of Relevant Security. The mathematics of the method takes a random number that is combined with the authentication key to create a message identifier. The random number is then combined with the second key creating a temporary key that is then cut in half where the result is used as a message key for a standard cipher like AES. The starting keys are then updated by combining the first key with the random number and the second key is updated by combining the original first and second keys.

The processes of combining the random number with the keys to get the authentication and encryption keys, and the original keys with each other to get the updated keys are algebraic functions that are part of the patent. These functions rely on a process of taking one number and combining it with itself based on a second number, progressively offsetting the digits in the number applied to another digit in the number determined by a digit in the second number. The essence of this process is modulo arithmetic and is register-based mathematics at a computer level. Thus, in a computer, one number is in a memory register and is applied to another number is a second memory register. This is the reason for the computational efficiency and performance of RPM. Computer processors are optimized for this type of instruction set so they can execute the RPM method at a greater speed than other algorithms without the use of math coprocessors.

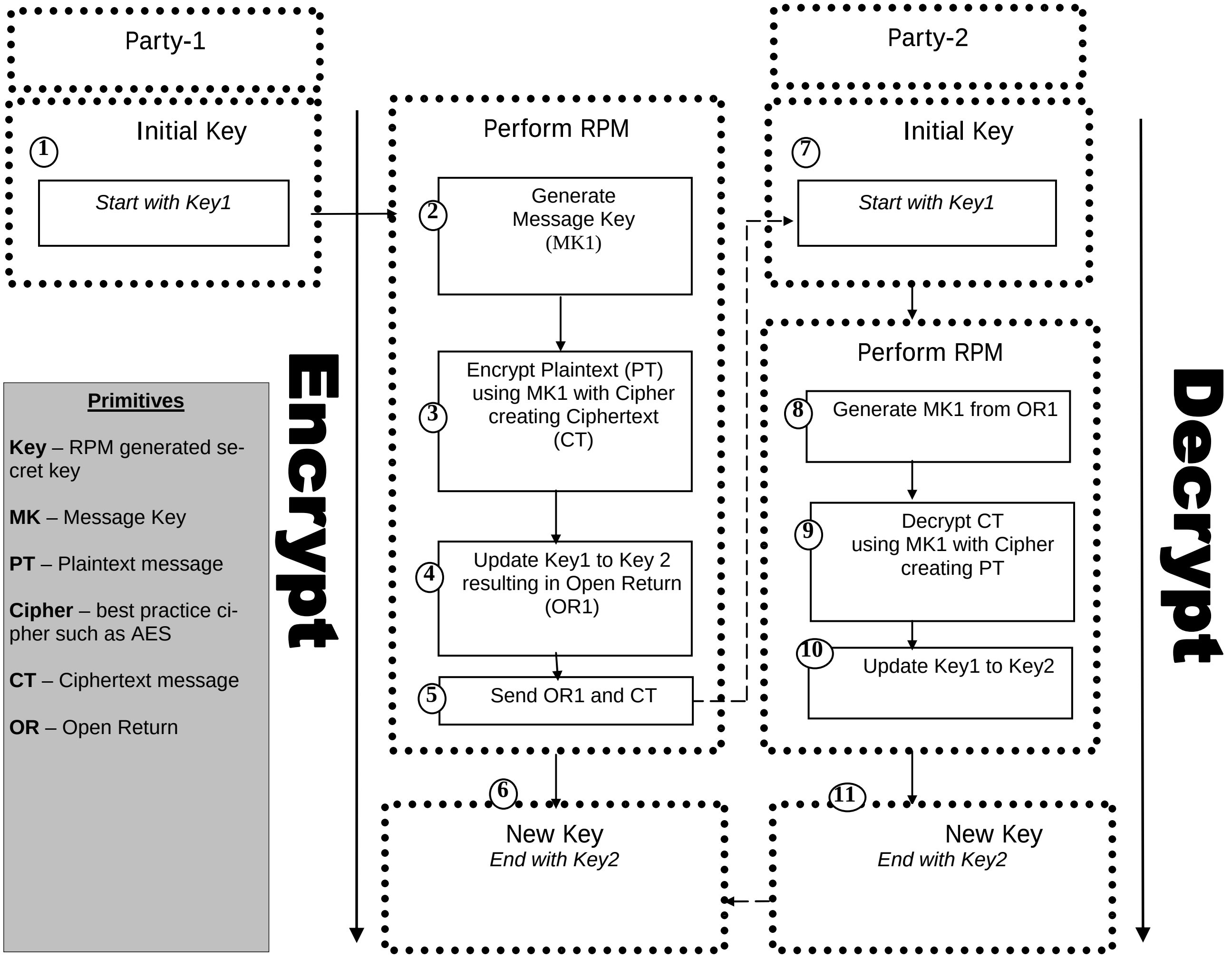
When the second participant receives a message, the receiver also has the original set of keys. The recipient takes the first key and uses it with the message identifier key to generate the random number. The random number is then used to create a decryption key that is applied to the encrypted message. If the authentication key matches then they have established the authenticity of the sender.

Secure Peer Communications

To conduct a direct communication between two parties securely the following process is conducted. Party-1 uses RPM and a starting key to generate an encryption key. The encryption key is applied to the message using a standard cipher like AES to create the encrypted message. The starting key is updated to the updated secret key and a message identifier. The message identifier and encrypted message are sent to Party-2.

Party-2 also starts with the starting key. Using RPM and the message identifier the encryption key is generated. The encrypted text is decrypted using the encryption key applied to the standard cipher. The resulting message is now known to Party-2 and the starting key is used to create the updated secret key. Now, since both parties have the next expected secret key in the updated secret key they can continue to communicate securely.

RPM Secure Communication



Primitives

Key – RPM generated secret key

MK – Message Key

PT – Plaintext message

Cipher – best practice cipher such as AES

CT – Ciphertext message

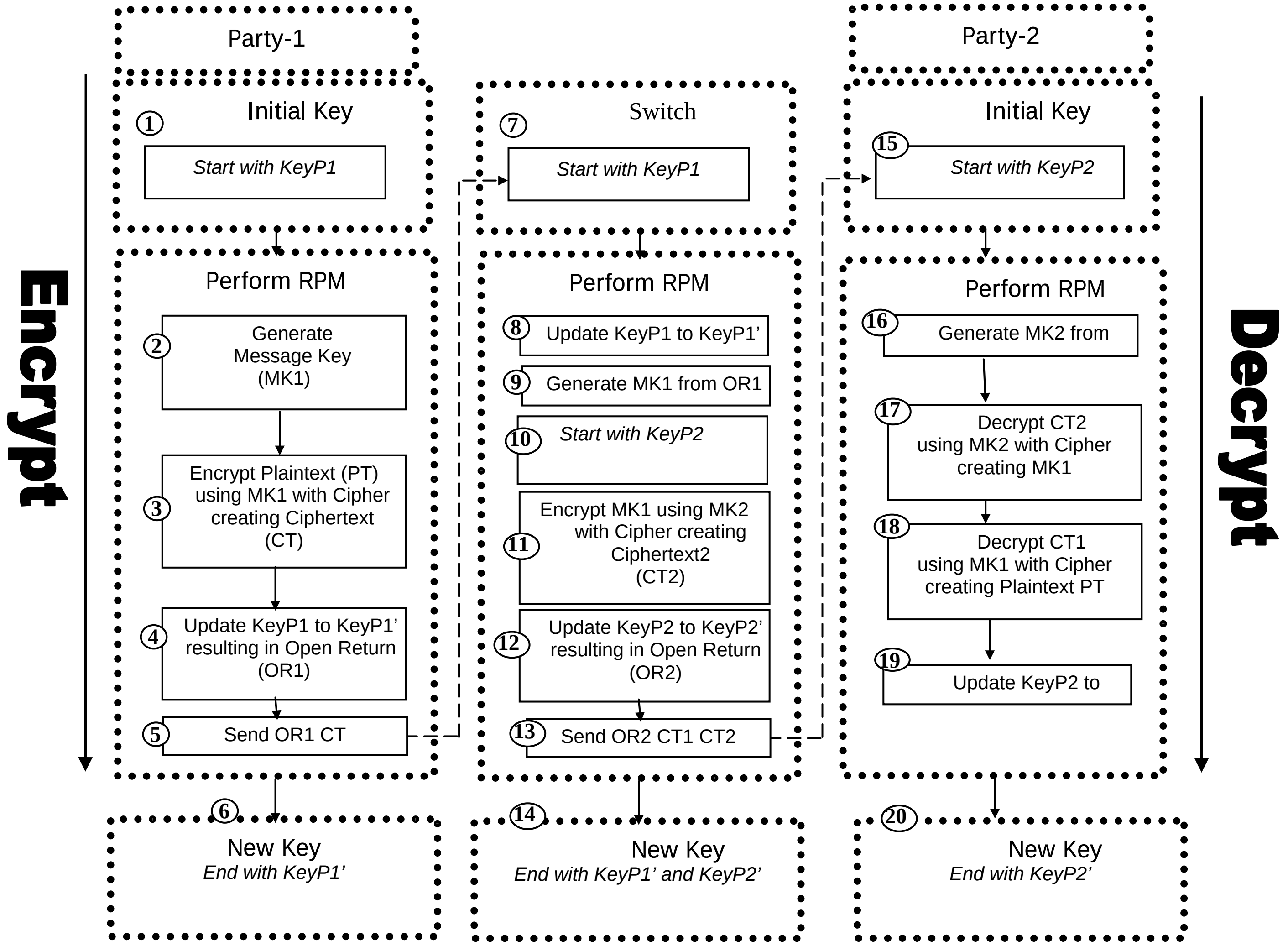
OR – Open Return

Establishing Secure Trust

There also may be case where one party does not have a trust relationship with a second party and yet both parties have a direct relationship with a third intermediate party. In this case if Party-1 wishes to communicate with Party-2 then the third party may act as a communications “switch” for the two communicating parties.

In this case the switch will know the keys for both Party-1 and Party-2, so here is the process. Party-1 starts with their initial key, applies RPM generates an encryption key and uses it to encrypt the message. Party-1 then updates their initial key to an updated key and creates a message identifier from this. Party-1 then sends the encrypted message and the message identifier to the “switch” party asking the switch to send to Party-2.

RPM Secure Communication


Party-1
Party-2
Encrypt
Decrypt
1 Initial Key
Start with KeyP1
Perform RPM
2 Generate Message Key (MK1)
3 Encrypt Plaintext (PT) using MK1 with Cipher creating Ciphertext (CT)
4 Update KeyP1 to KeyP1’ resulting in Open Return (OR1)
5 Send OR1 CT
6 New Key
End with KeyP1’
7 Switch
Start with KeyP1
Perform RPM
8 Update KeyP1 to KeyP1’
9 Generate MK1 from OR1
10 Start with KeyP2
11 Encrypt MK1 using MK2 with Cipher creating Ciphertext2 (CT2)
12 Update KeyP2 to KeyP2’ resulting in Open Return (OR2)
13 Send OR2 CT1 CT2
14 New Key
End with KeyP1’ and KeyP2’
Initial Key
15 Start with KeyP2
Perform RPM
16 Generate MK2 from
17 Decrypt CT2 using MK2 with Cipher creating MK1
18 Decrypt CT1 using MK1 with Cipher creating Plaintext PT
19 Update KeyP2 to
20 New Key
End with KeyP2’

Since the switch receives a message from Party-1 they get the Party-1 initial key. The switch then creates the updated Party-1 key from the initial key. Using the message identifier and the initial Party-1 key the switch generates the Party-1 encryption key used to encrypt the Party-1 message. The switch then takes the Party-2 initial key and generates a second encryption key. This second encryption key, created from the Party-2 key, is used to encrypt the Party-1 encryption key. The switch then updates Party-2 initial key to Party-2 updated key and creates a new message identifier for Party-2. The Party-2 message identifier, the encrypted Party-1 message and the encrypted Party-2 message are all sent to Party-2.

Now Party-2 uses their key to decrypt the Party-2 message identifier to get the Party-1 encryption key. Then Party-2 decrypts the original Party-1 message using this decrypted Party-1 encryption key getting the original Party-1 message. Party-2 then updates their initial key to an updated key.

Protection From Fraud

The RPM method of using secret keys to allow participants to know the next expected secret key provides the backbone for RPM security. This method protects the users from a number of different security attacks. Since RPM authenticates and encrypts every single transmission with these next expected secrets, authentication is a continuous process instead on just happening once, at the beginning of a session. We call this continuous mutual authentication as opposed to once, at-the-gate authentication.

This allows RPM to defeat active and passive eavesdropping, man in the middle attacks, spoofing, automated replay, as well as session hijacking. While the strongest security is provided by RPM performing mutual authentication and encryption of every transmission systems can also be configured for authentication only or session-based authentication and encryption, depending on the security requirements.

Outside Opinions

The mathematics and method of the RPM technology have been validated by outside mathematic and cryptography experts.

Dr. Hatsukazu Tanaka, at the 2006 Symposium on Cryptography and Information Security Hiroshima, Japan, Jan. 17-20, 2006, The Institute of Electronics, Information and Communication Engineers, Security-Function Integrated Simple Cipher Communication System stated that “the realized security is sharing a pair of common-credentials, sharing a common-key, secrecy of messages, sender authentication, common-key authentication, message authentication, common-key renewal, renewal of a pair of common-credentials, etc. Such a security-function integrated simple communication system will be useful for the future wireless communication system such as handy phones and ubiquitous networks”.

Similarly Dr. Alan T. Sherman on May 27, 2005 in An Initial Assessment of the Relevant Security Authentication and Key-Management System Highlights stated that “The core technology of the Relevant Security System is a new method for generating a sequence of master keys, with derived session and child keys, for use in encryption and authentication. This core technology is based on sound principles of randomization, derived keys, and presenting the adversary under certain attacks with underdetermined equations.”

Real Privacy, Real Solutions

The RPM product is available as Software Developer Kits (SDK) for C, C++, and Java.The RPM products are provided to users as a license for use of the patented intellectual property of Relevant Security.

Intellectual Property

Three U.S. patents have been granted for the Relevant Security core RPM method:

- Granted 5/00: Core underdetermined equation set
- Granted 12/99: Application of core to messaging
- Granted 9/02: Extended messaging to any binary/digital system

Two U.S. patents are pending:

- Submitted 2/02: single-PDAF equation set for authentication and data security, including stream cipher
- Submitted 4/05: Complete system (dual PDAF), including key updates, switch-communications paradigms, lost message recovery

RELEVANT SECURITY
CONTINUOUS AUTHENTICATION

990 South Broadway, Suite 400
Denver, Colorado 80209
(720) 836-7350

WWW.RSCORP.COM