PTP *Security*

PERSON TO PERSON™ PERSONAL ENCRYPTION TOOL

Confidential and Authenticated E-Communication

Who would you rather trust - a multi-national commercial company or yourself?

There are many people who would like to be able to send e-mail to a correspondent so that only they would be able to read it and for them to be certain of the originator. They would also like received data to be free from virus or other corruption. This means digital signing and encryption. There are many products which can do this. In general the customer must get to grips with technical matters in installation and obtaining certificates from third-party organisations. After doing this the customer frequently has only a vague understanding of why the system works and just how secure it is. This presents a barrier to utilising the benefits of RSA, an established and excellent technology.

Challenges Presented by Current Products

Installation and Integration An installation procedure must be carried out and the product integrated with the user's e-mail system. There will be preferences and settings to manage. Unless there are specific licensing arrangements, the product may only be used on one PC.

Obtaining a Digital Certificate Before you can begin, most products require the customer to obtain a Digital Certificate from a well-known supplier who takes on the role of Certification Authority. The customer must prove his identity to this authority using protocols similar to those to counter money-laundering and the overall procedure is not a short one. Potential correspondents must also go through this process.

Managing Certificates Certificates must be stored on the PC and managed for period of validity, revocation if necessary, etc. Certificates contain the public part of the RSA encryption key and may be freely distributed. When issuing a certificate the issuer stores the private key on the user's PC. This may be password-protected but it is secret data and as such represents

a serious vulnerability.

Changing Certificates Most security systems require that certificates are changed after a given period of time. This is because it is theoretically possible to break the key by using immense computational facilities over a long, but finite, period of time. This involves more third party involvement, more procedures.

Security Awareness The user is a vital part of the security process but is often overwhelmed by descriptions of the mathematical processes and myriad special features offered by suppliers competing for the market. Customers are expected to be re-assured by supplier assertions rather than factual information about the level of security and any areas of vulnerability.

Focus on the User's Needs - the PTP Solution

Internationally Established Algorithms The security is based on algorithms globally used for Chip and PIN (RSA and Secure Hash Algorithms).

Easy Installation PTP can be downloaded and installed in about five minutes.

No Certificates The principle of operation is that trust is established between correspondents, assisted by the software, using manual means. There is no requirement to prove identity with a Certification Authority. The principles involved in the use of certificates are used but certificates as such do not exist.

No Secret Data Store A normal digital certificate has a secret component, stored somewhere on the PC. PTP employs instead the user's head. A good password is chosen. From this the public and private parts of the keys used to encrypt, sign and authenticate are generated by a special algorithm at the start of a session and destroyed at the end. No secret data has to be shared with a correspondent and all persistent data wherever stored can be considered non-secret.

Change the Password If a user believes that someone else could know his/her password, it can be simply changed thus changing his RSA Key Pair.

Digital Signature Each file is digitally signed before encryption. This serves to identify the originator and to ensure that any virus infection, tampering or data loss is detected.

Because users can see what is happening to their files and are involved in the security process, this will contribute to a culture of increased confidence and understanding leading to a much more widespread and successful use of the encryption technology.

The Mechanics of RSA Encryption and Digital Signature

There are numerous descriptions of the subject. This, it is hoped is the shortest and reflects the particular application employed by PTP.

An RSA key set contains a Public Key and a Private Key.

Each correspondent will own a key set.

You can encrypt a piece of data with the Public Key but can only decrypt with the Private Key.

You can encrypt a piece of data with the Private Key but can only decrypt with the Public Key.

RSA Private Keys are never disclosed by the owner. RSA Public Keys can be shown to everyone.

To send a confidential file, encrypt it with the recipient's Public Key (which everyone can know). It can only be decrypted by the recipient's Private Key (which only the recipient possesses).

A Symmetric Key can encrypt and decrypt a piece of data. (DES is a symmetric encryption algorithm.)The key must be somehow transported to the recipient.

In practise, a Symmetric key is randomly chosen to encrypt the body of the file. The key is used on only one occasion. It is encrypted by the target recipient's RSA Public Key and accompanies the data. The recipient uses his RSA Private Key to decrypt the symmetric key and is then able to decrypt the data.

Signing a file consists of taking a hash (using the Secure Hash Algorithm) of the file data. This is a digest which would radically change on the smallest change in file data. This is encrypted using the originator's Private Key to produce the signature.

Authentication consists in similarly taking a hash of the file data and comparing it with the decryption of the signature obtained using the originator's Public Key.

Key Length

The more bits, the more secure is the RSA Key. Without going into details, there is a third part of an RSA key set called the Modulus (also a public quantity) which is a number being the product of two very large prime numbers. To break the key a hacker must factorise the Modulus into these two numbers.

For a key having length 1024 bits, the Modulus lies between:

$$1 \times 10^{308} \text{ and } 2 \times 10^{308}$$

for a key length of 256 bits the number of possibilities lies between:

$$5 \times 10^{76} \text{ and } 10 \times 10^{76}$$

Although it is considered infeasible to factorise such large numbers, procedures must take into account the possibility of a lucky occurrence - hence the requirement to be able to change keys.

Conventional Implementation

A globally trusted third party produces digital certificates which vouch for the identity of Alice, Bob etc. and provide the public and private key elements of the RSA keys.

Each key pair has an expiry date, after which new digital certificates must be purchased. The keys must be managed. In general use the private as well as the public element must be stored on a computer, vulnerable to hacking. If it is suspected that a key pair has been compromised, a revocation procedure must be carried out.

Keys are not usually longer than 256 bits and this is not considered high strength. (To get an idea what a key looks like, multiply the number of bits by 0.3 to give the approximate number of decimal digits of which it is comprised.). There are therefore cost, management and security risk issues in this method.

PTP Implementation

PTP operates on a 'Person To Person' basis and does not involve a trusted third party.

PTP does not require the use of digital certificates. The functions performed by digital certificates are carried out but in a way which is transparent to the user.

PTP does not store secret keys on the computer. The keys are derived by a proprietary algorithm when required and are destroyed at the end of a session. No secret data of any kind is retained on the computer or transmitted by any means among correspondents.

The system is based on the use of a password which is never given to anyone else and can be changed without repercussions if it is thought to be compromised. Passwords of up to 32 characters can be used consisting of numbers, upper and lower-case letters, spaces and symbols.

PTP manages the group of correspondents by adding the identity of the sender and the sender's public key to the receiver's contact list whenever a received file is processed.

Instead of using a trusted third party to authenticate the identities of participants, correspondents authenticate each other. They do this on the assumption that one correspondent is known personally to another. Each has an identity code derived by a one-way function from his/her public key and they use telephone, email or post to confirm their codes. This eliminates impersonation or 'man-in-the-middle' attacks.