



ESCROW schema
developed and used by
GreenHouse Software & Consulting
Version 08. August 2002

The nature of software, developed by GreenHouse, is, that it uses privileged system procedure calls. This makes the GreenHouse products system software rather than application software. To ensure a customer that GreenHouse is a competent and trustworthy partner, GreenHouse is willing to put the product sources into escrow. The procedure below describes the preferred solution.

This is a new way in putting software into escrow. The proposed solution works with cryptographic methods. The procedure of choice is based on the free ware Pretty Good Privacy (PGP), which is available with all its sources as well as documentation world wide, and which can be ported to any platform. It is a world wide known and de facto standard.

PGP is based on RSA (asymmetric algorithm, public key) to do the key management, and IDEA (block cipher, symmetric algorithm) to perform bulk encryption.

Theory

1. PGP is used by *GreenHouse* to generate a key pair (Secret and Public key)
2. The key pair (secret key as well as the public key) is given to the escrow agent along with the used PGP version (executables, sources, documentation). This is one floppy disk, or a CD. And this is all to be delivered to the escrow agent.
3. The public key of the key pair is given to the customer.
4. The public key is used to encrypt the software in question.
5. The customer gets the software in question (sources, libraries etc.) in encrypt form.
6. In case the customer has the right to get to the software, the escrow agent simply delivers the secret key to him, thus allowing him to decrypt the code in question.
7. A contract will be signed by the customer, *GreenHouse*, and the escrow agent, which regulates the key disclosure.



Praxis

1. PGP is used to generate a key pair. The used version of PGP is given to the customer (sources, executables, documentation, as received from Internet, and checked for validity). This is a one time task.
2. The used key length will be at least 1024 bit.
3. The key generation is done by *GreenHouse* at customer site.
4. The generated key pair is put on a floppy, which will be sealed and put into escrow. Once the key is in escrow, there are never ever any changes required. A copy of this key pair will also be held by *GreenHouse*.
5. The public key is given to the customer.
6. In case (new) software has to be delivered, *GreenHouse* comes on site and
 - compiles the software from the sources at customer site; this ensures, that the right sources are used to produce the software in question
 - encrypt all sources on site, using the public key given to the customer this ensures that the customer knows what is encrypted
 - hand the encrypted software to the customer
7. In case of the occurrence of a pre-defined event, the customer gets the private key from the escrow agent. This key allows him to decrypt the files in question.

This method has a lot of advantages, making it the preferable solution:

- Only a small piece of information is in escrow.
- This piece of information does NOT change at all when the protected software changes.
- The escrow agent is contacted once.
- The handling is simple.

Costs

- The customer has to pay the costs of the escrow agent.
- A requested compile of new software at customer site will be charged with US \$ 1,000 and travel costs, plus V.A.T where applicable.
- Delivering the encoded software directly from *GreenHouse* is for free.

Literature

Contemporary Cryptology - The Science of Information Integrity 1991
Gus J. Simmons
ISBN 0-87942-277-7

Applied Cryptography - Protocols, Algorithms, and Source Code in C 1996
Bruce Schneier
ISBN 0-471-11709-9

Network and Internetwork Security - Principles and Practice 1995
William Stallings
ISBN 0-02-415483-0

