Requirements for storing PGP keys in the Directory

PG 99-007v2
16.03.99

Abstract

PGP is developing into one of the main public key infrastructures (PKI) in the Internet. This paper argues that Directory support of PGP infrastructure can help overcome some of the drawbacks of this PKI. It also states some general requirements for a storage model for PGP keys.

Status of this document

This is not an Internet Draft. It is a statement intended to further the discussion on an Internet Draft on a Directory storage model for public PGP keys. The term Directory as used in this document refers to X.500 [1] as well as to LDAP [2]. All of its content is open to discussion and amendments. Any comments are therefore most welcome. The discussion should take place at the open mailing list pgp-directory@dante.org.uk. A final version of this draft will be published on the Web.

About PGP

PGP is developing into one of the main public key infrastructures in the Internet [3]. It is used for signing, integrity certification and/or encryption of email and other text documents, as well as source code and database requests. It is also capable of doing this with any other types of data as for instance multimedia data and of course for the certification of the PGP public keys. PGP was recently used as authentication mechanism in the RIPE database [4]. The X.509 model of strong authentication is also implementable with PGP technology.

The newest standard PGP message format has been defined by the IETF openPGP WG [5]. It contains several enhancements, e.g., the subkey concept which gives a greater flexibility in terms of what to sign, but simultaneously creates a greater complexity. The new key format also contains more detailed information on the issuer of a certificate including the user ID of the signing key, signature expiration date etc.

Drawbacks of PGP and Directory as solution

The currently applied trust model, the so-called "web of trust", where the PGP users certify the keys of other PGP users, has some inherent problems. One is that some user may take signing of another's key too lightly, i.e. sign without having proved the identity. Again a PGP user has to belong to a big group, that sign each other's key to make a certification path probable. In fact up to now we don't have a "web of trust", but rather "groups of trust" and even "hermitages of trust", which can be seen from statistics on public keys [6]. [Note: these data are quite old, Dec 1997; are there any newer statistics?]
Some other disadvantages are in terms of manageability (e.g. revocation management) and of verifying certificates, caused by the missing possibility to delete information in a once published public key in combination with the high probability that some keys in the web of trust loose their trustworthiness.

The "web of trust" model could be easily replaced by a hierarchical trust model, involving "Trusted Third Parties" or Certification Authorities (CA). There is no reason why PGP couldn't be deployed with such a trust model. Such an approach has been followed, e.g., in the UK [7] and in Germany [8]. One means to implement the publication of CA signed PGP keys would be the Directory that fits in perfectly because of its hierarchical structure.

In the face of the new concept of subkeys, again the hierarchical model of the Directory has its advantages.

A further drawback of the current PGP technology lies in the non-distributedness of the current PGP public key server concept [9]. If the increase of numbers of PGP users continues, this server concept will soon or later become obsolete, because it is not scalable up to much more than 2 million keys. New keyserver concepts, e.g. its integration into the DNS haven't been followed up.

The distribution concept of the Directory makes this technology again an ideal tool providing a scalable and fast responding public key server. The simple protocol for PGP client and public key server communication is easily realisable with directory technology combined with email and HTTP interfaces. These interfaces should not only be able to simulate the key server to PGP client communication, but also the keyserver to keyserver communication, for replication with standard key servers. Both are described in [9].

The usage of the Directory as public key server as used by the current applications is not the only thinkable usage though. For other applications it might be more feasible to store a public key directly inside or below a person entry instead of collecting the keys in one part of the DIT dedicated as key server space.

Requirements for a storage model

The only prerequisite to store PGP keys in the Directory is the definition of appropriate object classes and attributes, which could be used in X.500, as well as in LDAP directories. There already has been an initiative to define such object classes, the long expired Internet Draft draft-ietf-asid-pgp-02.txt [10], which failed to provide a solution for multiple PGP keys of one person, since it defined several attributes, to be included in one person entry. Since there is no definite order for multiple values of one attribute, the affiliation between the values of the different attribute couldn't be stated. Hence a more flexible approach is needed. A new Directory concept the Family of Entries, developed parallel in the IETF [11] and in the ITU [12], which defines a

hierarchical structure inside a Directory entry, could provide a solution for the requirements stated below.

Since not all future usage of PGP technology can be foreseen, a major requirement for the storage model is that it is open enough to reflect the flexibility of PGP technology. We need an abstract enough model together with a flexible way to point to public key information.

The storage model should be able to map:

- Several independent PGP public keys for one person entry or Role occupant entry.
- Several user Ids per public key belonging to one person or roles.
- Several user Ids per public key belonging to different persons or roles.
- Several subkeys in one key which themselves have the same flexibility as the whole key.

It should include:

- Several searchable fields of information necessary for a keyserver implementation, such as keyID, userID, fingerprint, key creation date, etc. in addition to the ASCII armoured key itself.
- Other searchable fields of information necessary for CA implementations, such as pointer to the certificate issuing key, key expiration date, signature status, revocation status and certificate revocation lists, etc.
- Other usefull information such as key size, public key algorithm, key server preference, validity, etc.

Both scenarios, the PGP key stored in or below a person entry, as well as stored among other PGP keys in a dedicated PGP key subtree, should be implementable with the storage model.

The storage model should take concern about the signature included in keys. It should provide the means for a CA to publish the keys signed by it. Applications should be able to retrieve a certification path from the information in the Directory.

Although it is reasonable to concentrate on one technology the possibility of likewise storing public keys of other infrastructures than PGP should be kept in mind. The concept of the storage model should therefore be as PKI technology independent or adaptable as possible.

References

[1] ITU-T Rec. X.501, "The Directory: Models",1993.
[2] Kille, S., Wahl, M., and T. Howes, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997
[3] Atkins, D., Stallings, W. and P. Zimmermann, "PGP Message Exchange Formats", RFC 1991, August 1996
[4] Bukowy, M and J. Snabb, "RIPE NCC Database documentation update to support RIPE DB ver. 2.2.1", RIPE189, January 1999
[5] Callas, J., Donnerhacke, L., Finney, H. and R. Thayer, "OpenPGP Message Format", RFC 2440, November 1998

[6] McBurnet, N., "PGP Web of Trust Statistics", http://bcn.boulder.co.us/~neal/pgpstat/
[7] University College of London, http://www.cs.ucl.ac.uk/research/ice-tel/pgp/pgp_pca/index.html
[8] DFN-PCA, http://www.pca.dfn.de/eng/dfnpca/
[9] Horrowitz, M, "A PGP Public Key Server", http://www.mit.edu/afs/net.mit.edu/project/pks/thesis/paper/thesis.html
[10] Hedberg, R., "Definition of X.500 Attribute Types and a Object Class to Hold public PGP keys", draft-ietf-asid-pgp-02.txt, February 1996 (expired draft)
[11] Chadwick, D.W., "Families of entries", draft-ietf-ldapext-families-00.txt, December 1998 (work in progress)
[12] PDAMs to ISO/IEC 9594 Parts 1, 2, 3, 4, 5, 6, 7 and 9 to support the ITU-T Rec. F.510 "Automated Directory Assistance, White Pages Service Definitions", Collaborative ITU-T/SG7/Q15 and JTC1/SC6/WG7 OSI Directory Meeting 16-23 September 1998, Beijing, China, ftp://ftp.dante.net/pub/flowservices/NameFLOW/mirror/OSIdirectory/BeijingVancouver98Output/F510PDAMv12.pdf, Appendix 1 - Families

Author's Address

Peter Gietz
DANTE
Francis House
112 Hills Road
Cambridge CB2 1PQ
United Kingdom

Phone +44 1223 302 992
Email: peter.gietz@dante.org.uk
DN: cn=Peter Gietz, o=DANTE, c=GB