ASID Working Group
INTERNET-DRAFT
<draft-ietf-asid-pgp-02.txt>
Expires: 20 August 1996

Roland Hedberg
Umea University
20 February 1996

Definition of X.500 Attribute Types and a Object Class to Hold public PGP keys.

Status of this Memo

Abstract

Pretty Good Privacy (PGP) as definied by [1] is a high security cryptographic software application for MSDOS, Unix, VAX/VMS, MacOS and other operating systems.
There is a need to store public PGPkeys in the X.500 [2,3] Directory as a means to ease the publication of public keys, and thereby the use of PGP as a cryptographic system.

This document builds on the experimentation to date and defines four new attribute types and an auxiliary object class to allow PGP keys to be included in X.500 Directory entries in a standard way.

It is intended that the schema elements defined in this document

will be progressed according to the process defined by the Internet X.500 Schema Working Group [4].

Schema Definition of PGPkey Attribute Types

```
   Name:             pGPKey
   ShortName:
   Description:      PrettyGoodPrivacy public key certificate
   OID:              umuAttributeType.9 (1.2.752.17.1.9)
   Syntax:           IA5String
   SizeRestriction:  None
   SingleValued:     True

   Name:             pGPKeyRev
   ShortName:
   Description:      PrettyGoodPrivacy public encryptionkey
                     revocation
   OID:              umuAttributeType.10 (1.2.752.17.1.10)
   Syntax:           IA5String
   SizeRestriction:  None
   SingleValued:     False

   Name:             pGPKeyID
   ShortName:
   Description:      PrettyGoodPrivacy encryptionkey key ID
   OID:              umuAttributeType.12 (1.2.752.17.1.12)
   Syntax:           caseIgnoreString
   SizeRestriction:  None
   SingleValued:     True


   Name:             pGPUserID
   ShortName:
   Description:      PrettyGoodPrivacy encryptionkey user ID
   OID:              umuAttributeType.13 (1.2.752.17.1.13)
   Syntax:           caseIgnoreString
   SizeRestriction:  None
   SingleValued:     True

   Name:             pGPKeyURL
   Shortname:
   Description:      URL for a PGPkey with optional label
   OID:              umuAttributeType.18 (1.2.752.17.1.18)
   Syntax:           caseExactString
   SizeRestriction:  None
   SingleValued:     False
```

Discussion of the pGPKey Attribute Types

The value for pGPKey and pGPKeyRev that is to be stored in X.500 is the ASCII armored text format [5], as produced by the command pgp -kax, with possibly one small modification as described below.

The attribute syntax used is the IA5String .

IA5String ::= OCTET STRING

The IA5String is a notational convenience to indicate that, although strings of IA5String type encode as OCTET STRING types, the legal character set in such a string is limited to the IA5 character set.

The reasoning behind using the IA5StringSyntax is that, since ASCII-armored PGPkey as it is produced by PGP software today consists of serveral pieces separated by linebreaks, it can only be stored in X.500 without modifications if the attribute syntax choosen allows the complete ASCII characterset.

The slight modification that might be necessary is due to the fact that linebreaks are defined differently in different Operating systems. The linebreaks stored in X.500 is therefore defined to consist of the pair CR (0x0d) plus LF (0x0a).

pGPKeyID and pGPUserID is needed if one wants to use a X.500 directory service to emulate a PGP key server since the key servers normally allows you to search for keyIDs as well as matching on parts of the UserID. Since one of the designcriterias was to make it ease to deploy the ideas in this draft I have choosen standard attributetypes instead of inventing new ones, therefore I have to limit pGPKey, pGPKeyID and pGPUserID to be singlevalued to keep the connection between these values.

pGPKeyURL should be used for those instances when there are sound reasons for not keeping the keys within the directory but rather storing them in some other place. pGPKeyURL is thought to be structured much in the same way as the labeledURL [6] attribute is, namely a URL optionally followed by one or more space characters and a label. The label in this case could for instance be the keyID of the pGPKey.

Schema Definition of pGPKeyObject Object Class

Name:	pGPKeyObject
Description:	Auxiliary object class that holds pGPKey information
OID:	umuObjectClass.4 (1.2.752.17.3.4)
SubclassOf:	top
MustContain:	
MayContain:	pGPKey, pGPKeyRev, pGPUserID, pGPKeyID, pGPKeyURL

Discussion of the pGPKeyObject Object Class

The pGPKeyObject class is a subclass of top and may contain the pGPKey, pGPKeyRev, pGPUserID, pGPKeyID and pGPKeyURL attributes. The intent is that this object class can be added to existing objects to allow for inclusion of pGPKey values. It is therefore viewed as a auxiliary objectclass.
This approach does not preclude including the pGPKey attribute type directly in other object classes as appropriate.

Security Considerations

The basis for the use of PGP public keys are that you may validate them in two different ways if you get the public key over the net. The first way depends on the fact that the public key as it is stored and received might contain a validation by someone that the receiver already has a validated public key for. If the receiver trusts the validator then the public key can be included in the receivers keyring without further ado.
If on the other hand the received public key contains no validation or no validation by someone that the receiver already has a public key for then the receiver has to resort to out-of-bands methods to validate the key. This could be using the phone or a meeting in person.

If you can not validate the public key by any of the above mentioned means you should never trust the public key.

Therefore the use of X.500, for storage of PGP public keys, as it stands today with almost no security in place poses no problem. Like all other PGP key servers on the net today it does NOT attempt to guarantee that a key is a valid key.

References

[1] Philip Zimmermann,
"The Official PGP User's Guide";
MIT Press
ISBN 0-262-74017-6

[2] The Directory: Overview of Concepts, Models and Service. CCITT Recommendation X.500, 1988.

[3] Information Processing Systems -- Open Systems Interconnection -- The Directory: Overview of Concepts, Models and Service.
ISO/IEC JTC 1/SC21; International Standard 9594-1, 1988.

[4] Howes, T., Rossen, K., Sataluri, S., and Wright, R., "Procedures for Formalizing, Evolving, and Maintaining the Internet X.500 Directory Schema", Internet Draft (Work In Progress) of the Schema Working Group, <URL:ftp://ds.internic.net/internet-drafts/draft-howes-x500-schema-02.txt>

[5] Atkins, D., Stallings, W. and Zimmerman, P., "PGP Message Exchange Formats", Internet Draft (Work in progress), <URL:ftp://ds.internic.net/internet-drafts/draft-pgp-pgpformat-00.txt>

[6] Mark Smith, "Definition of X.500 Attribute Types and an Object Class to Hold Uniform Resource Identifiers (URIs)", Internet Draft (Work in progress), <URL:ftp://ds.internic.net/internet-drafts/draft-ietf-asid-x500-url-02.txt>

Author's Address

Roland Hedberg
Umdac
Umea University
S-901 87 Umea, Sweden

Phone: +46 90 165165
Fax: +46 90 166766
EMail: Roland.Hedberg@umdac.umu.se

This Internet Draft expires March 20th, 1996.