This document provides recommendations on how to use the various methods available to AFRINIC Database users to enable protection of data against unauthorised deletion or modification (and in some cases also against unauthorised creation). Obtaining your maintainer object other objects, by sending an e-mail to auto-dbm@AFRINIC.net.

When using a maintainer to protect your data, you will have to choose one or more of the available authentication methods. These are defined in the "auth:" attributes of the mntner object. You can have any combination of the different methods and as many instances of each as you wish in a mntner object. However, be aware that authentication is a logical 'OR' of all the supplied instances of the "auth:" attributes values. Authorisation is passed when any one of the "auth:" attributes values
match any one of the credentials supplied in an update.

Four authentication methods are currently available:

*** CRYPT-PW:**

This method takes an argument consisting of a Unix style encrypted password.

When requesting a mntner object, the user must include an "auth:"
attribute with a value corresponding to a Unix style encrypted password and the CRYPT-PW keyword:

auth: CRYPT-PW

When submitting an update by e-mail to create, modify or delete an object protected by a maintainer using this method, the message sent to the database server must include a line containing: password:

This pseudo attribute must be in the body of the e-mail message. If it is a multipart mime message it must also be in the same mime part as the object. Other than these restrictions, it may appear anywhere in the message in relation to the objects. It only needs to appear once in the messageeven if the update contains several objects protected by the same maintainer.

If this password, when encrypted, matches the one stored in the mntner object the update will proceed. Otherwise it will be refused.

There is a cgi script here to generate a crypt-pw password for you http://afrinic.net/en/services/ip-tools/whoiscrypt

Note: This method may be subject to two types of attacks:

- Password cracking. This is the same kind of attack to which normal computer passwords

can be subject. There are programs available that can be used to attempt to decode the password, either by checking it against dictionaries or by attempting all possible combinations.

- Mail snooping. As the update message contains the password in clear text, there is a chance that the password will be seen if the message is intercepted in transit between the user's system and the database server machine.

*** MD5-PW:**

This method takes an argument consisting of an MD5 encrypted password. When requesting a mntner object, the user must include an "auth:" attribute with a value corresponding to an MD5 encrypted password and the MD5-PW keyword:

auth: MD5-PW

Creating, modifying or deleting an object protected by a maintainer using this method follows the same procedure as previously described for CRYPT-PW.

There is a cgi script here to generate an MD5 password for you.

http://www.afrinic.net/en/services/ip-tools/whoiscrypt

Please note that this method may be subject to the same types of attacks as previously mentioned
for CRYPT-PW.

*** PGPKEY:**

This is one of the strongest protection methods available. The user specifies a PGP key-id pointing to a key-cert object in the database that stores a PGP public key.

When sending updates to the database, the user must sign the message using his/her PGP private key. The database software will check the signature using the public key stored in the key-cert object referenced in the "auth:" attribute of the relevant mntner object. If the cryptographic signature is correct,
the update will proceed, otherwise it will be refused.

Note: This type of usage of PGP is considered as commercial use by PGP Inc. A commercial software license must be obtained if PGP software is used. Alternatively users may utilise the GnuPG software to generate and manage keys that are compatible with PGP software.

Note: AFRINIC makes no claims about the identity of the owner of the PGP key used. It just checks that
the signature in the e-mail message was made using the private key corresponding to the public key
stored in the database.

http://www.afrinic.net/en/library/membership-documents/212-pgp-authentication-supporting-doc

ument

*** X.509:**

This method too is one of the strongest protection methods available. The user specifies an X.509 certificate pointing to a key-cert object in the database that stores an X.509 certificate public key.

When sending updates to the database, the user must sign the message using his/her X.509 certificate private key. The database software will check the signature using the public key stored in the key-cert object referenced in the "auth:" attribute of the relevant mntner object. If the cryptographic signature
is correct the update will proceed, otherwise it will be refused.

Note1: AFRINIC makes no claims about the trust path of the certificate or of the revocation status of the certificate. It just checks that the signature in the e-mail message was made using the private key corresponding to the public key stored in the database.

Note2: At this point AFRINIC does not provide tool for Certificate Generation. If you don't already have one, you will have to generate a self signed certificate for yourself.

Read more about how to setup a X.509 authentication:

http://www.afrinic.net/en/library/membership-documents/213-x509-authentication-supporting-document

Simultaneous Use of Several Authentication Schemes

It is enough to match only one of the "auth:" attributes in the mntner object in order to update an object.

We recommend using only one type of authentication method in one mntner object. It should be the strongest type practical for the user.

The best possible protection method is to have either PGPKEY or X.509 authentication. If, for whatever reason, a user does not feel comfortable with only PGPKEY or X.509 and prefers to leave a "backdoor", please use CRYPT-PW or MD5-PW as an addition, choosing a good password. For daily operations,
always apply a signature to the updates.

More information

For a complete description of how to interact with the AFRINIC Database, including data protection, please see the following documents:

* AFRINIC Database Reference Manual
* All AFRINIC Database documentation

Phoca PDF

An empty template can be obtained using a whois client pointed to whois.AFRINIC.net as follows:

http://www.afrinic.net/en/library/membership-documents/219-objects-template#29