ArticSoft
Central Administrator

Centrally deploy and control users keystores. Define policy rules, key recovery and information recovery. Implement simple user revocation.

Central Administrator provides corporations with essential management tools for deploying and managing large numbers of FileAssurity OpenPGP across the enterprise.

Keystore Generation

Central Administrator lets you generate your own master CA key or you can import one from a suitable Certificate Authority (VeriSign, GeoTrust, etc.) or OpenPGP compliant product. The CA key is used to digitally sign the user keys you issue in your own system.

Keystores may be generated manually by the administrator or in batch mode reading commands in from a .csv format file. In manual mode the administrator may set policies for individual keys, whilst in batch mode, policy is the same for the batch of keys. Keystore passwords can be generated automatically at the administrator's request or can be taken from a supplied list.

Central Issue & Re-issue of Keystores

Once generated, keystores are saved to a central database and can be issued centrally on a network drive or accessed through your Intranet. Keystores can be re-issued to change policy settings, validity dates, etc. This is also handy should you want to bulk add new public keys or trusted authorities to all user keystores or to simply extend the key expiration date for certain users. Manual and batch modes are supported.

Roaming User support

Central Administrator provides full flexibility for allowing users to pick up and use their keystores securely from any computer that has access to the network.

Policy Rules

Central Administrator's policy rules ensure full manageability of user keystores with on-the-fly policy changes. You can define the following rights and authorities :

- import, export, generate, delete keys
- change their keystore password
- encrypt, digitally sign and securely delete files
- determine when they have to connect to the database (for validation, new policy enforcement and revocation)

A template is provided where you configure default settings for the master keystore (policy rules, key recovery options, etc.) from which user keystores are generated.

Central Database

Central Administrator stores user keystores and other specific user information (user name, email address, public key/certificate) in an SQL database. Any SQL compliant database is supported including MySQL. This database may be used to locate and make available other user's public keys and allows keystores to be recovered.

Key Recovery

Central Administrator provides a number of recovery mechanisms for both users and administrators

- key (information) recovery
- initial keystore password recovery
- administrator password recovery

If you have generated an information recovery key it will automatically be added to user keystores and cannot be deleted. Recovery keys can also be hidden from users so that they don't even know they exist. For security a two-tier recovery system is used where separate administrators are required for information recovery authorization.

Once users have changed the contents of their keystores they can upload them to the database for secure backup and retrieval.

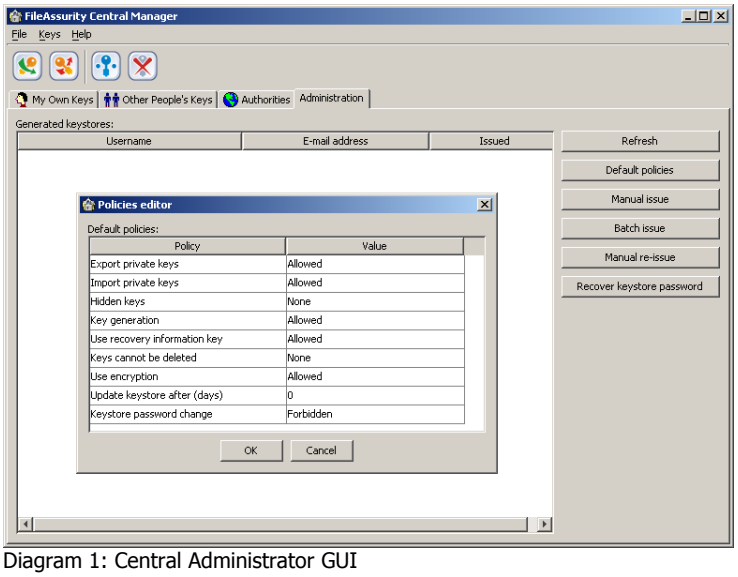

Diagram 1: Central Administrator GUI

User Revocation

User keystores can be verified at administrator specified intervals. If the user does not connect to the central database to verify their keystore (happens automatically) then the client will refuse to operate. This provides a simple method of user revocation without needing to implement LDAP, OCSP or similar technical mechanisms. User keystores can be temporarily removed and restored by the administrator without difficulty or any operational inconvenience.

ARTICSOFT