FileAssurity Central Administration

Outline Project Plan for implementing FileAssurity OpenPGP Central Administration

Introduction

This outline plan has been prepared in order to suggest an approach to system implementation. Every implementation of Central Administration will be unique. Not because there is anything different about the software, but because each organization will have its own unique requirements and method of operation of its information security system and strategy.

The plan has a series of strands, that may be the operational responsibility of different people, or even different organizations, inside the enterprise.

The strands are:

- security method and approach;
- database implementation;
- Central Administration implementation;
- policy definition;
- software distribution approach;
- requirement for Group keys;
- internal and external relationship requirements;
- user keystore generation methodology;
- user keystore maintenance methodology;
- keystore issuance method;
- user training program

Not every installation will need to consider all of these steps, and different implementations may select different ways of achieving the same objectives.

The steps below are grouped to follow the structure outlined above. After each step heading there is a short description of what is involved with that step and the issues that should be considered. A sample Pert chart is given at the end to outline a potential structure for the project and some of the likely dependencies between steps.

Security method and approach

1. there should be an overall approach to the security of the system itself considered. This should include:
   a. who should be in charge of which overall functions and what their responsibilities should be;
   b. how will operational problems such as forgetting passwords, requiring keystore updates, re-issuing keystores and recovering user files be managed;
   c. how will error handling be managed;
   d. how will problem escalation be managed.

2 an overall backup and recovery concept, covering user information as well as centrally held information, is required so that the overall service can be restarted in the event of disaster, not just the central functions.

Database implementation

1 select the database engine you wish to implement if you have not already implemented one in your organization.
   a. there are several issues to consider here. Whilst Central Administration is written to use standard SQL commands, current implementations have been tested using the MSSQL and MySQL databases. Whilst this is not a recommendation to you as a suitable database solution, potential difficulties with other SQL databases have not been fully investigated. Scalability and speed of throughput, and similar operational considerations should be supported by either of the tested database services
   b. you or your organization may not wish to include the Master Database as part of another operational database. Operational characteristics may be in conflict in a number of ways. The actual availability of the database may be affected by processing requirements, accessibility of the database to a wider group of users may be inappropriate if users may gain access to information when they should not, granting external users name and address lookup may be impractical given the security requirements of the other databases being hosted by the server.
2 decide on online or offline approach to handling the Master Database
   a. part of this decision will be based upon your overall security stance. You may not want the Master Database (original) to be directly accessible by anyone other than the Administrator, and to copy the Master Database over onto the operational environment whenever changes have been made.
   b. you may be content to update a single Master Database by connecting the Central Administration PC to it whenever alterations are required, and then taking a backup of the updated Master.
   c. Your organization may be geographically or logically distributed, and to provide appropriate user access it may be necessary to mirror the Master Database into many separate locations. Users may be able to connect to any of the mirrored databases, or just one, and you may choose to publish only the relevant part of the database for each user community.
3 if the strategy is offline decide on the naming convention(s) to be used for the mirrored databases and decide on which users will access which databases. You will also need to ensure that you configure the database access IP address for the Central Manager program correctly, and that when you come to configure the parameters to be sent to users that they point to the correct online database server and not to the offline server.
4 decide on backup/recovery strategy

5 decide on database name(s), but keep user names and passwords consistent across the system

6 configure the database and, if not already done as part of a wider operational system, set passwords to be encrypted (if this needs to be done separately) and set a password on the user root if that has not already been done

7 document the user name that Central Manager and the Tomcat updater service will need to be able to update the entries in the 'keystores' table

8 document the user name that all clients will have to be able to read entries from the database

Central Administration implementation

1 although the previous section impacts upon where the Master Database is going to be stored, it does not determine how the Central Manager program will be implemented. Factors to consider here include:

a. where the Administrator is going to operate the system on a day to day basis;
b. how the other Administrators will gain access to the Administration machine to authorise information recovery;
c. how the Master Database will be connected to;
d. any operational considerations.

Policy definition

1 It is never too early to start deciding on the policy definitions that will be applied to users. This may take some time in larger installations, particularly if users are going to be organised in Groups, or if management wish to have different capabilities from other users. It would be sensible to document:

a. if Groups are to be used;
b. if there are generic policies that will be applied to all users;
c. how to deal with users that are not connected to the internal network all the time and what other, external controls may need to be applied (how can they connect to the Master Database when necessary);
d. if there are special requirements for senior management, and how those can be met.
e. An example of how Policy might be configured for users and groups in a law firm have been included as Appendix 1 to this document. The example is not a definitive approach, but is to help the Administrator with a practical example of how the security and information access requirements of the business system could be configured and administered.

2 review the method and approach to key issuance. Factors to consider include:

a. consider the need to link the identity of the key to setup parameters configuring the client software on implementation;
b. consider if users need to be given configuration information, in particular for users who are not always connected to the internal network or who normally work in other locations, and how to provide that information to them;
c. consider user training requirements, and how these may be timetabled into the implementation plan.

3 Review the approach to setting passwords, automatic notification, delayed notification, using a secure printout etc and set your implementation program policy accordingly. Where central lists are maintained, consider keeping them as encrypted files that can be consulted when they are required, rather than holding them as physical documents. If lists are not maintained and there is a high (more than 3%) demand to recover passwords, you may need to consider training in the use of passwords, given that the keystore passwords do not need to be changed during the lifetime of the use.

Software distribution approach

1 The client software, FileAssurity OpenPGP Managed Client, needs to be distributed to all the users that are going to make use of it. There is no licensing restriction on the number of client software programs that are installed in your enterprise, but there is a restriction on the number of client keystores that can be generated for the Master Database. There are a number of issues that you should consider here:

a. is the software going to be distributed to all user desktops regardless, and then only activated on those that are authorised to have keystores by advising those users that they have a keystore available;
b. how are you going to coordinate the linking of user identity, certificate identity and the parameters that need to be put into the file switches.txt that is used at the time of program implementation so that the authorised user functions immediately. If you choose to allow or require users to configure their personal implementation, how are you going to provide them with the necessary information and provide sufficient explanation that they are likely to get it right;
c. are you going to automate user keystore generation and how is that going to be linked with software distribution;
d. if you are in an outsourced environment, what is the charging mechanism and how is it activated.

2 when you implement software on the desktop how are you going to manage software updates? The ArticSoft service provides a version updater but are you going to run that on every live desktop or once centrally and then push the updated files to the desktop instead?

Requirement for Group keys

1. the requirement for Group keys is something where it would be helpful if it could be identified from the beginning if it is going to be implemented easily. If you are going to run a pilot scheme first, with a limited number of users, prior to moving to a larger implementation then there is no need to worry about Group keys at the beginning because the number of users should not be so significant that you cannot re-issue the initial keystores to be consistent with requirements once you have the practical experience to define them. Issues you should consider include:
   a. will there be groups of internal users that will need to be able to communicate securely among themselves;
   b. are you intending to provide a method for external individuals/organizations to communicate with a business function rather than specific named individuals;
   c. are there individuals who would have the authority to digitally sign information as the Group, and how do you intend to manage that situation;
2. there are a number of ways of considering an organization in order to simplify the creation of Group keys. These are:
   a. national body (country);
   b. organizational function (accounts, legal);
   c. level within a function (manager, executive, VP).
3. these may help you develop a matrix by which you can decide what kind of Group structures would be most appropriate to your own structure. Each enterprise will find a model that suits it best to implement this kind of structure. There is no specific model that fits all possible organizations.
4. a outline guide to setting up policy tables for different environments is given at the end of this document to provide some suggestions about approaches to policy management.
5. Again, please see the example of how this might be used in practice in Appendix 1

Internal and external relationship requirements

1. normally the requirement for cryptography (digital signatures and encryption) occurs because one is having to deal with an external party. Internally it is possible to control networks, user identities, logons, information integrity and so on, so the need for internal protections mechanisms provided by cryptography should be limited. (Note: this may not be the case where the Information Systems of the organization have been outsourced and it is difficult (if not impossible) to be certain over the absolute reliability of the staff then running critical applications for the enterprise.) There are a limited number of reasons why internal communications would require cryptographic security, including:

a. information being transferred between individuals is sufficiently secret that it should not be accessible by e-mail or systems administrators;
b. some departmental functions routinely require to be able to keep information secret from other users (e.g. human resources, legal).

2 when dealing with external parties it is important to consider what interface you are going to offer for them to deal with. In particular you need to consider if the external parties are going to deal with your organization:
a. as individuals;
b. as corporate functions (and if so how are you going to publish your corporate function identities to them so that they can communicate effectively with you);
c. as a centrally managed function (in other words that either the IS department or the Administrator is going to decide which companies are going to be able to communicate securely with you);
d. as a distributed capability, where individual users will be able to open communications links with companies and individuals (always remembering that you are able to apply an information recovery keys so that subject to your own internal policy, you can gain access to any information they encrypt).

3 It may be necessary to discuss with external parties how they intend to behave with respect to the digitally signed and encrypted information that you are going to exchange with them. They may have different policies from you, that may have commercial impacts upon you. For instance:
a. they may have purchased digital identities from one of the Trusted Authorities and be relying upon their verification of identities of users rather than notifying you directly as to who is and is not authorised to represent them using these techniques;
b. they may be running their own controls (as you are) and controlling their relationship with you in the same way as they did before introducing encryption technologies;
c. they may be allowing individual users to work with cryptography under their own control, rather than relying upon a managed service such as the one that you are implementing.

4 do consider that each organization may have it's own specific approach to implementing cryptographic security, and that there is no single model that is correct for all organizations. You may have to operate with many different trust models in order to achieve a service that is of value to the business.

User keystore generation methodology

1 earlier, the approach to generating user keystores was considered. It is important to consider whether keystores will be generate manually, in batches, and, if in batches, if these will be initially in Groups, and how keystore passwords will be distributed. Critical issues to consider include:

a. how secure the internal network actually is, since the distribution of passwords by e-mail could provide an attacker with a significant opportunity to compromise the security system;
b. if passwords are to be distributed by another method, what is that method, how is it going to be implemented, and how are you going to take steps to prevent potential compromise of your chosen method by an attacker (external or internal);
c. are you going to adopt the ArticSoft password generation scheme or are you going to implement an alternative, and, if so, how are you going to integrate the approaches;
d. how are you intending to ensure that the Administrator is not able to compromise the service by being able to obtain user keystore passwords whilst knowing how to load a keystore onto any machine, thus being able to become the user (for the purposes of the security mechanisms that are being implemented. Please note that an e-mail administrator is able to compromise any e-mail account they supervise, just as a logon administrator is often able to compromise any of the accounts that they supervise. We are considering here a balance of forces rather than pursuit of absolute purity. Absolute security is an abstract concept that cannot be achieved. What is being considered here is a workable solution that balances the need for internal security controls that reflect the reliance that will be placed on information digitally signed and encrypted by the individuals using the system versus the difficulty of being able to implement those controls successfully.).

User training program

1 although ArticSoft have developed encryption services that they believe are easy to use and simple to implement, they recognize that, as a matter of the implementation of quality systems such as ISO 9000/15000, it is often essential that users receive adequate training and understanding of the computer systems that they use so that they can be held accountable for their actions. Issues that should be considered therefore include:
a. how many users are to be trained, and in what locations;
b. are there classes or types of user that require different training, and how will that be delivered;
c. can training be automated, or delivered together with other classes, or can it be based around the FileAssurity Managed Client User Manual;
d. is the training just to cover using the client product, or does it include more general topics such as the organizational stance on IS security;
e. there may be additional training that you wish to give concerning how to understand the messages concerning the verification of signatures and certificates, and what to do if errors or warnings are received;
f. is there a minimum level of technical awareness of the Windows operating system facilities (use of file system and right click access)

that is needed before users can be trained, and how will this be achieved;

2 the timing of the training program need not be linked to the implementation program. The client software can be installed on the user desktop, and, apart from seeing an additional icon in the user tray, the user will see no other change. Until they have a password to enable a keystore they cannot make use of the system.

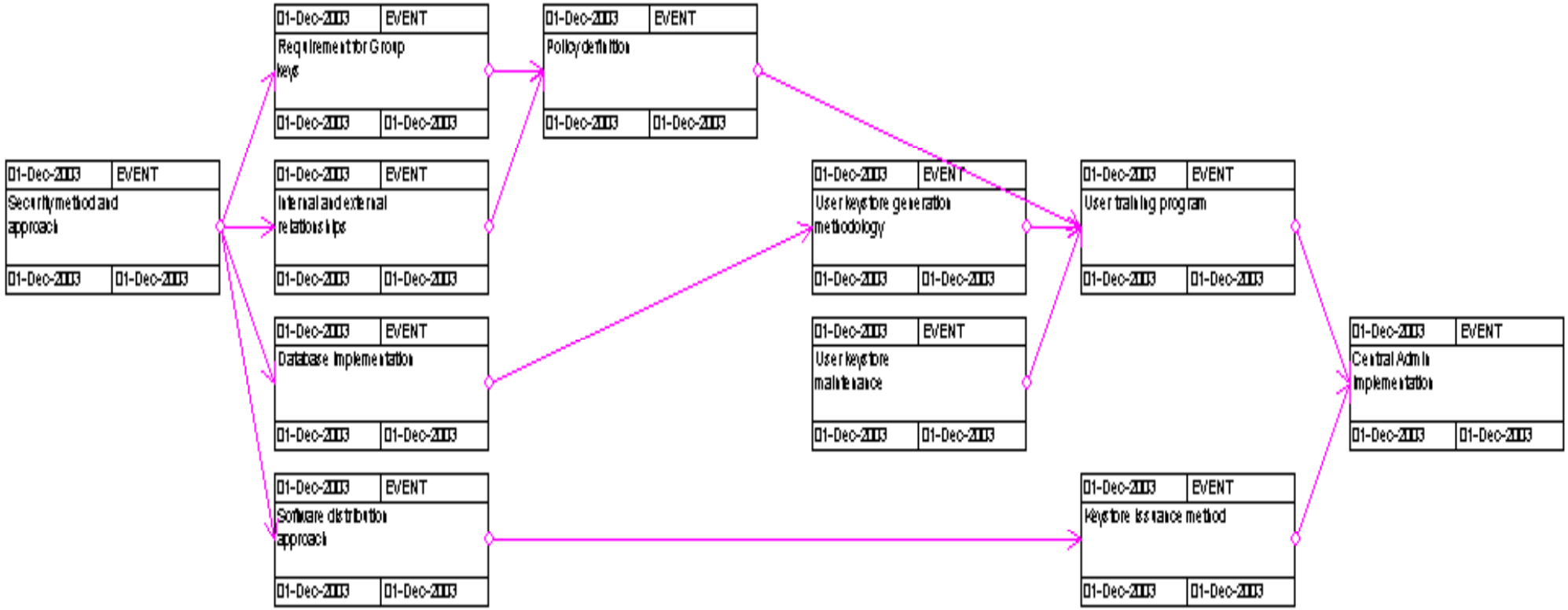

Figure 1: Sample Pert chart for Central Administration implementation project

Appendix 1

The first time that you consider policy for keystores it can be difficult to remember that features such as group keys are created by policy, and not by having a specific key pair definition. This is not because ArticSoft could not have created key pairs that had new definitions, obviously that could have been done. However, it could have created a situation where fields would be added to X.509 certificates to create group definition, and those fields could not be added to OpenPGP certificates because there are no fields available by which one might achieve that. So when defining an interoperable service so that people not using ArticSoft products could successfully interoperate without modifications, internal policy was defined as the mechanism for achieving an interoperable result. The use, by outsiders, of a single identity key that is used internally as a group key – say the public privacy key for the business, that can be used for a secure communication with anyone representing the organization, is not critical since it is not the use of a digital signature. So there are no security/identity issues to consider.

However, it may not always be clear which policy settings are best for which purpose. To give some assistance in making useful selection, we have prepared a scenario that might be chosen by a law firm as a means of relating keys and policies to use by individuals and within groups, as an example of how security objectives were defined and then policies selected.

In our example, all partners of the firm must be able to gain access to any information internal to the firm or sent by the firm at any time. This is achieved by manual control over the use of the information recovery key. There are several private groups that must be able to circulate information amongst themselves. These are the equity partners, partners and fee earners. A member of equity partners is a member of partners and fee earners, and all partners are members of fee earners. Two additional groups, paralegals and secretaries are included. These are present so that the partner responsible for HR matters can address both of these groups separately with confidential information.

If the firm wished to issue a single public key by which anyone could encrypt information to send securely to the firm, then an extra key pair would need to be generated. It would be included with every keystore generated, and it would be marked as not to be deleted and not for signing. It needs to be visible in all user keystores because everyone must be able to send the public key of the firm to anyone outside.

Sample policy settings for FileAssurity Central Administration

Environment	Law firm		
Purpose	Issue keys to equity partners, partners, fee earners, departments, general internal staff and clients		
Group keys required	Yes	Key short identifier for policy table	
	Equity Partners	EP	
	All Partners	AP	
	Departments	Dept - n	(department for which they have direct responsibility)
	Fee earners	FA	
	Paralegals	PA	
	Secretaries	SE	
Other keys required			
	Client keystores	(not considered in this example)	

Access rules:

Equity partners are a private group. An equity partner has that key added to their Partner keystore.
Partners also have access to anything in their department that comes in using the departmental key
Fee earners need to be communicated with as a group
Paralegals and secretaries are two groups who have a common key for exchanging information and may have departmental keys
Clients are issued keystores which have the firm's public keys locked into them, but they can use them for their own purposes
Mobile users must connect every three working days, users every logon and clients once per month

Policy rules to apply for each class of user

Equity Partner	Setting			
Export private keys	Recommend forbid unless there are strong business reasons			
Import private keys	Recommend forbid unless there are strong business reasons			
Hidden keys	None			
Key generation	Recommend forbid unless there are strong business reasons			
Use information recovery key	Allowed			
Keys cannot be deleted	EP	AP	Dept-n	FA : PA and SE may be available for HR purpose
Use encryption	Allowed			
Update keystore after	3 days			
Keystore password change	Recommend forbid unless there are strong business reasons			
Use signing	Allowed			
Keys not allowed to sign with	EP	AP		FA : PA and SE if present as cannot be deleted
Use secure delete	Allowed			

Partner	Setting			
Export private keys	Recommend forbid unless there are strong business reasons			
Import private keys	Recommend forbid unless there are strong business reasons			
Hidden keys	None			
Key generation	Recommend forbid unless there are strong business reasons			
Use information recovery key	Allowed			
Keys cannot be deleted		AP	Dept-n	FA, PA and SE may be available for HR purpose
Use encryption	Allowed			
Update keystore after	3 days			
Keystore password change	Recommend forbid unless there are strong business reasons			
Use signing	Allowed			
Keys not allowed to sign with		AP		FA : PA and SE may be available for HR purpose

Use secure delete	Allowed	

Departmental User / Fee earner

Export private keys	Forbidden	
Import private keys	Forbidden	
Hidden keys	FA	
Key generation	Forbidden	
Use information recovery key	Allowed	
Keys cannot be deleted		Dept-n
Use encryption	Allowed	
Update keystore after	0 or 3 days depending on requirement for roaming	
Keystore password change	Forbidden	
Use signing	Allowed	
Keys not allowed to sign with		Dept-n
Use secure delete	Forbidden	

Paralegal

Export private keys	Forbidden	
Import private keys	Forbidden	
Hidden keys	PA	
Key generation	Forbidden	
Use information recovery key	Allowed	
Keys cannot be deleted		Dept-n
Use encryption	Allowed	
Update keystore after	0 or 3 days depending on requirement for roaming	
Keystore password change	Forbidden	
Use signing	Allowed	

Keys not allowed to sign with		Dept-n
Use secure delete	Forbidden	