

dataSentinel Security Model

Product:	Distributed File System
Component Type:	Client
Component Name:	dataSentinel
Development Language:	Java (J2SE)
Proposed Initial Release Date:	1 st Quarter 2007

Revision History

Revised by:	Date:	Reason
Tom Chalker	Feb. 12, 07	Document creation
Tom Chalker	Sep. 19, 08	Added Emergency Access procedure

Table of Contents

1.	dataSentinel Security Model	4
1.1.	BASIC CONCEPT	4
1.2.	SUPPORTING DOCUMENTS	4
1.3.	SYSTEM ARCHITECTURE	4
1.4.	PERSONAL ENCRYPTION CODES REPRESENT DRIVES	5
1.4.1.	Private Drives for Each User	5
1.4.2.	Synchronization Drives.....	5
1.4.3.	Shared Drives.....	6
1.5.	PROTECTING YOUR PECs FROM LOSS	6
1.5.1.	Single Users	6
1.5.2.	Small Organizations.....	6
1.5.3.	How is this accomplished?.....	7
1.5.4.	Larger Organizations	8
1.6.	MANAGING THE DEPLOYMENT PROCESS	8

1. dataSentinel Security Model

1.1. Basic Concept

This document provides an overview of how security is maintained in the **dataSentinel** Distributed Storage system. It describes how small to mid-size organizations would be organized to simplify the control of company data.

1.2. Supporting Documents

The following pertain to topics in this document:

1. Pixecur-10266-3-3 Distributed Storage Specification.doc
2. Pixecur-10268-2-3 Personal Information Space.doc (Marketing)
3. Pixecur-10274-2-3 Security Space.doc (Marketing)

1.3. System Architecture

The **dataSentinel** Distributed Storage system consists of many server-class computers distributed across North America which collaborate to randomly store encrypted fragments of user files in such a way that much greater levels of security are achieved than through conventional file server installations.

The **dataSentinel** system uses a technique called 'Managed Redundancy' to ensure that the file fragments of a user are never lost even if server computers break down. For this reason, users of the **dataSentinel** system enjoy 100% availability to their data and never have to perform backup or restore procedures.

The **dataSentinel** client is distributed on a USB stick which can be plugged into any computer connected to the Internet. The end-user enters a password and is then able to view their entire file system.

Each end-user's USB stick is enabled by placing a small license file on it which identifies the user and the organization to which they belong.

The **dataSentinel** system organizes the end-users into small groups within a company to simplify the process of providing the USB sticks to the end-user when they originally become users or when they have accidentally lost their stick.

1.4. Personal Encryption Codes represent Drives

The file space of the user is broken into a set of independent drives. These are analogous to the lettered drives such as 'C:/' and 'D:/' of a Microsoft Windows operating system. Each is created by the process of generating a Personal Encryption Code or 'PEC' and storing it on the USB stick of the end-user.

Each PEC represents a fully hierarchical file system of directories and files that is completely separate from all other PEC drives. Access to the contents of a drive is only possible by having a copy of the PEC that was created for it. The PEC defines a set of 256 bit AES encryption keys for the encryption of all of the contents of the file fragments as well as to encode the location of all of the fragments across the servers.

dataSentinel does not install software on a computer, nor does it add mounted drives to the 'My Computer' list so it is not susceptible to virus programs which might scan all visible file systems, or file sharing systems that might try to make files visible to others. Interaction with PEC drives is accomplished exclusively by gestures such as double-click operations to open files or drag & drop operations to move files to and from the computer's file system. Removing the **dataSentinel** USB stick prevents any further access to a PEC drive.

1.4.1. Private Drives for Each User

The most important PEC for an end-user is known as their 'private' PEC. It is created the first time that they use their USB stick and is exclusive to them. Each user will notice the presence of a node named 'private' in the upper-left hand of the file system view that is displayed after the user plugs in their stick and successfully enters their password. Any files placed directly in the drive or any of the 'yellow' subdirectories below it are private to that user.

More PECs will be created by the end-user, but they will always be 'inside' or 'parallel' to their private space.

1.4.2. Synchronization Drives

New users of the **dataSentinel** system may transition from their existing methods of organizing files by creating Synchronization Drives. These are simply independent PEC drives that are associated with specific computers such that a continuous one-way sync is performed from that computer to its PEC drive while the USB stick is in the computer.

The user selects which directories on that computer contain useful data files and is then encouraged to leave the USB stick inserted while using the computer normally. When the user travels or goes home, all of this data is available by plugging their USB stick into a different computer. Should the user's office computer break down, all files would be available immediately by simply plugging in the stick into another computer.

Note that this is only recommended for desktop systems where reasonable physical security exists. Using a Sync Drive on a laptop compromises security because the original clear-text copy of the files remains on the laptop when the **dataSentinel** USB stick is removed. The ability to create Sync Drives is a permission that can be set for users or groups of users.

1.4.3. Shared Drives

It is also possible for end-users to create PECs for the purpose of sharing files among other trusted users. Such a PEC may be embedded anywhere with the 'private' drive space of an end-user, but its icon or files listing background will have a different color depending on its function:

- A read/write PEC drive will have a green icon and its directory listings will have a light green background. If this PEC is shared among two or more end-users, each end-user will be able to create or modify files and directories within that PEC drive.
- A read-only PEC drive will have a red icon and its directory listings will have a light red background. If this PEC is shared, end-users will only be able to view file or directory contents. Only the creator of the PEC is able to write to a read-only drive.

The PECs created for shared drives are stored on the USB sticks of the owner who is the user that created them and are protected in the same way as the 'private' PEC as described below. Non-owners of a shared PEC merely have a copy of the PEC embedded in their 'private' drive space.

1.5. *Protecting your PECs from loss*

The loss of your PEC results in a permanent loss of access to all of the contents of the drive specified by that PEC. It is not practical to reproduce the PEC if no copies of it exist. For this reason, **dataSentinel** provides a mechanism to help you manage your PECs. In technical terms, this would be known as a 'key escrow' policy.

1.5.1. Single Users

If you are a single user who is not part of a larger organization, your PEC is protected by simply saving a paper copy of the numbers that represent it. When you use your USB stick for the first time, you are asked to go through a short procedure to create a unique 'private' PEC and once ready, you are prompted to print a one-page document containing numbers representing that PEC. It is essential that you do print this page and place it in a safe and private place such as a safety deposit box in a bank.

Should your USB stick be damaged or lost, we can provide you with a replacement stick but it will not contain your 'private' PEC. The first time you use the replacement stick you will be able to enter the number from the paper document and resume access to your files. Note however, if you leave your printed PEC in an unsecure place, it would be possible for someone else to enter it into a different **dataSentinel** USB stick and gain access to your files.

1.5.2. Small Organizations

Businesses or small organizations can be organized to provide a more robust key escrow policy. The **dataSentinel** system recognizes the role of an 'Office Manager' within such an organization. This is a non-technical role which typically exists to coordinate office resource allocation among other employees, such as the use of the office photo-copier or distribution of office keys.

The Office Manager role is assigned to a specific individual within a company and their USB stick is licensed with an extra function. It is the duty of the Office Manager to support a small number (typically less than twenty) of end users within the organization. The responsibilities would include:

1. Provisioning a new user with a USB stick
2. Replacing a user's lost USB stick
3. Killing (defeating) a lost or discontinued USB Stick
4. Resetting a user's USB stick password

The typical workflow is as follows:

- The Office Manager provisions a **dataSentinel** USB stick for a new end-user
- The end-user plugs in the stick for the first time and specifies a password and creates a 'private' PEC'
- The end-user forgets the stick password. The stick locks out after three failures.
- The end-user contacts the Office Manager who resets the stick password remotely
- The end-user loses his/her stick
- The end-user contacts the Office Manager who immediately 'kills' the lost stick from his/her interface
- A malicious finder of the stick plugs it in to a computer. The license and PECs are immediately erased – this stick is no longer useful
- The Office Manager recreates the end-user license on a new stick from the office
- The end-user collects the stick. On next use he/she chooses a new password. The files in their 'private' drive are again available.

Emergency access to data on the road for a user who has lost or forgotten their stick is provided as follows:

- The user visits the **dataSentinel** or corporate website and clicks on a 'emergency access' link
- The **dataSentinel** interface comes up and asks the user for their name and company name
- The user calls the Office Manager on the telephone
- The Office Manager selects the name that the user entered from a list of names of currently connected **dataSentinel** users
- The Office Manager is presented with a newly created pass-phrase which he/she dictates over the phone
- The user enters this pass-phrase. When complete, the user's PEC is transferred over an encrypted channel to the user's computer
- The user now sees their files and operates the **dataSentinel** interface as normal
- The user closes the application (or it times out from inactivity) and the PEC is discarded

This procedure is repeated each time the user requires access. The user is provisioned with a new stick when they return to the office.

1.5.3. How is this accomplished?

The Office Manager and all of the end-users associated with that Office Manager exclusively share a special 'supervisory' PEC embedded within the license on their sticks.

When an end-user creates a new PEC (for example, when they create their 'private' PEC on their first use of a stick) a copy of that new PEC is placed in the 'supervisory' PEC space. The Office Manager also has another embedded PEC called the 'supervisory backup' PEC which is exclusively stored on his/her stick. The end-user's new PEC is transferred to this space and deleted from the 'supervisory' space at the first opportunity. The 'supervisory backup' space also contains copies of all of the users individual license files.

The end result of this process is that the Office Manager has the unique ability to re-provision their end users with a replacement USB stick without requiring that end-user to type in their PEC from a paper copy. No one outside of this group has access to these PECs.

Should the Office Manager role be filled by a new individual, all of the end-users would simply visit the new Office Manager to have their license files replaced with a new embedded 'supervisory' PEC. All of the user's license and PEC files would be transferred to a new 'supervisory backup' space created for the new Office Manager and deleted from the previous space. This ensures that future security is not compromised should the previous Office Manager retain a copy of their license file.

It is the choice of the organization as to whether all end-user sticks are updated in the event of a lost stick.

Note that that maintaining the 'supervisory backup' PEC is critical to preserving the all of the managed PECs of an organization. It is important that the Office Manager provision two or more sticks for themselves and store at least one off-site. Alternatively, the 'supervisory backup' PEC may be printed for safekeeping or a copy of the Office Manager's license file may be stored within a trusted data backup system.

1.5.4. Larger Organizations

dataSentinel recommends that larger organizations create a hierarchy of 'Office Manager' groups. At the lowest level, many independent office units exist each of which is managed by an Office Manager with their own 'supervisory' and 'supervisory backup' PECs.

On the next level above, one or more manager groups are formed from the Office Managers of the previous level. These management groups will contain their own 'supervisory' and 'supervisory backup' PECs that have a copy of the lower level Office Manager license files and therefore a redundant copy of the supervisory PECs embedded within those licenses. These would be known as Level 2 Managers, Level 3 Managers, etc..

At the top level, a single set of master 'supervisory' and 'supervisory backup' PECs will ultimately secure all of the PECs of the end-users in the lowest level of the hierarchy, however each layer provides redundancy for the supervisory PECs immediately below. It is critical that special measures be taken to protect this master license file, such as printing the 'supervisory backup' PEC for offsite safekeeping or storing a copy of it within a trusted data backup system

1.6. *Managing the Deployment Process*

dataSentinel maintains a billing system in the form of a web application that is used to manage all of the users created and their position within the hierarchy of their company. It automatically creates all of the 'supervisory' PECs and the 'supervisory backup' PECs and embeds them into the license files that it creates at the point of provisioning. It does not, however, retain the 'supervisory backup' PECs within its system. They exist within the supervisor's license file only and are the responsibility of the client organization. This ensures that **dataSentinel** has no access to the private files of the client.

The Office Manager simply logs into the **dataSentinel** billing system with a username and password and is able to create new users and provision them immediately with USB sticks. The Office Manager can also generate reports on the amounts of user data usage.

A Level 3 Manager logs into the **dataSentinel** billing system to create Level 2 Managers. Similarly, a Level 2 Manager logs into the **dataSentinel** billing system to create Office Managers.

Single user and small companies that comprise a single 'Office Manager' unit are served personally by **dataSentinel's** 'dataGuys' who will provision sticks on demand or visit a company site to train an Office Manager role and provide first level support.

Larger organizations may license an installation of the **dataSentinel** Billing system which may be configured to retain all 'supervisory backup' PECs and maintain private corporate records of its own users.