

A Brief Description of Future Hard Drive Evidence Copying Devices

CypheRix (Pty) Ltd

www.cypherix.co.za

+27-11-615-2035 (w)

+27-11-615-3517

info@cypherix.co.za

Author: Simon Rix

Short Title: Brief description of the Future Certified Hard Drive
Copier

File: InitialDescriptionofHardDriveCopierCertifier-
050413.doc

Classification: **Confidential**

Revision: Draft 1.01

Date Release : 13 April 2005

1 INTRODUCTION

CypheRix is considering expanding it's range of Evidence Gathering Devices beyond the current Digital Audio Recorders.

The current Certified Audio Recorder establishes irrefutability by a cryptographic digital certification scheme that an Audio Recording has not been changed. This should satisfy the stringent demands of a court of law. Digital Certification removes the onerous 'bag and tag' requirements for audio or other evidence.

The Certified Audio Recording technology can be used to record high-level meetings, legal proceedings, disciplinary hearings and interviews of any kind. It is also useful for various covert operations.

It is envisaged that the Hard Drive copying devices would be useful for any type of Forensic Auditing of PC Hard Drives seized as part of any investigation.

The digital certification process makes use of recognised cryptographic algorithms recommended by the National Institute of Standards and Technology (NIST) of the United States of America for use in cryptographic equipment. The Certified Audio Recorder makes use of SHA-1 for the hash, 1024 or 1600 bit RSA for the signature and AES for the optional encryption.

The Evidence Gatherer Digital Certificate Hierarchy allows any party to prove validate that the RSA public key is the correct corresponding public key to the secret key used to certify the recording or copy. This validation process proves conclusively that the recording was not altered in any way. This is ideal in a law court or anywhere needing a high degree of certitude.

There are additional novel yet simple features in the device that make it very easy to show in a non-technical court of law that the audio certificates or more senior certificates cannot be faked. Issues such as protecting any Evidence (Recordings or copies of hard drives) already gather from any form of compromise (technical or legal) should the device be lost during an investigation even if the device is analysed by an unfriendly technical laboratory have been addressed.

In order protect previous recordings the System Operator has the ability to update certain RSA keys in the Evidence Gathering Device. This needs to be done in a controlled manner so that the System Operator can prove when keys were updated. In order to do this the database is protected by a USB Local Security Token.

An optional extension to the system is that the copy of the hard drive may, under the control of the system operator, be encrypted. This is a separate function from the certification function. The USB Local security tokens ensure that only the Operator can decrypt the audio. This may be used to protect information between the Evidence Gathering Device and the Operator or to allow an encrypted copy of the information to be stored and only decrypted when required. If this option is required there will be an increment in the design (NRE) and unit cost.

At this time there is some discussion as to which hashing algorithm should be used for the possible hard drive copier. As stated we currently support SHA-1. Given the debate around MD5 and to a lesser extent SHA-1 as the project progresses we will need to choose which of the four hashing algorithms (SHA-1, SHA-256, SHA-384 or SHA-512) loosely referred to as SHA-2 should be used. The size of the selected hashing

algorithm may impact the cost of the product and the size of the memory needed to store the non-signed hashes. This may also result in the number of sectors being authenticated by the Sector hash being changed. In this document hereafter we will refer to SHA-1 as the selected hashing algorithm. SHA-1 will also be used in the current commercial estimates.

More information on the cryptographic architecture is available on signing a mutual NDA agreement. The cryptographic architecture is the same as the CypheRix Certified Audio Recording System. Note that the security of the system resides entirely in the keys. The system uses standard cryptography and its integrity does not rely on obscurity or any 'tricks'. The NDA is to hamper competitors.

2 INITIAL DESCRIPTION OF A DEVICE TO CERTIFY AND COPY HARD DRIVES

This description is an initial one. It is fully expected that potential users may modify the requirements of this device prior to the design finally happening so this description is not binding.

2.1 Physical Characteristics

At present we envisage a device with the following features:

- a. A small unit less than 10 cm in height.
- b. External 220 V connection, with an internal PC power supply unit able to supply the requirements of the internal PCB as well as three external hard drives. There will be three power supply cables suitable for plugging into the three hard drives emerging from the rear of the unit.
- c. The surface area of the device will be sufficient to allow three hard drives to be placed on the unit next to each other. The top of the unit will have some non-conductive material preferably with good anti-skid properties.
- d. The unit will have three external IDE interfaces, one read and two write interfaces. The hard drive to be copied and certified is placed on the read port and the hard drive(s) you want to transfer data to is placed on the write port(s).
- e. The read (source) interface will support IDE and Serial ATA interfaces.
- f. The write (destination) interfaces will probably be restricted to serial ATA and not support regular IDE.
- g. At present we do not aim to support SCSI interfaces on the read port.
- h. The destination drive(s) will be FAT32 only.
- i. The device will be controlled by a number of push buttons on the front panel and will have an LCD display.
- j. I would aim to be able to process at least 80GBytes of information per hour. I expect to be able to achieve significantly better times than this but I need to do a bit more work on the design before confirming expected transfer speeds. It must be emphasised that the speed of a copy is dependant on the characteristics of the source hard drive. If the source hard drive is slow there is nothing that can be done.
- k. The unit would have a secure Smart Card in chip form. This is used to sign the Certificates that authenticate the data that has been copied from the source drive and to generate all asymmetric and symmetric keys that may be required.
- l. An FPGA will be used to perform the IDE based copying of data from the source to the destination Hard Drive and for the SHA_1 and AES operations.
- m. If required the data on the destination drive may be encrypted with the 128 bit AES block encryption cipher.

2.2 Operational Description

A brief description of the proposed functionality is now given.

- a. The unit will copy the source hard drive to the destination hard drive(s). Bad sectors are skipped. The destination drive will have a low number of directories to which the source hard drive data is copied. This will allow a number of different source drives to be copied to one destination drive. The number of sub-directories will be limited to 16.
- b. Each source hard drive copied will be put in a unique subdirectory, one per source hard drive. This sub-directory will have two further sub-directories (sub-sub directories), one for the actual data itself and one of the hash and certificate values. Hence we are going to create a disk image.
- c. The unit will generate a SHA-1 hash value for every sequential 1024 sectors, this equates to 512Kbytes of data. The *1K Sector Hash* forms the basic building block for the certification structure. The low number of sectors here Sector Hash clearly aids
- d. These *1K Sector Hash* values are hashed together into hash of hashes. We will hash *1K Sector Hashes* together to create a *1M Sector Hash* (this gives one certificate per 512 Mbytes of copied data. The *1M Sector Hash* will be included in the RSA signed certificate along with other sequencing and time information. This 512 Mbytes of certified information is stand alone from a cryptographic point of view and is referred to as a *1M Cert Chunk*.
- e. The smallest evidence unit that can be verified in court is one or more sectors from the *1M Cert Chunk* plus all the *1K Sector Hashes* in the *1M Chunk* plus the certificate which contains the *1M Sector Hash*.
- f. The hash of hash results are cryptographically signed using the RSA Evidence Certification Key structure.

There will be two types of RSA based Sector Data Certificates:

- i. A "*1M Sector Data Certificate*" for every 1 Million sectors (around 3 and a half minutes at the expected transfer rate).
 - ii. An *All Sector Data Certificate* for the entire drive. This is simply a Certificate containing a hash of all *1M Sector hashes*.
- g. The device will conform to the same evidence certification method as the current audio recorder.

The Hard Drive Copier will generate a new File-Level RSA Key pair for every hard drive copied. The File Level secret key is used to sign all *1M Sector Data Certificates* as well as the *All Sector Certificate* for the whole hard drive.

The File-Level RSA Public Key is signed by more senior keys in the Hard Drive Copying Device Key hierarchy. The exact details of this key structure are available under NDA. The Hard Drive Copying Device's public key certificates can be used to verify the Sector Data Certificates and to prove which device certified the data copied from the source hard drive.

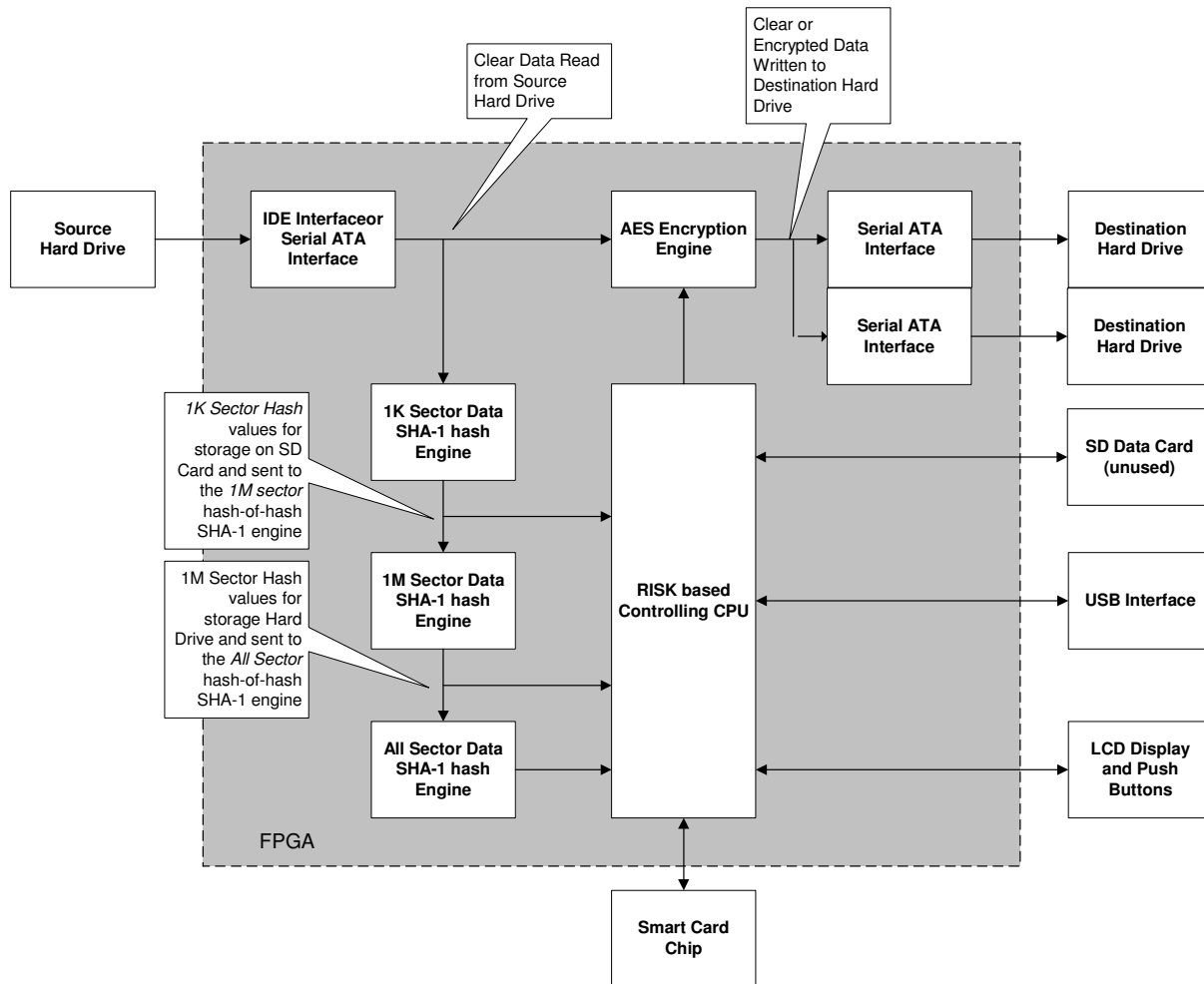
- h. If required the data copied to the destination hard drive can be **encrypted** using a 128 bit AES engine. The 128 bit session key used to encrypt the data will be

chosen by the Hard Drive Copying Device. The session key will be authenticated and encrypted. Only parties with either the Local or Master Control USB tokens will be able to decrypt the now encrypted destination hard drive. Please see the section on “An Overview of the PC Based Control System” for more information.

- i. During the coping the hashes and certificates will be copied in to the second sub directory. We will copy a number of hashes and certificates per write in order to maximise the write actions in the destination hard drives.
- j. The unit will be supplied with software that will allow the user to verify that the copy of the hard drive has not been altered. This is done by re-calculating the hashes for the data in the copy. These re-calculated hashes are then compared to the *IK Sector Hashes*. If they match the data is unaltered. The *IK Sector Hashes* are hashed together and compared to the *IM Sector Hash* in the certificate thereby validating the *IK Sector Hashes*.
- k. All control commands are sent to the unit using the USB interface. These are to do with device identify, status, and RSA key updating (Sequence Level and Local Control. See section on An Overview of the PC Based Control System.

2.3 Basic Block Diagram

Here is a basic block diagram of the Hard Drive Copying Device:



3 AN OVERVIEW OF THE PC BASED CONTROL SYSTEM

The Control system is identical to the Audio Evidence Gathering Devices. Should a customer already have Audio Evidence Gathering devices the Hard Drive Copying Devices will integrate into the head end.

3.1 Brief Description

The Control System is partitioned into two parts viz: a System Master and a Local User.

The System Master is the owner of the Evidence Gathering Device. The System Master is able to assign the Evidence Gathering Device to specific Local Users. Once an Evidence Gathering Device has been re-assigned to a new Local User the previous Local User can no longer control the Evidence Gathering Device. This gives maximal operational flexibility as the System Master can create small User groups for sensitive cases or simple assign a Evidence Gathering Device to different departments (or geographic regions) as operation requirements change. The System Master can also decrypt all encrypted hard drive files.

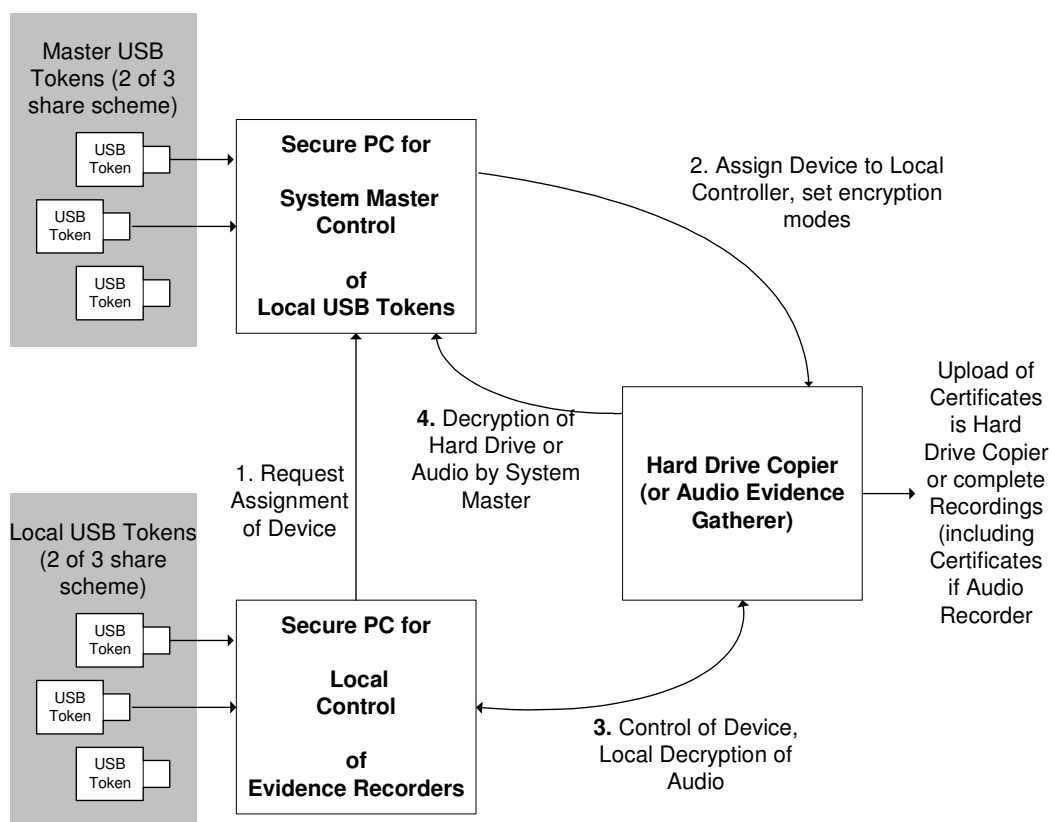


Figure 3 Overview Of the Control of Evidence Gatherers

The Local User controls the daily operation of the Evidence Gathering Device.

The Local User maintains a database of all Evidence Gathering Device processing actions. This enables the Local User to keep track of all RSA keys in the Certificate Hierarchy in its database.

The Local User is able to upload the Certificates of the Hard Drive copied from the Hard Drive Copier using the USB port. (In the case of the Audio Evidence Gatherer complete Audio recordings along with the certificates are uploaded using USB).

In the case of the Audio Recorder the certified audio file is in a proprietary format. In order to listen to the recording on a PC the application can convert the proprietary certified audio format to a separate WAV file. Please note that the storage of the actual certified audio recording and the optional WAV file is done externally to the Local application due to the size of the files.

Should the USB Security tokens be present the Local User can also decrypt the hard drive files or the audio recordings.

It is also required that keys in the Evidence Gathering Device are periodically updated. This is to ensure that earlier recordings are not compromised in any manner should the Device be subsequently lost.

3.2 USB Security Tokens

As cryptographic keys are used to control the Evidence Gathering Device and to decrypt the audio files USB-based security tokens are required to access the keys and to perform certain cryptographic operations.

The keys in the Data Bases are encrypted using a symmetric Super Master Key (SMK). The SMK is split into shares and stored on three, security modules. At least two of the three USB security tokens are required in order to reconstitute the SMK. The SMK is held in SRAM and is erased when triggered by intrusion detectors or on loss of power.

All RSA cryptographic functionality takes place in the USB Security token to protect the secret exponents. The USB security tokens are able to perform many additional asymmetric and symmetric cryptographic functions and can be tailored for specific requirements. Please ask us for more information.

4 THE CERTIFIED AUDIO RECORDER FIELD MODEL

Here, for interest, is a summary of the features of the existing Certified Audio Recorder Field Model:

1. The recorder has an internal Knowles microphone as well as a 3.5 mm socket for an external electret microphone.
2. The Recorder has an excellent audio quality in the range of 40 Hz to 4KHz with a dynamic range of > 70 dBs. Conversations can be heard up to 30 meters away in quiet conditions.
3. A slider switch activates the recording. This slider switch is mounted inside the recorder housing. Once the recorder has been activated and the slider closed the recorder cannot be deactivated by mistake. The recorder also supports external activation via the 2.5 mm external socket. The recording will be automatically restarted in the event of a power interruption if the slider is in the on position on power up.
4. During a recording the operator is able to listen to the audio being recorded. If the recording is running off batteries this will reduce the battery life of the recorder. The 2.5 mm socket is shared between a mono audio out and the external on off switch.
5. The certified audio information and the certificates are stored on an industry standard Multi Media Card (MMC) or Secure Digital (SD) Card.
6. There is a trade off between bandwidth (the amount of space needed to store the recordings) and quality. We have chosen to go for a high quality which results in a high bandwidth.

An hour of recording takes up 16Mbytes of space. The audio recording duration is a function of the size of the MMC or S/D card. A 128 M-Byte MMC holds over eight hours of recording. A 1.0 G-Byte SD card holds 64 hours of recording.

7. The certified audio recording can be copied to a Personal Computer via the USB 1.1 port. The audio can also be read using a standard MMC/SD reader if desired. The recorder cannot delete a file on the MMC. In order to delete all recordings on the MMC or SD card the memory cards must be plugged into a recorder and cleared by a USB transferred command from the software running on the PC.
8. At least twenty-four hours of continuous recording are possible with two (fresh) AA cells.
9. A Smart Card chip is used for the cryptographic functionality, both for rapid operation and to guarantee the security of the secret keys.
10. The audio can also be encrypted to ensure that only the intended party access the recording from the recorder. The recorder cannot decrypt the recording. Only authorised parties in possession of the correct USB control tokens can decrypt the audio files. Please see the section on Windows 2000 and XP based Control Systems.
11. The recorder has an on-board playback mode. The user can select audio files (tracks) and fast forward and reverse within the audio file. However there is no visual display of the track number or position within the recording. Playback is

only allowed if authorised by the system controller and the audio file has not been encrypted.

12. There is an external 6V DC external power socket. The user is advised to fit the internal AA batteries even when running from the external power supply. In the event of an interruption to the external power supply the internal AA batteries will act as a hot stand by for the recorder. This will result in one continuous recording even in the event of power interruptions. There is no charge drawn from the batteries when the recording is running from the external power supply.
13. The gain of the audio circuit is controlled in a digital manner. The user can change the gain settings using the USB port. The gain settings on the internal and external paths are independent.

It is possible to manually alter the audio gain setting of the by entering a special set up mode.