

A Certified Evidence Enrolment System

CypheRix (Pty) Ltd

Author: Simon Rix
Short Title: Electronic Evidence Enrolment
Customer: Internal
File: CypheRix_EvidenceEnrolment.doc
Classification: **Confidential**
Revision: Draft 1.6

Table of Contents

Table of Contents ----- 2

List of Figures ----- 2

1 CypheRix Evidence Enrolment for eGovernment and Business----- 3

1.1 Introduction ----- 3

1.2 Executive Summary ----- 4

1.3 Security Summary ----- 5

2 System Component Description ----- 6

2.1 Data Enrolment Overview ----- 6

2.2 The Evidence Enrolment Device----- 6

2.2.1 Audio Cassette Digitiser 9

2.2.2 Integrated Fingerprint 9

2.3 CypheRix USB Control Tokens----- 9

2.4 Master Controller ----- 10

2.5 Local Controller ----- 10

2.6 USB Token Certification Authority.----- 11

List of Figures

Figure 1: Example System..... 3

Figure 2 Block Diagram of the Evidence Enrolment Device..... 7

Figure 3 The Assignment of and Evidence Enrolment Device to a Local Control Function..... 10

1 CYPHERIX EVIDENCE ENROLMENT FOR EGOVERNMENT AND BUSINESS

1.1 Introduction

CypheRix one of the consortium members who will possibly perform the evidential enrolment of all electronic demographic information by the Department of Home Affairs in South Africa. The system also meets the requirements for other interested parties such as business, justice and law enforcement.

This document seeks to give a technical introduction to the Evidence Enrolment System designed and manufactured by CypheRix.

A typical system will consist of the Evidence Enrolment device, a PC and various other components used to capture data. In the demographic example the type of information will include:

- a. Demographic Finger Prints (for example 1024 DPI unprocessed raw images)
- b. Photographs.
- c. Signature Capture using a digital tablet.
- d. Scanned Documents.
- e. Fingerprint templates used to prove the enrolling official.
- f. Fingerprint templates of the applicant's acceptance of the presented Abode form.
- g. Audio Recordings.
- h. Any other information required.

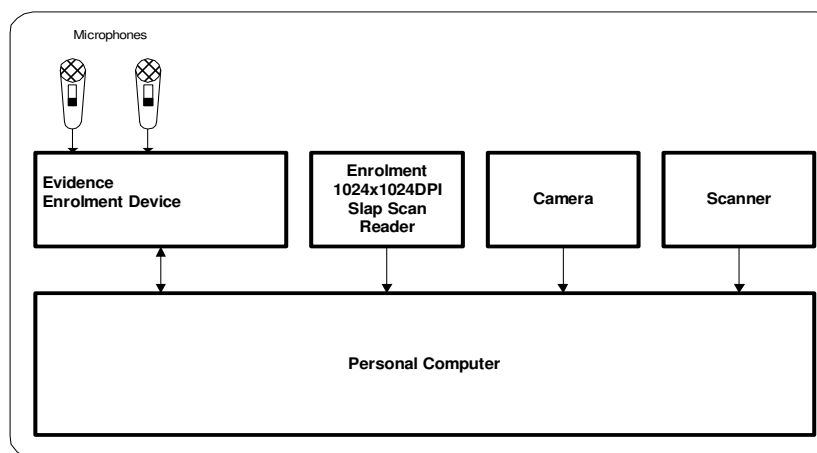


Figure 1: Example System

There are currently two existing variations of this novel equipment, all versions support the signature of files sent on the USB port. A brief summary is given below:

- a. Voice only.

- b.* An Audio Cassette Digitiser.
- c.* Integrated a fingerprint reader is being discussed.

1.2 Executive Summary

The Evidence Enrolment System offers system designers the following features:

- a.* The ability to enrol information in remote places or when the system is off line.
- b.* The ability to show that all demographic information is original and has not been tampered with even by the enrolling state entity.
- c.* A unique combination of voice recording with the ability to sign any documents submitted via the USB port.
- d.* The use of one-time RSA signing keys gives a high resistance to hardware attacks trying to discover the cryptographic secret key with a view to altering the enrolled information.
- e.* There is no Secret RSA exponent to attack. Others have to try and show that it is difficult to find the key. We can easily prove to non-technical (legal) people the strength of our products. We all know it is difficult to defend a static target.

The Evidence Enrolment System has following features:

1. The Evidence Enrolment Device will be used to digitally certify all the demographic information as it is enrolled and to make a certified audio recording of the interaction between the DHA official and the applicant. The audio recording is a separate file which goes to it's own database.
2. The Evidential Enrolment System makes use of 'One Time' RSA keys (see more detailed explanation below) to certify (create a digital signature) both the audio recording and the electronic demographic information submitted to it. Each data element will receive it's own certificate signed with the newly created RSA signing key.
3. At the end of the session the RSA secret key (RSA secret exponent) is deleted. This locks all information certified as without the secret key one cannot change the certificates.
4. As the same One Time RSA key (A File Level RSA Key Pair in our system) to sign both the audio stream and any electronic demographic information submitted it can be shown that all the information was enrolled during the same session.
5. The Evidence Enrolment System has been designed to withstand the most invasive technical attacks yet be simple enough to be explained to non-technical people. This will allow the Department of Home Affairs to show to the world that they have not changed any electronic demographic information on their system or databases without entering in to complex explanations of the entire system, audit trails and database security.
6. The Evidence Enrolment Device will generate certificates for enrolled data file that are appended to the fingerprint, photograph or scanned document. This allows all interested parties to cryptographically validate any data element in the Database. This will allow the separate data types to be extracted from the completed Form and sent to separate databases.

1.3 Security Summary

Our solution has the following security advantages:

1. The use of 'One Time' RSA keys locks the evidence immediately on enrolment.
2. There is no Secret RSA exponent to attack. Others have to try and show that it is difficult to find the key. We can easily prove to non technical (legal) people the strength of our products. We all know it is difficult to defend a static target. We were successful four years ago in extracting a 128 bit AES secret key using a variation of Differential Power analysis from a 0.35 micro smart card. We determined some 86 bits using power analysis and determined the rest by a brute force attack that took a single PC one weekend. If the key is static it can be found given enough time, money and interest.
3. Our product can operate completely off line. Once the session is complete the evidence is enrolled.
4. All RSA secret keys are generated up the device that uses it. There is no passing of secret information during personalisation.
5. A unique 2 out of 3 Cryptographic Token arming system for the control of the Evidence Enrolment devices.
6. Cryptographic control of the date and time.
7. Large RSA key sizes. The One Time RSA File Level Key pair's modulus is 1024 bits. The more senior keys are 1600 or 1536 bits.
8. Strong defence against preliminary known birthday attacks on SHA-1.

2 SYSTEM COMPONENT DESCRIPTION

This section gives an introduction to the data enrolment strategy proposed and the CypheRix Evidence Enrolment System elements. More details about the cryptographic methods and algorithms used are given in later sections.

2.1 Data Enrolment Overview

A brief description of the enrolment of electronic demographic information is now given:

1. At the start of a session the Evidence Enrolment Device generates a unique Session Index Tag. This Tag will allow all data elements to be bound together and of the validation of the Evidence Enrolment device used at any time in the life of the data being certified.
2. The Evidence Enrolment Devices generates a unique 1024 RSA signing key pair for each session (for clarity this is the same RSA key used to certify the audio stream and data files). The new secret RSA key is used to sign all certificates. At the end of the session the newly generated RSA secret key is deleted. This effectively locks the certificates. This is unique to the CypheRix Evidence Enrolment system and gives users confidence that documents enrolled are not tampered with.
3. Audio and any electronic information (files) will be sent to the Recorder and certified using the newly generated (One Time) RSA File Level Secret Key. Each element gets its own certificate. Hence each element can be independently validated as unchanged. Given the same "One Time" RSA key was used it can also be shown that all elements were signed at the same time.
4. Further each certificate has a date and time stamp. The user cannot alter the date and time in the Evidence Enrolment device. It is under the cryptographic control of the system administration (the local controller is in control of the date and time settings in all Devices that have been allocated to it).

2.2 The Evidence Enrolment Device

There are several versions of this equipment. The base version of the Evidence Enrolment Device is a USB2 interfaced device and has the external interfaces:

1. A USB2 interface used to submit external documents for signature and to control the Evidence Enrolment device. The device is also powered by the USB interface.
2. Two audio inputs. Each audio input can be configured either for an external microphone or to be a line input. Each channel has a 20Hz to 20KHz audio bandwidth.

Should the user enable both microphone channels they are summed before compression on to one channel.

We use ADPCM as the compression scheme. ADPCM is not the best compression scheme from a bandwidth perspective but it has excellent voice quality. The emotional tone of the conversation is clearly discernable. We support various sample rates. With an 8 KHz sample rate the device stores 16Mbytes per hour)

3. A 3.5 mm stereo headphone to allow the user to directly monitor the microphone inputs. (Channel1 appears on the left ear and channel 2 on the right ear).
4. An external button which if held in on power up will cause the Evidence Enrolment device to enter the loader mode.
5. A LED bezel to indicate the presence of power.

The block diagram of the device is shown below.

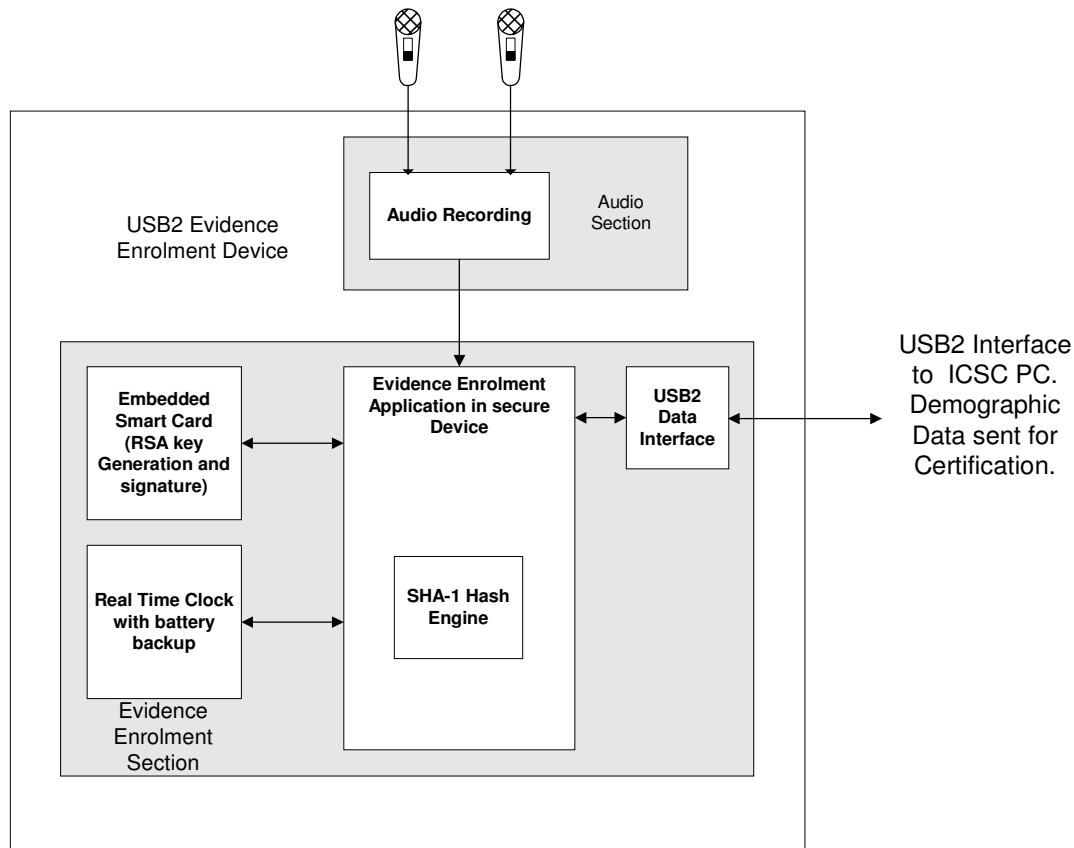


Figure 2 Block Diagram of the Evidence Enrolment Device

A functional overview of the Evidence Enrolment PCB is given below:

1. The heart of the device is an Atmel Smart Card in chip form. The Smart Card is used for:
 - a. The signing of all Digital Certificates for documents. These signatures are signed using RSA. The modulus size of the signature is 1024 bits. Each signature will take between one and two seconds.
 - b. The Smart Card is used to generate all RSA keys pairs used by the Enrolment Device. The Smart Card has an internal, Federal Information Processing Standards 140 (FIPs) certified, random number generator. The random number generator is used for all asymmetric and symmetric key generation.

- c. The Smart Card holds the unique cryptographic identity of the Evidence Enrolling Device.
2. A real time clock. The time is added to all document digital certificates. The time can only be updated by the assigned Local Controller. The time update function is sent as part of the updating of the Sequence Level Key and is cryptographically controlled. It is not possible for a user to alter the time. All the user can do is to reset the time to DOS/Unix time 0 which is 1970. Please note that this time will role over in 2106. At present in the audio Evidence Enrolment Device we allow the device to operate in this condition. In the DHA system I propose that we change this feature so that the device will not operate until the time is set. Given that the Evidence Enrolment Devices are normally connected via the network to the Local Controller the time can be updated with in a few minutes in the event of it being lost.
3. The Evidence Enrolment Device will be able to receive data from the Personal Computer at more than 1 Mega-Byte per second on the USB2 interface. The FPGA is able to generate a SHA-1 hashes for in the certificates at the speed of reception. Once each data element is available it must be immediately sent to the Smart Card for signature. This will reduce the time period between when the current session ends and the next session may begin.

Optionally the audio file may be encrypted (if that option is taken) using the AES symmetric block cipher in custom chain mode. The rump of the packet will be encrypted using a cipher text stealing technique.

4. The audio section will have a dual CODEC. When a recording is initiated the user can select between left channel, right channel or the sum of the two channels. Further there is a selection as to balanced or unbalanced sources.

There are two balanced audio input channels with two microphone inputs each using a separate 3.5 mm audio connector. There will be a stereo headphone monitor point using 3.5mm audio connector. The recorder will support +18V Phantom power for external microphones. The audio will be compressed using ADPCM compression.

- a. Audio Input 1. External microphone balanced input suitable for microphones such as the Beyerdynamic MPC22 with 18V phantom power. Two microphone level options exist:
 - i. The standard options is -38 to -26 dBV/Pa.
 - ii. This can be adjusted to -30 to -14 dBV/Pa.
- b. Audio Input 2
 - i. Balanced line input suitable for a conference system line output. The standard configuration is -20 dBV input level ± 3 dB or this can also be configured to $+3$ dBV input level ± 3 dB for Beyerdynamic. With this option there is no phantom power.
 - ii. A second external microphone input as per audio input 1.

2.2.1 Audio Cassette Digitiser

We had integrated our electronics with an audio cassette digitiser from Graff. This allows the user to digitise the cassette at 4x speed.

The application software that accompanies the device allows for the capture of a case number and description 'index record' as well as a photograph of the tape. The software allows for the control of up to 8 concurrent devices at one time.

The composite file is placed into an export directory for collection by the database system provide by an IT integrator. The 'index record' is placed early in the file to allow the IT vendor to read the 'index record' as use it for indexing in their application.

2.2.2 Integrated Fingerprint

We have developed other products using Suprema fingerprint readers. We can integrate this fingerprint reader with the Evidence Enrolment Device relatively quickly.

This will allow for the extremely strong enrolment of people. For example:

- a. The interview can be recorder and all details of the individual captured verbally.
- b. The fingerprint can en enrolled is a very conservative manner. The resulting fingerprint template is signed and added to the composite file. The template will be taken directly from the fingerprint reader and signed before it leaves the Evidence Enrolment device.
- c. A previously enrolled fingerprint can be returned to the Evidence Enrolment device and compared to the fingerprint that is presented. The results of this validation are captured and signed as part of that interview.

The applications where is can be used are not discussed here as that is seen as our partners competitive information and advantage.

2.3 CypheRix USB Control Tokens

Currently we use USB control tokens to control the Evidence Enrolment System. All RSA secret key cryptographic functionality is done inside the armed USB Control Token.

Three USB Control tokens are married together into a family. The intension of this is that each USB token can be given to a different person for safe-keeping. The USB token on it's own is useless. One needs to have two of the three members of the USB token family present to do arm (or enable) the Local or Master Control system.

Each Local and Master Control function (as discussed below) has a Secure Data Base that is encrypted using a Super Master Key (SMK). This SMK is shared using a 2 out of 3 share scheme between the family members. Two of the three USB Tokens must be present in order to arm the system as the individual share each token has cannot be used to arm the system.

In the arming process the two tokens check the legitimacy of the other party and only combine their respective share to form the SMK once they are satisfied of the others identity. The re-combining process results in one of the two USB tokens involved being armed in that the SMK is re-constituted by re-combining the cryptographic shares.

As stated before tokens are married into families of three devices.

The System consists of Master Controller, the Local Controller and the Evidence Enrolment Device itself. The relationship between these three elements is shown in the diagram below:

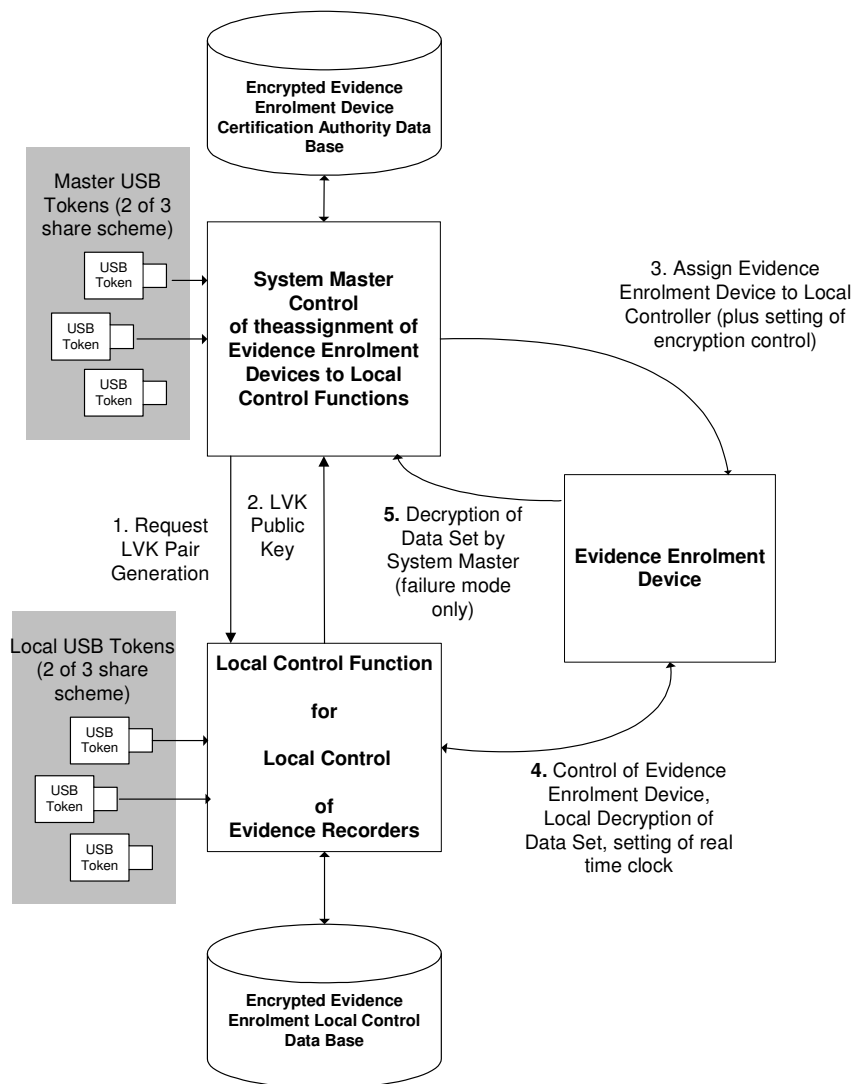


Figure 3 The Assignment of and Evidence Enrolment Device to a Local Control Function

2.4 Master Controller

The Master Controller is the Certification Authority and owner of the Evidence Enrolment Devices. The Devices as assigned (or re-assigned) to Local Controllers as operational circumstances dictate.

It is possible to use any HSMs from other vendors as the master function for Evidence Enrolment Devices. (It is not economic to use HSMs for the Local Control Functions so the CA authority may still be required of the manufacture of USB tokens).

2.5 Local Controller

The Local Controller (if the Evidence Enrolment Devices is assigned to it) can perform the following functions:

1. Decrypt the encrypted files (audio and data).
2. Set the Time.
3. Update one of the RSA keys used in the enrolment system (Sequence Level Key).

2.6 USB Token Certification Authority.

USB Control tokens have their own CypheRix Certification Authority and Marriage function.

It needs to be discussed with DHA if they wish to purchase a USB Control Token Certification Authority. If DHA keeps the all three of the Master USB tokens in a separate place CypheRix cannot access the Master Database.

It is however probable that each customer will wish to purchase their own Token Certification Authority.