

A Brief Description of the Certified Audio Evidence Recorders

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 Certified Audio Evidence
Recorders

File: CARec_BriefDescription-051116.doc

Classification: **Confidential**

Revision: Draft 1.07

Date Release : 16 November 2005

AN OVERVIEW OF CERTIFIED AUDIO EVIDENTIAL RECORDERS

Certified Audio Recorders are small, low-power, *audio* recording devices which secure the evidence recorded in a way that irrefutably guarantees it has not been altered.

Certified Audio Recorders establish irrefutability by a cryptographic digital certification scheme, satisfying the stringent demands of a court of law. Digital Certification removes the onerous 'bag and tag' requirements for audio evidence.

This 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.

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.

All the information required to establish the Digital Certificate Hierarchy is combined with the certified audio data into one single file for easy storage.

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. 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) 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 Recorder. 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 security token.

The audio recording may, under the control of the system operator, be encrypted. This is a separate function from the certification function. The USB security token ensures that only the System Operator can decrypt the audio. This may be used to protect audio between the recorder and the system operator or to allow an encrypted copy of the recording to be stored and only decrypted when required.

More information on the cryptographic architecture is available on signing a mutual NDA agreement. 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.

The Certified Audio Recorder - Field Model

Here is a summary of the features of this version of the recorder:

1. The Certified Audio Recorder has an internal Knowles microphone as well as a 3.5 mm socket for an external electret microphone. The microphone used is the Knowles WP-3502. This microphone is water resistant and will recover from submersion in 1 meter of water (the rest of the electronics may not survive!).
2. There is an external microphone 3.5 mm socket. A phantom power of 1.5V is available to power external electret microphones. In the current version of firmware the external microphone is automatically selected if the presence of an external microphone is selected. There is currently no manual override mechanism to allow the user to force the selection of the microphone. When the recording is started the Recorder will check to see if there is an external microphone. A selection now made between internal and external microphones which is retained through out the recording.
3. The Recorder has an excellent audio quality in the range of 40 Hz to 4KHz with a dynamic range of > 70 dBs. Simply put "Hearing is believing". In most applications the internal microphone is completely adequate.
4. The Recorder performs ADPCM compression. This is a moderately aggressive compression method which results in excellent quality (at the expense of some space). In order to limit the recording storage space required we have limited the audio sampling rate to 8KHz.
5. The certified audio information and the certificates are stored on an industry standard Multi Media Card (MMC) or Secure Digital (SD) Card.
6. 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 device holds 64 hours of recording. At present we have tested the Recorder on 32, 64, 128, 256, 512 and 1024 Megabyte Kingstone MMC and SD cards. We have tested with other vendors MMC and SD cards and so far all most seem to work. (see 8)
7. The certified audio recording can be copied to a Personal Computer via the USB 1.1 port. The audio can be can be read using a standard MMC/SD reader if desired. If a USB two multi-media reader is used the copy time can reduce to 5% of the time taken using the recorders USB 1.1 interface. The software supplied with the recorder allows the user to either connect to the Certified Audio Recorder or to connect to a multi-media reader to access the MMC or SD cards directly. There is no method of deleting recordings except via the USB interface. This prevents accidental deletion of recordings in the field. At present all recordings must be deleted at the same time was the Recorder formats the MMC or SD media.
8. At least twenty-four hours of continuous recording is possible with two (fresh) AA cells. All our tests are done using Duracell "Copper top" MN15000 LR6 batteries. This time is dependant on the type of MMC or SD memory card used. All testes were done using Kingston 1Gbyte SD cards. (High speed SD/MMC devices give worse results). For this reason we recommend using selected Kingstone MMC or SD cards. As the availability of particular MMC or SD cards is hugely variable please contact us before purchasing more media.
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 Recorder has a real-time clock. The time is added to the certificates to record the time of the recording. The back up battery has a lifetime of greater than 5 years. The battery is not user changeable. In order to set the time the Recorder must be connected to it's currently assigned USB Local Token which will set the time in the Recorder in a secure manner. Hence it is not possible for an unauthorised person to change the time on the Recorder.
11. A slider switch activates the recording. The recording will be automatically restarted in the event of an interruption in the power supply. This slider switch can be mounted inside the recorder or externally next to the microphone. The recorder supports external activation via the 2.5 mm socket.
12. The Certified Audio Recorder adds secure Digital Certificates to the compressed audio. 1024 bit RSA and SHA-1 are used for this function. Each recording is signed with a newly generated secret exponent. The act of deleting the secret exponent after the recording locks the recording forever. The public exponent (and modulus) is added to the stored audio recording and is subsequently used to verify the recording.
13. There is an extra optional encryption scheme to ensure that only the intended party can recover the audio data and decrypt it. The recorder cannot decrypt the recording. The encryption version typically costs 50% extra as compared to the certification only version. In order to decrypt the recordings the user needs to purchase USB control tokens. The recording time suffers little degradation when encryption is enabled.
14. The recorder allows playback if allowed by the operator and if the audio file was not encrypted the device. 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. This makes the mode somewhat difficult to use.
15. During a recording the operator can enable the 'audio-echo' mode to allow monitoring of the recording. The output has a 16 ohm impedance.
16. The recorder has a 2.5 mm socket. This socket is shared between the mono headphone monitor and an external recording trigger. In order to activate the recorder the external recording control must simply be grounded. Hence a simple single pole toggle switch can be used to short the middle ring of the socket to ground on the outer ring. The plug has the following assignments:
 - a. The tip is mono audio output.
 - b. The middle ring is the external recording control.
 - c. The long outer ring is ground.
17. The user is able to measure the battery voltage via the USB interface. This is helpful given the long recording times achieved to minimise operating costs.
18. There is a DC external power socket for use with an external 5.5 – 9.5 Volt power supply. The internal batteries are connected in such a manner as to allow a 'hot standby' during recording. Hence if there is an interruption of the external power the recording will continue uninterrupted as long as the batteries have charge.
19. The gain of the audio circuit is controlled in a digital manner. The user can change the gain settings using the USB port when switching between different microphones. If a microphone with a high output voltage is used the first pre-amp

stage can be by passed. The recorder stores the two gain settings, one for the internal microphone and one for the external microphone.

20. It is also possible to manually alter the audio gain setting of the by entering a special set up mode. The audio echo mode is enabled here to allow the operator to set this up. The device has to be switched off to exit this mode. There is 74 dB of audio gain in the input circuit. To give you some idea of the available range the current recommended gain setting used for the Knowles WP-3502 microphone is 30-36 dB.

Physical Dimensions and Photographs

The current physical dimensions of the box are 125mm deep x 62mm wide x 24mm high. The quoted dimensions when viewed from the side of the box with the USB.connector.



Figure 1 Front view

The following external interfaces appear on the front face of the device from left to right:

1. DC power connector.
2. On / Off Slider Switch
3. External Microphone Socket
4. Internal Microphone
5. Socket for external control input and mono-audio output.
6. USB Connector



Figure 2 Rear View with Slide Open showing Second On / Off slider switch with two other special mode control buttons on either side.

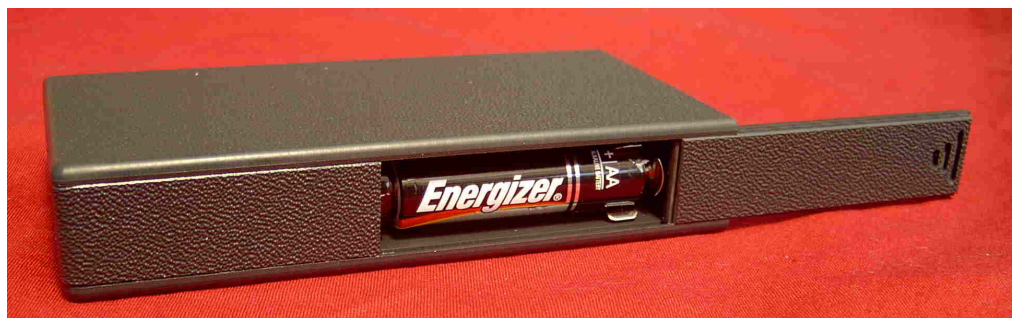


Figure 3 Side of the Device showing battery compartment

An Overview of the PC Based Control System

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

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

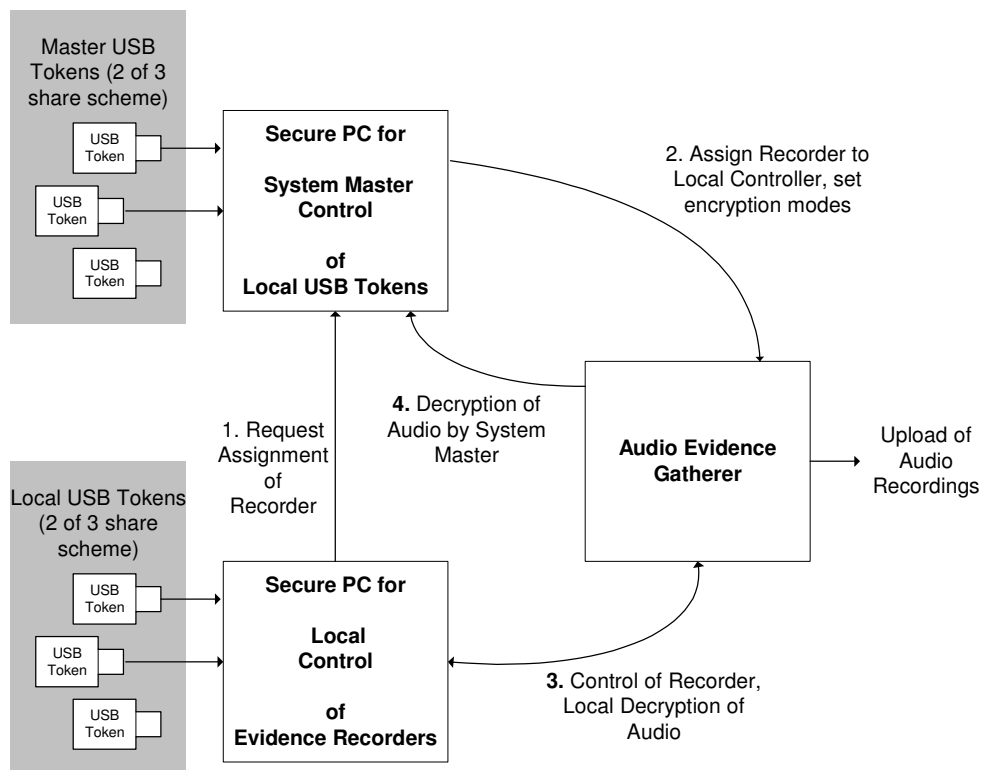


Figure 4 Overview Of the Control of Audio Recorders

The Local User controls the daily operation of the Recorder.

The Local User maintains a database of all Recorder 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 audio recordings from the Recorder using the USB port. 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 audio recording and periodically update keys in the Recorder. This is to ensure that earlier recordings are not compromised in any manner should the Recorder be subsequently lost.

USB Security Tokens

As cryptographic keys are used to control the recorder 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.

A Description of the PC Software

We allow the user to make as many copies of the software as they need. Often the same recorder is shared between several people.

The PC application software has the following functionality:

1. The user can connect to the Certified Audio Recorder and perform the following functions:
 - a. Copy a file (or files) from the Certified Audio Recorder to the PC. As part of the copy process the certified audio file is given a unique name (the unique name reflects the recorder used and other cryptographic details). This is done in such a manner as to guarantee that no other certified audio files can be accidentally overwritten.
 - b. Set the microphone gain (internal and external).
 - c. Check the time on the recorder.
 - d. Clear the MMC or SD card once all the audio files have been uploaded.
 - e. Check the battery voltage.

- f. Access details of the Recorder version and operation state.
 - g. Perform operator functionality such as generating new Sequence Level RSA key pairs or re-assigning the recorder to different Local Token sets. (One needs USB tokens for these functions).
2. Having uploaded the Certified Audio Files the user can:
- a. Check that the recording has not been altered. As part of the checking process the user can generate a cryptographic report of the check. This can be printed out and notarised to further enhance the evidence enrolment process.
 - b. During the check process the software will optionally create a wav file so that the user can listen to the recording.
 - c. View previous cryptographic reports.
 - d. The audio recordings (certified originals, wav files and the reports) are stored on the operator's PC. The recordings are according to the recorder that was used.
 - e. The user can add a description of the recording to the certified audio file to assist in the archiving process.
 - f. The software allows the user to easily extract all relevant information about a specific recording (certified file, wav file all reports) and to copy the data to a sub-directory. A standalone application is also copied to the sub-directory that will allow the recipient of the evidence CD to check that the recording has not changed. In the case of large recordings the stand alone software can also generate the wav files from the certified file to save storage space.
- The user can then use their preferred CD authoring software to create CD's of the recording.
3. The PC application can also be used to arm (or recombine) the USB control tokens so that the user can control the Certified Audio Recorders.
4. The software also keeps logs of all transactions done.

CE Approval

The Recorder has been successfully tested according to the following standards:

1. Radiated Emissions tests done according to CISPR22 Class B (Commercial and Light Industrial) from 30MHz to 1 GHz.
2. Radiated Susceptibility tests done according to IEC 61000-4-3 from 80 MHz to 1 GHz at a level of 3V/m (80% 1kHz AM).