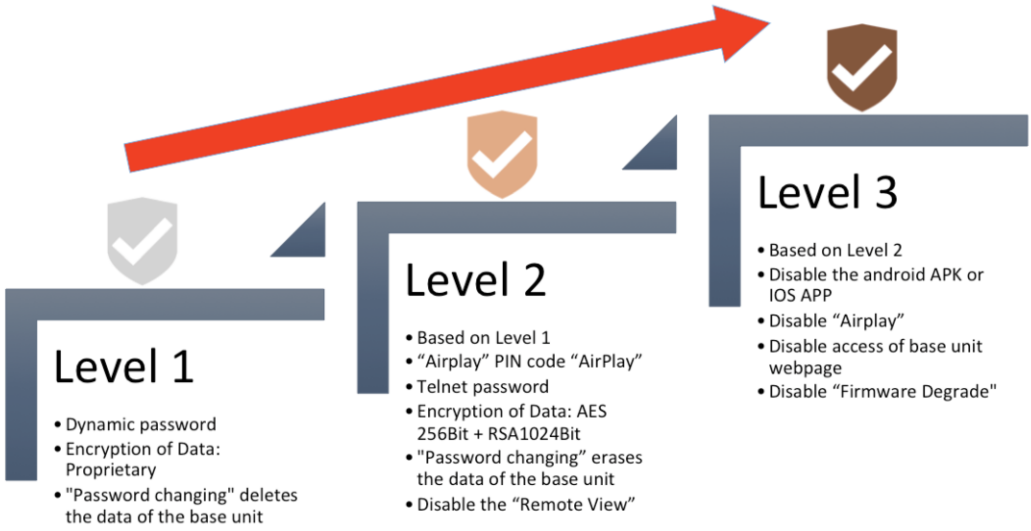
Kindermann Klick & Show

Security Level White Paper

WirelessMedia designs three different security levels to satisfy different security requirements, according to different security sensitive environments or security policies. It is divided into three different security levels; each refers to several different setting combinations, for several certain applications, such like

1. **Level 1**, keeps the security in normal and daily usage for any organization, such like classroom, regular meeting room etc.
2. **Level 2**, meets the need for higher security requirement for any organization, such like enterprise, global cooperation, government etc.
3. **Level 3**, meets the need for top-secret or national secret organization, such like financing institution, government etc.



Background:

WirelessMedia base unit can receive the media content from Microsoft Windows PC/Lap-top, MacBook, Android smart devices including tablet and smartphones, Apple smart devices including Iphone, Ipad etc.

A USB dongle, which is to be plugged into a PC/lap-top or, with the aid of an additional USB disk, with EXE/APP program inside it, including an a PC/Lap-top software driver (namely WirelessMedia "Launcher") which is to be copied and executed on a lap-top, is to capture the **VIDEO FRAMES** from the PC/Lap-top's video

frame buffer and **AUDIO** from the audio card, to be converted into one kind of data and transfer wirelessly to the base unit. **VIDEO FRAMES** is a string of captured pictures.

An APK (Android Package), which is to be installed into Android smart devices and run, is to capture the **VIDEO FRAMES** from the desktop of the android system, to be converted into one kind of data and transfer wirelessly to the base unit. In addition, the APK can also transfer media file content, including **PICTURES**, **VIDEOS**, and **MUSIC** etc. wirelessly to the base unit to be playback by the base unit.

In addition, this APK can transfer **OFFICE FILES** as original file format, including WORD, EXCEL, PPT, TXT and PDF etc. wirelessly to the base unit to be playback by the base unit.

An APP (Apple Application Program), which is to be installed into Apple smart devices and run, is to transfer media file content, including **PICTURES**, **VIDEOS**, and **MUSIC** etc. wirelessly to the base unit to be playback.

In addition, "**AirPlay**" is available one kind of wireless transmission technology with copyright by Apple Inc.

Memory:

WirelessMedia Base unit has a memory inside it, to store all the received media content, in the form of data. This memory consists two categories, including **RAM** (Random Access Memory) and **FLASH**.

RAM (Random Access Memory) is to receive the **VIDEO FRAMES** from the desktop of laptop, the **VIDEO FRAMES** from the desktop of the Android device, and the **MEDIA FILES**, including video file like *.mov, *.mp4 etc., music file like *.mp3 etc.

FLASH is to receive and store the **OFFICE FILES**, like Word, Excel, PPT, TXT, PDF etc.

Memory Deletion:

RAM (Random Access Memory) is volatile memory, which will be auto-deleted after power-off.

FLASH, is a non-volatile memory, which will not be auto-detected after power-off, unless the manual deletion. Manual deletion has two methods, **DELETION** or **ERASE**.

DELETION is a method, which is the same method as Micro-soft Company adopts in "Windows" operation system, refers to the act of eliminating a file, text, or another object from the computer hard other media. When data are deleted, they are only marked as such, but still exist on the hard drive until they are overwritten by other data. This condition is what makes data recovery possible.

ERASE is a method, to reformate the hard drive. When data is erased, they disappears and doesn't exist on the hard driver any more, thus the data can't be recover in future.

Password:

WirelessMedia adopts a connection password or **PASS**, for PC client software or Smart Device to connect to the base unit, to prevent the unauthorized device to access the base unit. This **PASS** is 8 digitals, which is shown on the centralized top of home page and could be transferred to other attendees orally, by written message or emails etc. Any change of this password will require all attendees to re-enter the new password to connect to the base unit.

WirelessMedia adopts an **Admin Password**, for administrator to enter when login the Setting menu on the home page to configure or manage the setting of the base unit.

Dynamic Password, is proprietary protection technology, to enable the password to be dynamically auto-changed every certain minutes or hours in a random algorithm, and stay on one password when the USB dongle connection or Wi-Fi connection to the base unit. This dynamic password technology adopts the sync technology to keep sync with the USB dongle, to avoid re-pair of the USB dongle when the change of password.

AirPlay "Pin-code", is an access code, which is appointed the same as the connection or **PASS** for AirPlay supportive device to enter before sharing the desktop.

Telnet Password, is a login password, which is appointed the same as the **Admin Password** for Telnet supportive device to connect and control the base unit over LAN (Local Area Network).

Encryption:

WirelessMedia adopts two different levels of encryptions, including **Wi-Fi SECURITY** encryption and **AES** (Advanced Encryption Standard) **PLUS RSA** encryption.

Wi-Fi security, is the prevention of unauthorized access or damage to base unit, using wireless networks. The most common types of wireless security are Wired Equivalent

Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. We currently adopt the WPA-PSK and WPA2-PSK.

AES, has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encryption and decrypting the data. The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.

The AES symmetric-key, is a pair of key, which resides transmitter and receiver. The key will change automatically every 30 seconds, to give the key-deduction effort into vain within 30 seconds.

RSA encryption is a public-key encryption technology developed by RSA Data Security. The RSA algorithm is based on the difficulty in factoring very large numbers. Based on this principle, the RSA encryption algorithm uses prime factorization as the trap door for encryption. Deducing an RSA key, therefore, takes a huge amount of time and processing power. RSA is the standard encryption method for important data, especially data that's transmitted over the Internet.

RSA encryption is to encrypt and transfer the AES key, by transferring the public-key from base unit to the transmitter and following encrypted transmission. The transmitter includes USB dongle, PC/lap-top software driver (namely WirelessMedia “Launcher”).

The RSA asymmetric-key, is a set of key, which initially resides on the base unit, of which the public-key will be transferred to the transmitter when the transmitter has synchronized with the base unit. The key will randomly changes, according to the changing frequency of the Wi-Fi password, and stay on one after the Wi-Fi password stays. Thus, it gives a very short time of a stable key status, to be very hard for key-deduction.

Note that, the RSA key changing time, which is equal as the Wi-Fi password, could be configured as auto-changeable from 5s to 30minutes.

PC Client Software Digital Signature:

The PC/Lap-top software driver (namely WirelessMedia “Launcher”), including either EXE program for Micro-Windows PC/Lap-top or APP application for Apple MacOS MacBook, which is to be copied and executed on a lap-top, has been protected by **Digital Signature**, to guarantee the legality, integrity and the responsibility.

The Digital Signatures include

1. WirelessMedia-Windows.exe driver for Micro-windows has been authorized and signed by the program of EV digital code in the name of “Wireless Media Tech Co., Ltd. ”, using the encryption key Microsoft-Windows authorized.
2. WirelessMedia-MacOS.app driver for MacOS has been authorized and signed by “Wireless Media”, with the development ID UZWBZDR665.

Digital Signature for Windows is a protection procedure, to show whether the PC/Lap-top software driver is the original one, by the authorized developer, by chopping the certificate. User could right-click the “property” of WirelessMedia-Windows.exe driver on Windows OS (operation system), and click “certificate" tab to find the digital signature.

Digital Signature for MacOS is a protection procedure, to show whether the PC/Lap-top software driver is the original one, by the authorized developer, by chopping the certificate. User could right-click the “property” of WirelessMedia-MacOS.exe driver on MacOS, to see it in the “copyright”.

It guarantees
Authentication: The driver is released by authorized developer.
Integrity: Any revision of PC/Lap-top software driver should be chopped by the Digital Signature, before it is formally released to public, to guarantee it’s identical as the original one.
Non-repudiation: It can’t be denied from the manufacturer, that the driver signed by WirelessMedia, is not sent or sold by WirelessMedia.

See more details about digital signature at the link of https://en.wikipedia.org/wiki/Digital_signature

Security Levels

	Security Level 1	Security Level 2	Security Level 3
Performance			
USB dongle or PC software “Launcher”	Yes	Yes	Yes
APK or APP from smart device	Yes	Yes	No
“AirPlay”	Yes	Yes	No
Access Webpage of base unit	Yes	Yes	No
Remote Viewing of the main screen from mobile device	Yes	No	No
“AirPlay” PIN code	No	Yes	No
Latency	20-130ms	20-140ms	20-140ms
Data Encryption			
Wi-Fi Access Password	Yes	Yes	Yes
Dynamic Password	Yes	Yes	Yes
Telnet Password	No	Yes	Yes
Wi-Fi Security	WPA-PSK /WPA2-PSK	WPA-PSK /WPA2-PSK	WPA-PSK /WPA2-PSK
Encryption of data	Proprietary	AES 256Bit + RSA1024Bit	AES 256Bit + RSA 1024Bit (optional 2048Bit)
Deletion of RAM	ERASE (Auto-Erase after power off)	ERASE (Auto-Erase after power off)	ERASE (Auto-Erase after power off)
Deletion of FLASH	DELETE (Password change deletes the data in the memory of base.)	ERASE (Password change ERASE the data in the memory of base.)	ERASE (Password change ERASE the data in the memory of base.)
Firmware Degrade	Yes	Yes	No
TOTAL			
Performance	Best	Good	Good
Security	Low	Medium	Top-secret