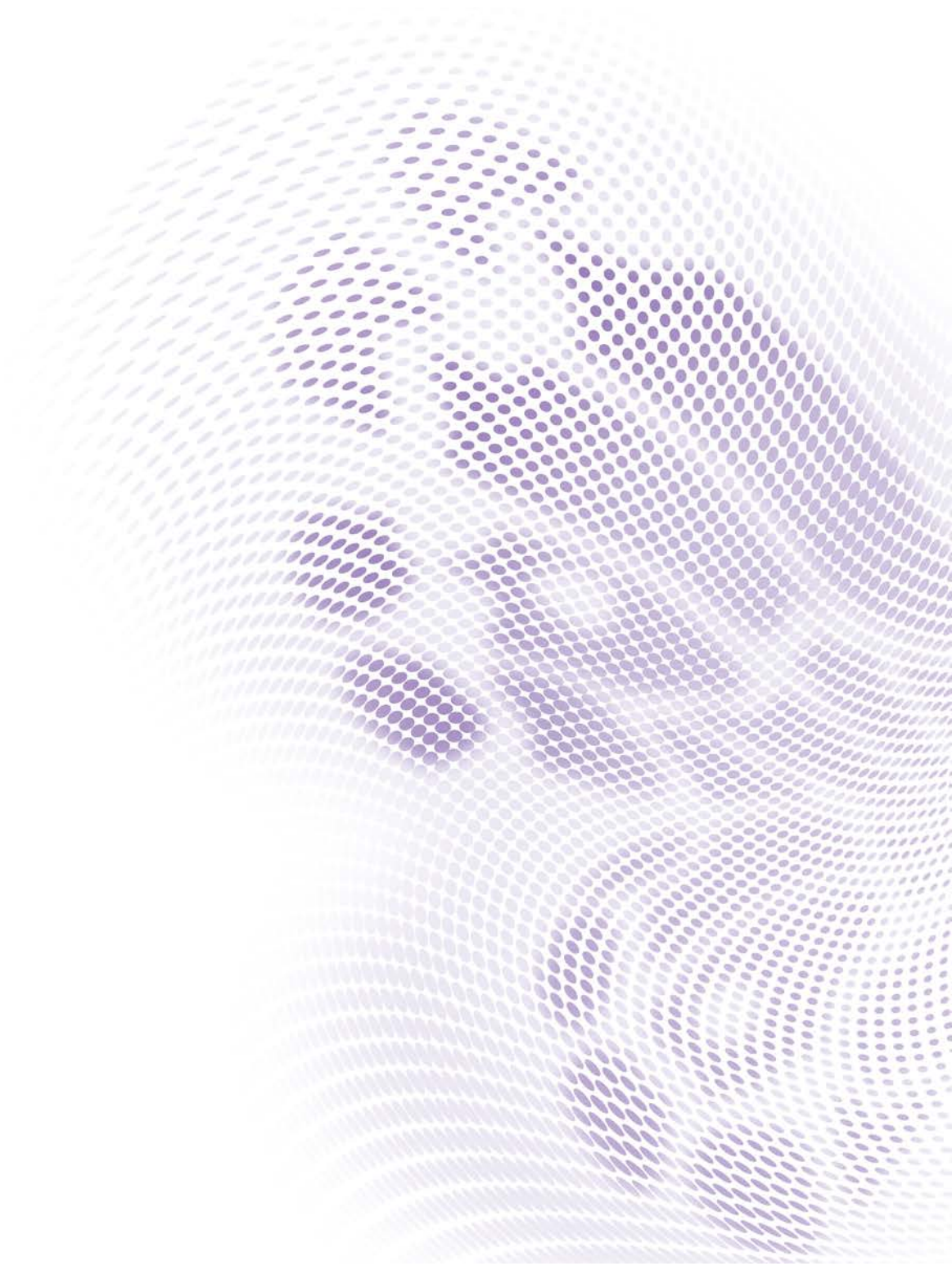
# WDC10
# InstaShow™
# Security White Paper



# Table of Contents

# Introduction

InstaShow™ is a next-generation commercial display solution, which code is WDC10. This product is primarily featured of high definition, plug-and-play, no driver software, and configurable security.
For a next-generation commercial display solution, a wireless connection method is used to replace a traditional wired connection, and a security mechanism is added to this wireless streaming path to provide a secure wireless transmission scheme. Since InstaShow™ imaging interface is a high-definition multimedia interface (HDMI), if a device on a client supports HDMI output, there is no need to worry about the requirement for execution of additional software. As such, it prevents malicious software attacks or threats, and may ensure that customers and users of InstaShow™ are protected. This is why we are concerned about security, and streaming data protection is one of our major design criteria.
This white paper focuses on security, including details of architecture and technical control for InstaShow™.

# The InstaShow™ System

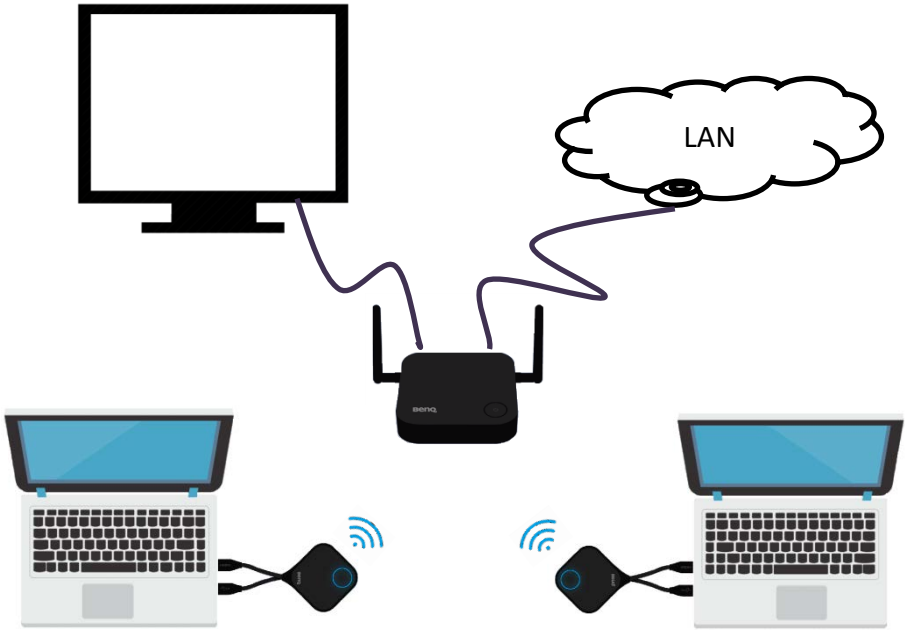
BenQ released WDP01, the first generation wireless video & audio transmission product, in the end of 2014, followed by releasing InstaShow™ (WDC10), the first generation commercial wireless image transmission display scheme, in the end of 2015. The release of InstaShow™ provides a new wireless image transmission concept in the market.

## The InstaShow™ Setup

Two main capabilities are implemented for InstaShow™ product. For the first capability, everyone is allowed to have the opportunity to share contents by simply clicking the button on InstaShow Button to present a content on the home screen. For the second capability, the content on the home screen is switched to a content of another sharer quickly and easily without waiting for system installation.
InstaShow™ product consists of:
Host: This is the core of the entire system and the receiving equipment as well, which can establish wireless connections with 16 Buttons concurrently, and is mainly responsible for receiving the streaming data delivered by Button as well as for ensuring that video & audio is displayed on the display device correctly.
ITS staff of an enterprise can add Host to an enterprise domain through a LAN port. When Host becomes one of the equipment in the enterprise domain, the Web UI provided by Host can allow the ITS staff to monitor the status of InstaShow™ remotely.
Even if Host becomes one of the domain equipment in a local area network, the monitoring staff still cannot obtain the content of the streaming data through intrusion or threat.
Button: This is the transmission device of the entire system. USB cable is mainly responsible for system power supply, and HDMI cable is for receiving video & audio data in HDMI format, such as laptops, PS4,

Blu-ray/DVD players etc.

By clicking the button on InstaShow Button, it will compress HDMI streaming signals as video & audio codes, which are sent to the display device connected to Host side via Wi-Fi immediately.




## System physical interface and firmware introduction

The operating system for InstaShow™ Host and Button is embedded Linux OS. Linux OS acts as

*. Bootloader access*

*. Linux CLI access*

Physical I/Os of Host include:

.LED

*GPIO control*

.Button(s)

*GPIO Scan*

.Ethernet:

*Web UI*

*REST API*

*Communication with Client*

.Wi-Fi:

*Web UI*

*Communication with Client*

.Micro USB

*Power supply*

.HDMI

*Video / Audio output*

Physical I/Os of Button include:

.LED

*GPIO control*

.Button(s)

*GPIO Scan*

.Wi-Fi:

*Communication with Host*

.USB:

*Power supply*

.HDMI

*Video / Audio input*

# The InstaShow™ is a strong security system

For InstaShow™ product, in the early stage of development, system designers and R&D engineers provided a number of solutions for threat and security of wireless transmission, modules which eliminate security threats by system modularization, together with several module improvements to result in the InstaShow™ architecture.

## Power Consumption Module System

The power system for Button and Host of InstaShow™ uses DC 5V to DC 3.3V conversion as the main supply voltage for the system. According to the law of energy conservation, the supply current is increased by reducing the voltage, such that low power is sufficient to support the operation of the entire system. The power consumption module system passes 20,000 hours of long-term MTBF power supply verification, and Host complies with (EC) No 107/2009 Regulation.

## Video & Audio Module System

The source interface of InstaShow™ video & audio is HDMI. HDMI is an all digital image & sound transmission interface, which is capable of transmitting uncompressed audio and video signals. HDMI can transmit audio and video signals simultaneously and is protected by HDCP regulation. The HDMI input source or output source for InstaShowTM system is compliant with regulations for HDMI 1.4b and HDCP 1.4b certifications. Devices of Source and Sink support HDMI 1.4b / HDCP 1.4b, both of which are compatible with InstaShowTM.

The certification number obtained for InstaShowTM is ATCTW-16031 (Host), ATCTW-16032 (Button).

## Video & Audio Encoding/Decoding Module System

HDMI interface is for uncompressed audio and video signals. The amount of data for uncompressed 1080p@60Hz audio and video signals is huge. If wireless transmission is used for this large amount of streaming data without compression, a considerable bandwidth will be occupied inevitably. In order to solve such a dilemma, InstaShow™ imports video & audio encoding and decoding methods for compressing the

bandwidth required for video & audio to 40Mbps. Also, R&D engineers are devoted to the balance between audio & video quality and transmission bandwidth usage, and further import dynamic encoding techniques to adjust the compression ratio dynamically in conjunction with the quality of the wireless bandwidth in the environment.

## Wireless Transmission Module System

The Wi-Fi transmission protocol for InstaShow™ is 802.11ac with WPA2 AES 128 bits encryption mode, and WPA2 is the best encryption technology for Wi-Fi connection at present stage.

However, existence of vulnerabilities for WPA2 is reported recently: "An attacker in the wireless range of Wi-Fi network can exploit these vulnerabilities through **Key Reinstallation Attack** (KRACKs). According to the research report for KRACKs provided by Mathy Vanhoef, the attack is targeted to the 4-way handshake mechanism of WPA2 for client equipment (for example, laptops, smart phones or tablets etc.), instead of using the base station." For more information about KRACK, click this link: https://www.krackattacks.com

Host of InstaShow™ is a base station, and Button is a client equipment. Although Button is affiliated to the client equipment, Button system is a closed system, so that external threats cannot reside in and attack the system through HDMI interface or pure power supply purposed USB interface.

Wireless transmission module system also passes certifications of RF security regulations of various countries, such as CE (EN 301 893), FCC (47 CFR FCC Part 15.407), NCC (NCC LP0002), TELEC (ARIB STD-T71) and so forth.

## WAN/LAN Module System

InstaShow™ is a closed wireless local area commercial display scheme, and Host is not capable of WAN access. When the WAN port of Host is connected to an enterprise router, the enterprise router provides Host with access to the Internet. However, any wireless equipment, such as a smart phone or a laptop etc., which connects to SSID of Host, cannot access information of Internet through Host, so that external hackers cannot intrude into the wireless equipment on a client by Host.

The WAN/LAN module of InstaShow™ is provided mainly for users to configure the system. The interface for configuration is Web UI.

## Web UI management module system

InstaShow™ is capable of Web UI management. Web UI can query system status, Wi-Fi settings, system updates, etc. A device of a user can connect to the SSID of Host through Wi-Fi or connect to Host by using LAN. The user is required to provide an account and a password to login the home page of Web UI.

## Light Module System

InstaShow™ provides a friendly indication system. A light indicator is the most direct prompt approach for InstaShow™. The ring light on a button displays current status of the system intuitively. System designers and R&D engineers use special means to soften point light sources, which do not stimulate vision, so that the user feels comfortable to read the status.

## EMI/ESD Module System

InstaShow™ can prevents network hacking attacks. Also, the engineers further adhere to security regulations for products. InstaShow™ is compliant with EN55032 and EN55024 regulations.

## PCB Module System

InstaShow™ is also dedicated to the prevention of hazardous substances and environmental pollution, such that PCB meets lead-free, halogen-free environment friendly processes for printed circuit boards; there is a comprehensively planned control mechanism from control of raw materials, material picking process to post inspection and inventory check.

## BenQ ecoFACTS Self-declaration

Since 2011, ecoFACT green labels have been added on all products of BenQ, which clearly indicate green designs and green materials used by BenQ products.

To develop earth friendly green products, BenQ vitalizes all of its products by promoting green policy actively, instead of making products compliant with green regulations passively!

InstaShow™ adheres to ecoFACTS regulation, indicating that the best effort has been made for replacement of hazardous substances, material selection, package design, energy-saving design and other aspects.

# Streaming flow protection

Through threat analysis of system modeling, the security of the system can be divided into external hacking and internal protection management. Regardless of the threat, its purpose is nothing but destruction and theft.

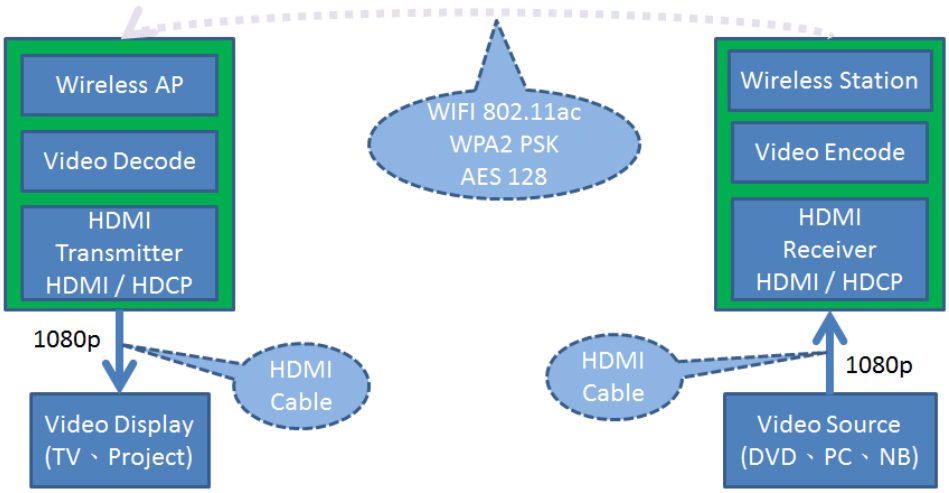
InstaShow™ is a wireless network transmission display system. The network system of InstaShow™ is not capable of external network access and can avoid invasion of external hackers. InstaShow™ video & audio transmission interface is based on HDMI, and software support is not required for video & audio streaming path. The biggest security threat in an enterprise is software. InstaShow™ does not have the software requirement about which an enterprise is worried, and can meet the need of an enterprise which requires wireless multi-user screen sharing.

## InstaShow™ system architecture

For the operation flow of InstaShow™, Button receives video & audio streaming signals from Source device HDMI, and transmits the video & audio streaming signal to Host in a wireless manner, followed by transmitting the video & audio streaming signal to Sink equipment by HDMI.

According to the procedure of process, InstaShow™ system architecture is categorized into:

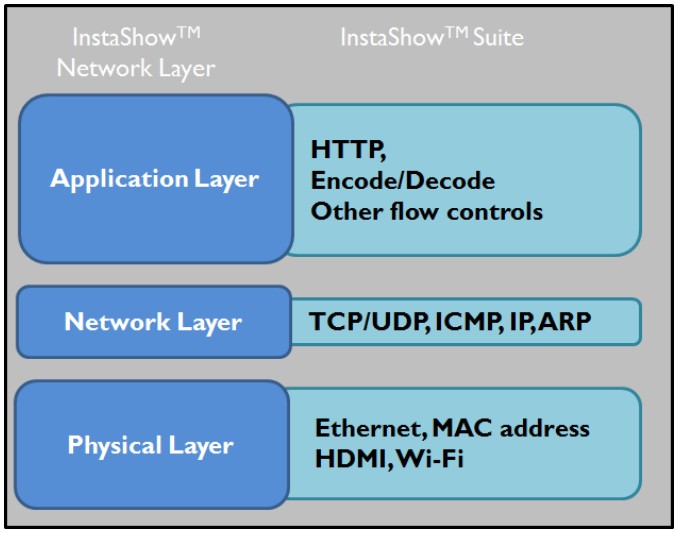
(1) HDMI signal decode
(2) Video and audio signal compress
(3) Video and audio stream with encryption over Wi-Fi
(4) Video and audio signal decompress
(5) HDMI signal encode




| Flow | Transmission medium/interface | | Note |
|---|---|---|---|
| **HDMI source** | HDMI Connect | Laptop, PS4 or BD/DVD player | |
| ↓ | HDMI cable | HDCP 1.4b or not(by content) | |
| **Button** | HDMI Connect | 1. HDCP decode or not<br>2. Video and audio encode<br>3. Double encryption encode | InstaShow™ |
| ↓ | Wi-Fi | ***802.11ac WPA2 PSK AES 128*** | |
| **Host** | HDMI Connect | 1. Double encryption decode<br>2. Video and audio decode<br>3. HDCP encode | |
| ↓ | HDMI cable | HDCP 1.4b or not(by content) | |
| **HDMI sink** | HDMI Connect | Display | |

## InstaShow™ network architecture

For InstaShow™, in the operation flow, the system architecture must comply with confidentiality, integrity, and availability to ensure that it is a secure system. Transmission can be divided into wired and wireless transmissions. Wired connection is advantageous of high immunity to interference. An environmental space with wireless communication can be often interfered with intentional or unintentional electromagnetic waves. InstaShow™, which is a wireless transmission system allowing the system to operate normally by reducing electromagnetic interference, is very applicable to conference or home environment. The architecture of InstaShow™ transmission system may be divided into physical layer, network layer and application layer, which architecture and operation will be explained later.




## 1. Physical Layer

The physical interfaces supported by InstaShow™ include USB/Micro USB, HDMI and Ethernet. The security issue with the most direct impact in a system is the physical interface. An intruder might utilize the interface to perform firmware interpretation of reverse-engineering, as well as to load malicious malware on equipment. The physical interface of the protection system equipment has the same importance as other layers for protecting the system.

USB: It provides 5V/0.9A power supply for Button simply without providing one-way and two-way data exchange mechanisms.

Micro USB: It provides 5V/1.5A power requirement for Host without providing one-way and two-way data exchange mechanisms.

HDMI: Entrance and exit for video & audio transmission, supporting HDCP protection.

Ethernet: Web UI login settings are provided, and updating firmware does not support Internet function.

The verification mechanism for Host and Button transmissions is not performed through the above interface function. Hackers cannot steal all data and parameters shared by Host and Button through the physical interface.

For firmware upgrade procedure, format integrity and signature for firmware will be verified, otherwise the upgrade procedure is not supported.

Another hidden interface of the system is Wi-Fi, which has an integral security control. In this system, Wi-Fi of Host provides Button with incoming verification and video & audio transmission. Additional controls for authentication, confidentiality, and integrity are required for other devices to access the application layer of Host.

## 2. Network Layer

The network system of InstaShow™ can be divided into WAN (Wide Area Network) and LAN (Local Area Network).

The method for WAN is to connect network server through Ethernet interface. InstaShow™ cannot access

Internet through this network server but only allows system network administrator to control the system fully in the application layer through enterprise web server and authentication mechanism. The network system and other access controls for InstaShow™ are independent VLAN separated from enterprise data network.

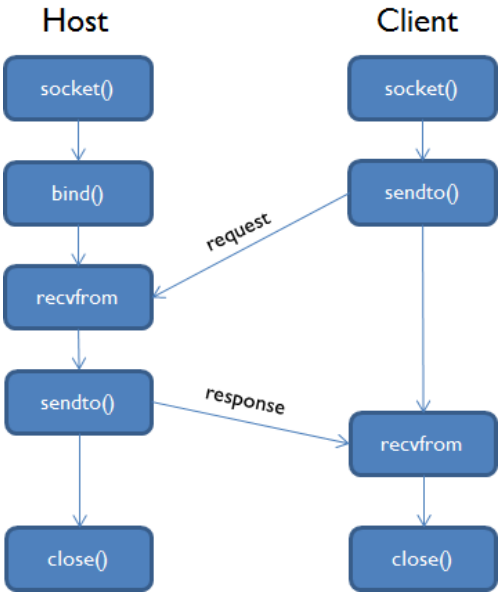
LAN establishes local area connection with Button or other Wi-Fi devices by using Wi-Fi. The protection mechanism of Wi-Fi is based on the IEEE 802.11i security standard that provides WPA2-PSK with a pre-shared key (PSK) authentication. WPA2-PSK encryption ensures confidentiality and integrity of all data over wireless channel. The encryption mode uses AES having a 128-bit key with a character length greater than 8 and less than 63. Integrity is achieved by using Counter Mode CBC-MAC Protocol (CCMP) plus a check method called MIC (Message Integrity Check). WPA2-PSK password and SSID are used, both of which can be configured by the administrator on the network interface of Host.

## 3. Application Layer

The core operating system for Host and Button of InstaShow™ is the Linux OS. This application layer provides system setup, wireless pairing management, wireless screen transmission network & communication performance management, video & audio format conversion and video & audio format decoding/encoding.

**Wireless pairing management:** Before full operation of the system, Host and Button must establish a Wi-Fi connection. The network connection is established at the TLS (Transport Layer Security) layer on the network level. When the authentication is created on the Host side, Button has to be identified with respect to whether the security verification code of InstaShow™ is matched. After connection is established between both sides, Host still needs an additional Button verification step (MAC address).

**Wireless screen transmission network & communication performance management:** The content of the wireless screen transmission runs through UDP (User Datagram Protocol) because UDP does not need to establish a connection like three-way handshake, such that communication is very efficient. In UDP frame architecture diagram, a client requires only two steps (socket and sendto) to initiate a request, while the server also requires only three steps to receive messages (socket, bind, recvfrom) from the client.




**Video & audio format conversion and video & audio format decoding/encoding:** Conversion of video & audio stream data is an important part in InstaShow™. The amount of HDMI data with 1080p lossless compression is about 6GB. InstaShow™ cannot reach 6GB transmission amount by using 802.11ac. With respect to the four steps for video & audio format - conversion, compression, decompression and video & audio format recovery, the system is allowed to operate smoothly with excellent image quality through high-performance core processor, dynamic video & audio compression ratio adjustment, in conjunction with wireless screen transmission network & communication performance management.

**System setup:** The system setup for InstaShow™ uses a Web interface to ensure authentication connection with Host via only HTTP service. HTTP performs transmission with device browser through plain text directly, and performs interactive conversation in a general (non-secure) mode. Therefore, the content on internet may be intercepted by intentional people. This is a vulnerability that needs to be improved in this system. Login of Web interface is bound to a cookie session that remains effective until logout or expiry.

**Security level:** Three security levels are used for InstaShow™. Security levels are divided based on the number of provided functional protections. It is described as follows

Level 1,

. The identity authentication and password required for connection of Button to Host Wi-Fi

. Account and password required for Web UI login (HTTP)

Level 2,

. Connection can be established only if Button Mac Address is in Host List.

. Screen Lock on Web UI setting

Level 3,

. No access to Web UI via Wi-Fi

# Conclusion

Design of InstaShow™ is based on all HW solution, plug & play, no SW executed and nothing to learn. We believe that InstaShow™ can provide a certain degree of data protection, environmental maintenance and friendly products, and promise no implementation of back door or hidden transmission. BenQ will continue to invest in our platform, allowing you to benefit from our products in a secure and transparent manner.