BRAVIA Professional Display Security White Paper

Version 1.2

Table of Contents

1. Acronyms and Abbreviations

owner: persons who own or manage BRAVIA Professional Display for the purpose of their business. (e.g. hotel operator)
anonymous end-user: persons who actually use BRAVIA Professional Display. (e.g. guests of a hotel)

2. References

[PromodeManual]	https://pro-bravia.sony.net/guides/
[PromodeOverview]	Professional Mode Overview Document

3. Platform Security Features

BRAVIA Professional Display platform itself has security mechanisms to protect against unauthorized software applications being substituted for the factory image. At power-on, BRAVIA Professional Display performs a cryptographic checksum of the software to be loaded and executed by the platform processor and then validates the calculated value against the signed value stored in Flash memory. The key used for validation is permanently stored at manufacture in the secure memory of the dedicated cryptographic processor subsystem of the platform's SoC LSI and is inaccessible outside the processor IC. If tampering with the executable application is detected, the CPU will not load the corrupted image into system RAM for subsequent execution. This security feature defeats the ability to repurpose or reprogram for unauthorized access or redistribution of content.

4. Android TV

BRAVIA Professional Display platform is compliant with Android TV security policy. You can refer to http://developer.android.com/training/articles/security-tips.html .

- Every software version for BRAVIA Professional Display passes the CTS.
- BRAVIA Professional Display prohibits any activity from unlocking the boot loader, there being no way of putting custom ROMs on the device.
- System priviledge is not given to the 3rd party application
- BRAVIA Professional Display doesn't approve of getting root access.

5. Network

IP Control

BRAVIA Professional Display supports IP Control, so user can control BRAVIA by sending IP Control commands.
IP Control function has authentication mechanism to prohibit unexpected commands from unauthorized user.

Root CA certificates

The CA certificates of BRAVIA Professional Display HTML5 Application Runtime are compliant with Android TV. You can get CA certs information via https://android.googlesource.com/platform/ .
HTML5 Application Runtime on BRAVIA Professional Display prohibits an access to any untrusted sites.

6. Connectivity

Each interface can be disabled by settings menu.

- RS-232C control
  - Android 8.0: "Settings" > "Network & Accessories" > "RS232C control"
  - Android 9.0: "Settings" > "Remotes & Accessories" > "RS232C control"
- HDMI CEC
  - Android 8.0: "Settings" > "External inputs" > "BRAVIA Sync settings"
  - Android 9.0: "Settings" > "Inputs" > "External inputs" > "BRAVIA Sync settings"
- Bluetooth
  - Android 8.0: "Settings" > "Network & Accessories" > "Bluetooth"
  - Android 9.0: "Settings" > "Remotes & Accessories" > "Bluetooth settings"
- Wi-Fi
  - Android 8.0: "Settings" > "Network & Accessories" > "Advanced Settings" > "Built-in Wi-Fi"
  - Android 9.0: "Settings" > "Network & Internet" > "Wi-Fi"
- Android voice control
  - Android 8.0: "Settings" > "Voice Remote Control"
  - Android 9.0: "Settings" > "Remotes & Accessories" > "Bluetooth settings"
- Google Cast
  - "Settings" > "Apps" > "Chromecast built-in" (or "Chromecast Android Shell")
- Wi-Fi access point
  - "Settings" > "Pro settings" > "Wi-Fi access point"

7. Digital Rights Management

Streaming

HTML5 Application Runtime on BRAVIA Professional Display supports the following Digital Rights Management functions used to protect Licensed Content via license keys:

- For DASH:
  - Widevine(“cenc” scheme)
  - Microsoft PlayReady SL2000
- For SmoothStreaming:
  - Microsoft PlayReady SL2000
- For HLS:
  - Sample AES

HDMI

BRAVIA Professional Display is compliant with HDCP2.3.

8. Pro mode

BRAVIA Professional Display platform provides specific operation mode called Pro mode for professional usage. (see [PromodeOverview] and [PromodeManual])

This mode provides configuration to realize the following functions.

- to erase below in power-off trigger
  - all account information stored in the AccountManager
  - selected application's own data storage
- to prevent anonymous end-users from
  - an access to any security related settings by disappearing setting UI
  - using installed applications the owner does not want
  - installing new applications
  - operating the display by remote controller commands or display buttons

In order to change above configuration, the special key-sequence is needed. In addition, PIN based lock function is available.
