7. Security

SmartCast TV supports a robust security methodology.

7.1 Anti-hacking Measures

	Anti-Hacking Requirement
1	Bootloader, kernel and specific rootfs/system files shall be hashed, secured, and validated at runtime with a chain-of-trust traceable to specific keys instantiated in the SoC silicon.
2	Whereas silicon instance keys may result in stronger code protection, a scheme must be identified so the system shall run (at least the first time in the factory) with the same code image on every unit, installed at board build time.
3	No specific security equipment shall be installed at the factory.
4	All code protections shall be such that code and key are PGP encrypted from Qterics. Not emailed in the clear.
5	SoC shall provide a DRAM encrypting feature that is HW based and transparent and shall not be accessible by software. This is to preclude an attack by monitoring DRAM data. This is to protect partner content.
6	JTAG and PCI ports shall be disabled on all production chips.
7	Debugging console output shall be disabled on production systems and only enabled withva special unlock key controlled by VIZIO.
8	Production systems shall not allow any console input (serial).
9	All development and debugging ports and services (e.g. telnet) shall be disabled in production products. All open ports shall be identified and reviewed (with justification required) during security reviews.
10	The platform implementation shall preclude loading or launching any code elements not subject to signature validation or from a secure store. This mechanism shall be designed to preclude a hacker from performing an attack by file system substitution.
11	Field replacement of a secure code set with an unsecure one shall be systematically prevented to ensure that all system components remain completely secure. If not signed firmware then TV shall not boot because lacking correct key ladder.
12	Anti-rollback (ARB) should be implemented to prevent reloading of older firmware with exposed exploits.
13	Platform shall provide TLS 1.2 and 1.3.
14	SELinux kernel security module shall be provided along with a mechanism supporting access control security policies, including mandatory access controls.

7.2 Secure Key Hiding

SMARTCAST TV shall implement key protection, in-the-field provisioning, and revocation using the Qterics (ULI) provisioning infrastructure.

	Secure Key Hiding Requirement
1	Secure storage, traceable via a chain of trust to VIZIO and enforced with silicon specific pre-shared hardware keys, shall be provided for all secure elements on the platform, including secure keys.
2	All key protection schemes shall be in accordance with the respective service partner robustness rules.
3	Each secure service shall require specific keys and attributes to be persistently stored. Ingestion and management of such keys is accomplished by Qterics (ULI) using a secure platform infrastructure.
4	Ingested DRM keys should be individualized with the device unique root key prior to storage. This ties them to a particular unit thereby eliminating possible device cloning.

7.2.1 Trusted Execution Environment support for IoT

The trusted execution environment (TEE) requires API extension for IoT to support new cert provisioned from Qterics for SCPL layer.

7.3 Secure Boot

Secure boot shall be supported as follows:

	Secure Boot Requirement
1	The system shall implement a secure boot method.
2	All portions of code, except for the lowest level ROM boot code shall be capable of being securely updated in the field.
3	Normally, secure boot shall be accomplished in a multi-step process, in which each subsequently loaded code component is validated by the one before it. In general, this sequence involves a low-level, tamper resistant ROM that shall use a secure hardware key to decrypt and launch a bootloader, which, in turn, contains the secure keys necessary to decrypt, verify the integrity of the next code element (in general, the system kernel), and transfer execution to it. Each code set and library shall be validated in turn (possibly using a digsig utility) and loaded. Application code shall also be security validated (either by accessing a secure store or by digsig validation) prior to being loaded and run. Other methodologies determined to provide the equivalent level of security shall be deemed acceptable.
4	The security chain of trust shall ensure that only VIZIO signed code is capable of running on the bootloader, kernel and certain system files.
5	A security exception shall be noted and the system shall halt when any code validation or verification step fails.
6	The core hardware keys used in the boot chain-of-trust shall be permanent and unique (at least on a platform family basis).
7	Component authentication during boot shall be required to make sure compromised devices won't run. The authentication is tied through a chain of trust to an OTP root key **. Control of the secure boot sequence shall start with a trusted, low level loader. TIf the bootloader is properly signed it is allowed to run. The bootloader shall subsequently load the kernel and that same signature check is repeated. If the kernel passes the signature check,it is allowed to run. The kernel mounts the filesystems and in those file systems will be certain files that also need to be authenticated. ** VIZIO would prefer to not have the root key be symmetric, because that would necessitate that it be shared with the factory. It would of course be better that this be the public half of an asymmetric RSA key (although bit length can be prohibitive for OTP), or the hash of the public key which could be built in to the bootloader.
8	Component authentication shall run in a trusted execution environment and it is tasked with loading and authentication of the bootloader.
9	A mechanism is required to 1) at signature time define which files need to be authenticated and 2) an authenticator mechanism that can be tied through the chain of trust back to the root key. A full rootfs/system authentication is NOT required because the processing time would be excessive.
10	If the image update/validation/boot fails, return back to the last known good image. This can be achieved by using ping-pong partition for the previous and current images.

7.4 Penetration (PEN) Testing

To ensure security, Penetration (PEN) testing is required as follows.

	PEN Testing Requirement
1	Penetration (PEN) Testing shall be required every year based on changes on the software stack. PEN testing shall be performed by an outside testing house every two years. Internal PEN testing is required: 1) New Firmware and 2) Major production releases.
2	PEN testing shall include both white and black box testing.
3	PEN full results shall be shared with VIZIO and reviewed.

7.5 Cast Certification

The Cast receiver shall rely on platform to provide secure access to Cast certificate and private key used for device authentication. Google provides a cast certificate private key that shall be secured by secure processor and must not be accessible to CPU in clear form.

Vendor shall follow all process controls and requirement specifications provided by google for certifications and shall address all relevant issues until the certification passes all tests. Vendor shall closely work with both Vizio during such process.

7.6 AirPlay Certification

AirPlay shall rely on platform to provide secure access to the MFI and FPS certifications are used for device authentication for AirPlay and HomeKIt integrations. Apple provides these certificates via a Qterics delivery, that shall be secured by secure processor and must not be accessible to CPU in clear form.

Vendor shall follow all process controls and requirement specifications provided by Apple for certifications and shall address all relevant issues until the certification passes all tests. Vendor shall closely work with both Vizio during such process.

7.7 HTML5 Security

The following requirements for applications developed for SmartCast TV shall be required to maximize platform security while balancing the needs of our services partners to minimize content delivery costs.

	HTML5 Security Requirements
1	All browser connections shall be initiated as HTTPS: with the server-side certificates traceable to the Root CA certificates provisioned by VIZIO on the platform. Upon request, VIZIO can provide a list of approved and supported Root CAs (subject to change at any time).
2	The platform application launch infrastructure shall actively block any non-HTTPS (TLS) initial requests.
3	The platform browser infrastructure shall block any attempt to perform a non-authenticated (HTTP) load of mixed active content. That is, all content accessed by the browser, including any references made within HTML or other scripts served to the platform, shall be subject to HTTPS (TLS) access except passive content, such as images, audio and video content. This specific relief of the TLS requirement for passive content is allowed to reduce the cost impact of serving large-format content, while still preserving the desirable security aspects of ensuring all active content is subject to TLS.
4	For further information about mixed content handling, see the W3C “Mixed Content Specification” (https://www.w3.org/TR/mixed-content/). In the parlance of the W3C specification, the platform shall block all “Blockable Content” and ALLOW all “Optionally Blockable” content.
5	All accesses shall by services shall be subject to the CORS standard.