

MATTER ATTESTATION OF SECURITY REQUIREMENTS**Product Identification**

Product Developer Information	
Company Name:	LG Electronics
Contact Name (First, Last):	Sungmok Shin
Contact Email:	sungmok.shin@lge.com
Work Phone:	+821024182664
Product Submitted for Matter Certification	
Product Name:	webOS TV
CSA Specification(s) Rev.#(s) and any Errata at Time of Request:	Matter 1.0
Software Component Revision:	webOS TV 23
Hardware Revision:	O22N
Firmware Revision:	webOS TV 23

Robustness Security RequirementsInstructions:

For each security requirement, the applicant must

- State Yes/Partial/No/NA compliance
- (Optional) Justify compliance with a brief explanation (for 3rd-party security certification, the Certificate reference should be provided)

Cryptography (§13.6.1)		Compliance
13.6.1.a	Devices and Nodes SHOULD include protection against remote attacks that can be used to extract or infer cryptographic key material.	Yes/Partial/No/NA Yes
	Justification: Click or tap here to enter text.	
13.6.1.b	Devices SHOULD protect the confidentiality of attestation (DAC) private keys. The level and nature of protection for these keys may vary depending on the nature of the Device.	Yes/Partial/No/NA N/A
	Justification: DAC won't be applied as the DUT is commissioner & controller	
13.6.1.c	Nodes SHOULD protect the confidentiality of Node Operational Private Keys. The level and nature of protection	Yes/Partial/No/NA

	for these keys may vary depending on the nature of the Nodes.	Yes
	Justification: Click or tap here to enter text.	
13.6.1.d	Cryptographic keys SHALL be randomly chosen using a cryptographically secure random number generator in accordance with algorithms defined in Section 3.1, "Deterministic Random Bit Generator (DRBG)"	Yes/Partial/No/NA Yes
	Justification: Click or tap here to enter text.	
13.6.1.e	Devices SHALL use non-repeating initialization vectors for a given session key.	Yes/Partial/No/NA Yes
	Justification: Click or tap here to enter text.	
Commissioning (§13.6.2)		Compliance
13.6.2.a	Manufacturers SHOULD control the number of DACs issued under their vendor ID.	Yes/Partial/No/NA N/A
	Justification: The DUT performs commissioner & controller role.	
13.6.2.b	Where practical, the setup code SHOULD NOT be photographable or visible when installed (e.g., QR code hidden with a flap).	Yes/Partial/No/NA N/A
	Justification: The DUT performs commissioner & controller role.	
13.6.2.c	Uncommissioned Devices SHOULD only be available to be commissioned with some form of physical proximity user interaction (e.g. power cycle or button press).	Yes/Partial/No/NA N/A

	Justification: The DUT performs commissioner & controller role.	
13.6.2.d	For Devices subject to physical tampering (e.g. doorbell, camera, door lock, devices designed for outdoor use cases), the physical interaction to initiate commissioning and/or the setup code (QR code, NFC Tag or Manual code) SHOULD NOT be accessible to a physical attacker. E.g. setup code is removable or not on the device, the button used to initiate commissioning for the lock is inside the house. Justification: The DUT performs commissioner & controller role.	Yes/Partial/No/NA N/A
13.6.2.e	A Commissioner or Administrator SHOULD only add Root Certificates that it trusts to a Node. Justification: During commissioning, the Root CA created by LG is reliably delivered to the controller.	Yes/Partial/No/NA Yes
13.6.2.f	A device manufacturer SHOULD implement Basic Commissioning Method only for devices that adequately secure the Passcode. Justification: The DUT performs commissioner & controller role.	Yes/Partial/No/NA N/A
Firmware (§13.6.3)		Compliance
13.6.3.a	Vendors of Matter implementations (including their suppliers of Matter functionality) SHOULD have a public vulnerability reporting mechanism and policy and actively monitor, identify and rectify in a timely manner security vulnerabilities throughout the publicly stated security lifecycle policy of the product. Typical responsible disclosure guidelines allow vendors from 60 to 120 days to patch a vulnerability, but the implementation of such a program is at each vendor's discretion.	Yes/Partial/No/NA Yes

	<p>Justification: Click or tap here to enter text.</p>	
13.6.3.b	<p>Devices SHOULD have a verified boot based in an immutable root of trust to verify the authenticity of firmware. Commissioners SHOULD only be loaded on a computing platform that has such a verified boot. If devices cannot support verified boot, devices SHOULD perform verification on any firmware update before applying the new firmware.</p> <p>Justification: Click or tap here to enter text.</p>	<p>Yes/Partial/No/NA</p> <p>Yes</p>
Manufacturing (§13.6.4)		Compliance
13.6.4.a	<p>Fusing of Devices in production SHOULD be done to limit unintended access to hardware components. For example, vendors may disable debug interfaces, and program trust anchors for secure boot. There are multiple options to secure fusing on the factory floor (e.g., physically securing the fusing station, pre-fusing the silicon, etc).</p> <p>Justification: Click or tap here to enter text.</p>	<p>Yes/Partial/No/NA</p> <p>Yes</p>
Resiliency (§13.6.5)		Compliance
13.6.5.a	<p>Matter implementations SHOULD implement resiliency features (e.g., responding to secure boot failures with recovery or error signaling mode) to detect and handle compromise.</p> <p>Justification: Click or tap here to enter text.</p>	<p>Yes/Partial/No/NA</p> <p>Yes</p>
Battery Powered Devices (§13.6.6)		Compliance
13.6.6.a	<p>Battery powered Devices SHOULD respond to excessive queries by rate limiting (even limiting the rate to zero if desired).</p> <p>Justification: The DUT is not a Battery powered device.</p>	<p>Yes/Partial/No/NA</p> <p>N/A</p>

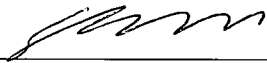
Tamper Resistance (§13.6.7)		Compliance
13.6.7.a	Protection against physical attacks (especially those that impact cybersecurity) MAY be needed for some devices, as determined by the manufacturer.	Yes/Partial/No/NA Yes
	Justification: Click or tap here to enter text.	
Distributed Compliance Ledger (§13.6.9)		Compliance
13.6.9.a	Vendors SHOULD avail themselves of the DCL store-and-forward functionality so that they can control posting of data about their products to the DCL.	Yes/Partial/No/NA Yes
	Justification: Click or tap here to enter text.	
13.6.9.c	Vendors SHOULD run and use their own Observer Nodes and restrict access to it to make sure that it stays available to the vendors' DCL clients.	Yes/Partial/No/NA Yes
	Justification: Click or tap here to enter text.	
13.6.9.d	Vendors SHOULD protect DCL private keys in Hardware Security Module (HSM) equipped servers.	Yes/Partial/No/NA N/A
	Justification: The DUT performs commissioner & controller role.	
General Comments on Robustness Security Requirements Attestation		

Please use this section to provide any additional information, reasoning, or rationale to explain the product specificities and support the claims above:
Click or tap here to enter text.

I declare and certify that the facts set forth in this attestation are true and correct.

NAME: Sungmok Shin

TITLE: Senior Research Engineer

SIGNED: 

DATE: 10/4/2022