EN18031 Google Home Speaker

Table of Contents

1

Executive Summary

DEKRA was contracted by Google to conduct a cybersecurity assessment of the Google Home Speaker. This assessment is specifically focused on evaluating the device's compliance with the essential requirements of Article 3.3(d) and (e) of the Radio Equipment Directive (RED) 2014/53/EU, as well as Commission Implementing Decision (EU) 2025/138, using the harmonized standards EN 180311:2024 and EN 180312:2024.

The Google Home Speaker is an internet-enabled smart speaker designed to provide high-quality audio playback, hands-free voice control via Google Assistant, and integration with smart home ecosystems. The device supports WiFi and Bluetooth connectivity for streaming audio and interacting with connected services and platforms. The version of the device tested was:

- Hardware version: G99E5
- Firmware version: T171800

2

Key Findings

The Google Home Speaker meets all the provisions of EN 180311:2024 and EN 180312:2024, covering common security requirements for internet-connected radio equipment. Key security features include a secure boot process with firmware integrity validation, hardware-based cryptographic key protection, and digitally signed OTA updates delivered over TLS encrypted channels. Access is tightly controlled through RBAC policies and two-factor authentication, while all device communications - WiFi, BLE, and Thread - are encrypted using industry-standard protocols. The system also ensures resilience to outages, minimal service exposure, and comprehensive data protection for both storage and transmission.

3

Google Home Speaker Compliance Summary

EN18031-1

Requirements	Pass	Fail	NA	Comments
Access control mechanisms	2	0	0	Role Based Access Control (RBAC) for File Permissions, Access Tokens, and Trusted Execution Environment (TEE) ensure the access control of the security/network assets.
Authentication mechanism	5	0	1	The device authenticates a service using certificates over HTTPS/TLS. 2FA is employed on the external Google Home application. Thread, an IPv6 based, low power mesh networking technology for Internet of Things (IoT) products, is used on this device. Google Home authenticates media receivers based on a certificate that chains up to a trusted root.
Secure update mechanism	3	0	0	OTA updates are performed over TLS 1.2 with proper *ciphersuites* at transport layer. Furthermore, the updated packages are signed according to best practices.
Secure storage mechanism	3	0	0	Trusted Execution Environment (TEE), One Time Programmable Memory (OTP), File system with SELinux, File-based encryption using authenticated encryption schemes, and disabled debugging ports ensure the proper storage of sensitive assets.
Secure communication mechanism	4	0	0	BLE communication is encrypted at the application layer, following best practices. All communications with cloud services are performed over TLS 1.2. The DUT communicates with other thread enabled devices in the same structure for improved connectivity and ciphersuites according to best practices.
Resilience mechanism	0	0	1	This requirement is not applicable to the product.
Network monitoring mechanism	0	0	1	The device is not intended to process communication between networks, which also involves public networks.
Traffic control mechanism	0	0	1	The device is not intended to process the communication between networks which also involves public networks.
Confidential cryptographic keys	3	0	0	All confidential cryptographic keys are unique per device and/or are generated following best practices standards such as NIST SP 800-57, FIPS 140-3.
General equipment capabilities	6	0	0	The device minimizes the exposed attack surfaces and is up-to-date software/hardware public vulnerabilities.
Cryptography	1	0	0	All cryptographic algorithms comply with industry best practices, using recommended key lengths and secure modes of operation (e.g., AES-GCM, SHA-256, ECDSA). No deprecated or broken algorithms are used.

EN18031-2

Requirements	Pass	Fail	NA	Comments
Access control mechanisms	2	0	4	Role Based Access Control (RBAC) for File Permissions and Access Tokens ensures the access control of the security/network assets.
Authentication mechanism	3	0	3	The device authenticates a service using certificates over HTTPS/TLS. 2FA is employed on the external Google Home application. Google Home authenticates media receivers based on a certificate that chains up to a trusted root.
Secure update mechanism	3	0	0	OTA updates are performed over TLS 1.2 with proper *ciphersuites* at transport layer. Furthermore, the updated packages are signed according to best practices.
Secure storage mechanism	0	0	3	There are no security/privacy assets that are stored persistently on the DUT, so this evaluation case is considered not applicable.
Secure communication mechanism	4	0	0	BLE communication is encrypted at the application layer, following best practices. All communications with cloud services are performed over TLS 1.2.
Logging mechanism	1	0	3	Event logging relies on cloud services, managed by the account and the app.
Deletion mechanism	1	0	0	Removing the device via the app will clear the settings and data from the device.
User notification mechanism	0	0	2	The GHA itself is the method used to notify the users when a new version of the privacy policy is made.
Confidential cryptographic keys	3	0	0	All confidential cryptographic keys are unique per device and/or are generated following best practices standards such as NIST SP 800-57, FIPS 140-3.
General equipment capabilities	7	0	0	The device minimizes the exposed attack surfaces and is up-to-date software/hardware public vulnerabilities.
Cryptography	1	0	0	All cryptographic algorithms comply with industry best practices, using recommended key lengths and secure modes of operation (e.g., AES-CCM, SHA-256, ECDSA). No deprecated or broken algorithms are used.

4

DEKRA EN18031 Methodology

This section outlines the comprehensive methodology employed by DEKRA for evaluating the cybersecurity posture of internet-connected radio equipment, such as the Google Home Speaker, in accordance with the requirements specified in EN 18031-1:2024. The assessment supports the presumption of conformity with the essential requirements under Article 3.3 (d), (e), and (f) of the Radio Equipment Directive 2014/53/EU. The process incorporates both documentary review—based on the completed RED-DA Intake Form—and practical verification testing, with traceability to test cases derived from the standard's normative requirements. The evaluation ensures each security control is technically sound, appropriately implemented, and effective in mitigating foreseeable risks. The following requirement families are individually assessed:

[ACM] Access Control Mechanisms

DEKRA verifies that mechanisms are implemented to control access to configuration interfaces, administration services, and data endpoints. This includes enforcing least privilege principles, validating user roles, and ensuring interface-level restrictions are in place for both local and remote access (e.g HTTPS or app-based provisioning). Logical port exposure is assessed against the device's threat model and service justification.

[AUM] Authentication Mechanisms

Authentication is scrutinized at the system and application levels. Tests confirm that the device enforces strong credential policies (e.g. password length, entropy, rotation), validates credentials before granting access, and resists brute-force or replay attacks. Secure session management (e.g. token expiration, timeout policies) is also analyzed, along with the ability to update authenticators securely.

[SUM] Secure Update Mechanisms

The assessment includes validation of secure boot, cryptographic signature checks for update packages, and trust chain verification. DEKRA checks whether rollback protection is implemented and confirms that updates are delivered via encrypted channels (e.g. TLS 1.2+). Update automation settings, failure recovery behavior, and the ability to restrict unauthorized update injection are tested.

[SSM] Secure Storage Mechanisms

DEKRA examines how the device stores sensitive data such as user credentials, network keys, and configuration states. Evaluation includes analysis of hardware-backed storage (e.g. TPM or TEE), file system permissions, key derivation practices, and tamper-resistant access controls. Logging of access attempts and forensic traceability of storage operations are also verified.

[SCM] Secure Communication Mechanisms

Data-in-transit protections are evaluated across all communication interfaces, including device-to-cloud, device-to-device (mesh), and mobile app APIs. Tests ensure encryption (TLS 1.3 or equivalent), mutual authentication, integrity checks (e.g. MAC, digital signatures), and replay protections are applied. Communication fallback paths (e.g. legacy protocols) are identified and analyzed for exposure risks.

[LGM] Logging Mechanisms

The assessment verifies the presence and adequacy of logging mechanisms used to record security-relevant events, such as authentication attempts, firmware updates, and configuration changes. DEKRA evaluates whether the system persistently stores log data, protects it against tampering, and includes sufficient detail (e.g. timestamps, event types) to support post-incident analysis. The assessment also reviews whether access to logs is controlled and if audit data can be exported or reviewed in a secure and user-appropriate manner.

[DLM] Deletion Mechanisms

DEKRA examines whether the product includes mechanisms to securely delete sensitive data, including user credentials, configuration profiles, and cryptographic material. The evaluation focuses on ensuring that deleted information cannot be recovered by unauthorized parties. Tests confirm the effectiveness of factory reset procedures, data zeroization practices, and user-initiated deletion functions. If non-volatile memory is used, the assessment verifies that overwriting or erasure methods are properly implemented and comply with relevant standards.

[UNM] User Notification Mechanisms

DEKRA assesses whether the device or its associated interfaces provide appropriate and timely notifications to users regarding security-relevant events. This includes alerts related to firmware updates, pairing status, authentication failures, or attempted access to protected resources. The evaluation ensures that notifications are delivered in a user-recognizable format, are free from ambiguity, and support users in making informed security decisions. The mechanism is also tested for responsiveness to changes in the device's security state or risk posture.

[CCK] Confidential Cryptographic Key

The key management lifecycle is examined, including key generation (e.g. hardware RNG), provisioning, rotation, revocation, and zeroization. DEKRA verifies that preinstalled keys are unique per device, no static default values are used, and that keys are protected during both runtime and storage. If FIPS 140-2/3 components are used, certification references are recorded.

[GEC] General Equipment Capabilities

This category includes systemic security properties such as:

- Regular patching and absence of known exploitable vulnerabilities (CVEs)
- Input validation and sanitization across network and user interfaces
- Removal or disabling of unnecessary services, ports, and debug interfaces
- Documentation and control of exposed APIs and service endpoints
- Prevention of code injection or format string exploits
- Integrity validation of runtime memory and code execution flows
- Support for system reset, safe state recovery, and operational fallback

[CRY] Best Practices Cryptography

The equipment uses best practices for cryptography and are implemented for the protection of any assets.

DEKRA's EN 18031 methodology incorporates both manual and automated techniques, including penetration testing tools, static code analysis (where possible), configuration review, and fuzz testing. This methodology ensures that each device undergoes a holistic cybersecurity assessment, providing confidence in its compliance under the new RED-DA framework and robustness against modern cyber threats.

DEKRA

Contact

Would you like more information?

Visit our Website!