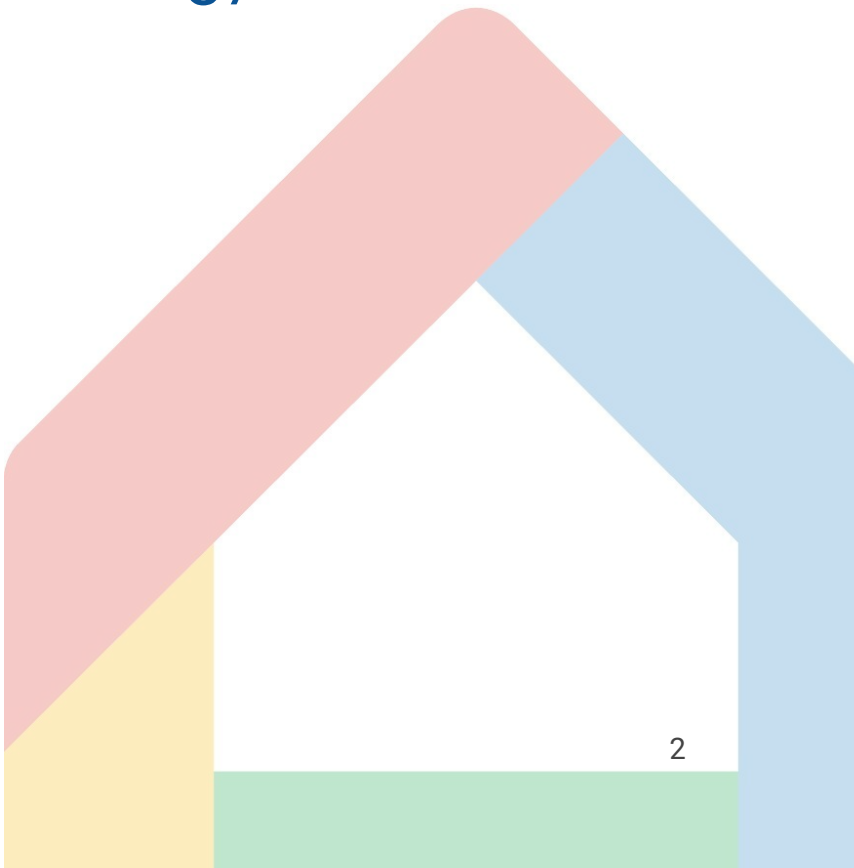
Google

EN 18031 Google Nest Doorbell (wired, 3rd gen)

November 2025

Google

Table of Contents



Google

1 Executive Summary

The following is a cybersecurity assessment of the Google Nest Doorbell (wired, 3rd generation). This assessment evaluates the device against the harmonized standards **EN 18031-1:2024** and **EN 18031-2:2024.** These standards define the technical specifications required to ensure the device does not harm the network and adequately protects the user's personal data and privacy.

The Google Nest Doorbell (wired, 3rd generation) is a high-definition, internet-connected doorbell camera designed for continuous home security monitoring, intelligent event detection, and seamless integration with the Google ecosystem. It communicates via Wi-Fi and Bluetooth Low Energy (BLE), incorporating advanced imaging sensors, on-device AI for person and motion detection, and end-to-end encrypted video transmission to Google Cloud. Users can interact with the device remotely through the Google Home app, receiving real-time notifications, accessing video history, and issuing voice commands via Google Assistant. The version of the device tested was:

Hardware Version	Software Version
G6PPP	internal_1.75_bla4_xua4_2rs4_gm_0day_hotfix_bla4-user_504809_bla4-ota-504809

2 Key Findings

The Google Nest Doorbell (wired, 3rd generation) complies with the applicable provisions of EN 18031-1:2024 and EN 18031-2:2024, addressing common security requirements for internet-connected radio equipment. The device is built with security features including verified secure boot with firmware integrity validation, hardware-based key protection using a Trusted Execution Environment (TEE), and robust secure update mechanisms over TLS. Google account verification and app-based management enforces strict access control and user authentication. Communications and encryption in transit is protected by TLS 1.2. The device is designed to ensure minimal service exposure and effective mitigation of known vulnerabilities. The device relies on Wi-Fi and BLE. It ensures it does not harm the integrity or availability of networks, misuse network resources, or interfere with other systems. Logging of critical events is performed via Google Cloud infrastructure.

Google

3 Compliance Summary

EN18031-1

Requirements	Pass	Fail	NA	Comments
Access Control Mechanisms	2	0	0	Trusted Execution Environment (TEE), Access Tokens, RBAC policies and SElinux ensure the access control of the security/network assets.
Authentication Mechanism	3	0	3	Device authenticates service-by-service certificates over HTTPS/TLS. 2FA is available on the external Google Home application.
Secure Update Mechanism	3	0	0	OTA updates are performed over TLS 1.2 with proper ciphersuites at the transport layer. Furthermore, the updated packages are signed according to best practices.
Secure Storage Mechanism	3	0	0	Secure storage mechanisms are implemented, ensuring integrity and confidentiality of stored information and network assets.
Secure Communication Mechanism	4	0	0	Bluetooth communication is encrypted at the link layer following best practices. All communication with cloud services are performed over TLS 1.2 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.

Google

EN18031-2

Requirements	Pass	Fail	NA	Comments
Access Control Mechanisms	2	0	4	Bluetooth access control of the security/network assets. Parental access controls requirements are not applicable to the product.
Authentication Mechanism	3	0	3	Device authenticates service-by-service certificates over HTTPS/TLS.
Secure Update Mechanism	3	0	0	OTA updates are performed over TLS 1.2 with proper ciphersuites at the transport layer. Furthermore, the updated packages are signed according to best practices.
Secure Storage Mechanism	3	0	0	Privacy assets are stored securely by using Trusted Execution Environment (TEE), File Base Encryption (FBE) or One-Time Programmable (OTP) memory.
Secure Communication Mechanism	4	0	0	Bluetooth communication is encrypted at the link layer following best practices. All communication with cloud services are performed over TLS 1.2 and ciphersuites according to best practices.
Logging Mechanism	1	0	3	Event logging relies on Cloud services.
Deletion Mechanism	1	0	0	Factory reset clears pairing data and user configuration securely.
User Notification Mechanism	0	0	2	Firmware update status, pairing events, and connection issues are reported via the companion app.
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.

Google

4 Assessment Methodology

The assessment was based on the following EN 18031-1:2024 and EN 18031-2:2024 requirement categories:

[ACM] Access Control Mechanisms

Mechanisms that control access to administration services, configuration interfaces, and data endpoints are verified. This includes validating user roles, enforcing least privilege principles, 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 verified at the application and system levels. Enforcement of strong credential policies (e.g., password length, entropy, rotation), validation of credentials before granting access, and resistance of brute-force or replay attacks are tested on the device. Secure session management (e.g., token expiration, timeout policies) and the ability to update authenticators securely is validated.

[SUM] Secure Update Mechanisms

Validation of secure boot, cryptographic signature checks for update packages, and trust chain verification is assessed. Rollback protection implementation is evaluated 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

Analysis of how the device stores sensitive data such as user credentials, network keys, and configuration states is performed. File system permissions, key derivation practices, hardware-backed storage, and tamper-resistant access controls are evaluated. Forensic traceability of storage operations and logging of access attempts are also verified.

[SCM] Secure Communication Mechanisms

Data in transit tests ensure encryption (TLS 1.2 or higher), 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. All communication interfaces, including device-to-cloud, device-to-device (mesh), and mobile app APIs are evaluated.

[LGM] Logging Mechanisms

Logging mechanisms used to record security-relevant events, such as authentication attempts, firmware updates, and configuration changes are analyzed. The evaluation includes 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 validates the logging mechanism and 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 Mechanism

Evaluation of mechanisms to securely delete sensitive data, including user credentials, configuration profiles, and cryptographic material is performed. The analysis 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

Examination of user notifications that provide appropriate and timely notifications to users regarding security-relevant events is performed. This includes alerts related to authentication failures, pairing status, firmware updates, or attempted access to protected resources. The evaluation ensures that notifications are delivered free from ambiguity, in a user-recognizable format, and support users in making informed security decisions.

[CCK] Confidential Cryptographic Key

The key management lifecycle is evaluated, including key generation (e.g., hardware RNG), provisioning, rotation, revocation, and zeroization. Preinstalled keys are verified to be 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

Systemic security properties are assessed by verifying the absence of known vulnerabilities (CVEs) and effective patching. Input validation is tested across interfaces to prevent injection exploits. Unnecessary services, ports, and debug interfaces are confirmed disabled, while exposed APIs are reviewed for proper controls. Runtime integrity, code execution flows, and safe recovery mechanisms are also evaluated.

[CRY] Best Practices Cryptography

Best practices for cryptography and its implementation for the protection of assets are analyzed. This analysis requires that standardized and secure cryptographic algorithms (e.g., strong ciphers and hashing methods) are selected. It verifies that key lengths and operational parameters are adequate to meet modern security requirements and resist known attacks.