Security & Privacy Disclosure, Final Report

Nuki Smart Lock for Android (io.nuki)

A smart lock that names everyone who comes through your door, and what its operator says about keeping that record.

PUBLIC DISCLOSURE, 21 NOVEMBER 2026, EMBARGO REACHED. REPLY OF 18 NOVEMBER 2026 RECEIVED FROM A SENDER AT UT11.NET SIGNING FOR NUKI, ANSWERING THE THREE QUESTIONS IN PART. THE SENDER'S AUTHENTICITY IS NOT VERIFIED.

Target	Nuki Home Solutions GmbH, Münzgrabenstraße 92/4, 8010 Graz, Austria
Versions Audited	2026.8.1 / versionCode 1369 (analysed 2026-08-23), base APK 63.4 MB from an 84.6 MB split bundle
Supervisory Authority	Datenschutzbehörde, Austria (presumptive lead, the operator is established in Austria)
Notice / Publication	2026-08-23 / 2026-11-21 (90 days, unchanged)
Findings	6: 4 Medium, 2 Low (four from the first notice, reassessed, and two added)
Status	REPLIES OF 3 SEPTEMBER 2026 (CONTESTS THE FINDINGS) AND 18 NOVEMBER 2026 (RECEIVED FROM A SENDER AT UT11.NET SIGNING FOR NUKI, ANSWERS THE THREE QUESTIONS IN PART). AUTHENTICITY OF THE SENDER NOT VERIFIED. FIREBASE QUESTION UNANSWERED.
SHA-256 (base APK)	`0ff8a236a86ab63adf500d146197151c76a3513cabce45d147adcd10f1fe052d`

security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Graz, Austria

Contents

1 Executive Summary 4

2 Finding Status at a Glance 6

3 Subject & Operator Analysis 6

4 Architecture & Data Flow 7

5 Findings 8
- 5.1 C1: Remote lock and unlock is a marketed backend capability over a persistent connection . . . 8
- 5.2 C2: Named activity log of people who are not account holders, with retention stated only as a paid feature . . . 9
- 5.3 H1: Database that very likely holds the BLE pairing secret is included in cloud backup and device transfer . . . 10
- 5.4 H2: Firebase and Google API key, project identifiers and database URL readable in the package . . . 11
- 5.5 M1: Three exported components without intent filter or permission, including the courier-access entry point . . . 12
- 5.6 M2: No network security configuration and no certificate pinning on the control channel . . . 13

6 Impact Analysis 13

7 The Complete Chain 14

8 Household Access, Couriers & Bystanders 14

9 Data Protection: Article by Article 15

10 Regulatory & Legal Landscape 15

11 Indicators of Compromise & Reproducible Evidence 16

12 Disclosure Timeline & Outcome 17

13 What Nuki Got Right 18

14 Residual Risk & Recommendations 18

Executive Summary

Nuki Smart Lock is the Android companion app of the Nuki Smart Lock, Smart Door, Opener and Box hardware, published on Google Play by Nuki Home Solutions GmbH of Graz with more than 500,000 installs. On 23 August 2026 RFI-IRFOS sent a coordinated disclosure notice under REF NUKI-2026-R1 after a root level code analysis of version 2026.8.1. The notice itemised four findings, two Critical and two High, and asked three written questions.

The case turns on what a smart lock necessarily knows. Every credential on a Nuki lock, whether the owner's phone, a child's fob, a cleaner's keypad code, a fingerprint or an Austrian Post courier's temporary access, receives a name typed by the account owner and appears under that name in the activity log with the actions Locked, Unlocked and Opened door. The people named are not Nuki account holders and never see a Nuki notice. Separately, the app sells remote locking and unlocking as a subscription feature, and the only concrete retention figure in the app's strings, six months, appears as a bullet point of the paid Smart Hosting subscription.

Two further findings concern key material. The backup rules include nuki.db in Android cloud backup and device transfer while excluding device_private.xml by name, and a Room schema string in the package defines an authorizations table with a column shared_key BLOB NOT NULL. A Firebase and Google API key set, with the project noki-826, is readable in the package. Two lower findings concern three exported components and the absence of a network security configuration.

This report is stricter than the first notice. The four findings of the notice are all reassessed. The two Critical labels become Medium and Medium and the two High labels become Medium and Medium. The reasons are given in each finding. Two further findings from the same analysis, M1 and M2, were not itemised in the notice and are added here at Low. The strongest reduction follows from the app's own wording: the activity log is stored on the Nuki device and is copied to Nuki servers only when Nuki Web is used. The remote command path is a documented product feature and no weakness in it was shown.

Nuki's support desk answered twice. A holding reply on 24 August 2026 (ticket 860439) promised a complete response. On 3 September 2026 (ticket 869292) Nuki wrote that the findings stem from misinterpretations of an automated analysis and do not correspond to technical or legal reality. That reply states no retention period, does not say whether shared_key is encrypted by the application, and describes no transparency mechanism for the people named in the log. RFI-IRFOS answered the same day with the literal strings, sent a reminder on 17 October 2026 and a 6-day notice on 15 November 2026. On 18 November 2026 a reply arrived at security@rfi-irfos.com from a sender at ut11.net who signs as Head of Software Engineering of Nuki Home Solutions GmbH and gives a nuki.io address in the signature. The sender domain differs from nuki.io and RFI-IRFOS has not verified that the sender speaks for Nuki, so the report records the content as stated in that reply. The reply states that Nuki keeps no copy of the activity log on any server unless the user signs up for Nuki Web, which stores data for 3 months, or 12 months with an active Smart Hosting subscription. It states that shared_key is encrypted through platform means in cloud backup and that the log lists only names defined by the device administrator, who alone can see them. It does not address the Firebase question (H2). The report is published on 21 November 2026, 90 days after delivery.

Scope: Root level code analysis of Nuki Smart Lock 2026.8.1 (versionCode 1369): AndroidManifest.xml, decoded resources, backup and data extraction rules, and the dex string pool of six classes*.dex files. No full smali pass was run, so every claim that would need code flow beyond strings and manifest is marked UNVERIFIED. The package came from the APKPure mirror after its version string matched the live Google Play listing, because the audit device was not reachable on the analysis day. No account was created, no Nuki server was called, no key was tested and no runtime instrumentation was used. The privacy policy text was not part of the evidence in the case folder, so statements about what the policy says are UNVERIFIED. CVSS v4.0 measures exploitability. Most findings here concern data governance, so CVSS-B scores are low and the report states where the rating is raised for the people affected.

ID	Severity	Title
C1	MEDIUM	Remote lock and unlock is a marketed backend capability over a persistent connection
C2	MEDIUM	Named activity log of people who are not account holders, with retention stated only as a paid feature
H1	MEDIUM	Database that very likely holds the BLE pairing secret is included in cloud backup and device transfer
H2	MEDIUM	Firebase and Google API key, project identifiers and database URL readable in the package
M1	LOW	Three exported components without intent filter or permission, including the courier-access entry point
M2	LOW	No network security configuration and no certificate pinning on the control channel

ID	Disclosed	This report	Status on 21 November 2026

Finding Status at a Glance

ID	Disclosed	This report	Status on 21 November 2026
C1	CRITICAL	MEDIUM	Neither reply (3 September and 18 November 2026) addresses the command path. Reassessed.
C2	CRITICAL	MEDIUM	Reply of 18 November 2026 (the sender at ut11.net signing for Nuki): server copy only with Nuki Web, 3 months, 12 months with Smart Hosting, names visible to the administrator only. Not verified. Reassessed.
H1	HIGH	MEDIUM	Reply of 18 November 2026 (the sender at ut11.net signing for Nuki) cites platform encryption in backup and states no application-level encryption. Reassessed.
H2	HIGH	MEDIUM	Reply of 3 September 2026: public client IDs, Security Rules and attestation. Deny-by-default and App Check question unanswered on 21 November 2026. Reassessed.
M1	Not itemised	LOW	Added in this report. Not addressed in any reply.
M2	Not itemised	LOW	Added in this report. Not addressed in any reply.

Subject & Operator Analysis

Nuki Smart Lock (package io.nuki) is published on Google Play by Nuki Home Solutions GmbH, Münzgrabenstraße 92/4, 8010 Graz, Austria. On 23 August 2026 the listing showed more than 500,000 installs and a rating of 4.5 from 19.9 thousand reviews. The listing carries PEGI 3, which is the household-utility category. No minors-specific mismatch was observed and none is asserted. The app controls Bluetooth smart-lock hardware (Smart Lock, Smart Door, Opener, Box) and optional services such as Remote Access, Nuki Web, Smart Hosting and an In-Home Delivery integration with Austrian Post.

The package targets Android API 36 with minSdkVersion 26, is built in Kotlin and Java, and ships six classes dex files of about 45.7 MB combined. The operator contacts used in the notice were android-support@nuki.io, developer@nuki.io and contact@nuki.io. A data protection officer or separate representative was not found in the package or on the listing. This is UNVERIFIED and is not asserted as a gap, because an operator established in Austria needs no Art. 27 representative.

Nuki is an Austrian operator working with an Austrian partner. No third-country transfer question arose from this analysis.

Architecture & Data Flow

- Phone to lock over Bluetooth Low Energy. The authorizations table in the local database stores the pairing secret shared_key per credential, with name, location fields and an admin PIN.
- Phone to Nuki backend over HTTPS to api.nuki.io and phoenix-api-prod.nuki.io, and over Server-Sent Events from sse.nuki.io.
- Remote commands over a persistent MQTT connection managed by io.nuki.core.communication.CommunicationService, available through the Remote Access subscription.
- Activity log stored on the lock. Copied to Nuki servers when Nuki Web is used (in-app wording). Deactivation stops recording and storage.
- In-Home Delivery: a courier from the Austrian Post partnership receives temporary access, and the owner can check entry in the activity log.
- Firebase project noki-826 provides crash reporting and messaging identifiers. Analytics collection, performance collection, automatic screen reporting and advertising ID collection are disabled by manifest flags.

The architecture is conventional for a connected lock. The risks sit in who is named in the log, how long the server copy is kept and how the key material travels, not in tracking SDKs.

Findings

C1: Remote lock and unlock is a marketed backend capability over a persistent connection

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), reassessed from CRITICAL in the first notice, rated MEDIUM by blast-radius escalation

The app ships purchase copy for a Remote Access subscription, a CommunicationService with an MQTT client error path in the dex string pool, and three operator hosts: api.nuki.io, phoenix-api-prod.nuki.io and sse.nuki.io. The operator's infrastructure can by product design command a physical door lock over the internet. This is a disclosed consumer feature and not a hidden backdoor.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because CVSS gives a documented feature with no demonstrated weakness 0.0. The finding is rated MEDIUM because a server that can reach into a physical door is a different risk category from one that only receives data, because the households affected include children and elderly residents who do not manage the account, and because the authorization checks before a command is relayed are not visible in the package. CRITICAL, as disclosed on 23 August 2026, is withdrawn because no weakness in the command path was shown.

```
<string name="purchase_remote_accss_title_1">Remote Control</string>
<string name="purchase_remote_accss_text_1">Open your door or securely lock –itno
    matter where you are.</string>
<string name="purchase_remote_accss_text_2">Grant virtual keys spontaneously to family
     members or friends.</string>
<string name="purchase_remote_accss_text_3">Check remotely who has locked your door
    and if it is securely closed.</string>
<string name="order_free_bridge_dialog_message">With the Nuki Bridge you can control
    your Smart Door from afar. For the first 30 days Remote Access is for free!</
    string>
```

```
<service android:enabled="true" android:exported="false" android:name="io.nuki.core.
    communication.CommunicationService"/>
<service android:enabled="true" android:exported="false" android:name="io.nuki.core.
    scanning.DeviceScannerService"/>

classes4.dex string: "dropping unparseable mqtt message on topic="
Hosts: https://api.nuki.io  https://phoenix-api-prod.nuki.io  https://sse.nuki.io (
    Server-Sent Events)
```

The capability is stated by the operator's own purchase text, so it is not an inference from remote-config plumbing. It is reported because a lock that can be commanded over the network belongs in every assessment of this product, not because it is hidden. Two questions cannot be answered from the package and are UNVERIFIED: which authentication and authorization the backend enforces before it relays a lock or unlock command, and whether the backend keeps its own audit trail for remote commands apart from the on-device activity log.

Impact: A household that buys Remote Access hands the operator's backend a path to its front door. Residents who do not manage the account, such as children, a partner or an elderly parent, depend on checks they cannot see. No failure of those checks is shown by this report.

Fix: Publish a short description of the authorization and audit model for remote commands, confirm that a DPIA exists for remote physical access control, and consider certificate pinning for the command channel (see M2).

C2: Named activity log of people who are not account holders, with retention stated only as a paid feature

---

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N, 0.0 (CVSS-B), reassessed from CRITICAL in the first notice, rated MEDIUM by blast-radius escalation

Fobs, fingerprints and keypad codes are named by the account owner and appear under that name in the activity log. Through the In-Home Delivery partnership with Austrian Post a courier receives temporary physical access and the owner can check in the log whether the courier entered. The only retention figure in the app strings, 6 months data storage, is bullet point 7 of the paid Smart Hosting subscription.

RFI-IRFOS blast-radius escalation: raised from NONE/0.0 to MEDIUM because CVSS gives a transparency gap with no attacker 0.0. The finding is rated MEDIUM because the people recorded are bystanders, such as children, cleaners and delivery staff, who cannot see a notice, cannot object and do not choose the label attached to their presence, and because the log records entry into a private home. CRITICAL, as disclosed on 23 August 2026, is withdrawn for two reasons. By the app's own wording the log is stored on the Nuki device and is copied to Nuki servers only when Nuki Web is used, so the first notice's word permanent is not supported for the default state. Server-side retention was not observed.

```
<string name="choose_fingerprint_name">Choose a name for your fingerprint</string>
<string name="fob_setup_device_change_fob_name_headline">What name should be assigned
    to this Fob in the activity log?</string>
<string name="ihd_description_clickable">By signing up for this service, you can allow
     Austrian Post to deliver parcels inside your home by opening the front door with
    your Nuki Smart Lock.<br/><br/>You can check if a courier has entered your home in
     the activity log.</string>
<string name="text_activity_log_action_locked">Locked</string>
<string name="text_activity_log_action_unlocked">Unlocked</string>
<string name="text_activity_log_action_unlatched">Opened door</string>
```

```
<string name="dialog_data_and_privacy_activity_log_text">The activity log is only
    stored on the Nuki device.<br/><br/>When using Nuki Web the activity log is
    synchronized from your device to the Nuki servers.<br/><br/>By deactivating the
    activity log in the Nuki App, the information will neither be recorded, nor stored
    . A subsequent activation or a deletion of individual entries is therefore not
    possible.</string>
<string name="smart_hosting_subscription_bulletpoint_7">6 months data storage</string>
```

The operator's disclosure for the deactivated state is plain and specific. For the active state

the strings give no retention period for the copy on Nuki servers. The only figure, six months, is listed next to a 15 percent accessory discount and a 3-year warranty as a Smart Hosting benefit. Whether the privacy policy states a period for users without Smart Hosting is UNVERIFIED because the policy text is not part of the evidence in the case folder. The Austrian Post integration is entered through io.nuki.in_home_delivery.InHomeDeliveryActivity. On 18 November 2026 the sender at ut11.net signing for Nuki stated that Nuki stores no copy of the activity log on any server unless the user signs up for Nuki Web, a service separate from general use of the Smart Lock, and that Nuki Web stores data for 3 months, or 12 months with an active Smart Hosting subscription. The app strings attach six months to Smart Hosting, so the two figures differ. The reply does not say where the retention period is stated to users under Art. 13(2)(a). The statement is not verified by RFI-IRFOS.

Impact: A cleaner, a teenager with a fob or a parcel courier is recorded by name and time at the door of a home, and the person has no way to learn how long that record is kept or who can see it. The courier in particular has no relationship with Nuki and receives no notice from it.

Fix: State to every user, in the app and the policy, how long the activity log is kept on Nuki servers for users with and without Smart Hosting, and describe how Art. 13 and Art. 14 information reaches fob holders, keypad users and delivery staff.

H1: Database that very likely holds the BLE pairing secret is included in cloud backup and device transfer

MEDIUM, CVSS v4.0 AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 4.1 (CVSS-B), disclosed as HIGH on 23 August 2026, rated MEDIUM in this report

data_extraction_rules.xml excludes device_private.xml from cloud backup and device transfer by name and includes nuki.db and fence-db in both. A Room schema string in classes4.dex defines an authorizations table with name, latitude, longitude, admin_pin and shared_key BLOB NOT NULL. No SQLCipher, SupportFactory or EncryptedSharedPreferences string was found in any of the six dex files.

```
<!-- res/xml/data_extraction_rules.xml, cloud-backup (device-transfer is identical)
    -->
<include domain="sharedpref" path="io.nuki.debug_preferences.xml" />
<include domain="sharedpref" path="io.nuki_preferences.xml" />
<exclude domain="sharedpref" path="device_private.xml" />
<include domain="database" path="nuki.db" />
<include domain="database" path="fence-db" />

<!-- AndroidManifest.xml -->
<application android:allowBackup="true" android:fullBackupOnly="true" android:
    backupAgent="io.nuki.BackupAgent" ...>
```

```
CREATE TABLE `authorizations` (`_id` INTEGER, `nuki_id` ..., `name` TEXT, `local_name`
    TEXT,
`shared_key` BLOB NOT NULL, `mac` TEXT, ..., `latitude` REAL, `longitude` REAL, ...,
`admin_pin` ..., `remote_allowed` ..., ...)
```

Two points are inferences and are marked UNVERIFIED. First, nuki.db is the only application-

named SQLite database in the string pool and is very likely the file behind the authorizations table, but the link was not shown by opening a backup. Second, whether shared_key is encrypted by the application before storage is unknown, because absence of SQLCipher strings does not exclude another encryption method. Two AndroidKeyStore string hits exist elsewhere and were not traced to this table.

RFI-IRFOS rates this finding MEDIUM on CVSS. An attacker needs the backup, which Android protects with the account credentials, as Nuki's reply of 3 September 2026 points out, or physical access to a device during transfer. If the key survives in cleartext in the backup, the consequence for a household is large, which is why the question about application-level encryption stays open. Rating it HIGH or CRITICAL on a configuration fact would overstate what was shown. On 18 November 2026 the sender at ut11.net signing for Nuki stated that shared_key is encrypted through platform means when it travels through cloud backup, since Android 9, and that nuki.db is required to restore access to locks after a backup is restored while device_private.xml is not. The reply states no encryption by the application before storage, so that question remains open. The statement is not verified by RFI-IRFOS.

Impact: If the pairing secret is stored unencrypted, a person who obtains a household member's backup could use it to authenticate to the physical lock. That outcome is not demonstrated. What is shown is a deliberate exclusion for one file and an inclusion for the database that likely holds the key.

Fix: Exclude nuki.db from cloud backup and device transfer or encrypt shared_key with a hardware-backed key before it is stored, and document the Art. 32 risk assessment for the choice.

H2: Firebase and Google API key, project identifiers and database URL readable in the package

---

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), disclosed as HIGH on 23 August 2026, rated MEDIUM in this report

res/values/strings.xml contains one Google API key reused for three declared purposes, the Firebase project noki-826 with its sender ID, app ID, Realtime Database URL, storage bucket and web client ID. All of it is extractable with apktool from any Play Store download. Restriction of the key and the Security Rules were not tested.

```
google_api_key                AIzaSyBFBSxCLiAcpA8dZ3HPaRatm9IZxM4nbGs
google_crash_reporting_api_key  AIzaSyBFBSxCLiAcpA8dZ3HPaRatm9IZxM4nbGs
google_play_services_api_key   AIzaSyBFBSxCLiAcpA8dZ3HPaRatm9IZxM4nbGs
google_app_id                 1:281434593386:android:a67d86e002fcbbe7
gcm_defaultSenderId           281434593386
firebase_database_url         https://noki-826.firebaseio.com
google_storage_bucket         noki-826.appspot.com
project_id                    noki-826
default_web_client_id         281434593386-20j9lpaeggtmekpl6bdip28oaghu9up9.apps.
    googleusercontent.com
```

Nuki's reply of 3 September 2026 states that the keys are public client IDs by design and that security is enforced server-side through Security Rules and app attestation. That is a legitimate architecture and RFI-IRFOS takes it at face value as a description. It is a vendor statement and is UNVERIFIED by this report, because no Nuki server was contacted. On 3

September 2026 RFI-IRFOS asked Nuki to confirm that the Security Rules on noki-826 are deny-by-default and that App Check or an equivalent is enforced in the current production build. The reply of 18 November 2026 does not address that question, which therefore remains unanswered on 21 November 2026.

The project identifier noki-826 differs from the product name. This is an operational observation and not a weakness.

Impact: Anyone can read the keys from the public app. If the key is unrestricted or the rules are permissive, a third party could consume quota or write to project resources. The effect on lock users would be indirect and none of it is demonstrated.

Fix: Restrict the key by package name and signing certificate, enforce App Check in production, and confirm in writing that the Security Rules are deny-by-default.

M1: Three exported components without intent filter or permission, including the courier-access entry point

---

LOW, CVSS v4.0 AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 2.1 (CVSS-B), added in this report, not itemised in the first notice

InHomeDeliveryActivity, GarminService and HarmonyWearService are declared exported with no intent filter and no android:permission. Another app on the same device can start them with an explicit intent. Behaviour after such a start was not exercised.

```
<activity android:exported="true" android:name="io.nuki.in_home_delivery.
    InHomeDeliveryActivity" android:screenOrientation="portrait" android:
    windowSoftInputMode="adjustResize"/>
<service android:exported="true" android:foregroundServiceType="connectedDevice"
    android:name="io.nuki.wearable.service.GarminService"/>
<service android:exported="true" android:foregroundServiceType="connectedDevice"
    android:name="io.nuki.wearable.service.HarmonyWearService"/>
```

Most other exported components in the manifest are protected by system-signature permissions (BIND_JOB_SERVICE, BIND_COMPANION_DEVICE_SERVICE, BIND_REMOTEVIEWS, DUMP) or are androidx and Firebase boilerplate. Impact depends on what the components do when launched outside their normal navigation, which is UNVERIFIED because dynamic testing was not part of this analysis.

Impact: A malicious app on the same phone could open the courier-access screen or start the wearable services. Whether this changes anything for the lock is not shown.

Fix: Set exported to false where no outside caller is needed, or protect each component with a signature-level permission, and verify the caller state in the component.

M2: No network security configuration and no certificate pinning on the control channel

LOW, CVSS v4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.3 (CVSS-B), added in this report, not itemised in the first notice

No res/xml/network_security_config.xml exists and the application tag carries no android:networkSecurityConfig attribute. At targetSdkVersion 36 the platform default blocks cleartext and uses the system CA store. No application-declared pinning exists for api.nuki.io, phoenix-api-prod.nuki.io, sse.nuki.io or the MQTT channel.

The platform default is a sound baseline and the absence of pinning is a proportionality question, not an automatic flaw. It is on record because the channel carries physical-access commands (C1). Whether the MQTT channel is encrypted with TLS is UNVERIFIED because no code flow was traced.

Impact: An attacker who can issue a certificate trusted by the phone and sits on the network path could observe or alter app traffic. That needs a trusted certificate on the device or a compromised authority.

Fix: Declare a network security configuration, consider pinning for the command hosts, and state the transport protection used for the MQTT channel.

Impact Analysis

- Household members and guests. A fob, fingerprint or keypad code is labelled by the account owner and shown in the log with times of locking and unlocking. The labelled person has no account and no notice (C2).
- Delivery staff. A courier on the Austrian Post integration is recorded entering a private home and has no relationship with Nuki (C2).
- Remote Access subscribers. They accept a network path to their door. Residents who do not manage the account depend on checks that are not visible in the package (C1).
- Users with cloud backup enabled. The database that likely holds the lock pairing secret travels with the backup, protected by the account and, if it exists, application-level encryption (H1).
- Operator and project. A readable client key set belongs to the operator’s own Firebase project. The effect on users is indirect (H2).

The Complete Chain

- 1. A household buys a lock and enrols a phone, a child's fob, a cleaner's code and a fingerprint. Each credential gets a name typed by the owner.
- 2. The lock records Locked, Unlocked and Opened door against each name. The log lives on the lock.
- 3. The owner uses Nuki Web or Smart Hosting. The log is copied to Nuki servers. Only the Smart Hosting bullet point mentions six months.
- 4. The owner signs up for In-Home Delivery. A courier enters and the entry is logged by name and time.
- 5. The owner buys Remote Access. Commands travel over MQTT through Nuki infrastructure.
- 6. The phone is backed up. nuki.db, likely holding shared_key for every credential, is included in the backup and in device transfer.

Each later section refers to one of these links. The harm is that the record of who enters a home, and the key that lets a phone open its door, are handled with less explanation than the person recorded would need.

Household Access, Couriers & Bystanders

A smart lock is a record of presence. Which credential opened the door and when describes who lives in a home, when they come and go, who visits and when the house is empty. Art. 9 GDPR is not engaged by that record as such, since no special category is shown, and this report does not rely on it. Art. 5(1)(e), Art. 13 and Art. 14 are engaged because the people in the log did not provide the data and did not receive a notice.

The household exemption of Art. 2(2)(c) may cover the account owner's use. It does not decide the operator's own position, because the operator designed the log, the naming flow and the courier integration. Nuki's reply of 3 September 2026 states that data subject rights apply in full and that the allegation of third-party processing without consent is incomprehensible. It names no mechanism that reaches a courier or a cleaner. On 18 November 2026 the sender at ut11.net signing for Nuki stated that the log lists only names defined by the device administrator, that only the administrator can see names and that the Austrian Post entry is a generic log line without a name. The reply names no Art. 13 or Art. 14 mechanism, and the statement is not verified by RFI-IRFOS. The question of the mechanism stands as asked.

Data Protection: Article by Article

Article	How it is engaged
Art. 5(1)(e)	Storage limitation. No retention period for the server copy of the activity log outside the Smart Hosting bullet point (C2).
Art. 5(1)(f)	Integrity and confidentiality. Database with the pairing secret included in backup (H1).
Art. 13(2)(a)	Storage period or criteria. Stated as a paid feature in the app strings. Policy text UNVERIFIED (C2).
Art. 13, Art. 14	Information for people logged without a Nuki account, among them Austrian Post delivery staff (C2).
Art. 25	Data protection by design. Selective backup exclusion for one file (H1), exported components (M1), remote control path (C1).
Art. 32(1)(a)	Encryption and state of the art measures. Pairing secret in backup (H1), no pinning (M2).
Art. 32(1)(b)	Integrity and resilience. Remote command path (C1), client key set (H2), exported components (M1).
Art. 35	DPIA for remote physical access control. Existence UNVERIFIED (C1).

Regulatory & Legal Landscape

The Datenschutzbehörde is the presumptive lead authority for an Austrian controller. It and the EDPS were informed for transparency. Research on the published package is protected by Art. 17 StGG and follows ISO/IEC 29147.

Industry comparison: Nuki's explanation of what deactivating the activity log does is a good model of plain disclosure. The same clarity is missing for the active state and for the people named in the log.

Indicators of Compromise & Reproducible Evidence

Every point below can be reproduced from the public package. The package was obtained from the APKPure mirror because the audit device was not reachable on the analysis day, and its version string matched the live Google Play listing before download.

```
Package       io.nuki
Version       2026.8.1 / versionCode 1369
Base APK      63.4 MB, SHA-256 0
    ff8a236a86ab63adf500d146197151c76a3513cabce45d147adcd10f1fe052d
Source bundle 84.6 MB XAPK (base + config.arm64_v8a + config.xxhdpi)
SDK           minSdkVersion 26, targetSdkVersion 36, compileSdk 36
Dex           six classes*.dex, about 45.7 MB combined
```

```
https://api.nuki.io
https://phoenix-api-prod.nuki.io
https://sse.nuki.io
https://noki-826.firebaseio.com
noki-826.appspot.com
Project ID     noki-826
Sender ID      281434593386
App ID         1:281434593386:android:a67d86e002fcbbe7
API key        AIzaSyBFBSxCLiAcpA8dZ3HPaRatm9IZxM4nbGs
Web client ID  281434593386-20j9lpaeggtmekpl6bdip28oaghu9up9.apps.googleusercontent.
    com
Privacy policy https://nuki.io/en-at/legal/data-privacy (Play listing)
In-app consent link https://nuki.io/legal/data-privacy
```

```
android-support@nuki.io   Play Store developer contact
contact@nuki.io            read from res/values/strings.xml
developer@nuki.io          Play Store developer contact
Support ticket 860439      reply of 2026-08-24 (Nuki Customer Operations)
Support ticket 869292      reply of 2026-09-03 (Nuki Customer Operations)
Reply 2026-11-18           from a sender at ut11.net signing for Nuki, authenticity
    not verified
```

Disclosure Timeline & Outcome

Date	Event
2026-08-23	Analysis of version 2026.8.1. Notice REF NUKI-2026-R1 sent to android-support@nuki.io and developer@nuki.io, copied to the Datenschutzbehörde and the EDPS. Three written questions.
2026-08-24	Holding reply from Nuki Customer Operations (ticket 860439). Nuki will gather the information and respond once everything is reviewed.
2026-09-03	Reply from Nuki (ticket 869292). It states that the findings stem from misinterpretations of an automated analysis, that none of the points is a security risk or a GDPR violation, and that the keys are public client IDs secured by Security Rules and app attestation. No retention period, no statement on application-level encryption of shared_key and no transparency mechanism for logged third parties is given.
2026-09-03	RFI-IRFOS answers on the same thread with the literal strings from the package and restates the questions. It asks Nuki to confirm deny-by-default Security Rules on noki-826 and enforced App Check.
2026-10-17	Reminder from security@rfi-irfos.com, 35 days before publication. Three questions unchanged. Written answers requested before 21 November 2026.
2026-11-15	6-day notice from security@rfi-irfos.com. Three questions unchanged, publication on 21 November 2026.
2026-11-18	Reply to security@rfi-irfos.com from a sender at ut11.net (subject line beginning Private Nachricht betreffend), signed as Head of Software Engineering of Nuki Home Solutions GmbH with a nuki.io address in the signature. Retention of 3 months for Nuki Web and 12 months with Smart Hosting, platform encryption of shared_key in backup, names in the log visible to the device administrator only. No statement on the Firebase question. Authenticity of the sender not verified, because the domain differs from nuki.io.
2026-11-21	Publication of this report, 90 days after delivery of the notice.

The operator received the same embargo date in every message. No request to extend it was made and none was granted. The third reply arrived on 18 November 2026, three days before publication.

What Nuki Got Right

- Firebase Analytics collection, performance collection, automatic screen reporting and advertising ID collection are disabled by manifest flags. No pre-consent Firebase Analytics was found.
- No advertising or attribution SDK was found among AppsFlyer, Adjust, Mixpanel, Amplitude, Segment, AppLovin, MoPub and Meta Audience Network.
- No Chinese or sanctioned-jurisdiction SDKs. The string hits for pangle and umeng were checked and are false positives (sweepAngle and a BouncyCastle Dilithium class).
- A GDPR consent dialog with a privacy policy link is present, and a data export feature (DataReportActivity) supports Art. 15 and Art. 20.
- The explanation of what deactivating the activity log does is honest, plain and specific.
- device_private.xml is excluded from backup and device transfer by name. The developers applied backup hygiene to at least one store, which makes H1 a specific, correctable gap.
- An app-level authentication gate (securitypin, PrivacyActivity) lets users require screen lock or biometrics before the app opens.
- Operator and partner are Austrian. No Art. 44 or Art. 46 question arose.
- On 18 November 2026 a reply from a sender at ut11.net signing for Nuki answered the three questions in writing and gave concrete retention periods for the server copy of the activity log. The authenticity of the sender is not verified.

Residual Risk & Recommendations

All six findings remain open at the severities stated. The reply of 18 November 2026 from a sender at ut11.net signing for Nuki answers the three questions in part. It gives retention periods for Nuki Web, states platform encryption for shared_key in backup and says that logged names are visible to the device administrator only. The Firebase question is unanswered and the authenticity of the sender is not verified. Versions after 2026.8.1 are not covered by this report. Server-side behaviour, the content of nuki.db in a real backup and the restriction of the Firebase key were not examined.

- State the retention period of the activity log on Nuki servers for every user, with and without Smart Hosting, and describe how Art. 13 and Art. 14 information reaches fob holders, keypad users and delivery staff.
- Say whether shared_key is encrypted at the application layer, and exclude nuki.db from cloud backup and device transfer or encrypt the key with a hardware-backed key.
- Confirm in writing that the Security Rules of noki-826 are deny-by-default and that App Check is enforced in production, and restrict the API key by package and certificate.
- Document the authorization and audit model for remote commands and the DPIA for remote physical access control.
- Set the three exported components to non-exported or protect them with signature permissions, and add a network security configuration with pinning for the command hosts.

RFI-IRFOS security@rfi-irfos.com • rfi-irfos.com

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Root level code analysis of the published application.

No Nuki servers or accounts were probed and no key was tested. Severity per CVSS v4.0 (CVSS-B) with explicit blast-radius escalation where stated. Final report, published 21 November 2026. ISO/IEC 29147, Art. 17 StGG, GDPR Art. 89. RFI-IRFOS, ZVR 1015608684, GISA 39261441. REF NUKI-2026-R1.