immoGenio

No. 02
April 2026

SMART-LOCK

Nuki neben Tapkey: Multi-Provider-Smart-Lock-Strategie für Übergaben, Handwerker und Hausmeister

Nuki als zweiter Smart-Lock-Provider neben Tapkey — OAuth 2.0, time-limited Grants im Übergabe-Wizard und Provider-Interface für gemischte Bestände.

AUTOR
ImmoGenio

VERÖFFENTLICHT
16. April 2026

ONLINE
www.immogenio.de/blog

— AUF EINEN BLICK

Inhalt

Die Geschichte eines gemischten Bestands

Eine Hausverwaltung in Süddeutschland betreut 612 Einheiten — verteilt auf 47 Liegenschaften, davon 18 Neubauten aus den Jahren 2022 bis 2025 und 29 Altbauten zwischen Baujahr 1964 und 2005. In den Neubauten ist von Beginn an Tapkey verbaut, weil der Bauträger das System der Verwaltung empfohlen hat. In den Altbauten gibt es ein anderes Bild: 38 Wohnungen sind nachträglich mit Nuki-Zylindern bestückt worden, weil einzelne Mieter ihr bisheriges Schloss elektronisch erweitern wollten und Nuki im Privatmarkt der etablierte Standard ist. In neun Wohnungen wurde der Mieter-eigene Nuki nach Auszug von der Verwaltung übernommen.

Das Ergebnis vor Einführung der Multi-Provider-Integration war eine doppelte Werkzeug-Landschaft. Die Sachbearbeiterin in der Verwaltung pflegte Tapkey-Grants über die Tapkey-Weboberfläche, Nuki-Berechtigungen über die Nuki-Web-App. Zwei getrennte Audit-Logs, zwei Login-Flows, zwei unterschiedliche Begriffe für „zeitlich begrenzte Berechtigung". Bei einer Übergabe in einem Altbau-Mehrfamilien-Haus mit gemischter Hardware musste die Sachbearbeiterin zwischen beiden Apps wechseln und sich für jede Wohnung erinnern, welche Hardware dort verbaut ist. Bei einem Wartungsauftrag des Hausmeisters über drei Wohnungen in einem Treppenhaus dasselbe Spiel — drei Klicks, drei Audit-Einträge, kein gemeinsames Log.

Die im April 2026 produktiv gegangene Multi-Provider-Erweiterung in ImmoGenio adressiert genau diese Lücke. Tapkey und Nuki erscheinen für den Verwalter als zwei austauschbare Provider hinter einem einheitlichen Workflow.

Warum Nuki und Tapkey beide existieren

Der Markt für elektronische Schließsysteme ist nicht ein Markt, sondern zwei. Auf der einen Seite stehen die Verwaltungs- und Gewerbe-Anbieter — Tapkey, Salto, iLoq, Kiwi.ki, dormakaba — mit Fokus auf Schließanlagen, Berechtigungs-Hierarchien und Integration in CAFM- oder Verwaltungs-Software. Auf der anderen Seite stehen die Consumer-Anbieter — Nuki, Yale Linus, Bold Smart Lock, Aqara — mit Fokus auf einfache Nachrüstung, Smart-Home-Integration und direkte Endkunden-Vermarktung. Tapkey gehört zur österreichischen Tapkey GmbH, Nuki zur österreichischen Nuki Home Solutions GmbH; beide Häuser kennen einander, adressieren aber unterschiedliche Käufergruppen.

In Wohnungsbeständen mischen sich diese Welten ständig. In einem Neubau entscheidet der Bauträger oder der erste Verwalter, was verbaut wird — in der Regel ein Verwaltungs-Produkt mit Schließanlagen-Logik. In Bestandsbauten dagegen entscheidet oft der Mieter, was an seiner Wohnungstür hängt. Nach § 535 BGB schuldet der Vermieter die Bereitstel-

lung der Mietsache; eine elektronische Aufrüstung der Wohnungstür ist ein Mieterausbau, der nach § 539 BGB bei Auszug rückgängig zu machen ist oder durch Ablöse übernommen wird. Genau diese Übernahme erzeugt die Realität: Die Verwaltung erbt nach und nach Nuki-Schlösser aus Mieterhand.

Ein zweiter Treiber ist die Hardware-Logik. Nuki rüstet auf einen bestehenden Profilzylinder auf — der mechanische Schlüssel bleibt funktional, das Knaufmodul wird innen aufgesetzt. Das ist in denkmalgeschützten Beständen und bei WEG-Gemeinschaften mit Beschluss-Pflicht nach § 20 Abs. 1 WEG attraktiv, weil der Eingriff in das Gemeinschaftseigentum minimal bleibt. Tapkey dagegen tauscht in der Regel den Zylinder selbst aus, was bei zentralen Schließanlagen mit Gleichschließung sinnvoller ist. Beide Systeme haben damit klare Anwendungsfelder — und die Verwaltungsrealität verlangt, beide bedienen zu können.

Provider-Strategy-Pattern in der Praxis

Die ImmoGenio-Architektur bildet beide Provider hinter einem gemeinsamen Interface ab. Das fachliche Konzept ist immer dasselbe: eine zeitlich begrenzte, an einen Kontext gebundene Berechtigung für eine bestimmte Tür für eine bestimmte Person. Die Unterschiede zwischen Tapkey und Nuki liegen ausschließlich in der konkreten API-Anbindung.

Auf der obersten Ebene definiert das Backend ein Interface `ISmartLockProvider` mit den Methoden `connect`, `listLocks`, `createGrant`, `revokeGrant`, `listAccessEvents`. Jeder Provider bringt eine konkrete Implementierung mit — `TapkeyProvider` und `NukiProvider`. Beide leben hinter derselben Service-Schicht, die der Übergabe-Wizard und das Task-Board konsumieren. Die Geschäftslogik kennt keinen Provider — sie kennt nur Locks, Grants und Kontext-IDs.

Im Datenmodell hält die Tabelle `smart_locks` einen Eintrag pro physischer Tür mit dem Attribut `provider_type` mit dem Wertebereich `'tapkey' | 'nuki'`. Die Whitelist ist als CHECK-Constraint formuliert und gemäß DSGVO Art. 32 Abs. 1 lit. b geschützt; eine versehentliche Wert-Ausweitung („salto", „kiwi") führt zum Insert-Fehler, nicht zu stiller Annahme einer unbekannten API. Die Tabelle `smart_lock_grants` referenziert über `lock_id` das jeweilige Schloss und übernimmt damit transitiv den Provider. Felder wie `start_at`, `end_at`, `context_type`, `context_id`, `revoked_at` und `provider_grant_id` sind provider-unabhängig.

Die Webhook-Verarbeitung läuft auf einem gemeinsamen Endpoint `/webhooks/smart-lock`, der eingehende Events anhand des Headers `X-Provider` und einer HMAC-Signatur identifiziert. Der HMAC-Verify nutzt pro Provider ein eigenes Secret aus dem SOPS-verschlüsselten Secret-Store; die Verifikation erfolgt vor jeder Geschäftslogik, sodass ungesignierte Events nach Art. 5 Abs. 1 lit. f DSGVO ausnahmslos verworfen werden. Nach er-

folgreichem Verify wird das Event an den jeweiligen Provider-Handler weitergeleitet, der das Tapkey- oder Nuki-spezifische Payload in das gemeinsame interne Format überführt. Diese Mechanik baut auf den im Tapkey-Vorgängerartikel beschriebenen OAuth-Token-Pattern auf — Auto-Refresh, Circuit-Breaker bei 401, mandanten-spezifische Token-Verschlüsselung.

Unterschiede der Anbieter — wo Nuki anders tickt

Hinter dem gemeinsamen Interface gibt es vier wesentliche Unterschiede, die für Verwaltung und Mieter spürbar werden.

Hardware-Footprint. Nuki Smart Lock 4.0 Pro wird als Knaufaufsatz innen montiert; der bestehende Profilzylinder bleibt unverändert, der mechanische Schlüssel weiterhin funktional. Bei Tapkey wird in der Regel ein neuer Schließzylinder eingebaut, der das mechanische Schließen entweder gar nicht oder nur über einen Tapkey-Notschlüssel zulässt. Für eine WEG mit Beschluss-Pflicht nach § 20 WEG ist Nuki damit deutlich beschluss-ärmer; für eine zentrale Schließanlage mit Generalschlüssel ist Tapkey die strukturell saubere Wahl.

App-Modell. Beide Provider setzen primär auf eine Smartphone-App des Endnutzers. Nuki erlaubt zusätzlich die Vergabe von numerischen Codes über das Keypad-Zubehör, das per Bluetooth mit dem Smart Lock kommuniziert. Tapkey unterstützt NFC-Token als Backup-Pfad. Beide Varianten sind in ImmoGenio als Fallback im Übergabe-Protokoll dokumentierbar; der Versand und die Rückgabe physischer Tokens läuft weiterhin außerhalb des Grant-Lifecycles.

Authentifizierung und Pairing. Beide Provider verwenden OAuth 2.0 mit Authorization-Code-Flow nach RFC 6749. Nuki ergänzt dies um eine Bluetooth-Pairing-Phase: Bevor ein Smart Lock über die Web-API steuerbar ist, muss es einmalig per Bluetooth mit der Nuki-App gekoppelt und dann mit dem Web-Account verbunden werden. Diese Initial-Pairing-Phase erfolgt außerhalb von ImmoGenio durch den Verwalter oder den Hausmeister vor Ort. Erst danach erscheint das Lock im API-Listing und kann im Portal registriert werden.

Bridge-Notwendigkeit. Damit ein Smart Lock aus der Ferne über das Internet erreichbar ist, braucht Nuki entweder die Nuki Bridge oder ein Smart Lock 3.0 Pro / 4.0 Pro mit eingebautem WLAN-Modul. Ohne Bridge ist das Lock nur per Bluetooth aus unmittelbarer Nähe steuerbar — was für Übergaben in größeren Beständen praxisuntauglich ist. Tapkey-Schlösser arbeiten nach dem Offline-Online-Hybrid-Prinzip: Ein Token wird vor dem Termin online geladen und ist danach auch ohne Verbindung zum Tür-Schloss verwendbar. Für die Verwaltung bedeutet das: Bei Nuki-Beständen ist die Bridge-Versorgung Teil der initialen Hardware-Planung; bei Tapkey reicht ein zuverlässiger Online-Zugang des Endgeräts vor dem Termin.

Format der Audit-Logs. Beide Provider liefern Zugriffs-Protokolle per REST-API. Tapkey gibt pro Event `userId`, `lockId`, `timestamp` und Grant-Referenz aus; Nuki liefert pro Event `smartlockAuthId`, `name`, `action`, `trigger` und `date`. Die ImmoGenio-Adapter normalisieren beide Formate auf ein gemeinsames Schema mit `lock_id`, `actor_ref`, `action_type`, `occurred_at` und legen es in der internen Tabelle `smart_lock_access_log` ab. Erst diese Normalisierung erlaubt ein provider-übergreifendes Audit-Log nach Art. 30 DSGVO.

Wie ImmoGenio das integriert

Die Provider-Auswahl beginnt im Wohnungs-Modul. Pro Einheit lassen sich beliebig viele Schlösser hinterlegen — Wohnungstür, Briefkasten, Keller, Tiefgarage — und pro Schloss wird der Provider gewählt. Die Auswahl ist nach dem ersten erfolgreichen Grant nicht mehr ohne weiteres änderbar, weil ein Provider-Wechsel im laufenden Betrieb eine Hardware-Aktion an der Tür erfordert. Wechsel sind möglich, werden aber als eigenständiger Hardware-Vorgang behandelt und im Audit-Trail dokumentiert.

Im Übergabe-Wizard erscheint pro Schloss ein einheitliches Bedien-Panel namens `LockGrantPanel`. Das Panel rendert provider-spezifische Setup-Hinweise — bei Nuki etwa der Status der Bridge-Verbindung und das letzte Online-Zeichen des Smart Locks, bei Tapkey der Status der Token-Synchronisierung. Die eigentliche Grant-Konfiguration ist providerunabhängig: Person auswählen, Start- und Endezeitpunkt setzen, Kontext-Bindung an die Übergabe automatisch übernehmen. Erst beim Absenden delegiert das Backend an den passenden Provider.

Der Grant-Lifecycle ist provider-übergreifend gleich. Ein Cron-Job läuft täglich um 04:00 UTC und markiert alle Grants, deren `end_at` in der Vergangenheit liegt, mit einem `revoked_at`-Zeitstempel. Parallel werden über die Provider-APIs Revoke-Aufrufe abgesetzt, damit das Lock selbst keine Berechtigung mehr akzeptiert. Bei Webhook-Events „Grant wurde manuell am Provider widerrufen" wird der interne Datensatz synchron auf `revoked_at` gesetzt. Diese Mechanik schließt eine Lücke, die im Tapkey-Vorgängerartikel als Fehlerbild „vergessenes Widerrufen" beschrieben war — die Konsistenz ist nun nicht mehr von der manuellen Disziplin der Sachbearbeitung abhängig.

Pro Tenant lassen sich beide Provider parallel aktivieren. Dafür liegen pro Provider eigene OAuth-Konfigurationen, eigene Refresh-Tokens und eigene HMAC-Secrets im verschlüsselten Mandanten-Datenraum. Die Implementierung folgt Art. 32 Abs. 1 lit. a DSGVO: Verschlüsselung personenbezogener Daten — der Refresh-Token gilt als Schlüsselmaterial für den Zugang zu personenbezogenen Zugriffs-Logs und ist entsprechend mit AES-256 symmetrisch im Datenraum abgelegt. Pro Lock bleibt allerdings genau ein Provider erlaubt — eine parallele Belegung derselben Tür durch zwei Anbieter ist in v1 nicht vorgesehen.

Praxis: Übergabe in einem Bestand mit beiden Anbietern

Ein Mehrfamilien-Haus aus Baujahr 1989 mit acht Wohneinheiten wird verwaltet. In Wohnung 1 hat der Vor-Mieter sein Nuki Smart Lock 4.0 Pro nach Auszug an die Verwaltung verkauft — die Bridge hängt im Treppenhaus an einer Steckdose der Allgemeinfläche und versorgt zusätzlich Wohnung 3 und Wohnung 6 mit. In Wohnung 2 ist im Rahmen einer Sanierung ein Tapkey-Zylinder eingebaut worden. Beide Wohnungen sollen am selben Tag an neue Mieter übergeben werden.

Im Übergabe-Wizard öffnet die Sachbearbeiterin nacheinander die beiden Übergabe-Vorgänge. Für Wohnung 1 zeigt das `LockGrantPanel` den Status der Bridge — zuletzt online vor zwei Minuten, Smart Lock antwortet auf Ping — und einen Hinweis, dass für den Mieter ein Nuki-Konto vorhanden ist. Sie wählt den Mieter aus, setzt den Start auf den 1. Mai 09:00 Uhr und das Ende auf das Mietende, bestätigt. Im Hintergrund läuft ein OAuth-Request gegen die Nuki Web API, ein Grant wird angelegt, die Grant-ID wird im Datensatz gespeichert.

Für Wohnung 2 ändert sich für die Sachbearbeiterin im Wizard nichts an der Bedienung. Sie wählt den Mieter, setzt Start und Ende, bestätigt. Im Hintergrund läuft jetzt ein OAuth-Request gegen die Tapkey-API mit derselben fachlichen Bedeutung — zeitlich begrenzter Grant, Kontext-Bindung an die Übergabe-ID. Im Audit-Log unter der Liegenschaft erscheinen beide Aktionen in derselben Liste; die einzige sichtbare Unterscheidung ist eine kleine Provider-Markierung in der Spalte „Quelle".

Zwei Tage später öffnet der Hausmeister beide Wohnungen für eine Schlüsselübergabe-Begleitung. Beide Zugriffe landen im selben normalisierten Access-Log mit `action_type='unlock'`, `actor_ref='hausmeister:18'`, `occurred_at`-Zeitstempel und der jeweiligen `lock_id`. Für den Verwalter ist die Sicht einheitlich; für die DSGVO-Auskunft nach Art. 15 sind alle Zugriffe einer Person provider-übergreifend abrufbar.

Compliance-Anker

Die Multi-Provider-Architektur erbt die Compliance-Logik der Tapkey-Erstimplementierung und erweitert sie um die Nuki-spezifischen Aspekte. Sechs Anker sind dabei verbindlich.

Vertraulichkeit nach Art. 5 Abs. 1 lit. f DSGVO. Jeder Grant ist an einen konkreten Kontext gebunden — Übergabe-ID, Task-ID, Mietverhältnis-ID. Ein „Master-Key-Versehen" mit unbefristeter Berechtigung ist im Datenmodell nicht erlaubt; das CHECK-Constraint auf `smart_lock_grants` verlangt ein `end_at` ungleich NULL.

Berechtigtes Interesse nach Art. 6 Abs. 1 lit. f DSGVO. Die Verarbeitung der Zugriffs-Logs stützt sich auf das berechtigte Interesse an Gebäudesicherheit und Nachvollziehbarkeit von Schlüssel-Bewegungen. Eine Mieter-Einwilligung ist nicht erforderlich, eine Information nach Art. 13 DSGVO im Mietvertrag und im Übergabeprotokoll dagegen Pflicht.

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO. Refresh-Token beider Provider sind AES-256-symmetrisch mit einem mandanten-spezifischen Schlüssel im Datenraum verschlüsselt. HMAC-Secrets für die Webhook-Verifikation liegen in SOPS-verschlüsselten Secret-Files und werden im Container nur zur Laufzeit entschlüsselt.

Verschaffungspflicht nach § 535 Abs. 1 BGB. Der Mieter muss zum vertraglich vereinbarten Zeitpunkt Zugang zur Wohnung erhalten. Der Grant-Lifecycle bildet diesen Anspruch ab; das Start-Datum des Mieter-Grants ist standardmäßig der erste Tag des Mietverhältnisses, eine spätere Aktivierung ist nur mit dokumentierter Begründung möglich.

Wohnungsgeberbescheinigung nach § 19 BMG. Der Vermieter ist zur Bestätigung des tatsächlichen Einzugszeitpunkts verpflichtet. Der erste Unlock-Event durch den Mieter wird im Audit-Log mit Datum protokolliert und kann bei einer behördlichen Rückfrage als ergänzender Nachweis herangezogen werden.

90-Tage-Retention für Zugriffs-Logs. Standardmäßig werden Zugriffs-Logs nach 90 Tagen über den Retention-Cron gelöscht. Diese Frist ist im Tapkey-Vorgängerartikel hergeleitet und gilt provider-übergreifend; eine Verlängerung ist nur anlassbezogen zulässig.

Grenzen v1

Die produktive Erweiterung trägt mehrere Einschränkungen, die in der Roadmap adressiert werden.

Pro Lock ist genau ein Provider zulässig — ein paralleles Multi-Provider-Setup an derselben Tür, etwa Tapkey-Zylinder plus Nuki-Knauf außen, ist im Datenmodell und im Wizard nicht vorgesehen. Salto, Kiwi.ki und iLoq sind als Provider-Implementierungen vorbereitet, aber nicht produktiv freigegeben; das Interface trägt sie, die konkreten Adapter sind in Vorbereitung. Eine eigenständige Lock-Verwaltungs-Oberfläche im Portal existiert nicht — Locks werden ausschließlich im Kontext einer Wohnung oder eines Übergabe-Vorgangs angelegt und gepflegt. Die Bluetooth-Pairing-Phase eines neuen Nuki Smart Locks erfolgt nicht aus dem Portal heraus, sondern weiterhin über die Nuki-App vor Ort durch den Verwalter oder Hausmeister.

FAQ

Brauche ich für Nuki eine zusätzliche Bridge?

Für die fernsteuerbare Vergabe von Grants über die Web API ist ein Online-Zugang des Smart Locks erforderlich. Bei den Geräten Nuki Smart Lock 3.0 Pro und 4.0 Pro ist das WLAN-Modul eingebaut; eine separate Bridge ist dann nicht nötig. Bei älteren Modellen oder bei den Standard-Varianten ohne Pro-Zusatz wird die Nuki Bridge benötigt, die im Treppenhaus oder in der Wohnung an einer Steckdose betrieben wird. Eine Bridge versorgt mehrere Smart Locks in Funkreichweite, was in Mehrfamilien-Häusern oft ausreicht.

Wie unterscheiden sich die Kosten zwischen Tapkey und Nuki?

Die Hardware-Kosten pro Tür liegen bei beiden Anbietern in einer ähnlichen Größenordnung, mit Schwankungen je nach Modell und Mengenrabatt. Tapkey-Zylinder erfordern den Tausch des kompletten Profilzylinders, was bei abweichenden Türstärken einen zusätzlichen Schlosser-Aufwand bedeuten kann. Nuki-Knaufaufsätze sind in der Selbstmontage unproblematisch, sofern ein zur Aufnahme geeigneter Profilzylinder bereits vorhanden ist. Auf Software-Seite fallen bei beiden Providern API-Lizenzkosten je Lock und Monat an; die genauen Tarife sind direkt mit den Herstellern zu vereinbaren und nicht Teil der ImmoGenio-Lizenz.

Kann ich später von Tapkey auf Nuki wechseln?

Ein Provider-Wechsel pro Schloss ist möglich, erfordert aber eine Hardware-Aktion an der Tür. In ImmoGenio wird der Wechsel als eigener Vorgang protokolliert: Der bisherige Provider-Eintrag wird deaktiviert und mit `revoked_at` versehen, der neue Provider-Eintrag wird angelegt, alle aktiven Grants werden auf den neuen Provider migriert mit einer dokumentierten Übergangsphase. Während dieser Phase müssen die Mieter ihre App-Konfiguration aktualisieren; das Übergabe-Modul stellt dafür eine Mieter-Information bereit.

Was passiert, wenn der Mieter sein Nuki-Konto löscht?

Die Berechtigung im Smart Lock selbst bleibt zunächst bestehen, weil der Grant auf der Verwaltungs-Organisation in der Nuki-Web-API liegt und nicht am Mieter-Konto. Allerdings verliert der Mieter den Zugang über die Nuki-App, sobald sein Konto gelöscht ist. In dieser Situation wird im Übergabe-Modul ein Warn-Event ausgelöst, und der Verwalter kann mit dem Mieter klären, ob ein neues Konto angelegt werden soll oder ob auf Keypad-Code als Zugangsweg umgestellt wird.

Können wir Nuki-Daten in unseren Audit-Trail integrieren?

Die normalisierten Zugriffs-Logs werden provider-übergreifend in `smart_lock_access_log` abgelegt und sind über die Standard-Audit-Trail-Sicht des Mandanten zugänglich. Eine zusätzliche Übergabe an externe SIEM-Systeme ist als API-Export vorgesehen und wird in Q4 2026 produktiv. Bis dahin steht der Export als CSV und JSON über das Audit-Modul zur Verfügung.

Welche Hardware ist für Nuki nötig?

Pro Tür wird ein Nuki Smart Lock benötigt — empfohlen sind die Modelle 3.0 Pro oder 4.0 Pro mit eingebautem WLAN. Optional ist das Nuki Keypad 2.0 für die Code-Eingabe ohne Smartphone. Bei Standard-Smart-Locks ohne WLAN ist eine Nuki Bridge je Liegenschaft notwendig, die zentral im Treppenhaus oder in einer der angeschlossenen Wohnungen betrieben wird und mehrere Locks in Funkreichweite versorgt.

Verwandte Beiträge

- Smart-Lock-Integration mit Tapkey, OAuth und time-limited Grants
- Wohnungsübergabe per Tablet mit eIDAS-Signatur und Mängelfotos
- Hausmeister-Vertrag und Task-Board mit Kanban und Gantt
- Audit-Trail, Mutationen und Revisionssicherheit über Append-Only-Strukturen

Wo wir stehen

Die Nuki-Anbindung ist seit April 2026 produktiv im Übergabe-Wizard und im Task-Detail neben Tapkey verfügbar. Bei den Pilot-Mandanten mit gemischten Beständen liegt die Provider-Verteilung pro Liegenschaft typischerweise zwischen 30 und 70 Prozent — keine Liegenschaft ist vollständig homogen, was die Notwendigkeit der Multi-Provider-Strategie in der Praxis bestätigt. Salto und iLoq sind als nächste Provider in der Roadmap; die Erweiterung des `provider_type`-Enums und die jeweiligen Adapter sind in Vorbereitung.

Kontakt

Fragen, Rückmeldungen oder eigene Erfahrungen mit Multi-Provider-Smart-Lock-Setups in der Hausverwaltung? Wir freuen uns über Ihre Nachricht an kontakt@immogenio.de.