

SMART-LOCK

Smart-Lock in der Wohnungsübergabe: Tapkey-OAuth, time-limited Grants — und die DSGVO-Frage zum Zugriffs-Log

Smart-Lock-Integration mit Tapkey: OAuth-Authorization-Code, time-limited Grants gebunden an Übergabe- und Task-IDs

AUTOR

ImmoGenio

VERÖFFENTLICHT

1. September 2026

ONLINE

www.immogenio.de/blog

Inhalt

- 01 Die Geschichte einer verlegten Schlüsselübergabe

- 02 Was die Smart-Lock-Integration leistet

- 03 Die OAuth-Anbindung im Detail

- 04 Time-limited Grants — der zentrale Sicherheitsmechanismus

- 05 Die Bindung an Übergabe- und Task-IDs

- 06 Die DSGVO-Frage zum Zugriffs-Log

- 07 Mehr-Provider-Strategie und ihre Grenzen

- 08 Die fünf häufigsten Fehler bei der Smart-Lock-Einführung

- 09 Praxis-Beispiel: Mieterwechsel mit Smart-Lock

- 10 Wie ImmoGenio die Smart-Lock-Funktion abbildet

- 11 Verbindung zu angrenzenden Modulen

- 12 Grenzen der aktuellen Lösung

13 Wo wir stehen

14 Kontakt

Die Geschichte einer verlegten Schlüsselübergabe

Eine Hausverwaltung mit 380 Einheiten in einem Mehrfamilien-Bestand führt jährlich rund 90 Mieterwechsel durch. Bei jedem Wechsel müssen Schlüssel ausgegeben, abgegeben und im Zweifel ausgetauscht werden. Eine Sachbearbeiterin rechnet vor: Vier Schlüssel pro Wohnung, dazu Briefkasten, Keller, Müll-Container, Tiefgarage. 24 Schlüssel pro Wohnungswechsel, mal 90 — gibt 2.160 Schlüsselbewegungen pro Jahr. Bei einem Verlust werden im Schnitt 1.200 Euro Kosten ausgelöst, weil die gesamte Schließanlage des Hauses zumindest in einem Strang neu eingerichtet werden muss. In den letzten zwei Jahren waren das fünf Verlustfälle, gerundet 6.000 Euro Schaden.

Im Sommer 2026 stellt die Verwaltung in einem Pilot-Objekt vier Wohnungen auf elektronische Smart-Lock-Schlösser um. Die Übergabe an den neuen Mieter läuft ohne physischen Schlüssel: Der Mieter erhält über sein Smartphone einen zeitlich begrenzten Zugang. Der alte Mieter behält bis zum Übergabetermin seinen Zugang, danach erlischt er automatisch. Schlüsselverluste sind nicht mehr möglich; das Risiko des Schließzylinder-Tauschs entfällt.

Was sich auf den ersten Blick wie eine reine Komfortverbesserung anhört, ist tatsächlich eine technisch und datenschutzrechtlich komplexe Architektur. Die OAuth-Anbindung, die Bindung der Berechtigungen an Übergabe- und Task-IDs und die Handhabung der Zugriffs-Logs müssen zusammenpassen — sonst entsteht ein Datenschutz-Risiko, das sich erst im Audit zeigt.

Was die Smart-Lock-Integration leistet

Die Integration in ImmoGenio erfolgt aktuell über Tapkey, einen marktführenden Anbieter elektronischer Schließsysteme. Die Architektur folgt drei Prinzipien:

- 1. OAuth-Authorization-Code-Flow.** Die Verbindung zwischen ImmoGenio und Tapkey läuft über OAuth 2.0 mit Authorization Code. Die Verwaltung autorisiert ihre Tapkey-Organisation einmal über einen Browser-Redirect; ImmoGenio erhält im Gegenzug Access- und Refresh-Token. Der Refresh-Token wird verschlüsselt im Mandanten-Datenraum gespeichert; der Access-Token wird automatisch 60 Sekunden vor Ablauf erneuert.
- 2. Time-limited Grants.** Jede Schliess-Berechtigung hat ein Start- und ein Endezeitpunkt. Ohne explizite Begrenzung wird kein Grant ausgegeben. Die Zeitfenster werden an die Lebenszyklen der Verwaltungs-Vorgänge gekoppelt — Mietbeginn bis Mietende, Übergabetermin bis 24 Stunden nach Übergabe, Wartungsauftrag bis Auftragsende.

3. Kontextgebundene Bindung. Jeder Grant ist im System mit einer Übergabe-ID, einer Task-ID oder einer Mietverhältnis-ID verknüpft. Wird der zugrunde liegende Vorgang abgeschlossen oder storniert, wird der Grant automatisch widerrufen. So entsteht keine „verwaiste“ Berechtigung, die nach Tagen oder Wochen noch existiert.

Die OAuth-Anbindung im Detail

Der Authorization-Code-Flow funktioniert nach RFC 6749. Der Verwalter klickt im Portal-Modul „Smart-Lock-Integration“ auf „Mit Tapkey verbinden“. Es öffnet sich ein Pop-up zu Tapkey, dort meldet er sich mit seinem Tapkey-Account an und genehmigt die Verbindung. Tapkey leitet ihn zurück zu ImmoGenio mit einem temporären Authorization-Code. Das Backend tauscht diesen Code gegen Access- und Refresh-Token ein.

Wichtig sind drei Aspekte:

Refresh-Strategie. Der Access-Token läuft typisch nach 60 Minuten ab. Vor jedem API-Call zu Tapkey prüft das Backend die verbleibende Lebensdauer. Liegt sie unter 60 Sekunden, wird automatisch über den Refresh-Token ein neuer Access-Token geholt. Der Aufrufer merkt davon nichts.

Circuit-Breaker bei 401. Wird die Tapkey-Organisation gelöscht oder die Verbindung am Tapkey-Ende widerrufen, schlägt der Refresh-Token-Tausch mit 401 fehl. Das Backend stoppt dann automatisch alle ausgehenden Grant-Requests, markiert die Integration als „nicht mehr verbunden“ und benachrichtigt den Verwalter. Vermieden wird so, dass das System minutenlang in 401-Schleifen läuft.

Verschlüsselung der Token. Refresh-Token sind langlebig (Wochen oder Monate). Sie werden mit einem mandanten-spezifischen Schlüssel symmetrisch verschlüsselt im Datenraum gespeichert. Bei Diebstahl der Datenbank ohne den Schlüssel sind die Token unbrauchbar.

Die gleiche Architektur kommt im Beitrag zu DATEV Connect via OAuth mit identischer Mechanik zum Einsatz — Token-Verschlüsselung, Auto-Refresh, Circuit-Breaker.

Time-limited Grants — der zentrale Sicherheitsmechanismus

Tapkey kennt zwei Grant-Typen: zeitbeschränkt und unbefristet. ImmoGenio gibt ausschließlich zeitbeschränkte Grants aus. Die Zeitfenster werden je nach Anwendungsfall berechnet:

Mieter-Zugang. Beginn: Tag der Schlüsselübergabe, 0:00 Uhr. Ende: Tag des Auszugs, 23:59 Uhr. Bei Vertragsverlängerung wird der Grant verlängert, nicht neu ausgestellt. Bei vorzeitiger Beendigung des Mietverhältnisses wird der Grant zum entsprechenden Datum widerrufen.

Hausmeister-Zugang. Bei einem Wartungs-Task wird der Grant für die geplante Wartungszeit plus zwei Stunden Puffer ausgestellt. Endet der Task durch Bestätigung der Erledigung, wird der Grant unmittelbar widerrufen — nicht erst nach Ablauf des Zeitfensters.

Übergabe-Zugang. Vor einer geplanten Wohnungsübergabe erhält der neue Mieter einen Grant für die zwei Stunden um den Übergabetermin. Nach Bestätigung der erfolgten Übergabe geht der Zugang in den dauerhaften Mieter-Zugang über.

Gewerblicher Dienstleister. Reinigung, Trockenbau, Maler — die Berechtigung läuft strikt nur an Werktagen zwischen 7:00 und 18:00 Uhr und nur für die geplante Auftragsdauer. Sonntags-Zugriff ohne Sondergenehmigung ist nicht möglich.

Jeder Grant hat damit eine klare zeitliche und inhaltliche Begrenzung. Vergessenes Widerrufen kann nicht zu dauerhaften Berechtigungen führen — der Grant erlischt spätestens mit Ablauf seines Zeitfensters automatisch.

Die Bindung an Übergabe- und Task-IDs

Tapkey selbst kennt keinen direkten Bezug zu „Übergabe“ oder „Task“ — diese Konzepte stammen aus ImmoGenio. Die Bindung erfolgt über Metadaten:

Jeder Grant in Tapkey wird mit einer ImmoGenio-internen Referenz angelegt — typisch im Format `uebergabe:42` oder `task:1018`. Diese Referenz erscheint im Tapkey-Audit-Log und im ImmoGenio-eigenen Audit-Trail. Wird im Portal eine Übergabe storniert oder ein Task abgeschlossen, sucht das Backend in Tapkey alle Grants mit der entsprechenden Referenz und widerruft sie.

Diese Bindung ist entscheidend für die DSGVO-konforme Handhabung. Wird ein Mieter aus dem System entfernt (etwa: nach Auszug und Ablauf der Aufbewahrungsfristen), werden alle ihm zugeordneten Grants widerrufen — nicht nur die aktiven, sondern auch die historischen Datensätze über Tapkey.

Die DSGVO-Frage zum Zugriffs-Log

Smart-Lock-Systeme protokollieren jeden Zugriffsversuch — wer hat wann welche Tür mit welchem Token geöffnet. Diese Daten sind aus Sicht der DSGVO personenbezogen, sofern sie einer natürlichen Person zugeordnet werden können. Drei Punkte sind zu klären:

1. Rechtsgrundlage. Die Verarbeitung der Zugriffs-Logs erfolgt auf Basis der Rechtsgrundlage „berechtigtes Interesse“ nach Art. 6 Abs. 1 lit. f DSGVO. Berechtigte Interessen sind die Sicherheit des Gebäudes, die Nachvollziehbarkeit von Schlüssel-Bewegungen und die Möglichkeit zur Aufklärung im Schadensfall. Eine Einwilligung des Mieters ist nicht erforderlich, aber eine transparente Information gemäß Art. 13 DSGVO ist Pflicht.

2. Aufbewahrungsdauer. Standardmässig sind die Zugriffs-Logs auf 90 Tage begrenzt. Das genügt für die Aufklärung von Vorfällen (Brand, Einbruch, Schaden) und steht im Verhältnis zum berechtigten Interesse. Längere Aufbewahrung — etwa 12 oder 24 Monate — ist nur bei konkretem Anlass zulässig (laufendes Ermittlungsverfahren, Schadensregulierung).

3. Auskunftsrecht und Löschung. Der Mieter hat nach Art. 15 DSGVO ein Recht auf Auskunft, welche Zugriffsdaten zu ihm gespeichert sind. Nach Auszug und Ablauf der berechtigten Aufbewahrung muss die Löschung umgesetzt werden. Bei einer Anfrage des ehemaligen Mieters ist die Verwaltung in der Pflicht, innerhalb eines Monats Auskunft zu geben oder zu löschen.

In ImmoGenio sind die Zugriffs-Logs an die Übergabe-IDs und Mietverhältnis-IDs gebunden. Beim Auszug eines Mieters und Ablauf der gesetzlichen Aufbewahrungsfristen werden die Logs automatisch über den Retention-Cron gelöscht. Die Mechanik ist im Beitrag zu den [Aufbewahrungsfristen in der Hausverwaltung](#) beschrieben.

Mehr-Provider-Strategie und ihre Grenzen

Tapkey ist nicht der einzige Anbieter. Nuki, Kiwi.ki, iLoq, Salto und einige weitere bieten ähnliche Funktionen mit eigenen APIs. ImmoGenio hat den Tapkey-Connector als Erstimplementierung produktiv und bereitet die Schnittstelle so, dass weitere Provider angebunden werden können — die Abstraktionsschicht trennt das fachliche Konzept „Grant für Wohnung X von Zeitpunkt A bis B“ von der konkreten API des Providers.

In der aktuellen Version ist allerdings nur Tapkey produktiv. Die Auswahl wird in der Praxis durch die Hardware getrieben: Welche Schlösser sind im Bestand verbaut? Welche Hardware passt zur jeweiligen Tür? Eine Multi-Provider-Strategie pro Wohnung (zwei verschiedene Anbieter parallel) ist nicht in der Architektur vorgesehen — die Komplexität der Sync-Logik wäre erheblich, der Mehrwert für die Verwaltung gering.

Die fünf häufigsten Fehler bei der Smart-Lock-Einführung

In der Praxis wiederholen sich fünf Fehlerbilder bei der Erstinstallation:

1. Pauschale Hardware-Beschaffung ohne Pilot-Phase. Eine Verwaltung kauft 200 Smart-Lock-Schlösser und scheitert an Türrahmen, Schließblechen oder Mängeln in der Funkabdeckung. Empfehlung: Pilot mit zehn Wohnungen über drei Monate, danach Roll-out.

2. Fehlende mieterseitige App-Vorbereitung. Mieter ohne Smartphone oder mit alter Android/iOS-Version können die App nicht installieren. Für solche Fälle ist eine Backup-Variante (NFC-Karte, mechanischer Schlüssel) vorzusehen.

3. Vergessenes Widerrufen bei Vorgangs-Storno. Ein Auftrag wird abgesagt, der Grant bleibt aktiv. Lösung in ImmoGenio: Der Grant ist an den Vorgang gebunden — wird der Vorgang storniert, läuft der Widerruf automatisch.

4. Aufbewahrungsfristen falsch konfiguriert. Zugriffs-Logs werden 24 Monate aufbewahrt ohne berechtigten Grund. Datenschutz-Aufsicht moniert. Empfehlung: 90 Tage Default, längere Aufbewahrung nur einzelfall-begründet.

5. OAuth-Token-Verlust ohne Wiederverbindung. Der Refresh-Token wird durch Datenbank-Migration oder Restore unbrauchbar. Das System läuft in 401-Schleifen, die Verwaltung bemerkt es erst nach Tagen. Lösung: Circuit-Breaker mit Status-Anzeige im Admin-Bereich.

Praxis-Beispiel: Mieterwechsel mit Smart-Lock

Eine 88-Quadratmeter-Wohnung wird zum 1. Oktober neu vermietet. Der bisherige Mieter hat zum 30. September gekündigt. Die Übergabe an den Vermieter ist auf den 30. September 14:00 Uhr terminiert, die Übergabe an den neuen Mieter auf den 1. Oktober 10:00 Uhr.

Im System läuft folgende Mechanik:

- Bisheriger Grant des alten Mieters: gültig bis 30. September 23:59 Uhr (mit Toleranz, falls die Übergabe sich verzögert).
- Begehungs-Grant für den Verwalter: gültig 30. September 13:00 bis 16:00 Uhr für die Endabnahme.
- Gewerblicher Grant für die Reinigungsfirma: 30. September 16:00 bis 18:00 Uhr für die Reinigung.
- Erstbesichtigungs-Grant für den neuen Mieter: 1. Oktober 9:00 bis 12:00 Uhr für die Übergabe.
- Dauerhafter Mieter-Grant für den neuen Mieter: ab 1. Oktober 10:00 Uhr (wird beim Bestätigen der Übergabe aktiviert) bis Mietende.

Alle fünf Grants werden im System aus den Vorgängen (Übergabe alt-Mieter, Reinigungs-Task, Übergabe neu-Mieter, Mietverhältnis-Beginn) automatisch erzeugt und an den richtigen Personen verteilt. Die Schlüsselübergabe per Hand entfällt vollständig. Der Verwal-

ter sieht im Audit-Log, wer wann die Tür geöffnet hat — am 30. September um 13:42 Uhr der Verwalter, um 16:08 Uhr die Reinigungsfirma, am 1. Oktober um 9:55 Uhr der neue Mieter.

Wie ImmoGenio die Smart-Lock-Funktion abbildet

Im Modul „Wohnungen“ wird zu jeder Einheit hinterlegt, welche Schliess-Geräte (Tapkey-Lock-IDs) zugeordnet sind. Bei einem Mieterwechsel oder einem Wartungsauftrag öffnet das System die Tapkey-API und legt die nötigen Grants an. Das GenioFlow-Workflow-Modul sorgt dafür, dass jeder Schritt im Übergabe-Prozess die zugehörigen Grants atomar erzeugt oder widerruft.

Bei der eigentlichen Übergabe arbeitet der Verwalter mit dem Tablet-Workflow zur Wohnungsübergabe — Mängelaufnahme, Foto-Dokumentation, eIDAS-Signatur. Mit Bestätigung der Übergabe geht der Zugang automatisch auf den neuen Mieter über.

Die Aufgaben-Verwaltung mit Kanban und Gantt integriert die Smart-Lock-Grants direkt in den Hausmeister-Workflow. Wer einen Wartungs-Task übernimmt, erhält automatisch den passenden Zeitfenster-Zugang. Wer den Task abschliesst, gibt den Zugang sofort wieder frei.

Verbindung zu angrenzenden Modulen

Bei der Wohnungsübergabe an den Mieter erfolgt die Aktivierung des Mieter-Grants nach Unterzeichnung des Übergabeprotokolls. Die Eltern-Beziehung Übergabe-zu-Grant ist im Audit-Trail festgehalten und im GoBD-konformen ZIP-Daten-Export referenziert.

Die User-Offboarding-Workflow nach DSGVO Art. 17 löscht beim endgültigen Auszug eines Mieters auch dessen Smart-Lock-Profile und das zugehörige Zugriffs-Log — sofern die Aufbewahrungsfristen abgelaufen sind. Die Trennung zwischen Mieter-Stammdaten (zu löschen nach Auszug + drei Jahre) und Buchhaltungs-Akte (zu erhalten 10 Jahre nach AO) gilt auch für die Smart-Lock-Daten.

Grenzen der aktuellen Lösung

Multi-Provider-Setup pro Wohnung ist nicht implementiert — eine Wohnung kann derzeit nur einen Smart-Lock-Provider haben. In Mischbeständen mit unterschiedlicher Hardware bedeutet das, dass jede Wohnung einem Provider zugeordnet werden muss; Wechsel sind möglich, aber mit administrativer Last verbunden.

Auch die Backup-Varianten (NFC-Karte, mechanischer Notschlüssel) sind im Portal nicht direkt abgebildet. Sie werden in der Schlüssel-Übergabe-Akte als Anlage geführt, aber das Versand- und Rückgabe-Tracking erfolgt nicht über das digitale Grant-System.

Wo wir stehen

Die Tapkey-Integration läuft seit Q3 2026 produktiv. Bei den Pilot-Mandanten ist der Grad der Smart-Lock-Aktivierung pro Bestand zwischen 20 und 40 Prozent – nicht alle Wohnungen sind hardware-seitig umgerüstet, das ist eine schrittweise Investition. Die DSGVO-Konformität wird durch Aufbewahrungs-Cron, kontextgebundene Grants und transparente Information der Mieter erreicht. Schlüsselverluste sind in den umgerüsteten Wohnungen seit Roll-out nicht mehr aufgetreten.

Kontakt

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