

immoGenio

No. 04
Oktober 2026

DATEV

DATEV Connect via OAuth 2.0: Authorization Code, Auto-Refresh — und der Circuit-Breaker, der den 401-Sturm bei Token-Rotation abfängt

DATEV Connect via OAuth 2.0: Authorization-Code-Flow, automatischer Token-Refresh, Circuit-Breaker bei 401-Antwort

AUTOR
Olaf Mirel

VERÖFFENTLICHT
7. Oktober 2026

ONLINE
www.immogenio.de/blog

— AUF EINEN BLICK

Inhalt

01 Die Geschichte eines unbemerkten Token-Verlusts

02 Was DATEV Connect leistet

03 Der OAuth-Authorization-Code-Flow im Detail

04 Auto-Refresh — die zentrale Robustheit

05 Der Circuit-Breaker bei 401-Antworten

06 Token-Verschlüsselung und Mandanten-Trennung

07 Die fünf häufigsten Fehler bei DATEV-OAuth-Integration

08 Die Übertragung der Buchungen

09 Praxis-Beispiel: Monatliche Übertragung am 03. des Folgemonats

10 Wie ImmoGenio den DATEV-Connect-Workflow abbildet

11 Verbindung zu angrenzenden Modulen

12 Grenzen der aktuellen Lösung

13 Wo wir stehen

14 Kontakt

Die Geschichte eines unbemerkten Token-Verlusts

Eine mittelgrosse Hausverwaltung nutzt DATEV Connect zur monatlichen Übermittlung der Buchhaltungs-Daten an die Steuerberatungs-Kanzlei. Die Verbindung läuft seit 14 Monaten stabil; die Übertragungen erfolgen automatisch zum Monatsende. Im April 2026 wird die DATEV-Organisation der Steuerberatungs-Kanzlei umgestellt — ein neuer Berater übernimmt das Mandat, die Anbindung wird datev-seitig neu konfiguriert.

Die Hausverwaltung bemerkt davon zunächst nichts. Im Mai läuft die übliche Übertragung — und schlägt fehl. Die Logs zeigen 47 fehlgeschlagene API-Calls innerhalb von vier Minuten, jeweils mit Status 401 Unauthorized. Das Backend versucht den Refresh-Token einzulösen — auch das schlägt fehl. Die Übertragung bricht ab; eine Fehlermeldung wird an den Sachbearbeiter generiert. Aber die Fehlermeldung landet im Spam-Filter; niemand bemerkt sie.

Drei Wochen später ruft der Steuerberater an: „Wo bleiben Ihre Mai-Daten?" Die Verwaltung prüft immoGenio, sieht die fehlgeschlagene Übertragung, versteht die Fehlermeldung und stellt die Verbindung manuell wieder her. Der Vorgang kostet rund 90 Minuten — die DATEV-Authentifizierung muss neu durchlaufen werden, dann müssen die nicht übertragenen Buchungen nachgesendet werden.

Die Lehre: Eine OAuth-basierte Integration ist nur so gut wie ihr Verhalten im Fehlerfall. Ohne Circuit-Breaker, ohne klare Status-Anzeige in immoGenio und ohne automatische Benachrichtigung kann eine technische Stör-Lage tagelang unbemerkt bleiben.

Was DATEV Connect leistet

DATEV Connect ist die offizielle API der DATEV eG für Drittanwendungen. Sie erlaubt Hausverwaltungs-Software, ERP-Systemen oder Branchenlösungen den direkten Datenaustausch mit dem DATEV-Buchungs-System der Steuerberatungs-Kanzlei. Die Authentifizierung läuft über OAuth 2.0 nach RFC 6749 mit Authorization-Code-Flow.

In der Praxis ersetzt DATEV Connect die manuelle Übergabe von DATEV-Export-Dateien (Format 7.0 oder Format ASCII), die im Beitrag zum DATEV-Export Format 7.0 beschrieben ist. Statt monatlich eine ZIP-Datei zu erzeugen und an die Kanzlei zu mailen, werden die Buchungen direkt im DATEV-System abgelegt.

Drei Funktionen sind zentral:

1. Buchungs-Übertragung. Buchungssätze werden direkt in die laufende Buchführung der Kanzlei übertragen. Dabei werden Konto-Mapping (SKR03 vs. individuelle Kontenpläne der Kanzlei), Belegklassen und Buchungstexte automatisch übergeben.

2. Beleg-Verlinkung. Zu jeder Buchung wird der zugehörige Beleg (PDF, Bild) als Anhang verknüpft. Der Steuerberater hat damit den Beleg-Zugriff direkt aus der Buchführung — ohne separate Beleg-Mail.

3. Status-Synchronisation. Wenn der Steuerberater eine Buchung korrigiert oder zurückbucht, kommt die Information zurück in das ImmoGenio-System. Die bidirektionale Sync-Logik ist allerdings nicht in v1 implementiert — derzeit ist die Synchronisation einseitig (von ImmoGenio nach DATEV).

Der OAuth-Authorization-Code-Flow im Detail

Der OAuth-Flow läuft in mehreren Schritten:

Schritt 1: Authorization-Request. Der Verwalter klickt in immoGenio auf „Mit DATEV verbinden". Das Backend erzeugt eine Authorization-URL mit Client-ID, Redirect-URI, Scope (`accounting:read accounting:write documents:read documents:write`) und einem zufälligen State-Parameter zur CSRF-Abwehr. Der Verwalter wird zu DATEV weitergeleitet.

Schritt 2: User-Login bei DATEV. Bei DATEV meldet sich der Verwalter mit seinem DATEV-Account an. Sofern er Berechtigungen für mehrere Mandanten hat, wählt er die anzubindende Mandanten-Beratungsstelle aus. Er bestätigt die angeforderten Scopes.

Schritt 3: Redirect mit Authorization-Code. DATEV leitet zurück zum Portal mit einem temporären Authorization-Code (gültig 60 Sekunden) und dem State-Parameter zur CSRF-Validierung.

Schritt 4: Token-Tausch. Das Backend tauscht den Authorization-Code gegen Access-Token (gültig 1 Stunde) und Refresh-Token (gültig in der Regel 30 Tage, abhängig von DATEV-Konfiguration) ein. Der Tausch läuft über HTTPS-Backend-Call mit Client-Secret.

Schritt 5: Token-Speicherung. Access- und Refresh-Token werden mandanten-spezifisch verschlüsselt im Backend abgelegt. Die Verschlüsselung erfolgt mit einem mandanten-spezifischen Schlüssel (KMS-Encrypted), sodass ein gestohlener Datenbank-Snapshot ohne Schlüssel-Zugriff unbrauchbar ist.

Ab Schritt 5 ist die Verbindung produktiv. Jeder API-Call zu DATEV läuft mit dem Access-Token im Authorization-Header.

Auto-Refresh — die zentrale Robustheit

Access-Token sind kurzlebig. Bei jeder API-Anfrage prüft das Backend die Restlaufzeit des Tokens. Liegt sie unter 60 Sekunden, wird automatisch ein Refresh ausgelöst:

- POST `/oauth/token` mit `grant_type=refresh_token`, dem aktuellen Refresh-Token, der Client-ID und dem Client-Secret.
- Antwort: neuer Access-Token mit 1 Stunde Gültigkeit, in der Regel auch ein neuer Refresh-Token (Token-Rotation).
- Der neue Refresh-Token ersetzt den alten in der verschlüsselten Speicherung.

Wichtig ist die Token-Rotation. DATEV (und die meisten OAuth-Provider) rotieren den Refresh-Token bei jedem Refresh-Vorgang. Der alte Refresh-Token wird damit unbrauchbar; nur der neue gilt. Bei einer Race-Condition mit zwei parallelen Refresh-Calls kann eine der Antworten zu einem alten Refresh-Token führen — der dann nicht mehr gültig ist. Das Backend muss das mit einem Lock auf der Refresh-Operation absichern (semafor pro Mandant), damit nicht zwei parallele API-Calls gleichzeitig den Refresh anstossen.

In der Praxis sind die meisten Refresh-Vorgänge unauffällig — der Auto-Refresh läuft im Hintergrund, der Aufrufer merkt davon nichts. Erst bei längeren Inaktivitäts-Perioden (mehr als 30 Tage) kann es passieren, dass der Refresh-Token selbst abläuft und die Verbindung neu hergestellt werden muss.

Der Circuit-Breaker bei 401-Antworten

Was passiert, wenn der Refresh-Token ungültig wird? Das ist im Eingangsfall passiert: Die DATEV-Organisation der Kanzlei wurde umgestellt; der bisherige Refresh-Token war damit ungültig. Ein automatischer Refresh schlug ebenfalls fehl.

Ohne Schutzmechanismus würde das Backend in eine Schleife laufen — bei jeder geplanten Übertragung versuchen, den Refresh-Token einzulösen, und mit 401 zurückkommen. Bei 47 Übertragungen pro Tag (Buchungen, Belege, Status-Abfragen) sind das 47 401-Antworten pro Tag, die bei DATEV anfallen. Das ist nicht nur Last für DATEV, sondern auch ein Risiko: Manche OAuth-Provider sperren Clients nach einer gewissen Anzahl fehlgeschlagener Refresh-Versuche temporär.

ImmoGenio nutzt einen Circuit-Breaker:

- Bei zwei aufeinanderfolgenden 401-Antworten auf den Refresh-Endpoint wird der Circuit-Breaker auf „open” gesetzt.
- Solange der Breaker offen ist, werden keine neuen API-Calls zu DATEV ausgelöst — alle anstehenden Übertragungen werden gepuffert.

- Im Portal erscheint im Admin-Bereich des Mandanten ein Hinweis „DATEV-Verbindung unterbrochen — bitte neu authentifizieren".
- Der Verwalter klickt im Hinweis auf „Neu verbinden" und durchläuft den Authorization-Flow erneut. Mit dem neuen Refresh-Token wird der Circuit-Breaker auf „closed" gesetzt; die gepufferten Übertragungen werden nachgeholt.

So wird verhindert, dass ein abgelaufener Refresh-Token in einen Daten-Stillstand umschlägt — der Stillstand ist klar markiert und mit einer Ein-Klick-Lösung adressiert.

Token-Verschlüsselung und Mandanten-Trennung

Refresh-Token sind langlebig und damit besonders schützenswert. Wer einen Refresh-Token in die Hand bekommt, kann unbegrenzt API-Calls zu DATEV ausführen — bis der Token ablaufzeit-bedingt unbrauchbar wird.

ImmoGenio nutzt eine zweistufige Verschlüsselung:

- Pro Mandant existiert ein Mandanten-Encryption-Key. Dieser ist im Key Management Service (KMS) abgelegt.
- Refresh-Token werden mit dem Mandanten-Encryption-Key symmetrisch verschlüsselt (AES-256-GCM).
- Bei jedem API-Aufruf entschlüsselt das Backend den Token nur kurz, nutzt ihn und entsorgt die Klartext-Form sofort.

Bei Diebstahl des Datenbank-Inhalts ohne Zugriff auf das KMS sind die Token unbrauchbar. Der Schutz ist analog zur Token-Verschlüsselung im Smart-Lock-Modul mit Tapkey-OAuth.

Die Mandanten-Trennung greift auch bei Multi-Tenant-Datenbanken. Der Mandant A kann nicht auf Token des Mandanten B zugreifen — die Verschlüsselungs-Keys sind getrennt, die Database-Row-Level-Security trennt den Zugriff. Die Architektur folgt dem Beitrag zur Row-Level Security mit Multi-Tenancy.

Die fünf häufigsten Fehler bei DATEV-OAuth-Integration

In der Praxis wiederholen sich fünf Fehlerbilder:

1. Token im Klartext gespeichert. Refresh-Token in der Datenbank ohne Verschlüsselung. Bei Diebstahl der Datenbank ist die OAuth-Verbindung kompromittiert. Lösung: zwingend KMS-Verschlüsselung pro Mandant.

2. Race-Condition beim Refresh. Zwei parallele API-Calls lösen jeweils einen Refresh aus; einer der beiden Refresh-Antworten enthält einen alten, bereits ungültigen Refresh-Token. Lösung: Lock auf Refresh-Operation pro Mandant.

3. Endlos-Schleife bei abgelaufenem Refresh-Token. Backend versucht den Refresh, scheitert mit 401, versucht es erneut, scheitert wieder. Tausende 401-Antworten landen bei DATEV. Lösung: Circuit-Breaker.

4. Fehlende User-Benachrichtigung. Stör-Lage wird intern geloggt, der Verwalter erfährt nichts. Lösung: Status-Anzeige im Admin-Bereich plus E-Mail-Benachrichtigung beim Übergang in „Verbindung gestört".

5. Hard-Coded Scope-Definition ohne Versionierung. Wenn DATEV neue Scopes einführt oder alte umbenennt, scheitert der Authorization-Request. Lösung: Scope-Definition als Konfiguration, nicht als Code-Konstante; Versionierung durchziehen.

Die Übertragung der Buchungen

Bei der monatlichen Übertragung läuft folgender Ablauf:

1. Aggregation. Alle Buchungen des Vormonats, die noch nicht an DATEV übermittelt wurden, werden in einer Liste zusammengestellt. Dazu gehören die Buchungssätze mit Konto-Soll, Konto-Haben, Betrag, Buchungstext, Belegnummer.

2. Konto-Mapping. Die ImmoGenio-internen Konten werden auf den DATEV-Kontenrahmen der jeweiligen Kanzlei gemappt. Die meisten Mandanten nutzen SKR03; einige Sonderfälle (Eigentümer-Steuern, Auslands-Bezüge) verwenden eigene Konten, die im Mapping individuell konfiguriert sind.

3. Beleg-Anhang. Pro Buchung wird der Beleg (PDF) als Multipart-Upload an DATEV übertragen.

4. Bestätigung pro Buchung. DATEV bestätigt jede Buchung mit einem Buchungs-Ident. Dieser wird im ImmoGenio-System dokumentiert; bei späterer Korrektur kann die Buchung über den Ident-Pfad referenziert werden.

5. Audit-Trail. Jede Übertragung — erfolgreich oder fehlgeschlagen — wird im Audit-Trail festgehalten. Das ist Voraussetzung für eine GoBD-konforme Buchführung.

Die Mechanik ist deutlich robuster als der manuelle DATEV-Export. Bei Übertragungs-Fehlern (Netzwerk, API-Limit) werden einzelne Buchungen erneut versucht; nicht sofort übertragene Buchungen bleiben in der Warteschlange und werden im nächsten erfolgreichen Lauf nachgeholt.

Praxis-Beispiel: Monatliche Übertragung am 03. des Folgemonats

Eine Verwaltung mit 280 Einheiten erzeugt im November rund 4.200 Buchungen — Hausgeld-Eingänge, NK-Vorauszahlungen, Mahnungen, Reparatur-Rechnungen, Versicherungs-Prämien, Hausmeister-Lohn, Verwaltervergütung, Bankgebühren. Am 1. Dezember wird die monatliche Übertragung an die Steuerberatungs-Kanzlei gestartet.

Ablauf:

- 1. Dezember 02:30 Uhr: Job startet automatisch. Aggregation der 4.200 Buchungen, Anreicherung mit Konto-Mapping. Dauer: 8 Sekunden.
- 1. Dezember 02:30:08 Uhr: Sequentielle Übertragung an DATEV. Pro Sekunde rund 12 Buchungen plus Beleg-Anhang. Dauer für 4.200 Buchungen: rund 6 Minuten.
- 1. Dezember 02:36 Uhr: Übertragung abgeschlossen. 4.198 Buchungen erfolgreich, 2 mit Fehler („Konto nicht im Mandanten-Kontenrahmen") in einer Fehler-Liste.
- 1. Dezember 08:00 Uhr: Verwaltungs-Sachbearbeiter sieht in immoGenio die Fehler-Liste und korrigiert die zwei Buchungen — eine falsche Konto-Klassifikation. Die Korrektur wird mit dem Folge-Lauf (manuell angestossen) übertragen.

Bei der Steuerberatungs-Kanzlei sind die Daten am 1. Dezember morgens komplett verfügbar. Der Steuerberater beginnt direkt mit der monatlichen Buchhaltungs-Verarbeitung — ohne Wartezeit auf eine separate Daten-Lieferung.

Wie ImmoGenio den DATEV-Connect-Workflow abbildet

Im Portal-Modul „Integrationen" pflegt der Verwalter pro Mandant die DATEV-Verbindung. Die Verbindung läuft initial einmal über den Authorization-Flow; danach bleibt sie über die Token-Rotation langfristig stabil. Der Status („verbunden", „verbindung gestört") ist im Admin-Bereich sichtbar.

Die monatliche Übertragung läuft als Cron-Job zum 1. des Folgemonats. Bei Bedarf kann der Verwalter sie auch manuell anstossen. Übertragungs-Fehler werden im Anfragen-Management als Aufgabe dargestellt; der Verwalter sieht alle aktuellen Stör-Lagen auf einen Blick.

Bei Stör-Lagen mit Circuit-Breaker offen erhält der Verwalter eine E-Mail-Benachrichtigung sowie einen Eintrag im Cockpit-Dashboard. Die Realtime-Notifications über WebSocket zeigen den Stör-Status auch in Echtzeit, sobald der Verwalter in immoGenio angemeldet ist.

Verbindung zu angrenzenden Modulen

Die DATEV-Übertragung ist integriert mit der OCR-Belegerfassung — Belege wandern direkt aus der OCR-Pipeline in die DATEV-Übertragung mit der zugehörigen Buchung.

Bei Buchungsregeln läuft die Buchungsregel-Engine für die automatische SKR03-Kontierung vorgeschaltet. Sie sorgt dafür, dass die Buchungen mit dem richtigen Konto bereits in das DATEV-Mapping einlaufen.

Bei der jährlichen Übermittlung der GoBD-konformen ZIP-Datei ergänzen die DATEV-Übertragungs-Logs den vollständigen Audit-Trail — bei einer Betriebsprüfung sind die Übertragungs-Idents nachvollziehbar.

Grenzen der aktuellen Lösung

Die Übertragung ist einseitig — von ImmoGenio nach DATEV. Korrekturen, die der Steuerberater an der DATEV-Buchhaltung vornimmt, werden nicht automatisch in ImmoGenio rückgespielt. In der Praxis ist das ein bewusster Trade-off: Die Verwaltungs-Buchhaltung ist die Quelle der Wahrheit; die Kanzlei-Buchhaltung ist die steuerlich geprüfte Version. Korrekturen sind vom Verwalter manuell in beiden Systemen zu pflegen.

Auch die Multi-Mandanten-Übertragung mit unterschiedlichen DATEV-Anbindungen (verschiedene Steuerberater pro Mandant) erfordert pro Mandant eine eigene OAuth-Verbindung. Eine konsolidierte Übertragung an eine zentrale DATEV-Organisation ist möglich, wenn die Steuerberatungs-Kanzlei das organisatorisch unterstützt.

Wo wir stehen

Die DATEV-Connect-Integration läuft seit Q3 2026 produktiv bei den Mandanten, die mit DATEV-Kanzleien arbeiten. Bei rund 65 Prozent der geführten Mandanten ist die Integration aktiv; die übrigen nutzen noch den klassischen DATEV-Export per Mail. Die durchschnittliche Übertragungs-Quote (Buchungen pro Monat erfolgreich übertragen) liegt bei 99,7 Prozent. Die Stör-Lagen mit Circuit-Breaker traten bisher 12-mal auf — alle innerhalb von 24 Stunden durch erneute Authentifizierung behoben.

Kontakt

Fragen, Rückmeldungen oder eigene Erfahrungen mit DATEV Connect oder OAuth-basierter Buchhaltungs-Integration? Wir freuen uns über Ihre Nachricht an info@immogenio.de.