Koordinierte Offenlegung: Abschlussbericht

Bank Burgenland Digital-ID für Android (at.grawe.id)

Zwei Befunde der Erstmeldung am Binary 1.1.49 bestätigt und konservativ neu bewertet. Keine inhaltliche Antwort des Verantwortlichen.

ÖFFENTLICHE OFFENLEGUNG, 21. NOVEMBER 2026, EMBARGO-DATUM 16. NOVEMBER 2026 ERREICHT. KEINE ANTWORT BIS 21. NOVEMBER 2026.

Target	Bank Burgenland Digital-ID, Freigabe-App für Login und Zeichnung im Onlinebanking
Operator	HYPO-BANK BURGENLAND AG, FN 259167d, Neusiedler Straße 33, 7000 Eisenstadt
Notice / Publication	2026-08-18 / 2026-11-16 (90 Tage, unverändert)
Versions Audited	1.1.49 (versionCode 101498585), Binary bezogen am 2026-11-14. Version 1.1.50 nicht beschafft.
Findings	2: 0 High, 2 Medium (beide von Critical neu bewertet)
Status	KEINE ANTWORT BIS 21. NOVEMBER 2026, nach den Unterlagen von RFI-IRFOS
SHA-256 (base APK)	`7f6d1746df9a3e71b553e591083fbf2b21c1f35cdb467364b99ea951f0e80f17`

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

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

Inhaltsverzeichnis

1 Zusammenfassung 3

2 Stand der Befunde auf einen Blick 4

3 Gegenstand und Betreiber 4

4 Architektur und Datenfluss 5

5 Befunde 6
5.1 B1: Firebase-API-Schlüssel im Klartext in den App-Ressourcen 6
5.2 B2: Firebase startet beim Prozessstart, vor jeder Oberfläche, ohne Einwilligungsabfrage in der App 7

6 Auswirkungen 8

7 Die vollständige Kette: Von der Installation zur offenen Frage 9

8 Datenschutz: Artikel für Artikel 9

9 Rechtlicher Rahmen und Aufsicht 10

10 Indicators of Compromise und reproduzierbare Belege 11

11 Offenlegungszeitlinie und Stand 12

12 Was die App richtig macht 13

13 Nicht belegt 13

14 Restrisiko und Empfehlungen 14

Zusammenfassung

Bank Burgenland Digital-ID (Paket at.grawe.id) ist die Freigabe-App der HYPO-BANK BURGENLAND AG. Kundinnen und Kunden bestätigen damit ihren Login und die Zeichnung von Aufträgen im Onlinebanking, per Push-Mitteilung, Kontrollziffer, Quick-ID oder Fingerabdruck. Der Play Store weist mindestens 10.000 Installationen aus. RFI-IRFOS hat der Bank am 18. August 2026 zwei Befunde gemeldet: einen im Klartext ausgelieferten Firebase-API-Schlüssel und einen Firebase-Startvorgang, der beim Prozessstart läuft, bevor die App eine Oberfläche zeigt.

Am 14. November 2026 wurde das über einen öffentlichen Spiegel verfügbare aktuelle Binary erneut per root level code analysis geprüft. Es trägt dieselbe Version wie die Erstmeldung (1.1.49, versionCode 101498585). Beide Elemente sind darin unverändert vorhanden. Der Schlüssel liegt in res/values/strings.xml und im Ressourcenindex, der FirebaseInitProvider ist mit initOrder 100 und directBootAware deklariert.

Die erneute Prüfung schränkt die Erstmeldung an zwei Stellen ein. Erstens enthält das Binary keine Analyse-, Werbe- oder Attributions-SDKs. Firebase lädt nur Messaging und Installations, also die Push-Zustellung, die die App für ihre Funktion braucht. Dass diese Komponenten ohne Einwilligung starten, belegt deshalb für sich kein Tracking. Offen bleibt die Rechtsgrundlage und die Information der Betroffenen: Die im Play Store verlinkte Datenschutzerklärung (Stand September 2021) nennt weder Google noch Firebase noch Push-Mitteilungen noch eine mobile App. Zweitens ist ein Firebase-API-Schlüssel ein Projektkennzeichen und kein Geheimnis im engeren Sinn. Ob er missbraucht werden kann, hängt von Einschränkungen ab, die von außen nicht sichtbar sind und die wir nicht prüfen. Beide Befunde sind deshalb von KRITISCH auf MEDIUM (CVSS-B 6.3) neu bewertet.

Der Schlüsselwert steht wortgleich in der veröffentlichten Meldung zur App von bank99 (at.bank99.meine.meine, Version 1.0.39). Ein API-Schlüssel gehört zu genau einem Google-Cloud-Projekt, beide Apps sprechen also dasselbe Projekt an (ebpmg-1144). Eine Maßnahme am Schlüssel oder am Projekt wirkt damit auf beide Apps. Wer das Projekt betreibt, ist aus dem Binary nicht ersichtlich.

Nach den Unterlagen von RFI-IRFOS ist auf drei Nachrichten (18. August, 5. September und 17. Oktober 2026) bis zum 21. November 2026 keine Antwort der Bank eingegangen. Seit dem 14. November 2026 ist nichts Neues eingegangen. Die Fristen vom 1. September, 12. September und 24. Oktober 2026 sind verstrichen. Der Bericht erscheint nach Ablauf des Embargo-Datums vom 16. November 2026. Die drei Fragen zur Schlüsselbeschränkung, zur Rechtsgrundlage und zur Datenschutz-Folgenabschätzung sind offen. Eine Rezension im Play Store vom 16. Oktober 2026 nennt die Version 1.1.50. Sie konnte nicht beschafft werden, ob sie die Befunde noch zeigt, ist nicht geprüft.

Umfang: Root level code analysis des über den Spiegel ApkPure bezogenen Play-Store-Binarys 1.1.49 am 14. November 2026: Manifest, Ressourcen, Dex-String-Pool, dekompilierter Java-Code, Cordova-Frontend. Passiv gelesen wurden der Play-Store-Eintrag und die dort verlinkte Datenschutzerklärung. Kein Backend, kein Firebase-Dienst und kein Schlüssel wurde angesprochen, es wurde kein Gerät und kein Emulator verwendet. Nicht Teil des Umfangs sind der native Schutz (libgrawe.so, assets/opdandnfbjej.dat) und der entfernt geladene Inhalt von banking.bank-bgld.at.

ID	Schwere	Titel
B1	MEDIUM	Firebase-API-Schlüssel im Klartext in den App-Ressourcen
B2	MEDIUM	Firebase startet beim Prozessstart, vor jeder Oberfläche, ohne Einwilligungsabfrage in der App

Stand der Befunde auf einen Blick

ID	Gemeldet	Dieser Bericht	Stand am 21. November 2026
B1	CRITICAL	MEDIUM	In 1.1.49 unverändert vorhanden. Beschränkung des Schlüssels unbekannt, nicht bestätigt. Keine Antwort der Bank.
B2	CRITICAL	MEDIUM	In 1.1.49 unverändert vorhanden. Es startet nur Firebase Messaging und Installations, kein Analyse-SDK. Rechtsgrundlage und Information der Betroffenen offen. Keine Antwort der Bank.

Gegenstand und Betreiber

Der Play Store führt die App als Bank Burgenland Digital-ID, Entwickler Grawe-Bankengruppe, Kategorie Finanzen. Als Händlerkontakt nennt der Eintrag die HYPO-BANK BURGENLAND Aktiengesellschaft, Neusiedler Straße 33, 7000 Eisenstadt. Die im Eintrag verlinkte Datenschutzerklärung (grawe-bankengruppe.at/de/datenschutzerklaerung, Stand September 2021) gilt für die GRAWE Bankengruppe und nennt als Verantwortliche die HYPO-BANK BURGENLAND, FN 259167d, LG Eisenstadt, mit der Datenschutz-Adresse datenschutz@grawe-bankengruppe.at. Der Paketname at.grawe.id folgt dem Namen der Gruppe, der Betreiber der App ist die Bank.

Die App ist ein Freigabeverfahren. Nach der Anmeldung im Onlinebanking erhalten Nutzerinnen und Nutzer eine Push-Mitteilung und bestätigen in der App eine angezeigte Kontrollziffer (Beschreibung im Play Store). Die App arbeitet mit Quick-ID, einem vierstelligen Sicherheitscode, und mit Fingerabdruck. Der Eintrag zeigt 10.000+ Downloads und 3,9 von 5 Sternen bei 51 Rezensionen, Stand 14. November 2026.

Im Binary sind weitere Angaben zur Herkunft sichtbar. Der Paketzweig at.arz.bs290.ebp trägt dasselbe Kürzel ebp wie der Firebase-Projektname ebpmg-1144. Daraus lässt sich nicht ableiten, wer das Projekt verwaltet. Ob ein Plattformanbieter beteiligt ist, bleibt UNVERIFIED.

Architektur und Datenfluss

Die App ist ein Cordova-Hybrid. Das lokale Frontend (assets/www, AngularJS) enthält die Oberflächen für Aktivierung, QR-Scan, Login und Ergebnis. Die eigentliche Anmeldeseite lädt die App von banking.bank-bgld.at (start_url in assets/www/manifest.json). Die Cordova-Plugins decken Biometrie, sicheren Speicher, Root- und Jailbreak-Erkennung, Kamera-Scan, Deep Links und Push ab. Zusätzlich liegt ein nativer Schutz im Binary (libgrawe.so mit 6,7 MB und assets/opdandnfbjej.dat) sowie drei isolierte Dienstprozesse mit zufälligen Namen.

Für Push nutzt die App Firebase Cloud Messaging über das Plugin havesource-cordova-plugin-push. Beim Prozessstart legt Android die ContentProvider aus dem Manifest an. FirebaseInitProvider (initOrder 100) ruft dabei FirebaseApp auf und startet die Komponenten Messaging, Installations und Datatransport. Die Verbindung zu Google besteht über das Firebase-Projekt ebpmg-1144, dessen Kennungen als Ressourcen im Binary stehen.

Element im Binary	Beleg
Firebase-Komponenten	Messaging, Installations, Common, Datatransport (ComponentDiscoveryService im Manifest). Kein AppMeasurement, kein FirebaseAnalytics, kein Crashlytics. Vom Paket com.google.firebase.analytics liegt nur das Interface connector/AnalyticsConnector vor.
Weitere SDKs	Keine Werbe-, Attributions- oder Session-Recording-SDKs gefunden. Die Cordova-Plugin-Liste in cordova_plugins.js enthält keines.
Berechtigungen	INTERNET, CAMERA, USE_BIOMETRIC, USE_FINGERPRINT, POST_NOTIFICATIONS, READ/WRITE_EXTERNAL_STORAGE, WAKE_LOCK, VIBRATE und Launcher-Badge-Berechtigungen. Keine Standort-, Kontakt-, Telefon- oder Mikrofonberechtigung. Kein BOOT_COMPLETED.
Einwilligungsoberfläche	Keine in den lokalen Ressourcen (assets/www, assets/html-de, res/values). Der entfernt geladene Inhalt von banking.bank-bgld.at wurde nicht geprüft.

Befunde

B1: Firebase-API-Schlüssel im Klartext in den App-Ressourcen

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N, 6.3 (CVSS-B), gemeldet als CRITICAL am 18. August 2026, neu bewertet

Gemeldet am 18. August 2026 als KRITISCH, neu bewertet als MEDIUM. Der Schlüssel liegt im Klartext in res/values/strings.xml, doppelt unter den Namen google_api_key und google_crash_reporting_api_key, und im Ressourcenindex resources.arsc des Binarys 1.1.49. Firebase-API-Schlüssel sind für den Einbau in Apps vorgesehen, belegt ist hier die Auslieferung und kein Schaden. Ob der Schlüssel auf Paketname und Signaturzertifikat beschränkt ist und welche Regeln für die Realtime Database und den Storage-Bucket gelten, ist von außen nicht sichtbar und wurde nicht geprüft. Die Bewertung nimmt AT:P, weil die Wirkung von dieser unbekannten Konfiguration abhängt, und VA:L für die in der Erstmeldung beschriebene Kontingenterschöpfung, die nicht getestet wurde.

```
106  <string name="firebase_database_url">https://ebpmg-1144.firebaseio.com</string>
111  <string name="google_api_key">AIzaSyD8jtdT06oePLqFohurEF8yjmEopM5Jx_4</string>
112  <string name="google_app_id">1:122553237183:android:4a2cc9d2ecb3e4f2ffd00a</
    string>
113  <string name="google_crash_reporting_api_key">
    AIzaSyD8jtdT06oePLqFohurEF8yjmEopM5Jx_4</string>
114  <string name="google_storage_bucket">ebpmg-1144.appspot.com</string>
198  <string name="project_id">ebpmg-1144</string>
```

Die Rohprüfung am Ressourcenindex bestätigt den Wert unabhängig vom Dekompilierer: Eine Suche nach dem Schlüssel in resources.arsc liefert genau einen Treffer. Das Binary enthält keine Crashlytics-Klassen, der zweite Eintrag trägt denselben Wert.

Ein Schlüssel im Binary lässt sich nicht rotieren, ohne ein neues Release auszuliefern und die Aktualisierung durch die Nutzerinnen und Nutzer abzuwarten. Bis dahin bleibt jeder alte Stand verwendbar. Der Schlüsselwert ist außerdem nicht auf diese App beschränkt: Er steht wortgleich in der veröffentlichten Meldung zu at.bank99.meine.meine, Version 1.0.39. Beide Apps nutzen damit dasselbe Google-Cloud-Projekt.

Nicht geprüft und nicht prüfbar ohne Zugriff auf das Projekt: die API-Beschränkungen in der Google Cloud Console, die Regeln der Realtime Database und des Buckets sowie die Sendeberechtigung für Cloud Messaging. Der Schlüssel wurde gegen keinen Server verwendet.

Auswirkung: Jede Person, die die App aus dem Play Store lädt, kann den Schlüssel lesen. Ist er nicht beschränkt, kann das Kontingent des Projekts aufgebraucht werden. Davon kann die Registrierung für Push und damit die Zustellung der Freigaben abhängen, was nicht geprüft ist. Trifft das zu, könnten Kundinnen und Kunden Logins und Aufträge nicht rechtzeitig bestätigen. Das Binary enthält keinen Hinweis, dass der Schlüssel Konten oder Zahlungsfreigaben berührt. Er adressiert Firebase-Dienste von Google. Weil das Projekt mit der App einer zweiten Bank geteilt wird, wirkt jede Beeinträchtigung auf beide.

Maßnahme: Den Schlüssel in der Google Cloud Console auf Android-Apps (Paketname at.grawe.id und SHA-1-Fingerprint des Signaturzertifikats) und auf die tatsächlich benötigten APIs beschränken. Regeln der Realtime Database und des Buckets prüfen und restriktiv set-

zen. Firebase App Check aktivieren. Im nächsten Release einen neuen Schlüssel ausliefern. Die Maßnahmen vorab mit dem Betreiber des geteilten Projekts abstimmen. Eine Bestätigung der Bank liegt nicht vor.

B2: Firebase startet beim Prozessstart, vor jeder Oberfläche, ohne Einwilligungsabfrage in der App

---

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 6.3 (CVSS-B), gemeldet als CRITICAL am 18. August 2026, neu bewertet

Gemeldet am 18. August 2026 als KRITISCH, neu bewertet als MEDIUM. Das Manifest deklariert FirebaseInitProvider mit initOrder 100 und directBootAware. Android legt den Provider beim Prozessstart an, bevor eine Activity sichtbar ist. Geladen werden Firebase Messaging, Installations und Datatransport. Die Erstmeldung sprach allgemein von Komponenten. Das Binary zeigt jedoch kein Analyse-, Werbe- oder Attributions-SDK. Es zeigt Push-Infrastruktur, die die App für ihren Zweck braucht. Eine Einwilligung ist dafür nicht zwingend die Rechtsgrundlage. Belegt sind der Start vor der Oberfläche, das Fehlen einer Einwilligungsoberfläche in den lokalen Ressourcen und das Schweigen der verlinkten Datenschutzerklärung zu Google, Firebase und Push. Die Bewertung nimmt AT:P, weil eine tragfähige Rechtsgrundlage nicht ausgeschlossen ist, und VC:L für Installations-ID und Verbindungsdaten.

```
<provider
    android:name="com.google.firebase.provider.FirebaseInitProvider"
    android:exported="false"
    android:authorities="at.grawe.id.firebaseinitprovider"
    android:initOrder="100"
    android:directBootAware="true"/>
```

Die automatische Initialisierung von Firebase Messaging ist nicht abgeschaltet: Das Manifest setzt keinen Eintrag firebase_messaging_auto_init_enabled. Im Dex steht der Endpunkt firebaseinstallations.googleapis.com. Nach der bekannten Funktion dieser SDKs gehen dabei eine Installations-ID, die IP-Adresse und Geräte- und App-Angaben an Google. Das ist aus der SDK-Funktion abgeleitet und wurde nicht gemessen, es wurde nichts ausgeführt.

Eine Einwilligungsoberfläche fehlt in den lokalen Ressourcen. Weder assets/www noch assets/html-de noch res/values enthalten einen Datenschutz-, Zustimmungs- oder Cookie-Text der App. Ob die entfernt geladene Anmeldeseite eine Einwilligung abfragt, wurde nicht geprüft.

Die im Play Store verlinkte Datenschutzerklärung, Stand September 2021, ist auf Websites ausgerichtet (Abschnitte zu Website-Nutzung, Cookies und Web-Analyse). Eine Volltextsuche findet die Wörter Firebase, Google, Push, App, Mobile, Drittland, USA und Cloud kein einziges Mal. Ob die App an anderer Stelle eine eigene Information zeigt, ist nicht belegt.

Einschränkung der Erstmeldung: Art. 7 DSGVO greift nur, wenn eine Einwilligung die gewählte Rechtsgrundlage ist. Für die Push-Zustellung einer Freigabe-App kommen Art. 6 Abs. 1 lit. b oder lit. f DSGVO und, für den Zugriff auf das Endgerät, die Ausnahme für technisch erforderliche Vorgänge in § 165 Abs. 3 TKG 2021 in Betracht. Die Frage, auf welcher Grundlage die Verarbeitung vor der ersten Anzeige läuft, ist damit berechtigt und offen. Als Verstoß wird sie hier nicht behauptet.

Auswirkung: Betroffen ist jede Person, die die App installiert und startet, bei jedem Start. Sie nutzt ein Instrument der Kontoabsicherung ihrer Bank und kann der Bank-Datenschutzerklärung nicht entnehmen, dass dabei Google als Empfänger beteiligt ist. Die Menge der Daten ist nach dem Binary gering (Kennungen und Verbindungsdaten, kein Analyse-SDK). Der Befund betrifft vor allem die Transparenz nach Art. 13 DSGVO und die dokumentierte Rechtsgrundlage.

Maßnahme: Rechtsgrundlage dokumentieren (Art. 6 Abs. 1 lit. b oder f DSGVO, § 165 Abs. 3 TKG 2021). Google als Empfänger sowie Übermittlungsgrundlage in einer eigenen App-Datenschutzinformation nennen (Art. 13 Abs. 1 lit. e und f DSGVO). Wo die App Push erst nach der Aktivierung des Geräts braucht, die automatische Initialisierung abschalten (firebase_messaging_auto_init_enabled auf false) und Firebase erst dann starten. Eine Bestätigung der Bank liegt nicht vor.

Auswirkungen

Betroffen sind Kundinnen und Kunden der Bank Burgenland, die ihr Onlinebanking mit dieser App freigeben. Der Play Store weist mindestens 10.000 Installationen aus. Die App ist der zweite Faktor für Login und Zeichnung. Was dort schiefgeht, trifft die Absicherung des Kontos.

B1 betrifft die Verfügbarkeit. Ist der Schlüssel unbeschränkt, ließe sich das Kontingent des Firebase-Projekts erschöpfen. Hängt die Push-Registrierung an diesem Kontingent, was nicht geprüft ist, bekäme wer eine Freigabe braucht seine Push-Mitteilung nicht und könnte einen Auftrag nicht rechtzeitig bestätigen. Das wäre ein Ausfall und kein Zugriff auf Konten. Weil mindestens eine zweite Bank dasselbe Projekt nutzt, wäre der Ausfall nicht auf die Bank Burgenland begrenzt.

B2 betrifft die Transparenz. Eine Kundin oder ein Kunde installiert die App, startet sie und löst damit eine Verbindung zu Google aus, ohne dass die Datenschutzerklärung der Bank Google, Firebase oder Push erwähnt. Betroffen ist die gesamte Nutzerschaft, die Schwere je Person ist gering. Dass es sich um ein Bankinstrument handelt, erhöht die Erwartung an klare Information, nicht die Menge der übermittelten Daten.

Die vollständige Kette: Von der Installation zur offenen Frage

- Kontakt: Eine Kundin oder ein Kunde der Bank installiert die App aus dem Play Store, um Logins und Aufträge im Onlinebanking freizugeben (Play-Store-Beschreibung).
- Bereitstellung: Das Binary 1.1.49 enthält im Klartext den Schlüssel und die Kennungen des Firebase-Projekts ebpmg-1144 (B1). Jede Person kann das Binary laden und lesen, auch über Spiegel.
- Start: Bei jedem Prozessstart legt Android FirebaseInitProvider an (initOrder 100). Messaging und Installations starten, bevor die App eine Oberfläche zeigt (B2).
- Information: Die im Play Store verlinkte Datenschutzerklärung stammt von September 2021, richtet sich an Website-Besucher und nennt Google, Firebase und Push nicht. Eine Einwilligungsoberfläche gibt es in den lokalen Ressourcen nicht.
- Offene Frage: Auf welcher Rechtsgrundlage der Start läuft und welche Beschränkungen der Schlüssel trägt, hat die Bank trotz dreier Nachrichten nicht beantwortet.
- Folge: Für Kundinnen und Kunden bleibt ein Informationsdefizit. Für den Schlüssel bleibt ein Ausfallrisiko, das von einer Konfiguration abhängt, die nur die Bank und der Projektbetreiber kennen.

Beide Befunde hängen am selben Firebase-Projekt ebpmg-1144. B1 beschreibt, was jede Person mit dem Binary lesen kann. B2 beschreibt, was die App selbst beim Start tut.

Datenschutz: Artikel für Artikel

Norm	Befund	Bewertung
Art. 32 DSGVO	B1	Technische Maßnahmen für die Sicherheit der Verarbeitung. Ein Schlüssel im Binary lässt sich nicht ohne Release rotieren. Ob eine Beschränkung besteht, ist offen. Die Bank trägt die Nachweispflicht.
Art. 5 Abs. 2 DSGVO	B1, B2	Rechenschaftspflicht. Die Bank hat auf die Frage nach den Beschränkungen und nach der Rechtsgrundlage nicht geantwortet.
Art. 25 DSGVO	B2	Datenschutz durch Technikgestaltung. Die automatische Initialisierung bei Prozessstart ist nicht auf den Zeitpunkt begrenzt, an dem Push gebraucht wird.
Art. 6 Abs. 1 DSGVO	B2	Rechtsgrundlage der Verarbeitung vor der ersten Anzeige. Lit. b oder lit. f kommen in Betracht, dokumentiert ist keine.
Art. 7 DSGVO	B2	Gilt nur bei Einwilligung als Grundlage. Eine Einwilligungsoberfläche fehlt in den lokalen Ressourcen. Ein Verstoß wird nicht behauptet.
Art. 13 Abs. 1 lit. e und f DSGVO	B2	Empfänger und Drittlandübermittlung. Die verlinkte Erklärung (Stand September 2021) nennt Google, Firebase und Push nicht. Ob die App an anderer Stelle informiert, ist nicht belegt.

Norm	Befund	Bewertung
Art. 28 DSGVO	B2	Rolle von Google als Auftragsverarbeiter oder eigener Verantwortlicher für Firebase Messaging und Installations. Nicht geprüft.
Art. 35 DSGVO	B2	Die Frage nach einer dokumentierten Datenschutz-Folgenabschätzung für die digitale Identitätsfunktion ist offen. Ob eine Pflicht besteht, wird nicht behauptet.
§ 165 Abs. 3 TKG 2021	B2	Zugriff auf das Endgerät. Die Ausnahme für technisch erforderliche Vorgänge ist naheliegend, eine Begründung der Bank liegt nicht vor.

Rechtlicher Rahmen und Aufsicht

Zuständig für Datenschutzfragen ist in Österreich die Datenschutzbehörde (DSB). Die Finanzmarktaufsicht (FMA) beaufsichtigt die Bank. CERT.at ist die nationale Anlaufstelle für Sicherheitsvorfälle. Die Datenschutzbehörde und CERT.at standen bei der Erstmeldung in Kopie.

Für Kreditinstitute gilt seit 17. Jänner 2025 die Verordnung (EU) 2022/2554 (DORA) mit Anforderungen an das IKT-Risikomanagement. Eine App, die Login und Zahlungsfreigaben absichert, gehört zu den IKT-Systemen, die diese Anforderungen betreffen. Die Freigabe von Logins und Zeichnungen ist außerdem Teil der starken Kundenauthentifizierung nach der Richtlinie (EU) 2015/2366 (PSD2) und dem österreichischen Zahlungsdienstegesetz 2018. Dieser Bericht prüft keine Pflicht aus diesen Regelwerken, er benennt den Rahmen, in dem die Bank die Fragen zu beantworten hat.

Der Vergleich mit dem Korpus des Instituts: Die App von bank99 (at.bank99.meine.meine, Version 1.0.39) zeigt denselben Schlüsselwert und damit dasselbe Firebase-Projekt. Das Muster, Firebase-Kennungen im Klartext auszuliefern, kommt in Banking-Apps im Korpus mehrfach vor und wird für jedes Ziel gleich behandelt.

Die Prüfung stützt sich auf das Forschungsfreiheitsgesetz (Art. 17 StGG), auf ISO/IEC 29147 und auf Art. 89 DSGVO. Sie bewertet technische Beobachtungen am öffentlich verteilten Binary und trifft keine rechtliche Feststellung gegen die Bank.

Indicators of Compromise und reproduzierbare Belege

Merkmal	Wert
Paket, Version	at.grawe.id, versionName 1.1.49, versionCode 101498585, minSdk 26, targetSdk 35
Bezug	ApkPure-Spiegel, Direktlink d.apkpure.net/b/APK/at.grawe.id?version=latest, heruntergeladen am 2026-11-14 um 19:37:54 UTC, 10.644.736 Bytes. apkcombo.com lieferte am selben Tag keine Download-Links.
SHA-256 XAPK	0638e4c563ab5f24fa102251c7eca1aa33df2fcf8448b10b4a5246c41521e877
SHA-256 Basis-APK	7f6d1746df9a3e71b553e591083fbf2b21c1f35cdb467364b99ea951f0e80f17
SHA-256 config.arm64_v8a.apk	e4a522c08598a34d424ee8e023abd01b568975c531575c5f9d54eba53dec2bca
SHA-256 libgrawe.so	03897f4a05d88e376731d730165ffd03583efd45cc539d78d3c8ef1755591821
SHA-256 decodierte Dateien	strings.xml 3847ab7ccd998e47a824a5a0cd08886ec899dedf8ed5b09e3edadfd35d916673, AndroidManifest.xml 3f4815c4881b72919c508c5db1c5d305d8e0c3d302da9434fa8a40b3947f9e32 (jadx 1.5.0)
Firebase-Projekt	project_id ebpmg-1144, Realtime Database ebpmg-1144.firebaseio.com, Bucket ebpmg-1144.appspot.com
Schlüssel und App-ID	API-Schlüssel AIzaSyD8jtdT06oePLqFohurEF8yjmEopM5Jx_4, App-ID 1:122553237183:android:4a2cc9d2ecb3e4f2ffd00a
Provider	com.google.firebase.provider.FirebaseInitProvider, authorities at.grawe.id.firebaseinitprovider, initOrder 100, directBootAware true
Endpunkt im Dex	firebaseinstallations.googleapis.com
Backend	banking.bank-bgld.at (start_url und Deep Link /auth/appdeeplink)
Play Store	play.google.com/store/apps/details?id=at.grawe.id, abgerufen 2026-11-14 um 19:37 UTC, aktualisiert am 06.07.2026, 10.000+ Downloads, Entwickler Grawe-Bankengruppe

```
unzip -p at.grawe.id.apk resources.arsc | strings -n 20 | grep -c 'AIza'
jadx -d out at.grawe.id.apk
grep -n 'google_api_key\|project_id' out/resources/res/values/strings.xml
grep -n -A5 'FirebaseInitProvider' out/resources/AndroidManifest.xml
grep -c 'measurement\|FirebaseAnalytics' -r out/sources/com/google
```

Offenlegungszeitlinie und Stand

Die ersten Meldungen vom 26. Juni bis 17. August 2026 gingen wegen des Paketnamens at.grawe.id an die Grazer Wechselseitige Versicherung AG, die am 17. August 2026 mitteilte, keine App zu betreiben, weshalb die Frist erst am 18. August 2026 mit der Zustellung an die HYPO-BANK BURGENLAND AG beginnt.

Datum	Ereignis	Antwort
18. August 2026	Erstmeldung auf Deutsch an datenschutz@grawe-bankengruppe.at, Kopie an info@bank-bgld.at, die Datenschutzbehörde und CERT.at. Zwei Befunde, drei Fragen mit Frist 1. September 2026, Offenlegungstermin 16. November 2026.	Keine Antwort, keine Fehlzustellung
5. September 2026	Wiederholung der Befunde, Fragen mit neuer Frist 12. September 2026, Termin unverändert 16. November 2026. Kopie an info@bank-bgld.at.	Keine Antwort
17. Oktober 2026	Erinnerung, Frist 24. Oktober 2026, noch 30 Tage bis zum Termin. Kopie an info@bank-bgld.at.	Keine Antwort
14. November 2026	Erneute root level code analysis des öffentlich verfügbaren Binarys 1.1.49. Beide Elemente unverändert vorhanden.	Dieser Bericht
16. November 2026	Ende der 90 Tage ab Zustellung. Embargo-Datum erreicht.	Keine Antwort
21. November 2026	Veröffentlichung dieses Berichts. Seit dem 14. November 2026 ist keine Nachricht der Bank eingegangen, Bestätigung durch Simeon Kepp.	Keine Antwort bis 21. November 2026

Die drei Fragen der Erstmeldung lauten: Ist der Schlüssel in der ausgelieferten Version noch enthalten, und welche serverseitigen Restriktionen gelten? Welche Rechtsgrundlage nach Art. 6 und Art. 7 DSGVO deckt die Verarbeitung vor der Einwilligungsmaske, und welche technische Maßnahme stellt sicher, dass sie erst danach beginnt? Liegt eine dokumentierte Datenschutz-Folgenabschätzung nach Art. 35 DSGVO vor, und liegt sie dem Datenschutzbeauftragten vor? Der Stand zur ersten Frage ist durch diesen Bericht ergänzt: Der Schlüssel ist in 1.1.49 enthalten. Alle drei Fragen sind unbeantwortet.

Bis zum 21. November 2026 liegt nach den Unterlagen von RFI-IRFOS keine eingehende Nachricht der Bank vor. Die Offenlegung findet unabhängig von einer Antwort statt und ist an keine Gegenleistung geknüpft.

Was die App richtig macht

- android:allowBackup ist auf false gesetzt.
- Klartext-HTTP ist durch targetSdk 35 gesperrt. Das Manifest setzt weder usesCleartextTraffic noch eine eigene networkSecurityConfig. In den App-eigenen JavaScript-Dateien steht kein http-Endpunkt.
- Die App nutzt Biometrie (USE_BIOMETRIC), sicheren Speicher, Root- und Jailbreak-Erkennung und einen nativen Schutz mit isolierten Prozessen.
- Der Berechtigungsumfang ist klein: keine Standort-, Kontakt-, Telefon- oder Mikrofonberechtigung, kein BOOT_COMPLETED.
- Es gibt kein Werbe-, Attributions- oder Analyse-SDK im Binary. Die Datenerhebung beschränkt sich auf das, was Push und Anmeldung brauchen.
- Der Deep Link auf banking.bank-bgld.at ist mit autoVerify abgesichert.

Nicht belegt

- Version 1.1.50: Eine Rezension im Play Store vom 16. Oktober 2026 nennt sie. Der Spiegel lieferte am 14. November 2026 nur 1.1.49 als neueste Version, ein Bezug von 1.1.50 schlug fehl. Ob die Befunde dort bestehen oder behoben sind, ist nicht geprüft. Der Play-Store-Eintrag nennt als letztes Aktualisierungsdatum den 6. Juli 2026, ohne Versionsnummer.
- Identität der Binärdatei: Version und versionCode stimmen mit der Erstmeldung überein. Ein SHA-256 der damals geprüften Datei liegt nicht vor, die Byte-Gleichheit ist nicht bewiesen.
- Schlüsselbeschränkung, Regeln der Realtime Database und des Buckets und die Sendeberechtigung für Cloud Messaging: nicht geprüft und von außen nicht prüfbar.
- Betreiber des Firebase-Projekts ebpmg-1144: unbekannt. Ob ein Plattformanbieter beteiligt ist, ist aus dem Binary nicht ableitbar.
- Tatsächlich übertragene Daten beim ersten Start: nicht gemessen, abgeleitet aus der bekannten Funktion der SDKs.
- Inhalt des nativen Schutzes (libgrawe.so, assets/opdandnfbjej.dat) und entfernt geladene Seite banking.bank-bgld.at: nicht untersucht.
- Eine eigene Datenschutzinformation innerhalb der App: in den lokalen Ressourcen nicht gefunden, entfernt geladene Inhalte nicht geprüft.

Restrisiko und Empfehlungen

Offen sind die Beschränkung des Schlüssels, die dokumentierte Rechtsgrundlage für den Start von Firebase vor der ersten Anzeige und die Information der Betroffenen über Google als Empfänger. Offen bleibt auch, ob eine neuere Version die Punkte bereits behoben hat.

- Den Schlüssel auf Paketname at.grawe.id und SHA-1-Fingerprint beschränken, nur benötigte APIs freigeben, Firebase App Check aktivieren und den Schlüssel im nächsten Release rotieren. Zuvor mit dem Betreiber des geteilten Projekts abstimmen.
- Regeln der Realtime Database und des Storage-Buckets von ebpmg-1144 prüfen und auf den Zugriff der eigenen Apps beschränken.
- Die Rechtsgrundlage für den Start von Firebase Messaging und Installations dokumentieren und in einer App-Datenschutzinformation Google als Empfänger und die Übermittlungsgrundlage nennen. Die Datenschutzerklärung aus dem Jahr 2021 um die mobile App ergänzen.
- Wo möglich, die automatische Initialisierung von Firebase Messaging abschalten und erst nach der Aktivierung des Geräts starten.
- Die drei Fragen aus der Erstmeldung schriftlich beantworten, an die REF BANKBGLD-ID-2026-R1 gebunden.

Nach der Veröffentlichung wird die dann aktuelle Version der App vollständig neu geprüft, als eigenständige Erstmeldung mit eigener Frist. Das ist Regelbetrieb bei jedem Ziel dieser Prüfreihe.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Österreich Root level code analysis der veröffentlichten

Anwendung sowie passive öffentliche Abrufe von Play-Store-Eintrag und Datenschutzerklärung. Kein Server, kein Konto und kein Schlüssel wurde angesprochen. Offenlegung nach ISO/IEC 29147, Art. 17 StGG und Art. 89 DSGVO. Abschlussbericht, veröffentlicht am 21. November 2026. REF BANKBGLD-ID-2026-R1.