



Security & Privacy Disclosure, Final Report

Visa Go (com.visa.eva) and Tap to Pay Ready (com.visa.kic.app.kernel)

Two Visa applications without any network security configuration, one exported payment kernel service without a permission gate, and two automatic receipts in 69 days with no human reply

PUBLIC DISCLOSURE, 17 OCTOBER 2026: EMBARGO REACHED 3 OCTOBER 2026, SIX MESSAGES SENT, TWO AUTOMATIC RECEIPTS, NO HUMAN REPLY, THREE QUESTIONS UNANSWERED

Target	Visa Inc. (Foster City, USA), listed developer of both applications; Visa Europe Limited appears as an affiliate in the Visa privacy notice
Packages	com.visa.eva v1.14.5 (Visa Go); com.visa.kic.app.kernel v25.06.21 (Tap to Pay Ready)
Platform Audited	Android, root level code analysis of both production APKs
Initial Disclosure (R1)	2026-07-05, one letter covering both applications, to privacy@visa.com, CC press@visa.com, globalmedia@visa.com , Austrian Datenschutzbehörde, EDPS
Disclosure / Embargo Date	2026-10-03
Report Published	2026-10-17
Overall Severity	HIGH
Findings	12 (4 High, 6 Medium, 2 Low, 0 Critical): 7 for Visa Go, 5 for Tap to Pay Ready
Correspondence	6 messages sent by RFI-IRFOS over 69 days (2026-07-05 to 2026-09-12), 2 automatic receipts from privacy@visa.com (2026-07-05 and 2026-09-12) pointing to the Visa Privacy Portal, 0 human replies; 35 days of silence after the last message
Authorities Notified	Austrian Datenschutzbehörde · EDPS

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	Subject & Operator Context	5
3	Engagement Summary	5
4	Findings	5
4.1	GO-H1: Visa Go: no network security configuration and no certificate pinning anywhere in the binary	6
4.2	GO-H2: Visa Go: pre-consent Firebase, Sentry and Flutter messaging auto-init	6
4.3	GO-M1: Visa Go: seven hardcoded Google API keys, AWS Cognito identifiers and a Sentry DSN	7
4.4	GO-M2: Visa Go: Eva assistant references a free public CORS proxy (api.allorigins.win)	7
4.5	GO-M3: Visa Go: advertising attribution permissions and a dual Firebase and AWS Pinpoint stack on an invite-only app	8
4.6	GO-M4: Visa Go: Art. 9 accessibility data shared with FIFA, no Visa Go specific privacy notice	8
4.7	GO-L1: Visa Go: RECEIVE_BOOT_COMPLETED declared without a receiver	9
4.8	TTP-H1: Tap to Pay Ready: exported payment kernel binding service without any permission	9
4.9	TTP-H2: Tap to Pay Ready: no network security configuration and no pinning library of any kind	10
4.10	TTP-M1: Tap to Pay Ready: Google test certificate and private key block bundled in the release dex	10
4.11	TTP-M2: Tap to Pay Ready: INSTALL_PACKAGES permission declared without observable wiring	11
4.12	TTP-L1: Tap to Pay Ready: BLUETOOTH_CONNECT without purpose, NFC declared required=false	11
5	Impact Analysis	11
6	The Complete Chain: Six Messages, 104 Days, Two Automatic Receipts, Zero Replies	12
7	Data Protection: Article by Article	12
8	Regulatory & Legal Landscape	12
9	Indicators of Compromise	13
10	Disclosure Timeline & Outcome	13
11	Residual Risk & Recommendations	14

Executive Summary

Visa Go is not a payment app. Its own store listings describe an invite-only event concierge for Visa guests, and the binary agrees: no payment processor SDK, no card linking, no KYC vendor. It carries a FIFA World Cup 2026 accessibility seating flow, an AI assistant named Eva, AWS Cognito in eu-west-1 and Sentry on its German ingest endpoint. Tap to Pay Ready is the opposite: a first-party Visa app that hosts an on-device multi-scheme EMV Level 2 contactless kernel (modules for Mastercard, Visa, American Express and Discover) and a PIN entry surface for third-party point-of-sale apps.

Four findings carry HIGH weight. Visa Go GO-H1: no network security configuration at all. Visa Go GO-H2: Firebase, Sentry and Flutter messaging providers start at process creation, with real consent screen copy that cannot precede them. Tap to Pay Ready TTP-H1: KernelMessengerService is exported with an intent filter for BIND_TO_PAYMENT_KERNEL and carries no permission, although the same manifest applies a signature permission elsewhere. TTP-H2: no network security configuration and no pinning library of any kind, while Apache HostnameVerifier classes including AllowAllHostnameVerifier ship in the dex. Medium findings cover seven hardcoded Google keys with AWS Cognito identifiers and a Sentry DSN (withheld), a free public CORS proxy referenced by the Eva assistant, advertising attribution on an invite-only app, Art. 9 accessibility data shared with FIFA without a Visa Go specific privacy notice, a Google test certificate with private key block in the Tap to Pay Ready dex, and the INSTALL_PACKAGES permission.

RFI-IRFOS sent the findings on 5 July 2026 and five follow-ups (24 July, 9 August, 24 August, 3 September, 12 September 2026) to privacy@visa.com. Automatic receipts arrived on 5 July and 12 September 2026. No human reply followed. The embargo of 3 October 2026 passed 14 days before this report publishes.

ID	Severity	Title
GO-H1	HIGH	Visa Go: no network security configuration and no certificate pinning anywhere in the binary
GO-H2	HIGH	Visa Go: pre-consent Firebase, Sentry and Flutter messaging auto-init
GO-M1	MEDIUM	Visa Go: seven hardcoded Google API keys, AWS Cognito identifiers and a Sentry DSN
GO-M2	MEDIUM	Visa Go: Eva assistant references a free public CORS proxy (api.allorigins.win)
GO-M3	MEDIUM	Visa Go: advertising attribution permissions and a dual Firebase and AWS Pinpoint stack on an invite-only app
GO-M4	MEDIUM	Visa Go: Art. 9 accessibility data shared with FIFA, no Visa Go specific privacy notice
GO-L1	LOW	Visa Go: RECEIVE_BOOT_COMPLETED declared without a receiver
TTP-H1	HIGH	Tap to Pay Ready: exported payment kernel binding service without any permission
TTP-H2	HIGH	Tap to Pay Ready: no network security configuration and no pinning library of any kind

ID	Severity	Title
TTP-M1	MEDIUM	Tap to Pay Ready: Google test certificate and private key block bundled in the release dex
TTP-M2	MEDIUM	Tap to Pay Ready: INSTALL_PACKAGES permission declared without observable wiring
TTP-L1	LOW	Tap to Pay Ready: BLUETOOTH_CONNECT without purpose, NFC declared required=false

Subject & Operator Context

Google Play and the Apple App Store list Visa Inc. as developer of Visa Go. Tap to Pay Ready carries a first-party signing certificate (CN=Tap to Pay Ready, OU=VAS, O=Visa, L=Austin) and states that it is developed and controlled by Visa, Inc. The Visa Global Privacy Notice covers Visa Inc. and its affiliates, names no Visa Go product section and no Tap to Pay Ready section, and contains no Art. 27 representative designation in the sources checked. No confirmed EU main establishment was identified, so the Austrian Datenschutzbehörde acts as the lead contact of this review; this remains a candidate determination for Visa to correct.

Engagement Summary

Visa Go and Tap to Pay Ready share a disclosure thread. The findings research first expected Visa Go to be a Visa Direct money transfer app; the binary shows an event concierge, and the R1 letter corrected this premise and evaluated Visa Go on that corrected basis. RFI-IRFOS addressed privacy@visa.com and copied the two media addresses and the authorities. From the follow-up of 3 September 2026 the authorities no longer appear in the CC line. The two automatic receipts direct consumer requests to the Visa Privacy Portal and carry no handling of the disclosure.

Findings

GO-H1: Visa Go: no network security configuration and no certificate pinning anywhere in the binary

HIGH, CVSS v4.0 AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 7.6 (Visa Go transport trust)

```
res/xml/: no network_security_config.xml ; AndroidManifest.xml: no android:
networkSecurityConfig
Lokhttp3/CertificatePinner; present, grep sha256/ pin values -> no match
libapp.so: SecureSocket_RegisterBadCertificateCallback
```

Impact: TLS trust rests on the device system CA store alone. A party that controls a trusted root on the device (enterprise MDM profile, security software, rooted or compromised handset) can read and modify the channel between the app and its backend. The app authenticates invited guests through AWS Cognito and carries accessibility data for FIFA requests. A shaded OkHttpClient CertificatePinner ships without pin values.

GO-H2: Visa Go: pre-consent Firebase, Sentry and Flutter messaging auto-init

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9 (pre-consent initialisation)

```
AndroidManifest.xml: SentryPerformanceProvider initOrder=200 ; FirebaseInitProvider
initOrder=100 ;
FlutterFirebaseMessagingInitProvider initOrder=99 ;
firebase_crashlytics_collection_enabled=true
libapp.so: "Cookie Preferences", "Analytics Consent", FirebaseAnalyticsHostApi.
setAnalyticsCollectionEnabled
```

Impact: Firebase and Google Measurement components initialise as ContentProviders during Application creation, mechanically before any screen or consent notice can render. Processing starts on first launch for every installation, before consent can be given. Consent screen copy for Cookie Preferences and Analytics Consent exists in the Dart string pool. Crashlytics collection is hardcoded to true, and Sentry starts before Firebase with no auto-init suppression. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the processing starts on every installation of an app that handles guest authentication and accessibility requests, before any consent surface can render.

GO-M1: Visa Go: seven hardcoded Google API keys, AWS Cognito identifiers and a Sentry DSN

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N, 6.9 (hardcoded identifiers)

```
res/values/strings.xml google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed  
privately in R1]  
libapp.so six further Google API keys: [REDACTED IN PUBLIC REPORT -- disclosed  
privately in R1]  
libapp.so Cognito User Pool ID, Identity Pool ID, Sentry DSN: [REDACTED IN PUBLIC  
REPORT -- disclosed privately in R1]
```

Impact: Seven Google API keys, a Cognito User Pool ID, a Cognito Identity Pool ID (both eu-west-1) and a Sentry DSN (German ingest) are readable from the shipped binary. Google and AWS document these as client-side identifiers; the exposure is quota abuse and reliance on restrictions the controller must demonstrate. No Realtime Database URL exists.

GO-M2: Visa Go: Eva assistant references a free public CORS proxy (api.allorigins.win)

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (third-party proxy reference)

```
libapp.so: https://api.allorigins.win/raw?url= adjacent to /  
ai_assistant_prompts_screen, eva_nav/ai_assistant_threads_screen
```

Impact: The string sits next to the AI assistant routes in the Dart string pool. A native Flutter client does not need a CORS proxy, so the reference may be inherited from a web build. If live, assistant queries transit an infrastructure provider without a processor agreement.

GO-M3: Visa Go: advertising attribution permissions and a dual Firebase and AWS Pinpoint stack on an invite-only app

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (attribution on invite-only app)

```
AndroidManifest.xml: AD_ID, ACCESS_AD SERVICES_ATTRIBUTION, ACCESS_AD SERVICES_AD_ID,
    BIND_GET_INSTALL_REFERRER_SERVICE
libapp.so: awsPinpointAnalyticsPlugin, awsPinpointPushNotificationsPlugin
```

Impact: AD_ID, both Privacy Sandbox permissions and the install referrer binding are declared, next to Firebase Analytics and AWS Pinpoint Analytics and Push. An invite-only guest product is not acquired through public advertising, so the attribution infrastructure has no evident function.

GO-M4: Visa Go: Art. 9 accessibility data shared with FIFA, no Visa Go specific privacy notice

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (special category data)

```
libapp.so: "I explicitly consent to Visa Go processing the health-related information
    I provide (such as accessibility requirements)..."
"...sharing it with FIFA solely for assessing and fulfilling my accessibility
    seating request."
```

Impact: Accessibility requirements for FIFA World Cup 2026 seating are collected under a purpose-specific explicit consent and shared with FIFA in Zurich. The Visa Global Privacy Notice never names Visa Go, so no product-specific disclosure covers this flow or the AWS, Sentry and Google processing around it.

GO-L1: Visa Go: RECEIVE_BOOT_COMPLETED declared without a receiver

LOW, CVSS v4.0 AV:L/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0 (permission hygiene)

```
AndroidManifest.xml: RECEIVE_BOOT_COMPLETED ; ACCESS_SUPERUSER ; no BOOT_COMPLETED
intent filter
```

Impact: RECEIVE_BOOT_COMPLETED has no registered BOOT_COMPLETED receiver in the manifest. ACCESS_SUPERUSER is explained by the root detection routine.

TTP-H1: Tap to Pay Ready: exported payment kernel binding service without any permission

HIGH, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N, 7.0 (exported kernel service)

```
AndroidManifest.xml (aapt dump xmltree):
  service .KernelMessengerService exported=true process=:thinclient
  property PROPERTY_SPECIAL_USE_FGS_SUBTYPE = "Optional transaction server service to
    speed up transaction processing"
  intent-filter action BIND_TO_PAYMENT_KERNEL ; no android:permission attribute
```

Impact: KernelMessengerService is exported in the :thinclient process, registers the action BIND_TO_PAYMENT_KERNEL and describes itself as a transaction server service for transaction processing. No android:permission guards it, although the same manifest defines and applies a signature permission elsewhere. Any app on the device can bind the service unless the code inside onBind validates the caller, a control the manifest does not show.

TTP-H2: Tap to Pay Ready: no network security configuration and no pinning library of any kind

HIGH, CVSS v4.0 AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 7.6 (kernel backend TLS trust)

```
res/xml/: no network_security_config.xml ; no android:networkSecurityConfig
strings classes*.dex | grep Lokhttp3/CertificatePinner -> no match
Lorg/apache/http/conn/ssl/AllowAllHostnameVerifier; NoopHostnameVerifier;
    trustAllHostnameVerifier
```

Impact: TLS trust rests on the device system CA store alone. A party that controls a trusted root on the device (enterprise MDM profile, security software, rooted or compromised handset) can read and modify the channel between the app and its backend. The kernel backend is cloudpos.digital.visa.com. The dex contains no OkHttp CertificatePinner at all, and ships the Apache AllowAllHostnameVerifier and NoopHostnameVerifier classes next to the safe verifiers.

TTP-M1: Tap to Pay Ready: Google test certificate and private key block bundled in the release dex

LOW, CVSS v4.0 AV:L/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0 (inert test fixture)

```
classes4.dex: PEM certificate + PKCS8 private key block + JWT with x5c header (key
    material not reproduced)
match: googleapis/google-http-java-client .../testing/json/webtoken/TestCertificates.
    java
```

Impact: The PEM certificate, PKCS8 private key block and JWT in classes4.dex match byte for byte the google-http-java-client TestCertificates fixture (CN=foo.bar.com, issuer CN=Root). The material is public and inert. Its presence shows a test class from a transitive dependency reaching the signed release. RFI-IRFOS blast-radius escalation: raised from LOW/2.0 to MEDIUM because a private key block of any origin inside a signed payment kernel release deserves a controller response even where the key is a public test fixture.

TTP-M2: Tap to Pay Ready: INSTALL_PACKAGES permission declared without observable wiring

MEDIUM, CVSS v4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 5.1 (capability declaration)

AndroidManifest.xml: android.permission.INSTALL_PACKAGES ; dex: PackageInstaller, PackageInstaller\$SessionInfo class references only

Impact: INSTALL_PACKAGES is a signature or privileged permission that a Play-distributed app cannot receive, so it is most likely inert. A payment kernel app has no function that needs it.

TTP-L1: Tap to Pay Ready: BLUETOOTH_CONNECT without purpose, NFC declared required=false

LOW, CVSS v4.0 AV:L/AC:H/AT:N/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N, 2.0 (permission hygiene)

AndroidManifest.xml: BLUETOOTH_CONNECT ; uses-feature nfc required=false, bluetooth required=false, usb.host required=false

Impact: BLUETOOTH_CONNECT has no BLE or GATT code path and no function in an NFC tap app. android.hardware.nfc is declared required=false although NFC is the core function.

Impact Analysis

Visa Go and Tap to Pay Ready differ in function and share one posture: no hardened transport configuration. The payment kernel service in Tap to Pay Ready carries the highest weight because the manifest ties it directly to transaction processing. The procedural record adds that the only responses in 104 days were two automatic receipts.

The Complete Chain: Six Messages, 104 Days, Two Automatic Receipts, Zero Replies

Step 1: Disclosure of both applications sent on 5 July 2026 with embargo 3 October 2026. An automatic receipt arrives the same day.

Step 2: Follow-ups on 24 July, 9 August and 24 August 2026. No reply and no receipt.

Step 3: Follow-up on 3 September 2026. No reply.

Step 4: Follow-up on 12 September 2026, 69 days after the disclosure. An automatic receipt arrives, no human reply.

Step 5: Embargo passes on 3 October 2026 with the correspondence unanswered.

Step 6: Publication on 17 October 2026, 104 days after the disclosure and 14 days after the embargo, with the full record intact: six messages, two automatic receipts, no human reply.

Data Protection: Article by Article

Art. 32(1)(a)(b), Art. 25(1) GDPR: GO-H1, TTP-H1 and TTP-H2, missing transport hardening and an unguarded payment kernel service.

Art. 6(1), Art. 7(1), Art. 5(1)(a) GDPR and Art. 5(3) ePrivacy: GO-H2.

Art. 9(2)(a), Art. 35, Art. 13/14 GDPR: GO-M4, accessibility data shared with FIFA without a Visa Go specific notice.

Art. 28, Art. 5(1)(f), Art. 32(1)(b) GDPR: GO-M2 and GO-M1. Art. 5(1)(c), Art. 25 GDPR: GO-M3, GO-L1, TTP-M1, TTP-M2, TTP-L1.

Regulatory & Legal Landscape

Visa Inc. is a US controller with no confirmed EU main establishment in the sources checked, so national authorities hold competence for their own users and the Austrian Datenschutzbehörde acts as the lead contact of this review. The Austrian Datenschutzbehörde and the EDPS were in CC on the first four messages.

Fine exposure under GDPR: Art. 83(4) applies to the Art. 25 and Art. 32 issues in GO-H1, TTP-H1 and TTP-H2, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 6, Art. 7 and Art. 9 issues in GO-H2 and GO-M4, up to EUR 20,000,000 or 4% of total worldwide annual turnover. For Tap to Pay Ready the Play Store data safety declaration states that no user data is collected, while Visa developer documentation describes card read and EMV cryptogram data sent to a Kernel as a Service backend.

Indicators of Compromise

Root level code analysis of the published application. No servers, accounts or infrastructure of the operator were probed. Credentials and identifiers referenced below are withheld from this public report; full values were disclosed privately in the R1 letter.

```
G0-H1: no network_security_config.xml, no android:networkSecurityConfig ; okhttp3.
      CertificatePinner shipped without pins ;
      SecureSocket_RegisterBadCertificateCallback in libapp.so

G0-H2: FirebaseInitProvider (100), FlutterFirebaseMessagingInitProvider (99),
      SentryPerformanceProvider (200) ;
      firebase_crashlytics_collection_enabled=true

G0-M1: seven Google API keys, Cognito User Pool and Identity Pool IDs, Sentry DSN [
      REDACTED IN PUBLIC REPORT -- disclosed privately in R1]

G0-M2: https://api.allorigins.win/raw?url= in libapp.so next to ai_assistant routes

G0-M4: FIFA accessibility seating consent strings, no Visa Go section in the Global
      Privacy Notice

TTP-H1: .KernelMessengerService exported=true, intent-filter BIND_TO_PAYMENT_KERNEL,
      no android:permission

TTP-H2: no network_security_config.xml, no okhttp3.CertificatePinner,
      AllowAllHostnameVerifier / NoopHostnameVerifier classes in dex

TTP-M1: classes4.dex contains a PEM certificate, a PKCS8 private key block and a JWT
      matching the google-http-java-client TestCertificates fixture

TTP-M2: android.permission.INSTALL_PACKAGES declared
```

Disclosure Timeline & Outcome

2026-07-05 Initial disclosure of both applications sent. Embargo stated as 2026-10-03. Automatic receipt from privacy@visa.com.

2026-07-24 Follow-up, 19 days. No reply.

2026-08-09 Follow-up, 35 days. No reply.

2026-08-24 Follow-up, 50 days. No reply.

2026-09-03 Follow-up, 60 days. No reply.

2026-09-12 Follow-up, 69 days. Automatic receipt only.

2026-10-03 Embargo date reached and passed with no human reply.

2026-10-17 This report published, 14 days after the embargo. Correspondence record: six RFI-IRFOS messages, two automatic receipts, zero human replies, zero of three questions answered.

Residual Risk & Recommendations

GO-H1 and TTP-H2: ship a network security configuration with pin-sets for the Visa Go and kernel backend domains; remove the Apache AllowAll and Noop hostname verifiers from Tap to Pay Ready.

TTP-H1: protect KernelMessengerService with a signature permission or a verified caller allow-list and document the caller check.

GO-H2: call setAnalyticsCollectionEnabled(false) before consent, disable Sentry auto-init and Crashlytics collection until consent is recorded.

GO-M1: restrict all Google keys and review the Cognito pools. GO-M2: remove the allorigins.win reference or replace it with a contracted processor. GO-M3: remove advertising permissions. GO-M4: publish a Visa Go specific privacy notice and the DPIA for the FIFA accessibility flow.

TTP-M1: exclude the google-http-client test fixtures from the release. TTP-M2: remove INSTALL_PACKAGES.

Procedural: route the disclosure to the Visa privacy office and reply in writing to the three questions. RFI-IRFOS will update this report with any substantive reply.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethnergasse 25/10, 8020 Graz, Austria All findings derive from root level code analysis of

the published application using publicly available tooling. No operator servers, accounts or infrastructure were probed. Credentials and database identifiers are withheld from this public report; full values were disclosed privately in the original R1 letter and remain available to the operator or to a supervisory authority on request. Research conducted under ISO/IEC 29147, the freedom of scientific research (Art. 17 StGG) and GDPR Art. 89. REF VISA-2026-R1-001.