



Security & Privacy Disclosure, Final Report

Bluecode Android (com.spt.bluecode)

A QR payment wallet ships its own certificate pinning machinery without a single configured pin, starts Firebase analytics on payment events before consent, and 104 days after the first disclosure five messages have drawn no reply of any kind

PUBLIC DISCLOSURE, 17 OCTOBER 2026: EMBARGO REACHED 3 OCTOBER 2026, FIVE MESSAGES SENT, NO REPLY OF ANY KIND, THREE QUESTIONS UNANSWERED

Target	Blue Code International AG (Lachen, Switzerland), controller; Secure Payment Technologies GmbH (Innsbruck, Austria), Art. 27 EU representative
Package	com.spt.bluecode v7.2.73.128094
Platform Audited	Android, root level code analysis of the production APK
Initial Disclosure (R1)	2026-07-05, to datenschutz@spt-payments.com, CC sup port@bluecode.com, press@bluecode.com, Austrian Daten- schutzbehörde, EDPS, CERT.at
Disclosure / Embargo Date	2026-10-03
Report Published	2026-10-17
Overall Severity	HIGH
Findings	5 (2 High, 2 Medium, 1 Low, 0 Critical)
Correspondence	5 messages sent by RFI-IRFOS over 63 days (2026-07-05 to 2026-09-06), 0 replies, 0 automatic acknowledgments, 0 bounces; 41 days of silence after the last message
Authorities Notified	Austrian Datenschutzbehörde (dsb@dsb.gv.at) · EDPS (edps@ edps.europa.eu) · CERT.at (cert@cert.at)

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	H1: No certificate pinning on a real-time payment authorisation channel	5
4.2	H2: Pre-consent Firebase/Google Measurement auto-init on payment lifecycle events, no CMP	6
4.3	M1: Advertising attribution surface open to all callers in a payment wallet . . .	6
4.4	M2: Firebase/Google API key and live Realtime Database URL hardcoded in the binary	7
4.5	L1: Fine location and clipboard permissions broader than the observable function	7
5	Impact Analysis	8
6	The Complete Chain: Five Messages, 104 Days, Zero Replies	8
7	Data Protection: Article by Article	8
8	Regulatory & Legal Landscape	9
9	Indicators of Compromise	9
10	Disclosure Timeline & Outcome	10
11	Residual Risk & Recommendations	10

Executive Summary

Bluecode is a QR-code instant payment scheme used in Austria, Germany, Belgium and Luxembourg and integrated into partner banking apps. Root level code analysis of production APK v7.2.73.128094 found real payment-grade engineering: AndroidKeyStore keys bound to a BiometricPrompt CryptoObject, a screen-capture detection permission, cleartext traffic disabled, backups disabled, an excluded payment SDK database, a reputable IDEMIA tokenisation SDK, no advertising SDK and a correctly designated Art. 27 EU representative.

Two findings carry HIGH weight. H1: the network security configuration trusts only the system CA store and contains no pin-set, although the app ships a shaded copy of the OkHttp CertificatePinner in its own token library. H2: FirebaseInitProvider and the Google Measurement components start at process creation and are wired to named events for qr_code_scanned, confirm_payment, payment_successful and wallet_generated, with no consent management platform in the binary. Two MEDIUM findings cover an advertising attribution surface opened to all callers and a hardcoded Firebase key with a live Realtime Database URL (both values withheld). One LOW finding covers location and clipboard permissions.

RFI-IRFOS sent the full findings on 5 July 2026 and four follow-ups (24 July, 9 August, 24 August, 6 September 2026) to datenschutz@spt-payments.com. No message drew a reply, an automatic acknowledgment or a bounce. The embargo of 3 October 2026 passed 14 days before this report publishes.

ID	Severity	Title
H1	HIGH	No certificate pinning on a real-time payment authorisation channel
H2	HIGH	Pre-consent Firebase/Google Measurement auto-init on payment lifecycle events, no CMP
M1	MEDIUM	Advertising attribution surface open to all callers in a payment wallet
M2	MEDIUM	Firebase/Google API key and live Realtime Database URL hardcoded in the binary
L1	LOW	Fine location and clipboard permissions broader than the observable function

Subject & Operator Context

Bluecode identifies Blue Code International AG, Lachen, Canton of Schwyz, Switzerland (CH-281.323.867) as controller in its own legal notice and privacy policy. Its privacy policy names Secure Payment Technologies GmbH, Müllerstrasse 27, 6020 Innsbruck, Austria as Art. 27 EU representative, which is the correct design for a Swiss controller serving EU users. The Android package namespace com.spt.bluecode belongs to this representative. The Austrian Datenschutzbehörde is the competent authority for the Austrian-initiated review; the data protection authorities of Germany, Belgium and Luxembourg each hold competence for users in their own markets.

Engagement Summary

RFI-IRFOS addressed the privacy contact published in the operator privacy policy, datenschutz@spt-payments.com, and copied the two published business addresses plus the Austrian Datenschutzbehörde, the EDPS and CERT.at. Each of the five messages restated the findings and three yes/no questions on certificate pinning, pre-consent analytics and the advertising attribution surface. The first four messages carried the regulators in CC; the fifth message of 6 September carried support@ and press@ in CC only.

Findings

H1: No certificate pinning on a real-time payment authorisation channel

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 (payment channel TLS trust)

```
res/xml/network_security_config.xml:
  <base-config><trust-anchors><certificates src="system"/></trust-anchors></base-
  config>
no <pin-set> element
classes*.dex: Lat/bluecode/sdk/token/libraries/com/squareup/okhttp3/okhttp/
  Lib__CertificatePinner$Builder;
grep -oE "sha256/[A-Za-z0-9+/]{30,}=" -> no match
```

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 ships a shaded OkHttp CertificatePinner in at.bluecode.sdk.token, so the capability exists in the codebase, and no pin value is configured anywhere in the binary.

H2: Pre-consent Firebase/Google Measurement auto-init on payment lifecycle events, no CMP

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 analytics)

```
AndroidManifest.xml: com.google.firebase.provider.FirebaseInitProvider initOrder=100
    directBootAware=true
    com.google.android.gms.measurement.AppMeasurementReceiver enabled=true
res/values/strings.xml: firebase_event_qr_code_scanned, firebase_event_confirm_payment
,
    firebase_event_payment_successful, firebase_event_wallet_generated
```

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. Analytics events cover QR scans, payment confirmation and payment success. The binary contains the bare IABTCF constants of the Google SDK and no consent management platform or consent copy. RFI-IRFOS blast-radius escalation: raised from MEDIUM/6.9 to HIGH because the processing begins on every installation of a payment app before any consent surface exists, and covers named payment lifecycle events.

M1: Advertising attribution surface open to all callers in a payment wallet

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 surface)

```
AndroidManifest.xml: ACCESS_AD SERVICES_ATTRIBUTION, ACCESS_AD SERVICES_AD_ID
res/xml/ga_ad_services_config.xml: <attribution allowAllToAccess="true"/>
```

Impact: The app declares ACCESS_AD SERVICES_ATTRIBUTION and ACCESS_AD SERVICE S_AD_ID and ships ga_ad_services_config.xml with allowAllToAccess=true. No advertising SDK is bundled, so the surface most plausibly derives from SDK defaults and serves no payment function.

M2: Firebase/Google API key and live Realtime Database URL hardcoded in the binary

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 (key and database URL)

```
res/values/strings.xml:  
  google_api_key: [REDACTED IN PUBLIC REPORT -- disclosed privately in R1]  
  firebase_database_url: [REDACTED IN PUBLIC REPORT -- disclosed privately in R1]  
  project_id, google_storage_bucket: [REDACTED IN PUBLIC REPORT -- disclosed privately  
    in R1]
```

Impact: A Firebase API key, project identifier, storage bucket and Realtime Database URL are readable from res/values/strings.xml. Google documents such keys as non-confidential; the exposure is quota and billing exhaustion plus reliance on correctly configured database rules, which the controller must demonstrate.

L1: Fine location and clipboard permissions broader than the observable function

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 scope)

```
AndroidManifest.xml: ACCESS_COARSE_LOCATION, ACCESS_FINE_LOCATION, READ_CLIPBOARD,  
  WRITE_CLIPBOARD  
assets/web/package.json: mapbox-gl 3.21.0, react-map-gl 8.1.1
```

Impact: ACCESS_FINE_LOCATION serves a merchant map built on Mapbox GL. Coarse location would satisfy a proximity map. READ_CLIPBOARD and WRITE_CLIPBOARD have no code path identified in static strings.

Impact Analysis

H1 and H2 are routine, fixable engineering gaps in an app that otherwise shows deliberate payment security design. The procedural record carries the weight of this case: five messages to the published privacy contact of a payment scheme operator over 63 days, with no acknowledgment of any kind.

The Complete Chain: Five Messages, 104 Days, Zero Replies

Step 1: Disclosure sent on 5 July 2026 with embargo 3 October 2026.

Step 2: First follow-up on 24 July 2026, 19 days after the disclosure. No reply.

Step 3: Second follow-up on 9 August 2026, 35 days after the disclosure. No reply.

Step 4: Third follow-up on 24 August 2026, 50 days after the disclosure. No reply.

Step 5: Fourth follow-up on 6 September 2026, 63 days after the disclosure. No reply.

Step 6: Embargo passes on 3 October 2026 with the correspondence unanswered.

Step 7: Publication on 17 October 2026, 104 days after the disclosure and 14 days after the embargo, with the full record intact: five messages sent, no reply, no acknowledgment, no bounce.

Data Protection: Article by Article

Art. 32(1)(a)(b) GDPR, security of processing: H1, TLS trust without configured pinning on a real-time payment authorisation channel.

Art. 6(1), Art. 7(1), Art. 5(1)(a) GDPR and Art. 5(3) ePrivacy: H2, analytics on payment lifecycle events starting before consent.

Art. 5(1)(c), Art. 25 GDPR, minimisation and design: M1 advertising attribution surface, L1 location and clipboard permissions.

Art. 32(1)(b), Art. 5(2) GDPR: M2 hardcoded Firebase key and Realtime Database URL; the controller carries the burden of showing the database rules are locked down.

Regulatory & Legal Landscape

Blue Code International AG is a Swiss controller with an Austrian Art. 27 representative. Switzerland benefits from a Commission adequacy decision, and the one-stop-shop mechanism does not apply to a controller without EU main establishment, so each national authority holds competence for its own users. 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. 32 issue in H1 and M2, up to EUR 10,000,000 or 2% of total worldwide annual turnover. Art. 83(5) applies to the Art. 6 and Art. 7 issue in H2, up to EUR 20,000,000 or 4% of total worldwide annual turnover. Five messages over 63 days without any acknowledgment from a payment scheme operator is a fact a supervisory authority may weigh when assessing how the disclosure was handled.

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.

```
H1: res/xml/network_security_config.xml, base-config trust-anchors src=system, no pin-  
set  
shaded okhttp3.CertificatePinner present in at.bluecode.sdk.token, no sha256/ pin  
value in classes*.dex  
  
H2: FirebaseInitProvider (initOrder 100, directBootAware), AppMeasurementReceiver/  
Service/JobService enabled  
events: qr_code_scanned, confirm_payment, payment_successful, wallet_generated,  
onboarding_started, onboarding_completed  
  
M1: ACCESS_AD SERVICES_ATTRIBUTION, ACCESS_AD SERVICES_AD_ID, ga_ad_services_config.xml  
allowAllToAccess=true  
  
M2: res/values/strings.xml google_api_key + firebase_database_url [REDACTED IN PUBLIC  
REPORT -- disclosed privately in R1]  
  
L1: ACCESS_FINE_LOCATION, READ_CLIPBOARD, WRITE_CLIPBOARD
```

Disclosure Timeline & Outcome

2026-07-05 Initial disclosure sent. Embargo stated as 2026-10-03.

2026-07-24 First follow-up, 19 days. No reply.

2026-08-09 Second follow-up, 35 days. No reply.

2026-08-24 Third follow-up, 50 days. No reply.

2026-09-06 Fourth follow-up, 63 days. No reply.

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

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

Residual Risk & Recommendations

H1: ship a populated pin-set in the network security configuration for the payment API domains, using the CertificatePinner capability already compiled into the token library.

H2: delay Firebase and Measurement initialisation until consent is recorded, as the manifest already does for Sentry with `io.sentry.auto-init=false`.

M1: remove the advertising attribution permissions and the `allowAllToAccess` configuration.

M2: restrict the Firebase key to the production signing certificate, confirm the Realtime Database rules deny by default, and rotate the key after disclosure.

L1: request coarse location only for the merchant map and document the purpose of clipboard access.

Procedural: RFI-IRFOS remains open to a substantive written reply to the three questions at any time and will update this report to reflect one.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 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 BLUECODE-2026-R1-001.