Coordinated Security & Privacy Disclosure, Final Report

ich.app for Android (at.psa.app.ich, v25.4.3)

Twelve written notices, ninety days, total silence – not one reply of any kind, from an app linking Austrian state identity to bank accounts

PUBLIC DISCLOSURE, 19 SEPTEMBER 2026 – ALL FOUR FINDINGS UNADDRESSED AFTER TWELVE NOTICES, ZERO REPLIES

Target	PSA Payment Services Austria GmbH
Product audited	ich.app for Android, at.psa.app.ich, v25.4.3 – an eID/payment application linking Austrian state identity to bank accounts
Disclosure reference	REF RFI-2026-PSA-001
R1 sent	2026-06-24
Disclosure / embargo date	2026-09-19
Report published	2026-09-19
Severity	CRITICAL (C1 a complete internal server-infrastructure enum in the production binary, including two cleartext HTTP endpoints to a raw Azure IP address, CVSS v4.0 9.3, unaddressed)

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

On 24 June 2026, RFI-IRFOS performed static analysis of the production ich.app Android application, an Austrian eID and payment app linking state-issued identity to bank accounts, and identified one CRITICAL and three HIGH findings: a hardcoded ServerType enum containing five non-production environment definitions alongside the production one, two of which (AZURE2A and AZURE2B) connect over unencrypted HTTP to a raw Azure IP address with no TLS and no hostname, and two more pointing to internal eidtest.at test and acceptance environments, all extractable from the public APK without root access via standard decompilation tooling, two hardcoded token-like strings (a 32-character and an 8-character alphanumeric value) within the same enum whose exact function, API token or OIDC client secret, RFI-IRFOS could not conclusively determine from static analysis alone, Firebase Analytics and Google AdServices advertising-attribution permissions present on an app that processes biometric authentication and links Austrian state identity to bank accounts, with no documented purpose limitation in the privacy policy, and a Firebase API key hardcoded in the production binary.

Across twelve written notices over ninety days, cc'd to the Austrian Datenschutzbehoerde from the fourth notice onward and to the European Data Protection Supervisor from the fifth, not one reply of any kind, human or automated, was ever received, not from PSA Payment Services Austria GmbH, not from the Austrian DSB, and not from the EDPS. None of RFI-IRFOS's three standing questions, on the Art. 6/32 legal basis and technical measures for shipping a complete internal server infrastructure in a production binary, which internal endpoints or credentials have since been removed or rotated, and whether an Art. 35 DPIA was conducted for payment and identity data processing, ever received an answer.

Scope: Static analysis of the publicly downloaded production ich.app Android APK (v25.4.3), via apktool decompilation, on an authorized test device, only. No PSA account, backend, or infrastructure was accessed or tested.

Disposition

R1 sent 24 June 2026 to datenschutz@psa.at, cc office@psa.at, subsequently cc'ing the Austrian Datenschutzbehoerde and the European Data Protection Supervisor. Across twelve written notices over ninety days, not one reply of any kind, human or automated, was ever received from PSA Payment Services Austria GmbH, the Austrian DSB, or the EDPS.

ID	Severity	Title
C1	CRITICAL	Complete internal server infrastructure enum in the production binary, including two cleartext HTTP endpoints
H1	HIGH	Hardcoded token-like strings in the ServerType enum
H2	HIGH	Firebase Analytics and Google AdServices permissions on an eID/payment app
H3	HIGH	Hardcoded Firebase API key in the production binary

Subject & Operator Analysis

PSA Payment Services Austria GmbH operates ich.app, an Austrian electronic-identity and payment application that links state-issued identity credentials to users' bank accounts.

Findings

C1: Complete internal server infrastructure enum in the production binary, including two cleartext HTTP endpoints

CRITICAL, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 9.3

at/psa/app/ich/business/models/ServerType.smali contains a hardcoded enum with five non-production environments alongside PROD: WDINT, AZURE2A, AZURE2B, ABN, and CUSTOM. AZURE2A (http://20.61.119.111:8081) and AZURE2B (http://20.61.119.111:8091) connect over unencrypted HTTP to a raw Azure IP address with no TLS and no hostname. WDINT and ABN point to internal eidtest.at test and acceptance environments. Extraction requires no root and is achievable via a single apktool d command.

No reply of any kind, across twelve notices, addressed whether any of these internal endpoints have been removed from the production build or rotated.

Impact: A complete map of internal, non-production infrastructure for an eID and payment platform, including two endpoints reachable over unencrypted HTTP at a public IP address, is shipped to every user who installs the app.

Fix: Remove all non-production ServerType entries from release builds, and ensure any surviving internal endpoints use TLS with proper hostname validation.

H1: Hardcoded token-like strings in the ServerType enum

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

Within the same enum's WDINT branch, two hardcoded string values are present: a 32-character alphanumeric string ('YmJc3vYzUv5iGPeDGHFDym4XY5fQhLLu') and an 8-character string ('5ibzwi1y'), possible API tokens or OIDC client secrets. RFI-IRFOS could not conclusively determine their function from static analysis alone.

No reply of any kind confirmed or clarified the function or sensitivity of these values.

Impact: Unidentified credential-shaped values ship in the production binary of an eID/payment app, with no confirmation of their scope or whether they grant access to non-production systems.

Fix: Identify, rotate if credential-bearing, and remove these values from the production build.

H2: Firebase Analytics and Google AdServices permissions on an eID/payment app

HIGH, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N, 8.7

The app processes biometric authentication and links Austrian state identity to bank accounts, while simultaneously bundling Firebase Analytics (app-measurement.com) and declaring ACCESS_ADSERVICES_AD_ID and ACCESS_ADSERVICES_ATTRIBUTION permissions, with no documented purpose limitation in the privacy policy.

No reply of any kind addressed the purpose or legal basis for these permissions on this specific app.

Impact: Analytics and advertising-attribution infrastructure operates alongside identity-verification and banking functionality with no documented purpose limitation separating the two.

Fix: Remove advertising-attribution permissions from an eID/payment application, or document a specific, limited purpose and legal basis for Firebase Analytics if retained.

H3: Hardcoded Firebase API key in the production binary

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

Firebase API key AIzaSyA9BSmFUUHfYxcxzUUAoG4OCuyf-0TQxeg is hardcoded as both google_api_key and google_crash_reporting_api_key in res/values/strings.xml.

No reply of any kind addressed this finding.

Impact: A production Firebase project's attack surface, on an app processing identity and payment data, cannot be independently ruled safe from outside the console once its key ships in every installed client.

Fix: Rotate the exposed key, restrict it to the correct package name and SHA-256 signing fingerprint, and confirm deny-by-default security rules.

Twelve Notices, Total Silence, From Anyone

Across twelve written notices over ninety days, addressed to PSA Payment Services Austria GmbH and, from the fourth notice onward, cc'd to the Austrian Datenschutzbehoerde and the European Data Protection Supervisor, no reply of any kind was ever received, not from PSA, not from either regulator. A search across the entire mailbox for any inbound message from psa.at, the Austrian DSB, or the EDPS on this case returned zero results.

Data Protection, Article by Article

Finding	Provision	Concern
C1	GDPR Art. 6, Art. 32	Internal server infrastructure, including cleartext endpoints, shipped in production
H1	GDPR Art. 32	Unidentified credential-shaped values in the production binary
H2	GDPR Art. 5(1)(c), Art. 13(1)(e)	Advertising-attribution infrastructure alongside eID/banking functionality
H3	GDPR Art. 25(1), Art. 32(1)(b)	Hardcoded Firebase key on an identity/payment app

Date	Event

Disclosure Timeline & Outcome

Date	Event
2026-06-24	R1 sent to datenschutz@psa.at, cc office@psa.at; 1 CRITICAL + 3 HIGH findings
2026-07-03	Follow-up, nine days silence, Austrian DSB added to cc for the first time
2026-07-07	Follow-up, thirteen days silence, EDPS added to the to-line
2026-08-28	Follow-up, sixty-five days silence
2026-09-12	Follow-up, eighty-one days since disclosure, fifteen days since the last message, three questions repeated verbatim, a new deadline of 26 September stated, embargo unchanged at 19 September
2026-09-19	Embargo, as stated identically throughout the correspondence, closes and this report publishes

Residual Risk & Recommendations

- Remove all non-production ServerType entries and the two cleartext HTTP endpoints from release builds.
- Identify and rotate the two hardcoded token-like strings, or confirm and document that they carry no sensitive access.
- Remove or strictly purpose-limit advertising-attribution permissions on an eID/payment application.
- Rotate the exposed Firebase key.
- Conduct and publish an Art. 35 DPIA covering payment and identity data processing.

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

ZVR 1015608684 • GISA 39261441 • UID ATU83405245 • Steuernummer 68 696/8736 • Elisabethinergasse 25/10, 8020 Graz, Austria Coordinated disclosure per ISO/IEC 29147. GDPR Art. 5, 6, 13, 25, 32, 35. REF RFI-2026-PSA-001.