Coordinated Security Disclosure, Final Report

A-Trust Signatur App (at.atrust.tanapp)

Qualified trust service provider, eIDAS Austria

Target	A-Trust GmbH, 1030 Wien, UID ATU50272100, FN 195738a
Product audited	A-Trust Signatur App, at.atrust.tanapp, versionName 5.1.7.0, versionCode 108
Disclosure reference	ATRUST-2026-R1 through R7
R1 sent	2026-06-20
Disclosure / embargo date	2026-09-17
Report published	2026-09-18
Severity	HIGH (AT-02, CVSS v4.0 7.4)

SHA-256 (base APK):

`caf10024be5606bc42b82fb6e9f06451f843c7961e7eb550dbc71352f347ea98`

rfi.irfos@gmail.com • rfi-irfos.com

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

Contents

Executive Summary

A-Trust GmbH is Austria's sole qualified trust service provider under eIDAS, the company whose signature carries the same legal weight as a handwritten signature for every Austrian citizen and business that uses ID Austria, the Handy-Signatur, or the A-Trust Signatur app directly. RFI-IRFOS's static analysis of the A-Trust Signatur app found that the root detection mechanism protecting qualified signature operations can be silently disabled through a user writable app preference, that the app performs no certificate pinning on the endpoints that carry signature requests, and that qualified signature audit logs are written to the device in plain text.

A-Trust's own Head of Legal and Operations, Christoph Klein, confirmed the absence of certificate pinning in writing on 2026-06-26, then on 2026-06-29 declined to discuss the matter further, disputed the accuracy of RFI-IRFOS's public ledger without pointing to a single factual error, and asked RFI-IRFOS not to publish the correspondence. RFI-IRFOS restated the open points twice more, on 2026-08-04 and 2026-09-04, without reopening the substantive debate. No remediation timeline, no confirmation of a fix, and no further reply followed.

The 90 day disclosure window closed on 2026-09-17 with the findings unresolved from RFI-IRFOS's perspective. This report is the scheduled public consequence of that silence, not a new escalation. The central issue is not that a bug exists, every software product has bugs, but that this particular bug sits inside the trust anchor of the Austrian digital identity system. A root detection bypass that any rooted device's user, or any app with root access on that device, can flip means the guarantee that a device is secure enough to sign is not enforced by the app itself, only requested of it.

Scope: Static, root level analysis of the publicly downloaded A-Trust Signatur app binary only. No servers, accounts, or A-Trust infrastructure were accessed or tested.

ID	Severity	Title
AT-01	HIGH	Root detection bypassable via user settable SharedPreference
AT-02	HIGH	No certificate pinning on qualified signature endpoints, confirmed by A-Trust
AT-03	MEDIUM	Qualified signature session logs written in plaintext to device storage
AT-04	MEDIUM	Firebase API key hardcoded in the release build
AT-05	LOW	Broad manifest level declaration of MANAGE_DEVICE_POLICY_LOCK_CREDENTIALS

Subject & Operator Analysis

A-Trust Gesellschaft fur Sicherheitssysteme im elektronischen Datenverkehr GmbH, UID ATU50272100, FN 195738a, Handelsgericht Wien, registered seat 1030 Wien, Landstrasser Hauptstrasse 1B.

A-Trust is the qualified trust service provider behind ID Austria, the national eID operated jointly with the Digitales Amt and BKA, the legacy Handy-Signatur, and the xIDENTITY EU cross border eID scheme. The shared cryptographic library at the heart of this report, at.a trust.mobsig.library, is not confined to the standalone Signatur app. It is embedded in ID Austria's own Android app, at.gv.oe.app, as well. A defect in this library is therefore a defect in the trust layer used by the entire national eID system, not a defect isolated to one consumer app. RFI-IRFOS disclosed the corresponding findings in ID Austria separately, REF DIGAMT-2026-001 and 002, to the Digitales Amt and BKA, whose own delivery addresses bounced repeatedly across a six week period. That disclosure is tracked and reported independently.

Correspondence contact: Mag. Mag. (FH) Christoph Klein, Head of Legal and Operations, c hristoph.klein@a-trust.at, signed every reply personally with his full name, title, and function. This is A-Trust's first appearance in the RFI-IRFOS disclosure corpus.

Architecture & Data Flow

The A-Trust Signatur app authenticates a user via PIN or biometric, then relays a signing request to a remote qualified signature creation device operated by A-Trust, which performs the actual cryptographic signing operation and returns the signed document or hash. Trust in this flow depends on three guarantees holding simultaneously: the device the user signs from has not been compromised in a way that lets an attacker intercept the authentication factor or substitute the document being signed, the channel between the app and A-Trust's signing backend cannot be intercepted or spoofed, and a tamper evident audit record of what was actually signed exists. The findings below show each of these three guarantees is weaker in practice than the architecture assumes.

The app also embeds Firebase (Google Cloud) for crash reporting and a realtime database reference, project tanapp-ba4be, and requests the Android 12+ MANAGE_DEVICE_POLICY _LOCK_CREDENTIALS permission at the manifest level without a narrowly scoped runtime guard visible in the binary.

Findings

AT-01: Root detection bypassable via user settable SharedPreference

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

MainActivity.smali calls RootBeer.isRooted(). If the device is rooted, the app checks PreferenceData.GetRootKitDetectionAccepted(). If that preference reads true, execution continues normally with no further block.

```
invoke-virtual {v1}, Lcom/scottyab/rootbeer/RootBeer;->isRooted()Z
move-result v1
if-eqz v1, :cond_29

invoke-static {p0}, Lat/atrust/mobsig/library/preferences/PreferenceData;->
    GetRootKitDetectionAccepted(...)Z
move-result v1
if-nez v1, :cond_29   ; preference true -> skip block, continue
```

On a rooted device, any process with superuser access, or the device owner via adb shell, can set this preference directly, silently disabling the check A-Trust relies on to keep qualified signing off compromised devices. eIDAS Art. 24(2)(b) and ETSI EN 319 401, section 6.5, require a qualified trust service provider to maintain the integrity of the environment its signing operations run in. A check that the environment itself controls whether it is enforced does not meet that bar. The same at.atrust.mobsig.library ships inside ID Austria, at.gv.oe.app, and was disclosed there separately as finding IDA-02.

Impact: A rooted device's qualified signature session runs with no enforced tamper barrier, undermining the eIDAS Art. 26(1)(c) sole control guarantee.

Fix: Remove the RootKitDetectionAccepted bypass entirely. For qualified signature operations, root detection must be a hard stop with no user bypassable preference. Use Android Keystore StrongBox where supported and verify attestation.

AT-02: No certificate pinning on qualified signature endpoints, confirmed by A-Trust

HIGH, CVSS v4.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N, 7.4

No network_security_config, no pin-set entries, and no CertificatePinner or custom X509TrustManager exist anywhere in the binary. TLS to the A-Trust signing endpoints trusts the full system CA store.

Confirmed in writing by A-Trust, 2026-06-26

Christoph Klein, Head of Legal and Operations, verbatim: Certificate Pinning war in einer fruheren Version umgesetzt, ist in der aktuellen Version allerdings nicht aktiv. Wir nehmen den Hinweis auf und prufen die Wiederaufnahme.

Pinning existed in an earlier version and was removed. A-Trust stated it would examine reinstating it. As of publication, 83 days after that confirmation and after two written requests for a timeline, 2026-08-04 and 2026-09-04, RFI-IRFOS has received no update. Without pinning, an MDM injected corporate root, a compromised intermediate CA, or a state level CA can intercept or manipulate the OIDC authorization flow and the signature request channel undetected by the app. Independently reproducible with any TLS intercepting proxy against a live signing session in under five minutes.

Impact: A network position attacker can intercept or alter the qualified signature request channel with no client side detection mechanism in place.

Fix: Implement certificate pinning via network_security_config.xml with a primary and backup pin for all A-Trust operated endpoints, on a scheduled rotation.

AT-03: Qualified signature session logs written in plaintext to device storage

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

LoggingOegv.smali, part of the shared at.atrust.mobsig.library, initialises a Logback FileAppender writing log-<date>.txt to device storage.

The exact content scope of these logs, whether authentication events, certificate serials, or signature operation metadata are included, could not be fully determined through static analysis alone. The existence of a persistent, unencrypted log file for a qualified signature client is itself a GDPR Art. 5(1)(c) data minimisation concern regardless of exact content, and persists across app sessions and possibly device backups.

Impact: A persistent, unencrypted on device log file readable by any process with root access, and possibly included in device backups.

Fix: Audit the log output of LoggingOegv to determine exactly what data is recorded. Redact authentication tokens, certificate identifiers, or personal data. Encrypt the log file and auto delete after 24 hours if file logging is needed for support.

AT-04: Firebase API key hardcoded in the release build

MEDIUM, CVSS v4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N, 4.8

A Google and Firebase API key is statically embedded in the release APK, res/values/strings.xml.

```
google_api_key = AIzaSyA4FveLgjGzGXXWUnh-UIxS2WQX6r3p3Pw
google_crash_reporting_api_key = AIzaSyA4FveLgjGzGXXWUnh-UIxS2WQX6r3p3Pw
firebase_database_url = https://tanapp-ba4be.firebaseio.com
```

Whether Google Cloud Console fingerprint restrictions are applied server side could not be verified from the client binary alone. A-Trust's 2026-06-26 reply characterised the key as not a secret, a position RFI-IRFOS rejected the same day, on the standard grounds that key exposure is a quota, billing, and backend access risk independent of whether the key is formally classified as secret.

Impact: Without server side restriction, the key can be used independently of the signed APK to access the Firebase project tanapp-ba4be.

Fix: Restrict the API key to the production APK's certificate fingerprint in Google Cloud Console and enable Firebase App Check.

AT-05: Broad manifest level declaration of MANAGE_DEVICE_POLICY_LOCK_CREDENTIALS

LOW, CVSS v4.0 AV:L/AC:H/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N, 2.6

MANAGE_DEVICE_POLICY_LOCK_CREDENTIALS and REQUEST_PASSWORD_COMPLEXITY are declared at manifest scope without a visible runtime guard limiting them to the signature PIN setup flow specifically.

In context, setting a device PIN for the signature authentication factor, this is explainable. Documented for completeness, no evidence of misuse found.

Impact: Low in isolation, worth tightening as defense in depth.

Fix: Verify at runtime that this permission is only exercised during the explicit signature PIN setup flow, and scope it narrowly.

Impact Analysis

The people affected are not an abstract user base. They are every Austrian resident, business owner, and public sector employee who relies on A-Trust's signature to have the same legal force as their own handwritten one under eIDAS Art. 25. AT-01 and AT-02 combine into a concrete scenario: a person signs a document, a rental contract, a tax filing, a power of attorney, on a device that is rooted, deliberately by the user or without their full awareness through a pre rooted budget device, or on a network path an attacker controls. The root check that should stop qualified signing on that device can be silently turned off. The TLS channel that should make request tampering detectable has no pinning to catch a substituted certificate.

Under eIDAS Art. 26(1)(c), a qualified electronic signature must be created under the sole control of the signatory. A device or network compromise that goes undetected because neither of these two protections is enforced breaks that guarantee in a way the signatory has no way to notice. They see Document A on screen and believe they signed Document A, with no technical assurance that Document B was not what actually reached A-Trust's signing backend.

The Complete Chain

- Point of contact: a person installs the A-Trust Signatur app, or uses the same underlying library through ID Austria, to sign a document that needs legal force, a contract, an official filing, a power of attorney.
- Trust assumption formed: the person believes, and is legally entitled to believe under eIDAS, that what they see on screen is what gets signed, and that only they control the signing action.
- Weak point one, AT-01: if the device is rooted, deliberately, through a pre rooted budget device, or through malware with root privileges, the app's own root check can be flipped off via a writable preference, with no further barrier.
- Weak point two, AT-02: even on a non rooted device, the network path is unprotected against certificate substitution. A compromised or MDM injected CA can sit in the middle of the signing request undetected, because the app trusts the full system CA store with no pinning.
- Consequence: an attacker positioned at either weak point can, in principle, alter the signing request between what the user sees and what reaches A-Trust's signing device. The person signs Document A while Document B is what is actually signed under their qualified certificate, with no technical mechanism in the app itself to catch the substitution.
- What stops this today: nothing inside the app. A-Trust's own confirmation that certificate pinning is currently inactive removes the one layer that would otherwise catch this class of interception. The stated intention to examine reinstating it has produced no confirmed fix, timeline, or update across 83 days and two written requests.
- End state at publication: the qualified signature chain for A-Trust Signatur users rests on the assumption that no rooted device and no compromised TLS path will ever be used to sign, an assumption the app does not itself verify or enforce to the standard eIDAS requires of a qualified trust service provider.

Data Protection, Article by Article

GDPR Art. 5(1)(c), data minimisation. AT-03's plaintext, persistent session log on device is a minimisation concern independent of its exact content. A qualified signature client should not retain unencrypted operational logs indefinitely on the device filesystem.

GDPR Art. 5(1)(f) and Art. 32, integrity, confidentiality, security of processing. AT-01 and AT-02 both bear directly on Art. 32's requirement for appropriate technical and organisational measures. A qualified trust service provider's own security architecture is a textbook case of what Art. 32 is meant to cover, and a confirmed inactive certificate pinning layer plus a user bypassable root check are measures that are not appropriate to the risk of qualified signature interception.

GDPR Art. 32(2) requires the controller to account for the risks in particular from accidental or unlawful alteration of processed data. A substituted signing request is precisely an alteration in the Art. 32(2) sense.

Regulatory & Legal Landscape

A-Trust operates as a qualified trust service provider under Regulation (EU) 910/2014, eIDAS, supervised in Austria by RTR, Rundfunk und Telekom Regulierungs-GmbH, as the national supervisory body for trust services, in coordination with the conformity assessment body that audits A-Trust against ETSI EN 319 401 and ETSI EN 319 411. A-Trust further qualifies as a wesentliche Einrichtung under NIS2 and NISG 2026 given its role in the Austrian digital identity and financial trust infrastructure, which brings coordinated vulnerability disclosure handling obligations under NIS2 Art. 12 and Recital 58. Data protection oversight sits with the Datenschutzbehorde, kept in BCC or CC across this entire correspondence.

A-Trust's 2026-06-29 reply stated it had itself informed the competent authorities and welcomed their independent review. RFI-IRFOS has not received confirmation from RTR, DSB, or CERT.at of the scope or outcome of that self referral, and notes the distinction between an internal referral and a completed, confirmed remediation.

Indicators of Compromise & Reproducible Evidence

Item	Value
Package	at.atrust.tanapp, versionName 5.1.7.0, versionCode 108
SHA-256 (base.apk)	caf10024be5606bc42b82fb6e9f06451f843c7961e7eb550dbc71352f347ea98
AT-01 location	smali_classes2/at/atrust/tanapp/MainActivity.smali
AT-02 evidence	no network_security_config, no pin-set, no CertificatePinner or custom X509TrustManager anywhere in the binary
AT-03 location	smali_classes2/at/atrust/mobsig/library/util/LoggingOegv.smali
AT-04 key	AIzaSyA4FveLgjGzGXXWUnh-UIxS2WQX6r3p3Pw, firebase_database_url https://tanapp-ba4be.firebaseio.com
AT-05 permissions	MANAGE_DEVICE_POLICY_LOCK_CREDENTIALS, REQUEST_PASSWORD_COMPLEXITY
Shared library note	at.atrust.mobsig.library is also embedded in at.gv.oe.app, ID Austria, disclosed separately under REF DIGAMT-2026-001 and 002

Date	From	Action

Disclosure Timeline & Outcome

Date	From	Action
2026-06-19	RFI-IRFOS	R1 sent for ID Austria, at.gv.oe.app, CC'd to A-Trust office and sales, shared library findings.
2026-06-20	RFI-IRFOS	R1 sent for A-Trust Signatur app, at.atrust.tanapp v5.1.7.0, to office and sales, BCC DSB, CERT.at, RTR.
2026-06-25	RFI-IRFOS	Urgent follow up after 5 days of silence, escalated to datenschutz and security.
2026-06-26	Christoph Klein	Substantive reply. AT-02 confirmed in writing, pinning existed in an earlier version, currently inactive, reinstatement to be examined. AT-01 scope accepted with a correction. AT-04 not a secret position raised. ID Austria findings correctly routed to BRZ.
2026-06-26	RFI-IRFOS	R3 sent, point by point response, AT-01 severity upheld with corrected ETSI reference, AT-02 confirmation welcomed with a remediation timeline request, AT-04 deflection rejected.
2026-06-29	Christoph Klein	Reply stating A-Trust would handle the matter through internal and regulatory channels only, would not discuss further substantively, requested no further public characterisation of the correspondence.
2026-06-29	RFI-IRFOS	R4 sent, naming four response patterns for the record: internal process burial, correspondence restriction request, attempted retraction of the AT-02 confirmation, request not to name the individual who signed every prior reply himself.
2026-06-29	Christoph Klein	Final substantive reply. Disputed the ledger's accuracy in general terms without identifying a specific inaccuracy. The one example given, an ETSI section number error, had already been self corrected by RFI-IRFOS in R3, before it was raised. Stated the matter had been referred to the competent authorities. Closed with: further communication in this matter will not take place.

Date	From	Action
2026-06-29	RFI-IRFOS	R5 sent, five points for the written record: verbatim AT-02 quote stands, self correction timeline refutes the fabrication characterisation, finding correctness is independent of authorship, NIS2, NISG, Art. 17 StGG and GDPR Art. 89 named as the legal basis for the research, welcomed the authority referral.
2026-08-04	RFI-IRFOS	R6 sent, explicitly not reopening the substantive debate, restating two still open points from A-Trust's own correspondence: AT-02 remediation timeline, reference number or timeframe for the stated authority review. Noted separately that ID Austria's own bounced addresses meant the shared library findings had to be redelivered independently to BKA.
2026-09-04	RFI-IRFOS	R7 sent, 13 day pre disclosure notice restating the same two open points and the fixed embargo date of 2026-09-17, unchanged since 2026-06-19.
	A-Trust	No reply received since 2026-06-29.
2026-09-17		Disclosure and embargo date reached. No remediation confirmation, no timeline, no further correspondence from A-Trust.
2026-09-18	RFI-IRFOS	Findings published on the permanent public ledger, rfi-irfos.com, and in this report.

Correction for the record

An earlier internal RFI-IRFOS tracking note briefly logged two automated ID Austria device linking notifications, 2026-08-07 and 2026-08-17, sender notification@a-trust.at , as a possible reply from A-Trust. On review, these are routine, automated ID Austria account notification emails sent to RFI-IRFOS's own linked ID Austria account, unrelated to this disclosure. They are not counted as correspondence in this timeline. A-Trust's last substantive communication on this matter remains its 2026-06-29 closing reply.

Residual Risk & Recommendations

Open at publication: AT-02, no certificate pinning, remains by A-Trust's own last statement unresolved. Pinning was removed at some point before this audit and, as of 83 days after A-Trust's written acknowledgement, no reinstatement has been confirmed. AT-01's SharedPreference based root check bypass has received no confirmation of a fix. AT-03 and AT-04 were not substantively addressed in any A-Trust reply.

- Remove the user or root writable bypass path for root detection entirely. For qualified signature operations this must be a hard stop, not a preference.
- Implement certificate pinning via network_security_config.xml with a primary and backup pin for all A-Trust operated signing endpoints, on a scheduled rotation.
- Audit and redact the content of LoggingOegv's file output, encrypt or eliminate on device plaintext session logs.
- Restrict the exposed Firebase and Google API key to the production APK's certificate fingerprint and enable Firebase App Check.

RFI-IRFOS re pulls and diffs the published APK on a rolling basis through the life of this ledger entry. A silent fix, a new release that reinstates certificate pinning without any accompanying public statement, will be recorded as a positive update to this entry, not treated as contradicting the finding. The finding was, and remains, that pinning was inactive as of the versions analysed and confirmed by A-Trust in writing.

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