MOBSF

ANDROID STATIC ANALYSIS REPORT

Wise (8.80.2)

File Name:	Wise.apk
Package Name:	com.transferwise.android
Scan Date:	Oct. 19, 2024, 5:16 p.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	5/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
5	30	3	2	2

FILE INFORMATION

File Name: Wise.apk
Size: 80.77MB
MD5: 35b7f3b952d3bd44c32fb052ca264aaa
SHA1: 3d65c1cb71bb86f7623a3b91c2c74fa042da83f4
SHA256: e7395fc6582c53300ee83d422e92514b5aeb3007376c29ab7a645559f9fb896c

APP INFORMATION

App Name: Wise
Package Name: com.transferwise.android
Main Activity: com.wise.notifications.presentation.preferences.NotificationPreferencesActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 8.80.2
Android Version Code: 1273

APP COMPONENTS

Activities: 253
Services: 20
Receivers: 10
Providers: 7
Exported Activities: 10
Exported Services: 3
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=UK, L=London, CN=Transferwise
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-03-20 14:37:28+00:00
Valid To: 2039-03-14 14:37:28+00:00
Issuer: C=UK, L=London, CN=Transferwise
Serial Number: 0x532afd28
Hash Algorithm: sha1
md5: 67ab431d02abb63fb4a9a1ae78a44481
sha1: 836f4c878866ba3f4f2b70dc5a48f882512adb6f
sha256: 149c4ea5825a81065589d27a60ea7e554df4b49e3c660cb65ba730025080dbd0
sha512: f067d70337a58c4afdf6176cad8aed64b97a9c3722484b3dcd697537a6e4424ce374e554c88b2c68a331fd0c1d24c589c74bb52643b6c7f9863265c12c67e2fd
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 006db799b66c5e8b9835625c44e529843c674cc06124398eddeb07f7404fde37
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.android.vending.CHECK_LICENSE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.transferwise.android.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>/home/mobsf/.MobSF/uploads/35b7f3b952d3bd44c32fb052ca264aaa/35b7f3b952d3bd44c32fb052ca264aaa.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check
possible Build.SERIAL check
SIM operator check
network operator name check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes4.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check possible VM check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes5.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes6.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check
Build.DEVICE check
Build.PRODUCT check
Build.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
network operator name check
possible ro.secure check
possible VM check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes7.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes8.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check Build.TAGS check SIM operator check network operator name check subscriber ID check</td></tr><tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

FILE	DETAILS
classes9.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.transferwise.android.activity.SplashActivity	Schemes: transferwise://, Hosts: main,
com.wise.deeplink.DeepLinkProxyActivity	Schemes: tw://, transferwise://, https://, Hosts: azonnalifizetes.hu, wise.com, transferwise.com, tw.onelink.me, Paths: /adyen/complete, /account/account-details, /account/limit/atm_withdrawal, /account/auto-conversions, /app-link, /authenticator-enrolment, /business-onboarding, /borderless-account/dashboard/add-money/start, /backup-phone-number/, /card-management, /cards/expiry, /cards/types, /cards/welcometocountry, /cards/welcometocountry/feedback, /contact, /disputes, /flows/open-balance, /flows/balances/add, /flows/groups/open, /flows/bank-details, /flows/account-details, /flows/amazon, /flows/assets-deeplink/open, /flows/links/enable-interest, /flows/request-setup, /help/contact, /kyc-flows/handoff, /kyc-flows/handoff/, /kyc-flows/recovery/, /kyc-flows/recovery, /openbanking/authorize, /paylikealocal, /pay, /transferFlow, /user/account, /user/recipients/list, /users, /user/verify/recovery, /user/verify/recovery/, /payments/wisetag, /payments/quickpay, /verification, Path Prefixes: /help/articles/, /invite, /pay/r/, /pay/c/, /recipients/charities, /self-serve/connected-accounts, /stories, /web-view, /7Sx7, /7qT9, /1858392014, Path Patterns: /budgets/groups/.*, /cards/order/.*, /cards/order/.*/resume, /cards/.*/add-to-wallet, /cards/.*/replace, /cards/.*/replace/.*, /cards/types/.*, /disputes/.*, /share/.*, /pay/me/.*, /user/account/activities/by-resource/transfer/.*, /transactions/activities/by-resource/.*, /pay/business/.*,

ACTIVITY	INTENT
com.adyen.threeds2.internal.ui.activity.ChallengeActivity	Schemes: https://, adyen3ds2://, Hosts: wise.com, com.transferwise.android, Path Prefixes: /adyen3ds2,
com.transferwise.android.forms.DeeplinkInterceptorAlias	Schemes: https://, Hosts: wise.com, transferwise.com,
com.wise.android.dynamicflow.DeeplinkInterceptorAlias	Schemes: https://, Hosts: wise.com, transferwise.com,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.transferwise.android,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **17** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Activity-Alias (com.transferwise.android.activity.SplashActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
3	Activity (com.wise.deeplink.DeepLinkProxyActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Content Provider (com.wise.common.util.provider.ValueProvider) is Protected by a permission. Permission: com.transferwise.android.READ_SHARED_CONTENT protectionLevel: signature [android:exported=true]	info	A Content Provider is found to be exported, but is protected by permission.
5	Broadcast Receiver (com.wise.ui.common.NotificationChannels$LocaleChangedReceiver) is not Protected. [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.wise.atmguide.impl.ui.AtmGuideActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity (com.wise.cards.presentation.impl.nfc.NFCDummyActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
8	Activity (com.adyen.threeds2.internal.ui.activity.ChallengeActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
9	Activity-Alias (com.transferwise.android.forms.DeeplinkInterceptorAlias) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
10	Activity-Alias (com.wise.android.dynamicflow.DeeplinkInterceptorAlias) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
11	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
12	Activity (androidx.biometric.DeviceCredentialHandlerActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
13	Activity (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
14	TaskAffinity is set for activity (com.braze.push.NotificationTrampolineActivity)	warning	If taskAffinity is set, then other application could read the Intents sent to Activities belonging to another task. Always use the default setting keeping the affinity as the package name in order to prevent sensitive information inside sent or received Intents from being read by another application.
15	Service (com.google.android.gms.nearby.exposurenotification.WakeUpService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.nearby.exposurenotification.EXPOSURE_CALLBACK [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
16	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
17	Activity (androidx.compose.ui.tooling.PreviewActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
18	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

NO	ISSUE	SEVERITY	DESCRIPTION
19	Service (com.google.android.gms.tapandpay.issuer.GeneratePaymentCredentialsService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.permission.SEND_ANDROID_PAY_DATA [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

</> CODE ANALYSIS

HIGH: **3** | WARNING: **10** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Ad/C7100e.java Am/C7140l.java Am/InterfaceC7142n.java Am/X.java B0/X.java B1/C7240h.java B1/W.java B8/g.java BF/d.java CH/b.java CH/e.java Ct/c.java Ct/d.java Ct/p.java EN/n.java Ed/e.java Eq/InterfaceC7644a.java Et/C7661g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Fp/C7719a.java Fq/C7720a.java GB/f.java H0/C7882l0.java J0/C8125t0.java J0/X0.java JA/b.java JA/d.java JA/o.java Jt/C8247b.java KD/e.java KD/m.java KE/c.java Kt/C8475A.java Kt/C8481G.java Kt/C8483I.java Kt/C8487M.java Kt/C8493f.java Kt/C8500m.java Kt/C8505r.java Kt/v.java Kt/x.java LB/j.java Lp/t.java MR/c.java Mz/G.java Nv/j.java OE/a.java Ov/C8941B.java PG/a.java PG/h.java PG/i.java PI/d.java Pk/h.java Q8/b.java Qq/m.java Rq/C9298b.java Rt/C9303a.java SB/b.java SG/b.java SG/c.java SG/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	SG/j.java TG/a.java TI/c.java UI/E.java VK/a.java Vl/C9629a.java Vl/b.java Vl/f.java YK/a.java YK/n.java Z7/b.java Zu/g.java a8/C10031e.java a8/w.java bQ/C11020c.java bq/C11149a.java bq/C11150b.java bw/C11191k.java cC/l.java com/braze/configuration/BrazeConfig.java com/braze/enums/CardKey.java com/rollbar/api/payload/data/Person.java com/singular/sdk/internal/BaseApi.java com/singular/sdk/internal/BatchManagerPersistenceSqlite.java com/singular/sdk/internal/Constants.java com/wise/contacts/presentation/create/d.java com/wise/contacts/presentation/list/picker/g.java com/wise/contacts/presentation/list/picker/m.java com/wise/design/screens/a.java com/wise/payerflow/impl/presentation/paywithwise/j.java com/wise/paymentrequest/impl/presentation/acquiring/k.java com/wise/paymentrequest/impl/presentation/refunds/f.java com/wise/profile/link/impl/presentation/s.java com/wise/ui/app_security/fingerprint/i.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/wise/all/app_security/FingerPrint.java com/wise/verification/ui/C12549f.java dw/m.java eC/C12912b.java eC/C12918h.java eC/p.java eJ/M.java ei/C13080a.java gQ/C13515a.java hq/EnumC14136c.java hw/C14156e.java jN/C14947d.java jn/AbstractC15075b.java jq/m.java kU/C15422h0.java kl/C15510b.java kq/AbstractC15555a.java ll/v.java lR/C15816e.java oq/C16789a.java org/jsoup/nodes/DocumentType.java q4/g.java qm/C17375k.java qm/C17376l.java qm/C17377m.java qm/P.java qm/x.java qv/C17422a.java qv/C17427f.java rb/C17649c.java s3/c.java si/C17927b.java sv/C17987c.java sv/C17989e.java sv/C17990f.java sv/C17992h.java u3/n.java uj/C18588g.java vf/C18785a.java vf/C18787c.java vf/f.java wb/D.java wb/E.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				wb/F.java wb/H.java xG/EnumC19301g.java xf/C19368b.java xf/C19370d.java xf/t.java xq/AbstractC19412k.java xq/C19402a.java xq/C19403b.java xq/C19404c.java xq/C19405d.java xq/C19406e.java xq/C19407f.java xq/C19408g.java xq/C19409h.java xq/C19410i.java xq/C19411j.java xq/C19413l.java xq/o.java xq/q.java xq/r.java xq/t.java
2	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	AV/c.java LU/a.java MU/a.java NU/a.java OU/a.java PU/a.java QU/c.java RU/e.java ba/C11068a.java fV/C13277a.java jV/h.java
				CU/c.java I5/A.java I5/C7971c.java I5/C7972d.java I5/t.java I5/x.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	J5/G.java K9/c.java M5/C8605i.java N/a.java O1/d.java P5/a.java Q1/o.java SV/j.java T1/f.java V7/g.java aP/C10141j.java com/singular/sdk/Singular.java com/singular/sdk/SingularJSInterface.java com/singular/sdk/internal/BatchManager.java com/singular/sdk/internal/BatchManagerPersistenceSqlite.java com/singular/sdk/internal/DeviceInfo.java com/singular/sdk/internal/InstallReferrer/SLGoogleReferrer.java com/singular/sdk/internal/LicenseChecker.java com/singular/sdk/internal/ReferrerLinkService.java com/singular/sdk/internal/SingularInstance.java com/singular/sdk/internal/SingularLog.java com/singular/sdk/internal/SingularRequestHandler.java com/singular/sdk/internal/Utils.java p5/C16878a.java p7/i.java q1/P.java r7/C17481A.java w4/C18959l.java xq/C19409h.java y/U.java zz/k.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	Xa/e.java com/mixpanel/android/mpmetrics/m.java com/singular/sdk/internal/BatchManagerPersistenceSqlite.java com/singular/sdk/internal/OfflineEventsMigrator.java com/singular/sdk/internal/SQLitePersistentQueue.java t5/C18106M.java t5/U.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	A4/b.java O4/D.java bo/app/as.java bo/app/cx.java bo/app/d60.java bo/app/dq.java bo/app/i80.java bo/app/iu.java bo/app/kc0.java bo/app/lq.java bo/app/mq.java bo/app/mt.java bo/app/nf0.java bo/app/om.java bo/app/pc.java bo/app/q.java bo/app/se0.java bo/app/t50.java bo/app/tx.java bo/app/vd0.java bo/app/z30.java com/braze/configuration/RuntimeAppConfigurationProvider.java com/braze/managers/BrazeGeofenceManager.java n4/C16218b.java n4/C16226j.java n4/P.java n4/T.java n4/c0.java u4/j.java
6	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	J3/g.java M9/e.java com/braze/support/StringUtils.java o4/C16604d.java w4/C18959l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	BU/h.java BU/i.java BU/l.java BU/m.java com/facetec/sdk/ku.java com/twilio/conversations/ConversationsClientImpl.java com/twilio/twilsock/util/SslContextKt.java xA/g.java
8	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	Ia/C8004a.java M9/b.java N4/a.java Po/s.java T9/d.java Ua/C9491b.java V9/C9580p.java com/singular/sdk/internal/Utils.java t8/C18139b.java
9	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	A/C7018u.java com/canhub/cropper/CropImageActivity.java i4/C14214c.java j6/C14857M.java jr/C15110b.java lh/C15863a.java t8/C18140c.java
10	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	Fa/b.java Y7/C9827i.java com/adyen/threeds2/internal/security/checker/SecurityCheckerImpl.java p7/w.java r7/j.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
11	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	Tq/C9461c.java com/wise/forms/ui/httpredirect/h.java com/wise/ui/payin/card/threeds/widget/ThreeDSWebView.java com/wise/ui/payin/webview/WebViewActivity.java eD/C12925f.java
12	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	Ia/C8004a.java Wk/C9701A.java Wk/m.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	E4/N.java K8/d.java b6/h.java bo/app/r20.java com/adyen/threeds2/internal/dispatchDisplayHint.java com/adyen/threeds2/internal/jose/jwa/contentencryption/ContentEncryptionAlgorithm.java com/adyen/threeds2/internal/util/StringObfuscator.java com/braze/support/IntentUtils.java com/facetec/sdk/bm.java com/facetec/sdk/bp.java com/facetec/sdk/ca.java com/facetec/sdk/da.java j$/util/concurrent/ThreadLocalRandom.java n4/r.java nr/k.java oS/AbstractC16729a.java oS/C16730b.java org/jsoup/helper/DataUtil.java pS/C16989a.java
14	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	E4/N.java com/adyen/threeds2/internal/deviceinfo/parameter/environment/GetExternalStorageState.java com/github/mikephil/charting/charts/Chart.java com/github/mikephil/charting/utils/FileUtils.java i4/d.java il/C14541a.java nr/k.java ol/p.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
15	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/wise/ui/payin/webview/WebViewActivity.java
16	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/adyen/threeds2/internal/persistence/PreferencesManager.java
17	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	Fa/C7685a.java
18	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	dA/g.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/24	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.READ_CONTACTS, android.permission.VIBRATE, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.GET_ACCOUNTS, android.permission.WAKE_LOCK, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	5/45	com.google.android.c2dm.permission.RECEIVE, android.permission.AUTHENTICATE_ACCOUNTS, android.permission.FOREGROUND_SERVICE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Malware Permissions:
Top permissions that are widely abused by known malware.
Other Common Permissions:
Permissions that are commonly abused by known malware.

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION

DOMAIN	STATUS	GEOLOCATION
appleid.apple.com	ok	**IP:** 17.23.96.16 **Country:** United States of America **Region:** California **City:** Cupertino **Latitude:** 37.316605 **Longitude:** -122.046486 **View:** Google Map
transferwise.com	ok	**IP:** 104.18.214.66 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
picsum.photos	ok	**IP:** 104.26.4.30 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
exceptions.singular.net	ok	No Geolocation information available.
.facebook.com	ok	No Geolocation information available.
graph.s	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
sdk-api-v1.singular.net	ok	**IP:** 59.103.93.49 **Country:** Pakistan **Region:** Islamabad **City:** Islamabad **Latitude:** 33.721481 **Longitude:** 73.043289 **View:** Google Map
www.wise.com	ok	**IP:** 172.64.148.140 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
appassets.androidplatform.net	ok	No Geolocation information available.
issuetracker.google.com	ok	**IP:** 142.250.183.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.wise.com	ok	**IP:** 172.64.148.140 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.facebook.com	ok	**IP:** 157.240.227.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
accounts.google.com	ok	**IP:** 74.125.71.84 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebaseml.googleapis.com	ok	**IP:** 142.250.70.74 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
infra-mechanic-754.firebaseio.com	ok	**IP:** 34.120.206.254 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
dev.facetec.com	ok	**IP:** 13.35.169.92 **Country:** United Arab Emirates **Region:** Ash Shariqah **City:** Diba **Latitude:** 25.619551 **Longitude:** 56.272911 **View:** Google Map
developer.android.com	ok	**IP:** 142.250.181.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.mastercard.com	ok	**IP:** 23.217.57.44 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.714272 **Longitude:** -74.005966 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
wise.com	ok	**IP:** 172.64.148.140 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
staging-2.authy.com	ok	**IP:** 18.214.90.101 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
github.com	ok	**IP:** 20.207.73.82 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
xml.org	ok	**IP:** 104.239.240.11 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
facebook.com	ok	**IP:** 157.240.227.35 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
sdk.iad-01.braze.com	ok	**IP:** 172.64.148.188 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
api.facetec.com	ok	**IP:** 18.161.69.5 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.slf4j.org	ok	**IP:** 195.15.222.169 **Country:** Switzerland **Region:** Basel-Stadt **City:** Basel **Latitude:** 47.558399 **Longitude:** 7.573270 **View:** Google Map
twcard.wise.com	ok	**IP:** 172.64.148.140 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
www.braze.com	ok	**IP:** 104.17.228.60 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.mixpanel.com	ok	**IP:** 107.178.240.159 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 172.217.17.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.183.14 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 172.217.19.227 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
sondheim.braze.com	ok	**IP:** 104.18.43.4 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.mastercard.co.uk	ok	**IP:** 104.108.240.93 **Country:** India **Region:** Delhi **City:** New Delhi **Latitude:** 28.635759 **Longitude:** 77.224449 **View:** Google Map
api.rollbar.com	ok	**IP:** 35.201.81.77 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
url.ignored	ok	No Geolocation information available.
sdk-android.authy.com	ok	**IP:** 52.4.47.158 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
maps.google.com	ok	**IP:** 142.250.183.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
graph-video.s	ok	No Geolocation information available.
cards-api.wise.com	ok	**IP:** 104.18.39.116 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
azonnalifizetes.hu	ok	**IP:** 130.93.209.133 **Country:** Hungary **Region:** Budapest **City:** Budapest **Latitude:** 47.498009 **Longitude:** 19.039909 **View:** Google Map
iamcache.braze	ok	No Geolocation information available.
goo.gle	ok	**IP:** 67.199.248.12 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
loki-v42zc5nx3sj7swjbm6zacmssmtcs2gck.wise.com	ok	**IP:** 104.18.39.116 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 172.217.17.34 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
dust.k8s.test-001.d-usw-2.braze.com	ok	No Geolocation information available.
console.firebase.google.com	ok	**IP:** 142.250.181.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
developers.facebook.com	ok	**IP:** 157.240.227.1 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
aim.s.twilio.com	ok	**IP:** 35.168.222.240 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://infra-mechanic-754.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
john.smith@wise.com	uu/C18633a.java
feedback@transferwise.com	com/wise/ui/settings/g.java
u0013android@android.com u0013android@android.com0	J5/r.java

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118
Singular	Analytics	https://reports.exodus-privacy.eu.org/trackers/251

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "01a3798ea6f74b03ba7470ad65fb221d"
"com_braze_image_is_read_tag_key" : "com_appboy_image_is_read_tag_key"
"com_braze_image_lru_cache_image_url_key" : "com_braze_image_lru_cache_image_url_key"
"com_braze_image_resize_tag_key" : "com_appboy_image_resize_tag_key"
"facebook_client_token" : "24b2356737efa40b31b490f04ac9719e"
"firebase_database_url" : "https://infra-mechanic-754.firebaseio.com"

POSSIBLE SECRETS
"google_api_key" : "AIzaSyDcNYrqqD4y8MEYkM1wCTI-J8FOO2p5Daw"
"google_crash_reporting_api_key" : "AIzaSyDcNYrqqD4y8MEYkM1wCTI-J8FOO2p5Daw"
"google_nearby_key" : "AIzaSyA6i2EehCbllgBpTX16GuS9Oej6fJycBk8"
"rollbar_access_token" : "2a8f9c7bec1f4bc99adae6f2a16e4f4b"
S1FoU0tEWndWQ0lQVUFkN0tYUTJhMUZHUlJBQFRIMThTMTRSUFV4cE9YVWVCd2RER3pRME5tVQ
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112316
109384903807373427451111239076680556993620759895168374899458639449595311615073501601370873757375962324859213229670631330943845253159101291214232748847898598 4
bd9a6230-e0e9-4f74-919a-35a16aba679d
b869c82b35d70e1b1ff91b28e37a62ecdc34409b
RlNSSE1WQlJRVzlKY2tZeFNCb3NLRDVEQUFAT2tBbVJURi1MUUFxRXlvZU1IaEZSaEV3ZFE
6880e254-93ce-11ea-bb37-0242ac130002
32670510020758816978083085130507043184471273380659243275938904335757337482424
TVhzN0pqa29XVjh3T204aFNRWm5ZeDR4ZkR4YkFtbG9YUUZrRVJGdlZVOGhVUU1oRVFAWGdsY0NGOWFQRHBSVkF0VEptOERGM0ZlRUU5MWNBWUhLVjRlZVhRTVBpcFREbk5UZmc
1157920892103562487626974469494075735299969552241357603424222590610685120443 69

POSSIBLE SECRETS
42debb9da5b3d88cc956e08787ec3f3a09bba5f48b889a74aaf53174aa0fbe7e3c5b8fcd7a53bef563b0e98560328960a9517f4014d3325fc7962bf1e049370d76d1314a76137e792f3f0db859d095e4a5b932024f079ecf2ef09c797452b0770e1350782ed57ddf794979dcef23cb96f183061965c4ebc93c9c71c56b925955a75f94cccf1449ac43d586d0beee43251b0b2287349d68de0d144403f13e802f4146d882e057af19b6f6275c6676c8fa0e3ca2713a3257fd1b27d0639f695e347d8d1cf9ac819a26ca9b04cb0eb9b7b035988d15bbac65212a55239cfc7e58fae38d7250ab9991ffbc97134025fe8ce04c4399ad96569be91a546f4978693c7a
115792089210356248762697446949407573530086143415290314195533631308867097853951
1157920892373161954235709850086879078532699846656405640394575840079088346716 63
962eddcc369cba8ebb260ee6b6a126d9346e38c5
2c41ba9d-5cee-449e-9e42-7a8ec338a988
2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
R0JseFhCWW9XaDRKYUc5bU1WUUhCU0ZxYWtWeU53QGUzWWNjbnhIUDJkaUdnWUxIeVpvYWxVSkFpQVJYQQ
RXdOWklIRTZIR2s4ZmhnNVNWVndEUVlORVVnc1RSVWRIeGNfZkRnRmVlUUBkMlozVWg1WWFrZGRFSHhMSmp3VUkzNTlmanRKS1R0MGNXUkxIVlJwSFFZ
9a8d03a1-27f4-42ab-aab8-b1714aeb0882
f8956461-4b1c-49b0-805b-678a45e48e9a
SmtsYUFCWlRjem9VSFVzRlhSUVlLUjRZUG5JNkwzWVpma0ZZQWtkUFFoRlVAUlNZM0xtVW1BMTltYVNOcU1IVnJSWDk2RUFCVlFBSjhEVEk5YkRNbUkzMG4
9cdbd84c9f1ac2f38d0f80f42ab952e7338bf511
RTFGeVkzMWNjQU5EU2c0V1pRZERkQ0JHQmhwY0NRQGR6UmNFUkktQmkwaUpHcGtDbTRuV2xnMmFXazViUQ

POSSIBLE SECRETS
eb71b779-1756-49e8-ab9c-3dcca09b87b5
NN8Oep8c8YkuRcBWtJc82BzPFlpAUNEa6krFpl+QCkI
235dbd17-7bff-44de-a5ce-e59595d04799
9b8f518b086098de3d77736f9458a3d2f6f95a37
Wmw4SWNsVWhQMjVUZTN3bkxDTkpPQ014YlJsMU1tZEVMQUBTU3h4QVNGRVVrRXlDd3dJZjFZNVhWRkVIbndISEFZMFJ3
f8183668ba5fc5bb06b5981e6d8b795d30b8978d43ca0ec572e37e09939a9773
29436b69b37fed7c21f32fa4297f611c
e9e642599d355f37c97ffd3567120b8e25c9cd43e927b3a9670fbec5d890141922d2c3b3ad2480093799869d1e846aab49fab0ad26d2ce6a22219d470bce7d777d4a21fbe9c270b57f607002f3cef8393694cf45ee3688c11a8c56ab127a3daf
37a6259cc0c1dae299a7866489dff0bd
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
QXV0aGVudGljYXRpb24gLSBEZXZpY2UgSUQgQ2hhbmdlZA
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057148
fd7f53811d75122952df4a9c2eece4e7f611b7523cef4400c31e3f80b6512669455d402251fb593d8d58fabfc5f5ba30f6cb9b556cd7813b801d346ff26660b76b9950a5a49f9fe8047b1022c24fbba9d7feb7c61bf83b57e7c6a8a6150f04fb83f6d3c51ec3023554135a169132f675f3ae2b61d72aeff22203199dd14801c7
ZVR4Q1ZnTkFNUU5UWWpsQUZUUUBWazg3SlhjbFhDd3hDMWR2WmtF

POSSIBLE SECRETS
41058363725152142129326129780047268409114441015993725554835256314039467401291
832571096148902998554675128952010817928785304886131559470920590248050319988441922443864376039294733307808651162787 1
TzFwWUhHaHRmSGw1UkdCZEJRNDVARkNraGJ4d0lFVllCSmdrektuMU0
fca682ce8e12caba26efccf7110e526db078b05edecbcd1eb4a208f3ae1617ae01f35b91a47e6df63413c5e12ed0899bcd132acd50d99151bdc43ee737592e17
TEhwRU5qVUNhM3BoSmpOMkVFNEFSbHdJYmh0VUBlQkloRmxGbkhSTUNReE1mWTI1eUtUTjhDMzk2
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
bd0d5417-084a-429e-8aeb-3b41d7087811
484395612939064517590525852527979142027629495260417479958440807 17082404635286
eyJhbGciOiJFUzI1NiIsImtpZCI6ImRkNmZiODU5IiwidHlwIjoiSldUIn0
678471b27a9cf44ee91a49c5147db1a9aaf244f05a434d6486931d2d14271b9e35030b71fd73da179069b32e2935630e1c2062354d0da20a6c416e50be794ca4
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
T0daMmMybC1jQkJwTkhkUFBFRndEdzg2TGoxekd3TWdNWEFETnd4WkJFNXpEZ0BlVVlTRmdzTEYzY01SbGNtVDJFUmUzdGJUVlVXZnlOVVhsQjNYMmw1UlQ0RElB
WVRsYlFoTldGSGxPSm5nN0Z4TTdRQjVsU0JNTU1CZHFOWFpCTndzT1pSa21FSFJhQm5CeGVXRkJJQUBOVkUtWW5vNFlCd3BWQkZQYmpOVUpqNFJJSFlzWTFNaEZSNGdSQ3RzQUh4SU1BQTdhd0FVQ3dRbERn
YXhVMEZRRmpjeEpwU0h4eU1rdE9UeklNT2xvZFNuQmJWejhhY0J0Z1R5UndCRDRlR0QxblhCY0BLbnNVY0d3V0gzTWRKdzVTV3podUxWZGxWRDA5UHdNLU14OXVIenNTT2twUWNGWjdPSHdYTERr
b0b4417601b59cbc9d8ac8f935cadaec4f5fbb2f23785609ae466748d9b5a536

POSSIBLE SECRETS
470fa2b4ae81cd56ecbcda9735803434cec591fa
YVRzR1N6Sk1NM0VPQVZaUkZEb1hTQzl6TUJrQENsUnJaVUFqWEFWdmJ6SWplMU56WmwwY1gyMA
85c13fc9-c119-4729-8126-6005d67235c9
c56fb7d591ba6704df047fd98f535372fea00211
30470ad5a005fb14ce2d9dcd87e38bc7d1b1c5facbaecbe95f190aa7a31d23c4dbbcbe06174544401a5b2c020965d8c2bd2171d3668445771f74ba084d2029d83c1c158547f3a9f1a2715be23d51ae4d3e5a1f6a7064f316933a346d3f529252
cc2751449a350f668590264ed76692694a80308a
e2719d58-a985-b3c9-781a-b030af78d30e
f9c81685-ae63-47cc-a4fb-08469d7ea860
f7e1a085d69b3ddecbbcab5c36b857b97994afbbfa3aea82f9574c0b3d0782675159578ebad4594fe67107108180b449167123e84c281613b7cf09328cc8a6e13c167a8b547c8d28e0a3ae1e2bb3a675916ea37f0bfa213562f1fb627a01243bcca4f1bea8519089a883dfe15ae59f06928b665e807b552564014c3bfecf492a
47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=

POSSIBLE SECRETS

VnlkU0FYQW9JUTFTQUNRYmJuRVlZVzBjWjM1NlF3d3BIM01GSW10S1JVNTBlRjhfWlhSUmZnd3hXaW9NY1I4bGNpOHJOVTFqYjBwa0ZoTjVMSGtwYmxZQUFVRTdSQU5TSUFZ
ZFB4UXFBMEpxT2pjLUNCSmlMVDhCUERWOWZDRkdQdzlmWXdCbGVBNFViUlIzV21aUU55UVJIaEkzTWlkOEx4SWtGWDR3YTBZa1BpRTZhQVV5SUVKNFkxeHNheEJtVkVZdW
FTcEFLWElwQ0JNQmZEWTRkd0ZrY21sSEZXTWhTMUlOSlZaUlJHdG5YeUZ0UEFGeERqNFJEU29xV0hZQ1B6Y1RlaGh2Q3pjSEYyb0tkeElNWlZJTEkxc1JLaXN3QWtFcWFXVkNabE
lvSVFNaUNDOHFVbHhVWEdSdWNSRkhUakk5TUEwb0VEUkZFMFpLQlYwZE1UeGVBaUJXYmhwR0l3UmVHM2tqVEFFSE5XWTFMV1prZVZRTlhVd2FYd1Y2TFFCSUd4Vk1Pd2cy
WkNzWkNRQjhlUTEzSVRNWGZuQThBVDFrWkhKTFRVb1BhRkIwUG0wZkxna01DMHcxWjNFNGRsVVVEakFuYnlRMUpnZ2taaVo2RGlScFV4aGZGSGhDQlJnUWUxTUZCVnNhW
mlRTGRUUlFVVzlVVVNOOFhGSWRkU1FlYkQ1b2NtRVZlMTFNY3o1LVZFMWJWRElMUWtaRVFERVRGd3RIVXhzaEZGQXlLanR4YWpVdkwza2RTbWR1S0NNVFVGWVphMEl6T2tK
Sk55UUJQbXBuTEJKQmNIa2NSQmtqRkZaaEdoOWNSVlZnRWtNU0xGQUNLQnRDWG5GQk5SOUxhRU14ZFhGMUdsaGtEMEJzTHk1SEVpd29EQlUzYVdabUExSWJOVDVYYYVY
wTkxGb2hHekFHQ3hRUlhXZFVKaXNER0VzRUVINThJaWNaSXlRUGFBVmxRUzl0VXljRVR6OWhkQklhTlR0Z0dFUmhjQjUzQUhWSlQwQmRMam8xVkVobkoySVNSUVpIZkY5TVl
SNHNFRnNyS2d3dVdnaDVOeEEtVEZ4ekd3SUxUVEU3R3dNREFCWS1KeFpZTHpKME0zUmxPbDFqQUFaYlBnTU9ZMU1JWTFGLUN5SjZNQlktZGxrblBBc2tMRG81Q2pKN2RuZ
GZRZ2RkS3lSbkIxOWZBVWdoTVZRV1MxWVJHaFFMSFVCQkRGdzVUQlFpTVFFYUloWllGQnRmWm0xVUZoMGpIMlJ4S1dsMWF3STFQZ3hoTlM5S0ttVVdQeDh3ZVJvWFVsVVJjV
FI5S1E4QlJYUkNVQmNOTEJrcWNRZ3ZJd1FKWDNaSlZ3QXRhVnhqWm1vOVh5QlJNek03SjNkdE1CUTNHSFk0WUM5QVV4NFRmbFUxVHlBMlVRMERJMHM4ZTNrWklGMUtMa
0pxUWlKN01FSmtPZ0pPV2hjMFZSWjZUUVplVlVsdlZrTlliaWtSVXlRQkVWQTJiUmdVSzBvRVJ5RVlMenQ1TndWUEZRQUNMUXhkZGhFLWR3dDFMVVIzSGtWeWRRRlNQMUJzQl
cxdGJtZGlEeGd1TDNaRE4yeHVZV1I5WFQ0akVSOUpPV29PUnlOSlQxQjNhVlVxVENCcURWNFVUak1BWHlCNE5Fa0FSVnN5SHg1YlhHeGRHenBFRVRGRmJSMXJBWHdZUWdG
REFEaE5SeGgxY2pjTFJsRlpYVWNJVkE4WUgxNXRYaTVKQ1RBRVEyczZQaDVkQUR3ZGRWSnFBRVVoSlN0NE9FUklNVFpqZHdjY056aHBGa0k5ZlFCWlpGdEVCUjRaQ1hjQVhuc09
ER3dwSFU5VVdnVmxkMHhYTzNOY2V4c3pOVmRoTUQ1akUzTkxmZ1Z1SUJGa2ZGOTZiMVVwSndCVEtYQTFLbTFsRHdaVUJ4eGxJVXh1RXlNQ1doRWxQZ0BHbTRiUlQxQ1lrNF
RjR3Q4THdaUkl5eDdMaXM0QlZaRmZFdHdaaTBvYWkwN0xoTU5IeU0zTzNsNGJteGJGSHhTTVVoeWZBWU1OUU1lZkNNOGJRNWdHVEZaVkRsNFBrSVlZbUZUYVZacldoWXJVU
Up6UlVNUldueFFaWEVyTFhBUGUwNFZMRk1oUFYxWkwxVXdHMWNGY21abWFWaG1aUllHUzFWeWJDUjNMVEpwYkd4TkxWUnJaQlFwTWhjb0ttQWtEZzVDQlVncGF6MWxa
RXAwTVdSTEFFWTFLeTBSUkRKdER4Qkhad3daS0FjRk5tTThYa1kzUG1SOE5GTklDelJUYkFkNEFsRVZTbDlGY0NSY05WTkJLQlZnWlRCMGZYMUZTd2RvR2p3YU5EOUtFa2xXUVd
wOEZnMHRIamNNUXloM0IzZHpja0JyVVd3QlJ3OHpTQmxNUm5JMFF4UWJPa014YlRVeFFqMVpCWFpKWVM5Q1lCd3RUQmxKT2pSVU5VUkplbW9MV1gwWWZrUjdKVUJIU0R
FcFBFOGZiSEJERlFkRVFrY2xMakFzQXh4TktUYzVmd1lxWjBSZVFqdHdKaWg4SUFSRlJuUm1BMlpYZmtZVVBINHdaWDAtWTJBYWJqa1FSMzllTFJGRWFoWlpEV0pnRUdNR0pDW
VJaVllxTldabE1sNWZObndQUERkWE9pNEJObFU0UHlnTUFrZENQVEzR1dsQmVtbDBHVzlvVWhKLWVXODBBSGhzYWo1Y2V6SXJhVlJrTVFkT09YZHBiWFl1WW1ONVZnNGdkb
VFpSFVsN0ZreHRVQjhuVUdrLWRnUUhRM05YV3pkWVcyd0hIeWdKZm5BUklUbGJSVEkwU3dFaVJIUXBhbThFWDJoUFZVeDJLeWNqUUJ3cEFWSXhNUlJsVGdOTVlsaC1hbHRtR3
dGbVhud3hRQnBSYWhZdWNoVjZaM001V1RVZ2Jrd25PMTFlSzBVd0VIZFhCbUVoWEJBYkUxVWtjRDFtTEE4TWRBbHdiUWxTZmdwMU5VRXhMRGNyT1hWSVVtMTZiMWthRW
0wUlVHSnFkVGtqYnpWb2ZsNW9iMmhpYUVKRWZTOFBZVkVsQWt3M2NUVlJhSFpwZVhKZVZTVk9DamhIYUV3T1lWNUdBQ3gyVG1COVhWRkJPRjVMT2pFdUpIQTRBSEltY1JvV
WJDdE1DQVpWQUdaUWUxdEpjQlFDVGpCVERYQmdWazlNYWtkc1VWMDROemdZUlV4UGFGSVFSUUVYUG5oU2IyY29CMGtwVHlweFNFdFpDRTlnR2lKSU5XSXZHV1ZEQnhN
MUZuaE1lVlY1SUdSWUZXVmxOeFFjTFdkOEFoVlJBQWxZRUVjbVoxcEtjZ0FwUjAxelRpUUlORzRSR3pGUlB3QkNEbGR6RXlKNVlnUi1IRGRQYUF4eWJBTU1lbWM1Y1E4bmUxc1h
MVnBEREZJc0h6WTRGd29ZSVFneUwwWi1FRVZtV3hsdkJIbGNlWHBuRDJ3dVkwSkFYMThlZVd4Z1JEazNGQ01PQVZKR1p6YzdMUThFRnpJRFNnbGZUeDRoQUNVT2JVeHZaRFF
rVUIwR0NnNHlEVzl5VlY0dWRpaGtCbUktS0FrUUtnUk5DVUpCT1IxdUtIWkRHMGs5QWlaR0NXTjFTMXBwRWowMVRYVVVZUU1jSFNvaWVEUk1jMjRnWkFFbUNGZE1RRjFjTUN
rZUVqWnBCCamRLZEc4b0hXWi1PWEV5SkNZVlVDNG5iSGN1TzJBdWVRNVJiMkVYV1hNSFZud2dOazR6Y0dBdmNoZE9PVU55RDJrQk1YMXdSejl0YXlsX09RUjdjd2NTRjJ3SlRoZ1J
WMFU1UTM4RVpnMG9XMHM1YVFZRlJtTUNTVDR3S3dnd0RneFBFVThyV2dwZmZ3OG9lVGNYZlZkU1FBNGpkbUpuS0V0MlJB

MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEIM5h9ht+dpwGqsXLVxaO2QhIRRnz6P9G8lS+sIv6n5smMb6ncs6tBsNSTsMyi3rltn2boIBUhjbXTyBk/Sg54Q==

275801935599597058778490118403890480930569058563615685214287073019886892413098608651362607648837451077654397612305755

394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426433

POSSIBLE SECRETS
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed
262470350957996892686231567445669818918529234911092133878156159009255188547380500890223880539757197866508724767320 87
44a72141-b436-44f4-b49d-4541445833ce
Y1JnV1IxVnlhZ1k5Wm0wTU9tOGJTeVZzQFhtdHZOQ0VYQnlsT0FrSjBXQVoxWkZZWg
9760508f15230bccb292b982a2eb840bf0581cf5
ZG16OnE2QWo1YTQ3Z01aOHlhZ2tSeDg4Zzd0U3F2N3ZobnNiRm5zQXFQOTZ0WjZSNE5reHFhUVpzNUtueFJoa3hlY3M=
VFM0cERYUUpFM0paTkQ1TFdESW9PRDRzQnhsQk1GRUBZbDFRZmdCc2ZsMDdYVkJrUGxOQlZFMU5ZWHh1UXlR
UzF4YlFTUXFWaFVFSVVWbVZBRjFHMVlzQUFAS0RNMmIwVkVNbWRyU0NGSUltUWJmejlDWnc
95475cf5d93e596c3fcd1d902add02f427f5f3c7210313bb45fb4d5bb2e5fe1cbd678cd4bbdd84c9836be1f31c0777725aeb6c2fc38b85f48076fa76bcd8146cc89a6fb2f706dd719898c2083dc8d896f84062e2c9c94d137b054a8d8096adb8d51952398eeca852a0af12df83e475aa65d4ec0c38a9560d5661186ff98b9fc9eb60eee8b030376b236bc73be3acdbd74fd61c1d2475fa3077b8f080467881ff7e1ca56fee066d79506ade51edbb5443a563927dbc4ba520086746175c8885925ebc64c6147906773496990cb714ec667304e261faaee33b3cbdf008e0c3fa90650d97d3909c9275bf4ac86ffcb3d03e6dfc8ada5934242dd6d3bcca2a406cb0b
eyJjZXJ0aWZpY2F0ZVBpbm5pbmciOnsiZGlnZXN0QWxnb3JpdGhtIjoic2hhMjU2IiwicGlucyI6W3siZG9tYWlucyI6WyJ3aXNlLmNvbSIsInRyYW5zZmVyd2lzZS5jb20iLCJ3aXNlLmNuIl0sImRpZ2VzdHMiOlsiNThxUnUvdXhoNGdGZXpxQWNFUnVwU2tSWUJsQkF2ZmN3N21FakdQTG5OVT0iLCJnclg0VGE5SHBaeDZ0U0hrbUNydnBBcFRRR282N0NZRG52cHJMZzV5Uk1FPSIsIisrTUJnREg1V0d2TDlCY241QmUzMGNSY0wwZjVPK055b1h1V3RRZFgxYUk9IiwiZjBLVy9GdHFUanMxMDhOcFlqNDJTckd2T0IyUHB4SVZNOG5XeGpQcUpHRT0iLCJOcXZESmxhcy9HUmNZYmNXRThTL0ljZUg5Y3E3N2tnMGpWaFplQVBYcThrPSIsIjkremUxY1pnUjlLTzFrWnJWRHhBNEhRNnZvSFJDU1ZOejRSZFRDeDRVOFU9Iiwici9tSWtHM2VFcFZkbSt1L2tvL2N3eHpPTW8xYms0VHlISWxCeWliaUE1RT0iLCJpN1dUcVR2aDBPaW9JcnVJZkZSNGtNUG5CcXJTMnJkaVZQbC9zMnVDL0NZPSIsInVVd1pnd0RPeGNCWHJRY250d3Ura1lGcGtpVmtPYWV6TDBXWUVaM2FuSmM9Iiwib0Mrdm9aTEl5NEhMRTBGVlQ1d0Z0eHpLS29rTERSS1kxb05rZkpZZSs5OD0iLCJhcGUxSElJWjZUNWQ3R1M2MVlCczNyRDROVnZrZm5Wd0VMY0NSVzRCcXYwPSIsImh4cVJsUFR1MWJNUy8wRElUQjFTU3UwdmQ0dS84bDhUalBnZmFBcDYzR2M9IiwiVmZkOTVCd0RlU1FvK05VWXhWRUVJbHZrT2xXWTJTYWxLSzFsUGh6T3g3OD0iLCJRWG50MllIdmRIUjN0SlltUUlyMFBhb3NwNnQvbmdnc0VHRDRRSlozUTBnPSIsIm1FZmxaVDVlbm9SMUZ1WExnWVlHcW5WRW9adm1mOWMyYlZCcGlPallRMGM9IiwiQzUrbHBaN3RjVndtd1FJTWNSdFBic1F0V0xBQlhoUXplam5hMHdIRnI4TT0iLCJkaUdWd2lWWWJ1YkFJM1JXNGhCOXhVOGUvQ0gyR25rdXZWRlpFOHptZ3pJPSIsIkt3Y2NXYUNncm5hdzZ0c3JyU082MUZnTGFjTmdHMk1NTHE4R0U2K29QNUk9IiwiSUNHUmZwZ21PVVhJV2NRL0hYUExRVGtGUEVGUG9EeWp2SDdvaGhRcGp6cz0iLCJ4NFF6UFNDODEwSzUvY01qYjA1UW00azNCdzV6Qm40bFRkTy9uRVcvVGQ0PSIsIkNMT21NMS9PWHZTUGp3NVVPWWJBZjlHS094SW1FcDloaGt1OVc5MGZlTWs9Il19XX0sImlhdCI6MTcyMjQxMzcyMH0

POSSIBLE SECRETS
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784
1157920892373161954235709850086879078528375642790749043826051631415181614943337
8138e8a0fcf3a4e84a771d40fd305d7f4aa59306d7251de54d98af8fe95729a1f73d893fa424cd2edc8636a6c3285e022b0e3866a565ae8108eed8591cd4fe8d2ce86165a978d719ebf647f362d33fca29cd179fb42401cbaf3df0c614056f9c8f3cfd51e474afb6bc6974f78db8aba8e9e517fded658591ab7502bd41849462f
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
77d0f8c4dad15eb8c4f2f8d6726cefd96d5bb399
8d5155894229d5e689ee01e6018a237e2cae64cd
UEVFU0gwNHBaMElrZHgwTERUaHZHVGhSQEV5VnpheThHQ3kxSEZuRWtiMUVCTmtzaw
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
1157920892103562487626974469494075735300861434152903141955336313088670978539 48
V3pkVEdHZ3hWSGN5VzFKaE1saEZQRzBzQ0RJQE9GZy1OaHRRSVFWYk1Id1NSem8yU0I5TmZGYw
ZlROT0tUOGFRbkV2QlFAVWtBN0JsMXpMRjVjY0E
85053bf24bba75239b16a601d9387e17
3613425095674979579858512791958788195661110667298501507187719825356841440510 9

POSSIBLE SECRETS
z7Nr1Qumfwj5NNIvfD0EcvSjXXkAvJ4nOn8Io8NfD5sJuAGeywr8cZnhKPUgX4UpJjIbqtBSwmw
VnpSaVBRd2hUQlpZSFVzQ0ZnVUJjRHRMTHlFUUNGdDhGUzR0VmtOUkFFTVJAT0VZRkUycFRLWE01Y3k5d2VXeGxCRlFrUTFJLWVqUVRZWEZPUGlZeWF5Wmo
T1ZKbFZDNTVDaUZRWkZVSkR5c0BGallFSUU5V1prNHpCVGttZkY0
cd0681bd-4522-4177-a3c7-1fa93e14734b
1372151224454a224018231c1e70414d78404a751c1978401a70451e71471376
de317432-fcee-4e07-b170-0ece6e78f13b
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19
55066263022277343669578718895168534326250603453777594175500187360389116729240
VGtJaUZnWUVFRFJyWnlWRWFGaGtDaUo5TEVvUkNVUmFJMFI2UjFvRUtRSXdhMjlkUWlacWFRMU5AR2lwSE5rbFhNRnNaUjFFc0RYZ3JXUUlMU1RoaVlDczBBeTBKWnpSclhTSkRIaDh0TFZRZURHbGo
29701fe4-3cc7-4a34-8c5b-ae90c7439a47
e605c449bdf99389fa3ba674d4f5d919
a86cda04-6a9a-4174-bf34-7d3838f02de2
1077efec-c0b2-4d02-ace3-3c1e52e2fb4b

PLAYSTORE INFORMATION

Title: Wise

Score: 4.648324 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** com.transferwise.android

Developer Details: Wise Payments Ltd., Wise+Payments+Ltd., 56 SHOREDITCH HIGH STREET, TEA BUILDING, LONDON E1 6JJ, https://wise.com, support@wise.com,

Release Date: Mar 24, 2014 **Privacy Policy:** Privacy link

Description:

Going somewhere? The Wise account is built to save you money round the world. 170 countries. 50+ currencies. One account. All in one place. So you can send, spend, and receive money simply, with high speeds and low fees. Join 16+ million people moving and saving money internationally. Take on the world with Wise - You'll always get the mid-market exchange rate on every transaction - Our tiny fees are always shown upfront Send and save money worldwide - Send money to 70+ countries - Do it fast: over half of international transfers arrive instantly Get a debit card that's always got the right currency - Spend and withdraw money in 170+ countries - Always pay in the local currency. Our automatic currency conversion gets you the lowest possible price - Shop online safely with a disposable digital card Hold and convert 50+ currencies - Keep all your currencies in one place — for free - Convert between your different currencies instantly Get paid like a local - Get your own account details for the UK, US, EU and more - Use them to get paid or have direct debits in multiple currencies, without the extra fees A business account for going global - Pay invoices and bills faster, at a fairer exchange rate - Use account details to get paid by clients and customers around the world - Quickly connect to supported platforms like Amazon, Stripe, Xero, and more Wise is regulated by the FCA in the UK, and other authorities globally. Check out wise.com for our full coverage and product availability.

SCAN LOGS

Timestamp	Event	Error
2024-10-19 17:16:36	Generating Hashes	OK
2024-10-19 17:16:37	Extracting APK	OK
2024-10-19 17:16:37	Unzipping	OK
2024-10-19 17:16:38	Getting Hardcoded Certificates/Keystores	OK

2024-10-19 17:16:43	Parsing AndroidManifest.xml	OK
2024-10-19 17:16:43	Parsing APK with androguard	OK
2024-10-19 17:16:45	Extracting Manifest Data	OK
2024-10-19 17:16:45	Performing Static Analysis on: Wise (com.transferwise.android)	OK
2024-10-19 17:16:45	Fetching Details from Play Store: com.transferwise.android	OK
2024-10-19 17:16:49	Manifest Analysis Started	OK
2024-10-19 17:16:52	Checking for Malware Permissions	OK
2024-10-19 17:16:52	Fetching icon path	OK
2024-10-19 17:16:52	Library Binary Analysis Started	OK
2024-10-19 17:16:52	Reading Code Signing Certificate	OK
2024-10-19 17:16:54	Running APKiD 2.1.5	OK

2024-10-19 17:17:27	Detecting Trackers	OK
2024-10-19 17:17:34	Decompiling APK to Java with jadx	OK
2024-10-19 17:19:56	Converting DEX to Smali	OK
2024-10-19 17:19:56	Code Analysis Started on - java_source	OK
2024-10-19 17:27:30	Android SAST Completed	OK
2024-10-19 17:27:31	Android API Analysis Started	OK
2024-10-19 17:34:21	Android Permission Mapping Started	OK
2024-10-19 17:36:38	Android Permission Mapping Completed	OK
2024-10-19 17:36:57	Finished Code Analysis, Email and URL Extraction	OK
2024-10-19 17:36:57	Extracting String data from APK	OK
2024-10-19 17:36:57	Extracting String data from Code	OK

2024-10-19 17:36:57	Extracting String values and entropies from Code	OK
2024-10-19 17:37:10	Performing Malware check on extracted domains	OK
2024-10-19 17:37:25	Saving to Database	OK

Report Generated by - MobSF v4.0.7

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.