Požadavky na sí?ovou konektivitu pro IT odd?lení zákazník?

- **Cílová skupina:** IT administrátoři a bezpečnostní specialisté zákazníka, kteří provozují KASA FIK Pokladna
- **Účel:** Definovat všechna odchozí spojení, která aplikace EtKasa pro Android vyžaduje, aby bylo možné předem připravit pravidla na firewallu / proxy / DNS, a nasazení proběhlo bez komplikací.
- **Aplikace:** KASA FIK Pokladna (`com.eetterminal.pos` a varianty pro jednotlivé zákazníky)
- **Minimální Android:** 6.0 (API 23) · **Cílový:** Android 14+ (API 34+)

---

1. Jak synchronizace funguje (stru?ný popis)

Aplikace nepoužívá jediné synchronizační spojení – pracuje paralelně se **šesti nezávislými odchozími kanály**, z nichž každý má svůj účel, periodicitu a úroveň zabezpečení. Veškerý odchozí provoz se vždy iniciuje **ze zařízení směrem do cloudu**. Zařízení **neotevírá žádné vstupní porty** a nepřijímá spojení z internetu.

#	Kanál	Účel	Směr	Kadence
1	**REST/HTTPS** (AWS API Gateway)	Oboustranná synchronizace master dat (produkty, kategorie, objednávky, zákazníci, směny, sklad, telemetrie)	Zařízení → AWS	Na vyžádání + plánovaně (každých pár minut)
2	**WebSocket / WSS**	Okamžité vzdálené příkazy z cloudu KASA FIK (změna nastavení, zaslání souboru, spuštění synchronizace, povolení vzdálené obrazovky)	Zařízení ← cloud KASA FIK	Trvalé dlouhodobé spojení
3	**MQTT**	Zasílání změn preferencí a událostí z pokladny směrem do backendu	Zařízení ↔ broker KASA FIK	Trvalé dlouhodobé spojení
4	**Firebase (FCM + Analytics + Crashlytics + Remote Config)**	Push notifikace, hlášení pádů, telemetrie, runtime konfigurace (včetně adresy OpenObserve)	Zařízení ↔ Google	Událostně

#	Kanál	Účel	Směr	Kadence
5	**SOAP/HTTPS** na vládní endpointy	EET (doklady)	Zařízení → státní správa ČR	Při každém dokladu
6	**Lokální síť (LAN)**	Hardware: fiskální tiskárny, platební terminály, pokladní zásuvky, zákaznické displeje, síťové tiskárny	Zařízení → 127.0.0.1 / LAN	Při každé transakci

Topologické pravidlo: Aplikace nikdy neotevře vstupní TCP port směrem z internetu. Každý kanál je iniciován klientem, odchozí a autentizovaný. Provoz v lokální síti je povolen záměrně – Android manifest povoluje nešifrovaný provoz (`usesCleartextTraffic="true"`), protože fiskální tiskárny a platební terminály typicky komunikují přes lokální proxy na `192.168.x.x` apod.

---

2. Požadavky na HTTPS / TLS

Aplikace explicitně **povoluje nešifrovaný (HTTP) provoz** – to **není chyba konfigurace**, ale nutnost pro lokální fiskální tiskárny a platební terminály. Viz:

- `AndroidManifest.xml`: `android:usesCleartextTraffic="true"`
- `res/xml/network_security_config.xml`: `<base-config cleartextTrafficPermitted="true">`

Používané verze TLS

Síťový stack (OkHttp + Conscrypt) vyjednává v tomto pořadí:

- **Android 10 a novější (API 29+):** výchozí TLS 1.3, fallback na TLS 1.2.
- **Android 6.0 – 9 (API 23–28):** TLS 1.3 injektované přes Conscrypt; `ConnectionSpec.RESTRICTED_TLS`.
- **Endpoint EET:** je vynucen **TLS 1.0 / TLS 1.1** (brána Ministerstva financí ČR pro EET nevyjednává TLS 1.2). Na cestě k `*.trzbyeet.gov.cz**proto neblokujte TLS 1.1**.

D?sledky pro firewall

Povolte samotné TLS spojení. Aplikace používá **systémové i uživatelské kořenové certifikáty** (`<certificates src="system" />`); Pokud provozujete TLS-inspection proxy (MITM), nainstalujte její CA certifikát do zařízení a aplikace bude přijímat i takto inspektovaná spojení.

---

3. API a služby – hlavní referen?ní tabulka

Skupiny podle oblasti důvěry. **Veškerý produkční provoz je HTTPS / TLS, pokud není výslovně uvedeno jinak.**

3.1 KASA FIK Cloud (primární backend)

Hostname	Port	Protokol	TLS	Směr	Účel
`m6vadtaz1h.execute-api.eu-west-1.amazonaws.com`	443	HTTPS	TLS 1.2 / 1.3	Odchozí	**Hlavní REST API** – produkty, kategorie, objednávky, zákazníci, směny, sklad, správa uživatelů/zařízení, telemetrie (cesta `/prod/` pro produkci, `/staging/` pro debug buildy)

> **AWS region:** `eu-west-1` (Irsko). IP rozsahy patří AWS – povolte AWS prefix listy `AMAZON` a `AMAZON-IRELAND`, případně konkrétní IP API Gateway po prvním překladu. ID API `m6vadtaz1h` se resolvuje na několik IP API Gateway.

3.2 KASA FIK Cloud – pomocná infrastruktura

Hostname	Port	Protokol	TLS	Směr	Účel
`ws.kasafik.cz`	443	WSS	TLS 1.2 / 1.3	Odchozí	**WebSocket** pro vzdálené příkazy v reálném čase (změna nastavení, push souborů, spouštění sync, povolení vzdálené obrazovky)
`mqtt.vps.kasafik.cz`	**1883**	**MQTT (čistý TCP)**	**Nešifrované**	Odchozí	Synchronizace preferencí, události zařízení, last-will přítomnost
`externi sluzby`	443	HTTPS	TLS	Odchozí	Externí REST pro white-label (Slevomat / FlexiBee / Abra proxy – jen základní URL, cesty přidává klient)

3.3 Vládní endpointy – ?eské EET (elektronická evidence tržeb)

Hostname	Port	Protokol	TLS	Směr	Účel
`trzbyeet.gov.cz`	443	HTTPS (SOAP/XML)	TLS 1.2	Odchozí	EET produkce – nový klient `eet20` (Finanční správa)
`pg.trzbyeet.gov.cz`	443	HTTPS (SOAP/XML)	TLS 1.2	Odchozí	EET playground – nový klient `eet20`

3.4 Zpracovatelé plateb

Hostname	Port	Protokol	TLS	Směr	Účel
`api.sumup.com`	443	HTTPS	TLS	Odchozí	SumUp OAuth (`/authorize`), settlement transakcí (pouze pokud je SumUp integrace povolena)
`*.vivapayments.com` (např. `*.apps.vivapayments.com`)	443	HTTPS	TLS	Odchozí	Platební terminál Viva Wallet – peer-to-peer HTTPS volání na IP terminálu, plus token endpoint
Vlastní URI schéma `vivapayclient://`	–	Intent (Android)	–	–	Předá řízení aplikaci Viva pro terminálové UI (Android Intent, ne síťové volání)

> **SumUp SDK** má vlastní interní endpointy (spravované SumUp, vše HTTPS/443, hostované na AWS). Pro přesný seznam endpointů SumUp SDK kontaktujte podporu SumUp. Pro běžný provoz stačí povolit obecný odchozí HTTPS do AWS.

3.5 Firebase / služby Google

Volitelné, nejsou nutné k provozu

Hostname	Port	Protokol	TLS	Směr	Účel

`fcm.googleapis.com`	443	HTTPS	TLS	Odchozí	Firebase Cloud Messaging – push zprávy
`firebaseremoteconfig.googleapis.com`	443	HTTPS	TLS	Odchozí	Remote Config – runtime příznaky včetně adresy a tokenu OpenObserve
`firebaselogging-pa.googleapis.com`	443	HTTPS	TLS	Odchozí	Firebase Analytics + Performance
`firebasestorage.googleapis.com`	443	HTTPS	TLS	Odchozí	Firebase Storage
`tactical-codex-116610.firebaseio.com`	443	HTTPS (WebSocket)	TLS	Odchozí	Firebase Realtime Database – legacy presence/sync (zastaralé, ale stále v kódu)
`generativelanguage.googleapis.com`	443	HTTPS	TLS	Odchozí	Google Gemini AI – AI asistent (opt-in)

3.6 OpenObserve (log shipping) – konfigurace za b?hu

Hostname	Port	Protokol	TLS	Směr	Účel
`openobserve.vps.kasafik.cz`	443	HTTPS (NDJSON / JSON)	TLS	Odchozí	Logování aplikace do zákaznického OpenObserve stacku.

3.7 White-label specifické externí integrace

Následující URL jsou konfigurovatelné v aplikaci a operátor je může měnit. V závorce jsou uvedeny výchozí hodnoty.

Hostname	Výchozí port	Protokol	TLS	Výchozí hodnota	Účel
`dochazka.efg.cz`	443	HTTPS	TLS	`https://dochazka.efg.cz/AktionNEXT.KASAFIK`	Integrace docházky (Aktion NEXT)
`ec.qrticket.cz`	443	HTTPS	TLS	`https://ec.qrticket.cz/`	Integrace QR ticketů

4. WebSocket endpointy – souhrn

Tři trvalá spojení WebSocket / STOMP:

Endpoint	TLS	Účel	Směr	Poznámky
`wss://ws.kasafik.cz/v1/websocket`	TLS	Vzdálené příkazy v reálném čase: změna preferencí, zasílání souborů, spuštění sync, povolení screen-share	Zařízení ← cloud KASA FIK	Heartbeat 20 s; reconnect s exponenciálním backoffem. Ověření hostname je v kódu pro tento host bypassnuto (legacy kompatibilita).
`wss://emsystem-dev.pc3000.sk/api/ws`	TLS	STOMP přes WebSocket (třetí strana)	Zařízení ↔ emSystem pro platbení terminály KASA PAY	Heartbeat 20 s / 20 s

Všechna spojení jsou **pouze odchozí** TCP/443 s TLS. Žádný vstupní listener se neotevírá.

---

5. EET a vládní endpointy (podrobn?)

Pro rychlé nasazení je zde konsolidovaný seznam povolených spojení pro **Ministerstvo financí ČR** a **SÚKL**:

```
# EET 2.0
trzbyeet.gov.cz:443     tcp  # HTTPS SOAP/XML  (nový eet20 produkce)
pg.trzbyeet.gov.cz:443  tcp  # HTTPS SOAP/XML  (nový eet20 test)
```

Odchozí provoz se iniciuje při každém daňovém dokladu. Typická velikost payloadu: 1–10 KB. Typická frekvence: 1 volání na účtenku (ihned, synchronně). Tyto endpointy nevidí žádný jiný provoz.

6. Autentizace a autorizace

Endpoint	Autentizace
REST API (AWS)	Bearer token (`Authorization: <token>`) + vlastní hlavičky `X-AppId`, `X-Date`, `X-IDC` (vydány při aktivaci)
WebSocket (kasafik)	Hlavička `Authorization: <token>` při WebSocket upgrade
MQTT (kasafik)	Uživatel `dev_<idZařízení>` / heslo `<idZákazníka>` (číselné)
EET / SÚKL	Vzájemný TLS (klientský PFX certifikát) + podepsaný XML payload (PKP/BKP dle specifikace EET)

Endpoint	Autentizace
S3 / SQS	AWS SigV4 (řeší AWS SDK, v aplikaci nejsou statické klíče)
Firebase	FCM token + Firebase App Check
SumUp	OAuth 2.0 bearer token, per-device
OpenObserve	Bearer token z Firebase Remote Config

---

7. Šablony pravidel pro firewall (kopírovatelné)

7.1 Minimální odchozí pravidla (produk?ní POS)

7.1.1 Linux iptables / nftables

```
# Primární REST API (AWS API Gateway, eu-west-1)
iptables -A OUTPUT -p tcp --dport 443 \
  -d m6vadtaz1h.execute-api.eu-west-1.amazonaws.com \
  -j ACCEPT

# Real-time sync
iptables -A OUTPUT -p tcp --dport 443  -d ws.kasafik.cz       -j ACCEPT  # WSS
iptables -A OUTPUT -p tcp --dport 1883 -d mqtt.vps.kasafik.cz   -j ACCEPT  # MQTT (cleartext!)

# AWS S3 / SQS (eu-west-1)
iptables -A OUTPUT -p tcp --dport 443 \
  -d fikpreferences.s3.eu-west-1.amazonaws.com \
  -j ACCEPT
iptables -A OUTPUT -p tcp --dport 443 \
  -m string --string "sqs.eu-west-1.amazonaws.com" --algo kmp \
  -j ACCEPT

# České státní endpointy
iptables -A OUTPUT -p tcp --dport 443 -d trzbyeet.gov.cz     -j ACCEPT
iptables -A OUTPUT -p tcp --dport 443 -d pg.trzbyeet.gov.cz  -j ACCEPT

# Firebase / Google

iptables -A OUTPUT -p tcp --dport 443 -d fcm.googleapis.com                      -j ACCEPT
iptables -A OUTPUT -p tcp --dport 443 -d firebaseremoteconfig.googleapis.com      -j ACCEPT
iptables -A OUTPUT -p tcp --dport 443 -d firebaselogging-pa.googleapis.com       -j ACCEPT
```

```
iptables -A OUTPUT -p tcp --dport 443 -d firebasestorage.googleapis.com           -j ACCEPT
iptables -A OUTPUT -p tcp --dport 443 -d tactical-codex-116610.firebaseio.com     -j ACCEPT

# Zpracovatelé plateb
iptables -A OUTPUT -p tcp --dport 443 -d api.sumup.com      -j ACCEPT
iptables -A OUTPUT -p tcp --dport 443 -d *.vivapayments.com -j ACCEPT
```

> **Doporučení:** výše uvedená pravidla povolte na firewallu **per zařízení** (per IP pokladny). Většina zákazníků provozuje pokladny ve vyhrazeném VLANu a whitelist je ideální aplikovat na úrovni VLAN / IP rozsahu.

8 P?íchozí pravidla – nejsou pot?eba

Zařízení **nepřijímá žádná příchozí TCP spojení z internetu**. Neprovádějte port-forward ani inbound NAT pro pokladny.

---

9. Bezpe?nostní profil – souhrn

Oblast	Stav	Poznámka
TLS pro všechny cloudové endpointy	TLS 1.2/1.3	Vyjma MQTT (viz níže)
Vzájemný TLS pro zdravotnictví	mTLS	PFX certifikát per zařízení
MQTT šifrování	⚠ **Čistý text na portu 1883**	Známé omezení; credentials jsou číselná ID zařízení
Cleartext na LAN	Záměrně povolen	ASPA, Ashburn, Adele, Aktion proxy jsou lokální služby
Vstupní porty	Žádné	Zařízení je čistě klient-iniciující
Data v klidu	Šifrována Android FBE / FDE	Na úrovni zařízení
Opt-out z telemetrie	Není v GUI	Firebase Analytics + Crashlytics běží ve výchozím stavu

---

10. Doporu?ení pro nasazení v prost?edí s p?ísnou bezpe?nostní politikou

1. **Izolujte zařízení ve spravovaném VLANu.** Veškerý cloudový provoz je odchozí; izolujte pokladny od firemní LAN a omezte laterální pohyb.
2. **Při TLS-inspection proxy:** přidejte její CA certifikát do důvěryhodného úložiště Android zařízení a přijměte proxy IP pro výše uvedené hostname.

3. **MQTT:** zacházejte s portem 1883 jako s akceptovatelným omezením pro KASA FIK broker. Pokud vaše bezpečnostní politika vyžaduje šifrovaný MQTT, požádejte vývoj KASA FIK o podporu MQTSS.
4. **DNS:** zařízení používá vlastní `DnsSelector` preferující IPv4. Pokud provozujete interní DNS, zajistěte, aby se výše uvedené hostname resolvovaly nebo byly forwardovány.
5. **OpenObserve:** adresa pro log shipping se konfiguruje přes Firebase Remote Config. Před nasazením koordinujte s KASA FIK registraci vašeho OpenObserve endpointu.
6. **White-label domény** (`dochazka.efg.cz`, `ec.qrticket.cz`, `*.vivapayments.com` apod.) jsou konfigurovatelné operátorem a mohou být pro dané nasazení jiné. S integratorem KASA FIK si ověřte, které integrace jsou ve vaší instalaci povolené.

Revision #5
Created 2026-09-17 03:45:27 UTC by Admin
Updated 2026-09-17 06:41:01 UTC by Admin