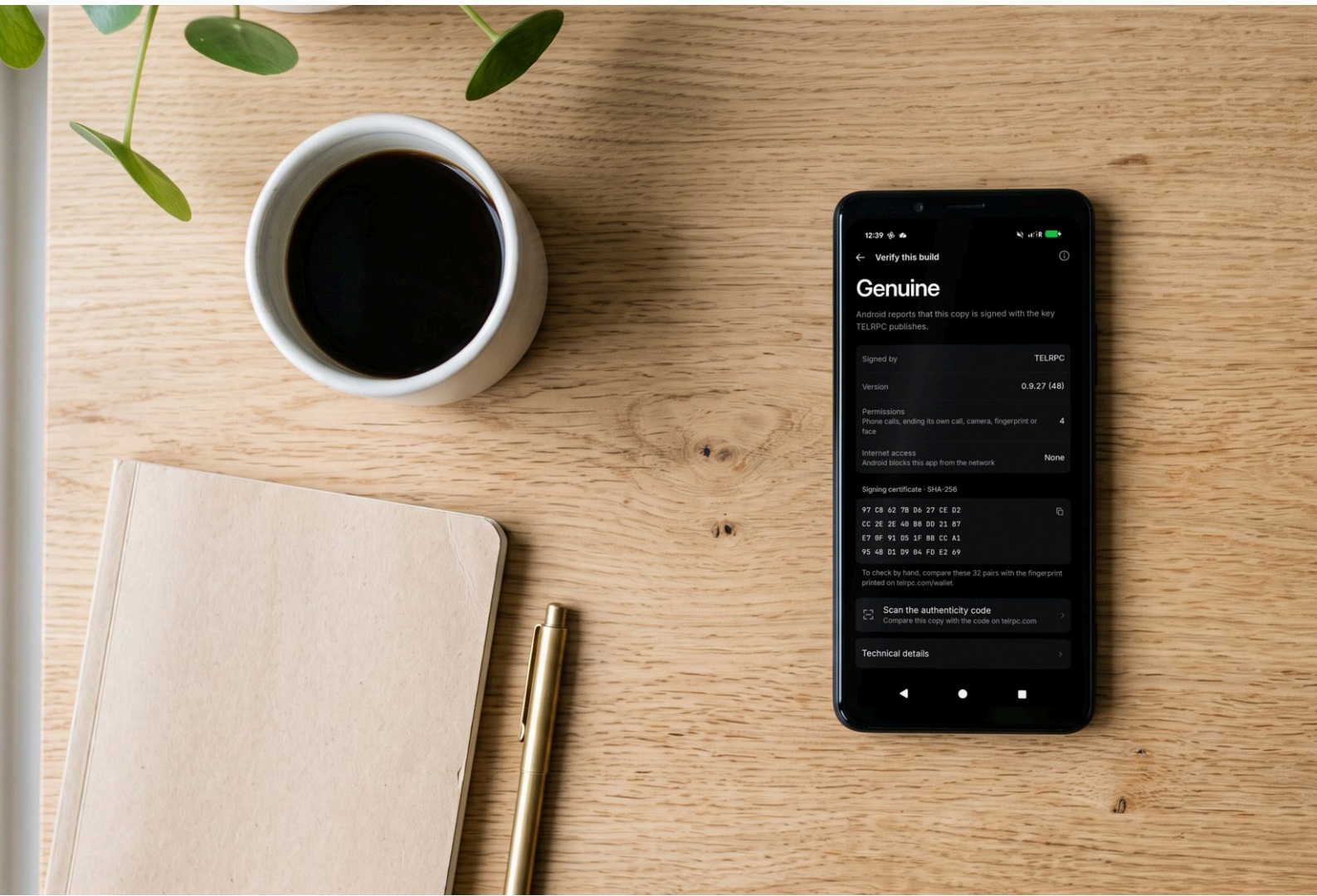




The TELRPC threat model

Security model

Contents

1	The adversary	2
2	What a compromised party can do	3
3	The properties that hold	3
4	Strongest configuration	4
5	Four ways to sync	4
6	Measured in the field	4

TELRPC keeps the key on a device with no network path and carries the signed transaction over an ordinary phone call to a grid that holds no key that can move user funds. The TELRPC Wallet declares no internet permission and four others, CALL_PHONE, ANSWER_PHONE_CALLS, CAMERA and USE_BIOMETRIC, verifiable in one command. In field runs on 9 and 11 October 2026 it sent USDC on Base over ordinary calls: garbled calls were refused and recovered automatically, and no transaction settled twice.

1 The adversary

The adversary may fully control the grid, the carrier path, and caller ID; may record, replay, reorder, drop, or inject digits; may place forged echo calls to the phone; and may show the wallet's camera a forged or stale state QR. The adversary does not hold the user's key and cannot break standard signatures (ECDSA/secp256k1, Ed25519, BIP-340 Schnorr). Every property below holds under that adversary.

0	4	0	0
internet permission on the wallet process. The OS grants it no network socket, for the life of the install.	permissions in the manifest: CALL_PHONE to place the broadcast call, ANSWER_PHONE_CALLS to end its own call if the network doesn't, CAMERA to read a state QR, USE_BIOMETRIC for fingerprint or face unlock. None can transmit. The echo adds Android's call-screening role (Android 10+), which reads an incoming caller ID and grants no network access.	TELRPC contracts on any chain. The grid deploys nothing; every send pays its own network fee.	bytes of key material on any channel, in either direction

2

What a compromised party can do

Every party outside the phone, from the grid to the carrier path to anyone imitating an echo, is limited to delay or refusal. None can redirect, alter or originate a payment, and none ever sees key material. The party-by-party adversary analysis is in the security audit pack, available under NDA.

3

The properties that hold

Binding

Payee, amount, and anti-replay material sit under the user's signature. Full grid compromise yields denial of service, never theft.

Replay resistance

Bounded per chain. Account nonces, spent outputs, durable-nonce advance. The same bounds make the automatic redial safe: a resend keys the identical signed transaction, so it can only land once.

Safe failure on the line

A garbled frame fails its checksum and is never broadcast. The grid hangs up quietly and signals a resend by echo, and the wallet redials by itself. The worst a compromised line can do is cause a delay, never a loss.

Key confinement

No protocol message carries key material, and neither the call path nor the camera path can. The channel cannot leak what is never serialized.

Output authority

The wallet, not the channel, sets the payee and the amount, from the owner's own input. The QR relay supplies only public ledger data: a nonce, a blockhash, a UTXO set. A forged or substituted QR can at worst produce a transaction that fails to broadcast; it can never produce one that pays a different address.

Confirmation integrity

The wallet computes the transaction id before the call. A confirmation echo moves its sequence forward only when its reference matches that id, so a forged echo is ignored, and a wrong sequence is corrected against the chain's real value.

Cryptographic identity

The account is the address recovered from the signature. Caller ID is a routing hint, never trust.

Statically verifiable

The absent internet permission is confirmed on the shipped APK in seconds by anyone: the manifest lists CALL_PHONE, ANSWER_PHONE_CALLS, CAMERA and USE_BIOMETRIC and no INTERNET. The call-screening role used by the echo is not a manifest permission and adds no network access. The operating system enforces the isolation per process: whatever radios the handset carries, the wallet process holds no permission to use them for data. A purpose-built device with no radio proves the same isolation by having no network interface at all.

4 Strongest configuration

TELRPC broadcast paired with hardware-wallet key custody: the key in dedicated signing silicon, the transaction built and broadcast with no internet path, the network nowhere in the wallet's life. This is the configuration these documents recommend. In this use TELRPC need not be the signer at all: the party generates keys and signs on its own device, hardware wallet, or MPC setup, and the rail serves only to broadcast the signed transaction and to read the state a send needs.

5 Four ways to sync

Send-state reaches the wallet by interchangeable methods, none opening a socket: the QR relay and the echo on every chain that needs state, plus a spoken state line and manual entry on an EVM account. Expiry-bound chains use durable constructions, so a signature stays valid for as long as the call takes: Solana signs against a durable nonce, and Bitcoin has no expiry at all.

6 Measured in the field

On 9 and 11 October 2026 a phone with no internet permission sent USDC transactions on Base over ordinary calls. Frames that arrived garbled were refused, each was redialled automatically with the same signed bytes, and it confirmed on-chain once, with no duplicate and no one touching the phone. A transfer took about 95 seconds of tones and about two minutes from call to confirmation. On 11 October 2026, for example, one USDC on Base left a phone with no internet permission over an ordinary call and confirmed in block 52,460,479 (0x54cc6ddc...78b1a7), public on any Base explorer.

T E L R P C

The rails that never go online.

Minutes Network FZ-LLC

Ras Al Khaimah
United Arab Emirates

World Mobile Group Ltd.

29 Holywell Row, London EC2A 4JB
United Kingdom, Company No.
13191263

Contact

contact@telrpc.com
telrpc.com