Confidential-MOBILE

Secured Mobile Telecommunication
Business & Personal

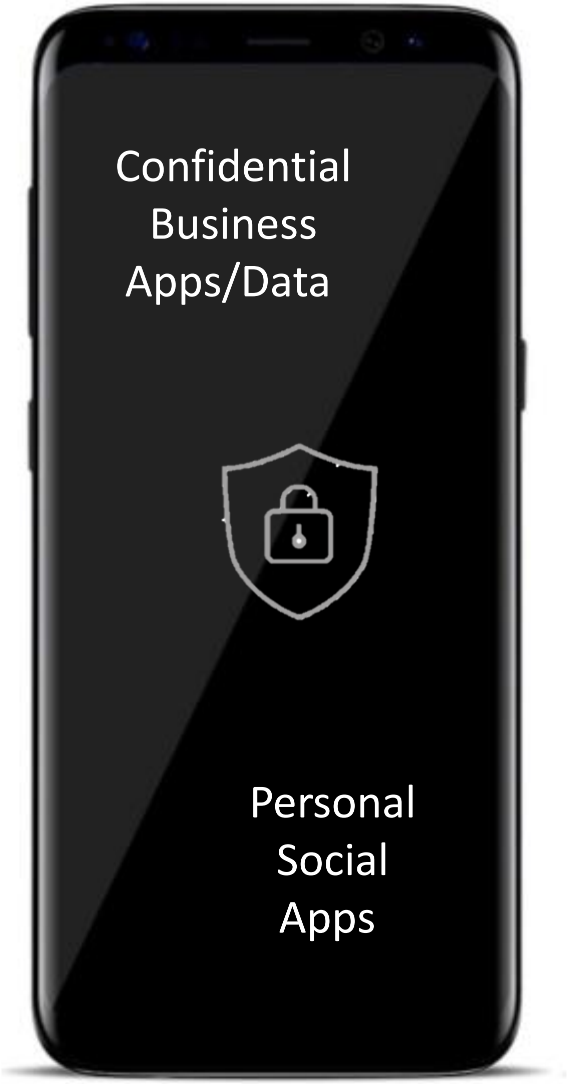
TSCM

Confidential-MOBILE

One
secured Samsung device for both business and personal usage.

Confidential
business apps and data are encrypted and totally separated from personal apps.

Secured
Android system with apps permission restrictions and user's data access.



Confidential Business Apps/Data

Personal Social Apps

Samsung
most advanced business class mobile device.

Secured
hardware & software mobile device.

Protected
from wired and wireless malicious injection.

Encrypted
data system protected from unauthorized data access/recovery.

Secured Mobile – Business & Personal Usage

Confidential Business Partition:

Secured encrypted end-to-end voice calls and text/media messages over secured private server.

Encrypted VPN connection for securing confidential business apps data over public wireless networks.

Anonymous WEB surfing over TOR network to keep user's privacy.

Confidential business apps and data are managed in secured encrypted container.

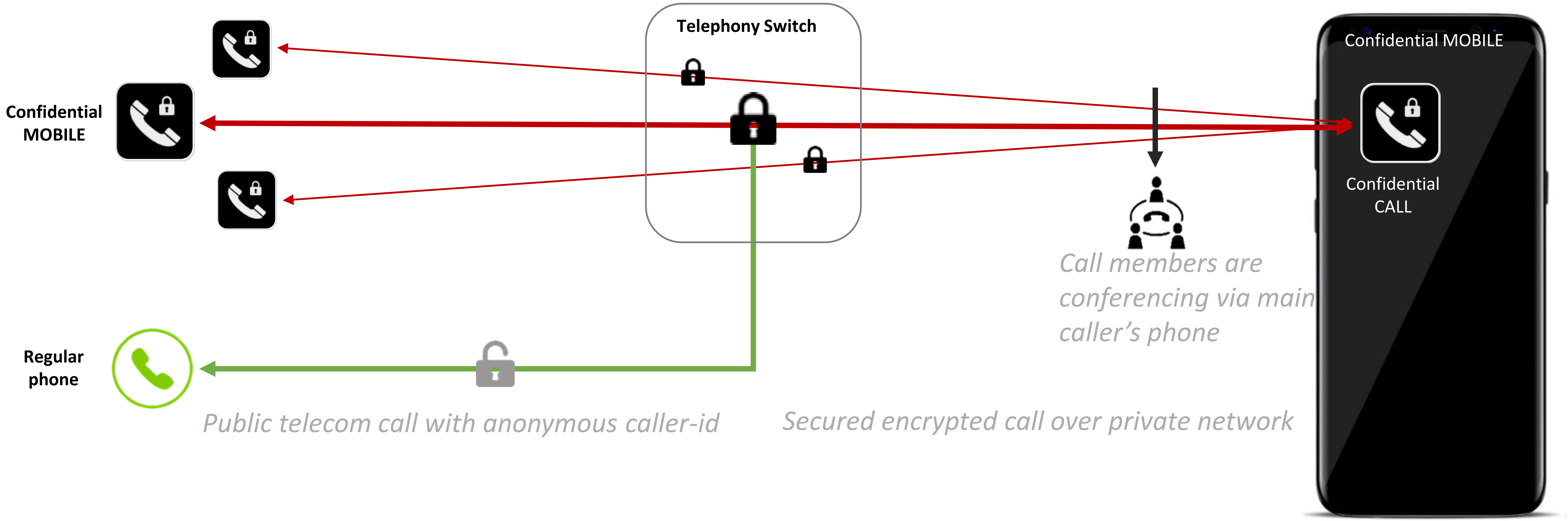
Personal Zone:

User can install apps from the Play-Store only. Installing from Unknown-Sources is disabled!

Developer options is disabled!

Admin MDM:
> Restricts apps installation with white/black list apps policy.
> Restricts Factory-Reset, Safe-Mode.
> Controls all mobile capabilities.
> Applies policy groups remotely.
> Manages multiple devices instantly.

Secured Encrypted Calls


Telephony Switch
Confidential MOBILE
Confidential MOBILE
Confidential CALL
Call members are conferencing via main caller's phone
Regular phone
Public telecom call with anonymous caller-id
Secured encrypted call over private network

End-to-End Encrypted Calls

- ✓ Secure encrypted end-to-end phone calls.
- ✓ Strong random fresh unbreakable encryption key per call initiation.
- ✓ Protected from call parties identification.
- ✓ Protected from call tracking.
- ✓ Protected from call eavesdropping.

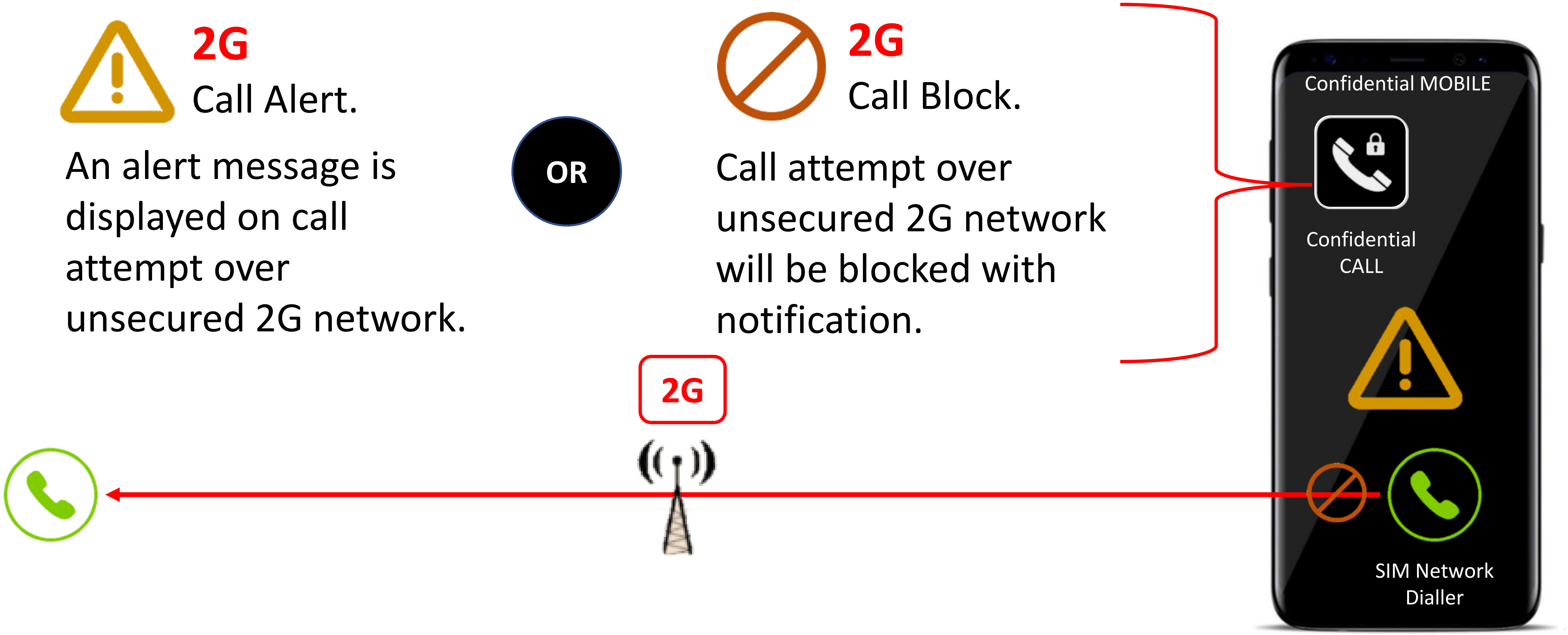
Advanced Call Features

- ✓ End-to-end encrypted conference calls.
- ✓ Secured anonymous outgoing/incoming calls to/from regular phone numbers.
- ✓ Anonymous caller-id virtual numbers from more than 50 countries and 200 regions.
- ✓ Confidential contact list with real-time status availability.

Secured Network Connectivity

- ✓ Monitoring mobile network connectivity.
- ✓ Alerting on unsecured 2G network calls (Optional).
- ✓ Forbidding calls on unsecured 2G network (Optional)
- ✓ Automatically rerouting outgoing/incoming calls of selected confidential contacts, from the SIM mobile network to the secured encrypted channel.

Secured Network Calls



2G

Call Alert.

An alert message is displayed on call attempt over unsecured 2G network.

OR

2G

Call Block.

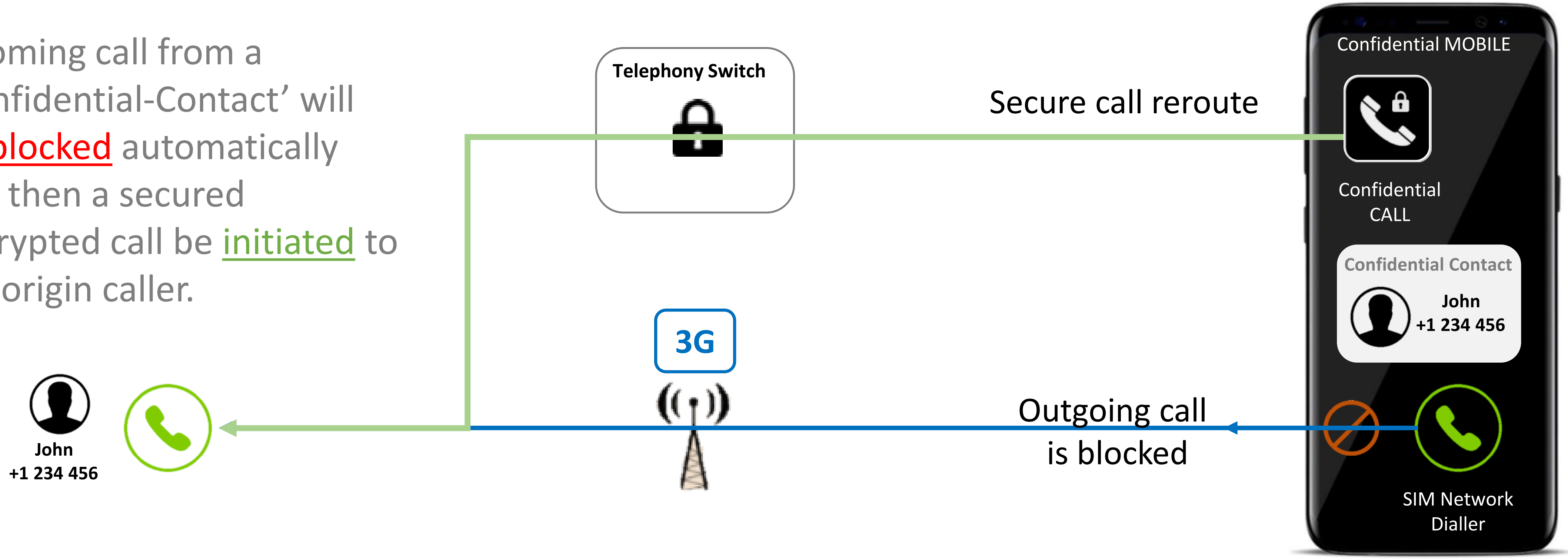
Call attempt over unsecured 2G network will be blocked with notification.

2G calls are highly vulnerable to IMSI-Catcher passive and active attacks.

Secured Network Calls | continue

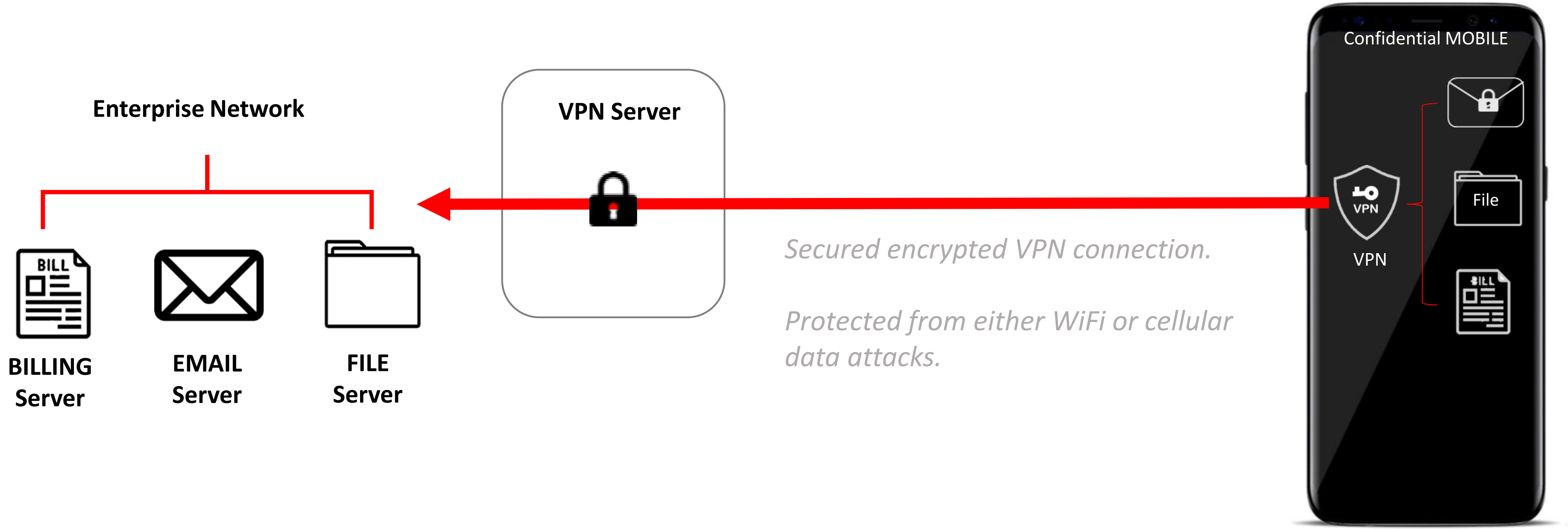
Outgoing SIM network call attempt to a predefined 'Confidential-Contact' will be blocked automatically and then get rerouted over the secured encrypted channel.

Incoming call from a 'Confidential-Contact' will be blocked automatically and then a secured encrypted call be initiated to the origin caller.



3G calls are better protected over the air from IMSI-Catchers but still can be monitored by mobile operators and officials agencies.

Secured Encrypted Enterprise Communication



Secured encrypted VPN connection.

Protected from either WiFi or cellular data attacks.

Routing confidential business apps’ data over a secured encrypted VPN connection to the enterprise network

Device Multi-Layers Security

REAL-TIME KERNEL PROTECTION INTEGRITY MEASUREMENT ARCHITECTURE

Periodic kernel measurement and real-time kernel work to constantly inspect the core software OS to ensure that any bypass attempt or sensitive data access are blocked.

SECURE / TRUSTED BOOT AND HARDWARE ROOT OF TRUST

Hardware root of trust is used to verify the boot process integrity,
to prevent security measures from being bypassed or compromised

SECURITY ENHANCEMENTS FOR ANDROID

Protecting applications and data by defining what each process is allowed to do and what data it can access, to separate, encrypt and protect sensitive enterprise data.

TRUSTZONE

Leveraging a processor architecture in which highly sensitive computations are isolated from the rest of the device's operation, protecting enterprise data.

Enterprise Mobile-Device-Management (MDM)

Configure

Configure custom secured device policy for individuals or for users group

Enroll

Enroll instantly multiple devices with their custom secured policy configuration

Manage

Manage remotely users’ secured connections and devices’ resources.

Secure

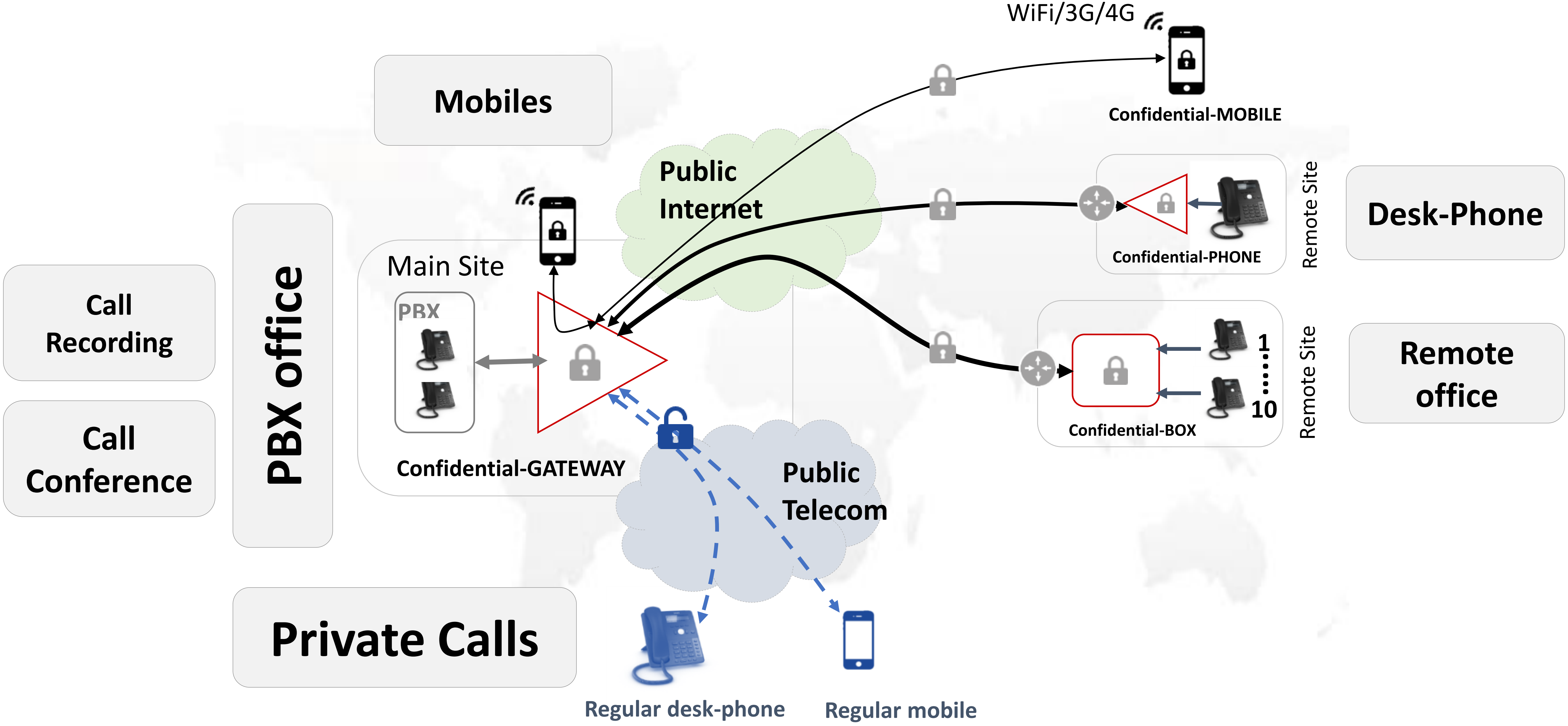
Secure user’s confidential apps and data from hardware and software breaking attacks.

Maintain

Maintain and update the device security policy over the air with new security measurements.

Confidential-GATEWAY *server*

Any-to-Any Secure Encrypted End-to-End Calls



Mobiles

Call Recording

Call Conference

PBX office

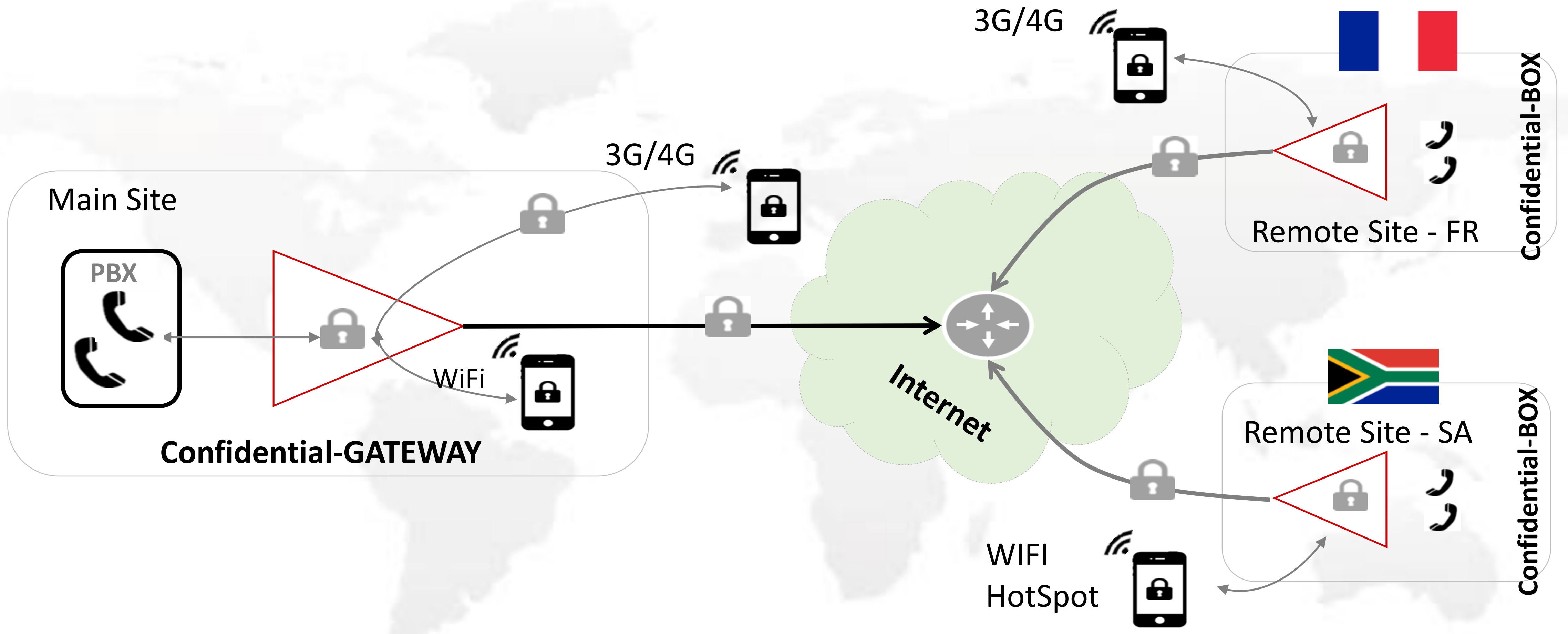
Private Calls

Desk-Phone

Remote office

Confidential-GATEWAY

Secure multiple global sites



Ministry of Foreign Affairs

Remote International Embassies

Confidential-MOBILE | Samsung Mobile

Confidential Telecom is a partner of Samsung Electronic which its most secure Knox mobile security solutions are implemented in the Confidential-MOBILE secured phone.
Samsung Knox mobile solutions have proven certifications by governments and related organizations around the world which have some of the most stringent information and technology security requirements.

Common Criteria

DISA (USA)

FIPS 140-2 (USA)

NCSC (UK)

ANSSI (France)

CCN (Spain)

AIVD (Netherlands)

NCSA (Finland)

ISCCC (China)

Kazakhstan

TSCM

Contact Us