Famoc
BY FANCYFON

FAMOC MOBILE SECURITY MANAGEMENT FOR GOVERNMENT

Digitally signed by Cornei Andrian
Date: 2018.12.21 19:28:18 EET
Reason: MoldSign Signature
Location: Moldova

ABOUT **FANCYFON**

Developer of industry leading mobile device management and security software solutions for enterprises and institutions

VALUE PROPOSITION

Enable organizations to easily control, manage and secure the use of mobile devices (BYOD or corporate), applications and documents within their organizations

KEY DIFFERENTIATORS

Broadest mobile platform support, seamless integration with 3rd party IT/security management systems, flexible deployment/configuration, out-of-the-box IT compliance

FLEXIBLE DEPLOYMENT

SaaS, private cloud and on-premise deployment options available

CUSTOMERS

More than 280,000 devices managed and secured across more than 700 enterprise customers

STRATEGIC TECH PARTNERSHIPS

In 2013 FancyFon achieved a Gold Samsung Partner status. In 2015 and 2017 FancyFon was highlighted at Mobile World Congress in Barcelona. Other partnerships include: Huawei, Sony, Lenovo and others.

COMPANY **TIMELINE**

2006

FancyFon Start

2008

FAMOC platform generally available; first enterprise customer deployment in Europe

2010

Gartner recognizes FAMOC in MDM Magic Quadrant

2012

- OEM partnership with HEAT Software

2013

Expansion of mobile operator focused GTM

2013

FancyFon awarded Gold status of Samsung partnership

2015

MS4B - distribution for South America
Sovaton – distributor in Africa

2016

FAMOC for Government

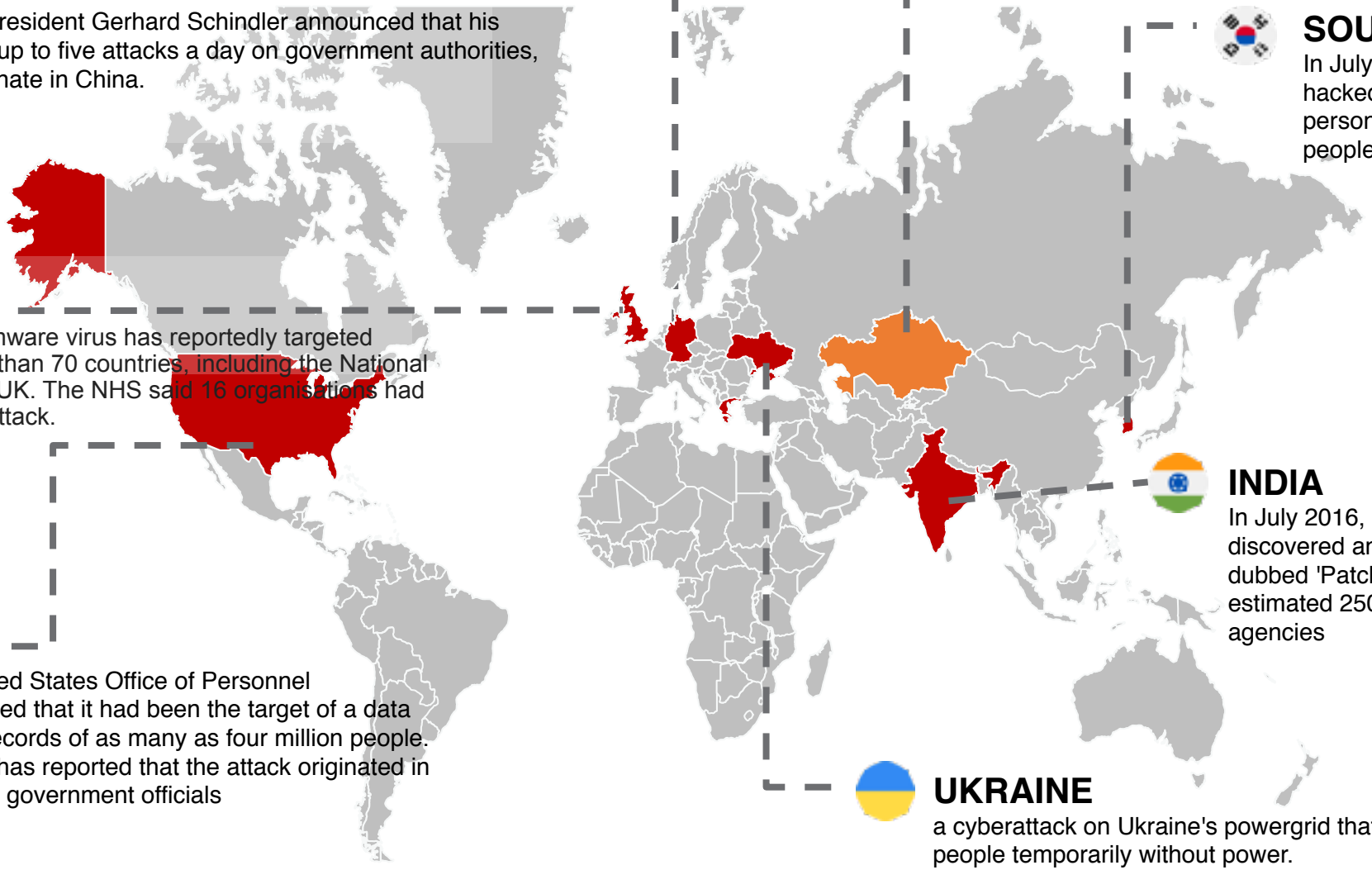
2017

FAMOC
Mobile Security Management for Government

2017

SMC - distributor for Central Asia

EXAMPLES OF **CYBERWARFARE**



KAZAKHSTAN

In July 2017, the Kazakhstan was hacked. There is no possibility to take smartphone and tablet to government office.

GERMANY

In March 2013, BND president Gerhard Schindler announced that his agency had observed up to five attacks a day on government authorities, thought mainly to originate in China.

SOUTH KOREA

In July 2011, the South Korean was hacked, resulting in the theft of the personal details of up to 35 million people.

UK

In May 2017, A ransomware virus has reportedly targeted organisations in more than 70 countries, including the National Health Service in the UK. The NHS said 16 organisations had been affected by the attack.

INDIA

In July 2016, Cymmetria researchers discovered and revealed the cyber attack dubbed 'Patchwork', which compromised an estimated 2500 corporate and government agencies

USA

In June 2015, the United States Office of Personnel Management announced that it had been the target of a data breach targeting the records of as many as four million people. The Washington Post has reported that the attack originated in China, citing unnamed government officials

UKRAINE

a cyberattack on Ukraine's powergrid that left more than 200,000 people temporarily without power.

FAMOC BUILT-IN **SECURITY CAPABILITIES**

Comprehensive device, operating system and app security coupled with native integration with Samsung Knox Workspace and Webroot security frameworks

DEVICE SECURITY

Device Restrictions

Policy Enforcement

Remote Wipe/Lock

Monitoring/Reporting

OS SECURITY

VPN Configuration

Data Encryption

Containerization (Android for Work & Samsung KNOX)

Connectivity Restrictions (GPS, WiFi, Bluetooth)

Apple Supervised Mode Support

APP SECURITY

Corporate App Store

App Blacklist

App Whitelist

App Reputation Verification

Secure Browser

Enterprise Wipe

FAMOC **KEY FEATURES**

CROSS-PLATFORM SUPPORT

Define and enforce universal policies across mobile platforms and also leverage each platform's unique management capabilities within the same unified console

MOBILE APPLICATION MANAGEMENT

Real-time view of all applications and information on their reputation and usage; ensures communication, configuration and data protection for all business apps

ADVANCED CONFIGURATIONS

Industry's most comprehensive Samsung Knox support, including advanced configurations for email, VPN, OTA app distribution/update/removal

SECURE MESSAGING/CONTENT

Enables secure email, content management and messaging, as well as continuous backup of mobile data with cross-platform data migration

REMOTE SUPPORT

Permission-based sessions provide OTA access to device, files and apps; automated diagnostics and troubleshooting

LOCATION MONITORING

Creation of geofencing rules and device policies based on location; scheduled or on-demand device location searches

IDENTITY/ACCESS MANAGEMENT

Advanced integration with enterprise identity management and network access control systems; support for certificate management; API-level integration

NETWORK PROXY

Proxy server optimized to control/protect mobile access to corporate data; identifies the device prior to granting access and filters devices via whitelisting and blacklisting features

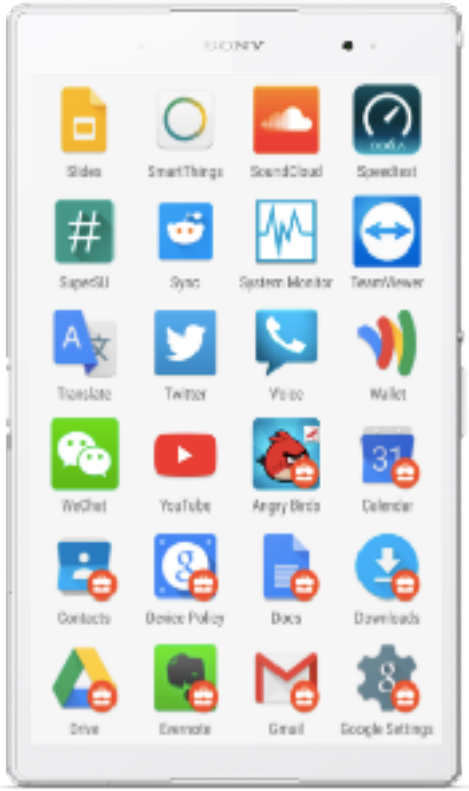
NATIVE SOLUTIONS **INTEGRATIONS**

iOS

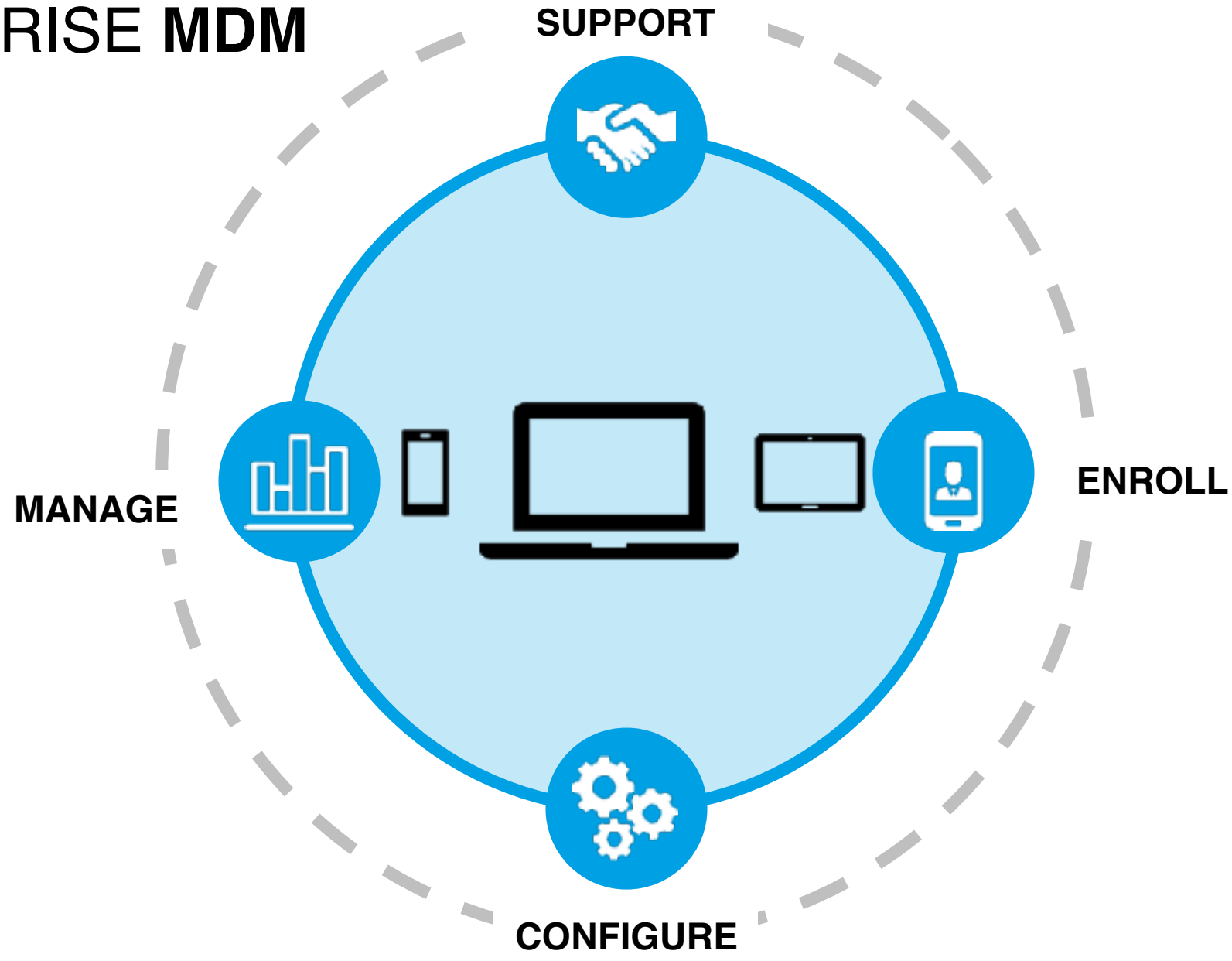
Samsung KNOX

GOLD PARTNER
SAMSUNG
ENTERPRISE ALLIANCE
PROGRAM

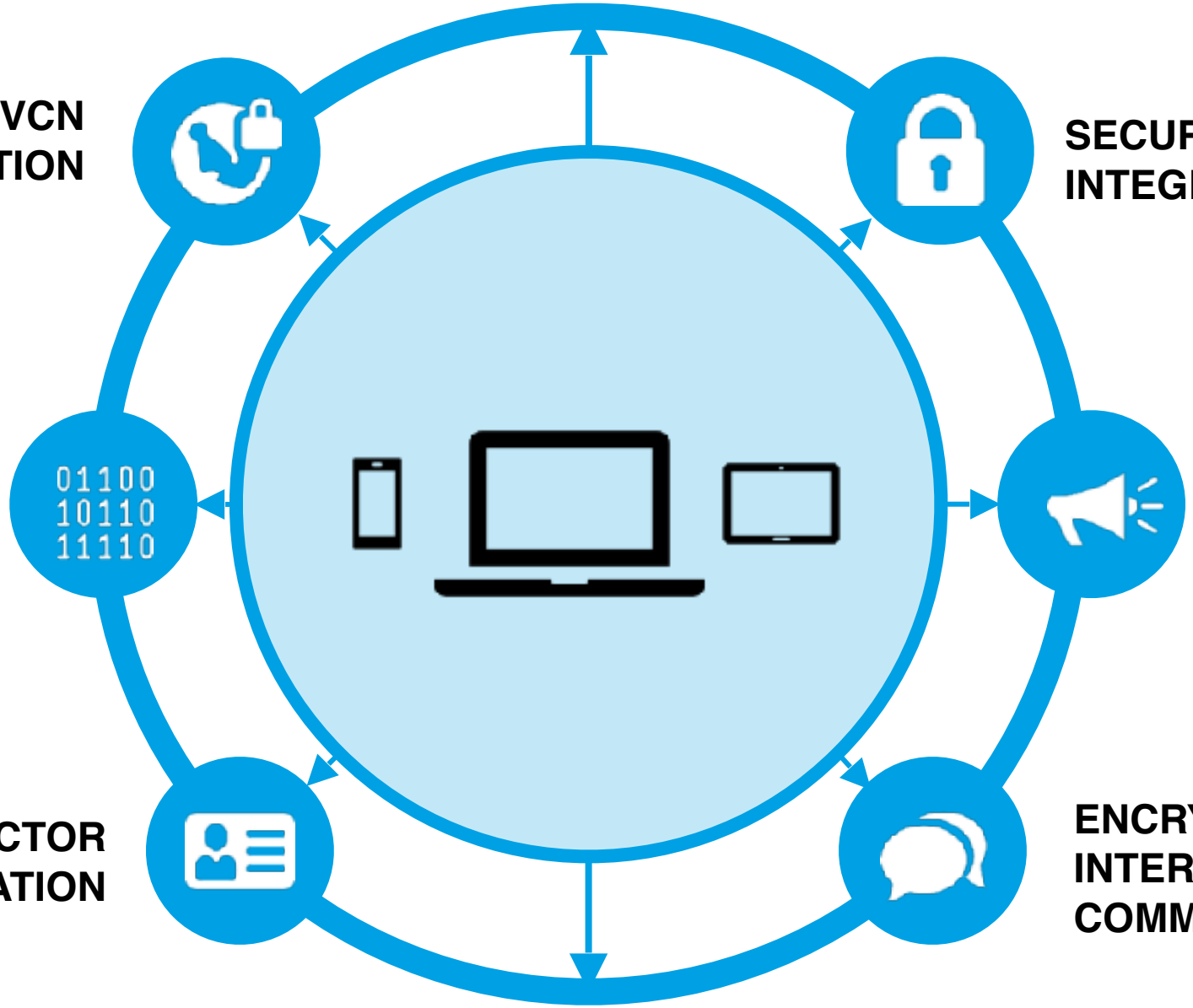
Android for Work



ENTERPRISE **MDM**



GOVERNMENT **SECURITY MANAGEMENT**



FAMOC FOR GOVERNMENT PLATFORM HIGHLIGHTS

BUILT FOR THE CUSTOMER

SOURCE CODE

MANAGEMENT – cross-platform mobile device lifecycle management; usage policy creation, monitoring and enforcement based on device, OS, application, role and contextual factors

SECURITY – protection of sensitive corporate data at the user, application, device and network levels to ensure containerization, data loss prevention; automated responses to security incidents/violations

GOVERNMENT-GRADE **SECURITY**

Security is critical to maintaining data integrity and trust. FancyFon has focused on providing government-grade security required to manage data and provide a shield against today's cyber threats.

Common Criteria Mode for Samsung KNOX Workspace

FAMOC is recommended as a tactical solution to support advanced functionalities of Samsung Android devices

VPN and dual APN support

For advanced security and granular control over devices

ISO-verified

Assessed and certified as meeting the requirements of ISO/IES 27001:2013

Separate environment

Secure on-site deployment with regular updates of the on-site solution

AES, 3 DES and 128 bit encryption

Vast customization options to meet country-specific requirements of government customers

Continuous verification

Ongoing penetration testing on a regular basis

FAMOC MOBILE OFFLINE **SECURITY MANAGEMENT**

FAMOC SECURITY AGENT AVAILABLE OFFLINE RESTRICTIONS

- WIPE or Corporate WIPE on
  - SIM change
  - x numbers of wrong passwords
  - USB data cable
  - low temperature *
  - SD card change *
  - no FAMOC server contact longer than X hours
- Other action on luck of connection to FAMOC server
  - after time Y - stop BT/NFC/WiFi, block USB
  - after time Z - try to send SMS to FAMOC SMS gateway with location and status
  - after time Z - change password to longer and re-encrypt data

FAMOC SECURITY AGENT AVAILABLE OFFLINE RESTRICTIONS

- Report of new SIM card to FAMOC direct or via SMS gateway
- Report of location on SIM card change
- Report of new SD card to FAMOC SMS gateway

Navayo Group

WEBROOT SecureAnywhere

SAMSUNG Knox

Android for Work

SECURITY INTEGRATIONS

Navayo Group

Android for Work

WEBROOT SecureAnywhere

SAMSUNG Knox

SECURITY INTEGRATIONS

CISCO

Extreme networks

Check Point SOFTWARE TECHNOLOGIES LTD.

Exchange

IBM Lotus

Microsoft

OTHER POSSIBLE INTEGRATIONS

Famoc

FAMOC FOR **GOVERNMENT**

HARDWARE LAYER

PORT'S SECURITY AND RESTRICTIONS

- **Control USB - OFF/ON/Always ON/Always OFF**
- **USB only for power charge**
- **Wipe on USB data force?**
- **GPS - ON/OFF/always ON**
- **Headset port ***
- **Wireless power ***
- **Accelerator sensor ***
- **Temperature sensor***
- **Memory SD card -** data encryption, only with certificate* only with secure element*

1 APPS LAYER

2 WYSP LAYER

3 DATA CONTAINER LAYER

4 OS LAYER

5 VPN LAYER

6 SIM LAYER

7 RADIO MODEM LAYER

8 SECURE BOOT LAYER

9 **HARDWARE LAYER**

FAMOC FOR **GOVERNMENT**

SECURE BOOT LAYER

SAMSUNG BOOT RESTRICTIONS

- KME - connection to Samsung or not started
- FAMOC always on
- Device belongs to owner
- Reboot will not change device setup and FAMOC management

ANDROID BOOT RESTRICTION for Oreo

- Reboot Support for Android Zero Touch simplifies bulk corporate device rollouts

ANDROID PRODUCER ver. lower than Oreo - BOOT RESTRICTIONS POSSIBLE WITH COOPERATION WITH PRODUCER (LG, LENOVO..)

- Boot restrictions possible with cooperation with producer but limited functions
- Reboot will not change device setup and FAMOC management

APPLE IOS

- Apple Supervise mode
- FAMOC always on
- Device belongs to owner
- Reboot will not change device setup and FAMOC management

1 APPS LAYER
2 WYSP LAYER
3 DATA CONTAINER LAYER
4 OS LAYER
5 VPN LAYER
6 SIM LAYER
7 RADIO MODEM LAYER
8 **SECURE BOOT LAYER**
9 HARDWARE LAYER

FAMOC FOR **GOVERNMENT**

RADIO MODEM LAYER

BLUETOOTH SECURITY AND RESTRICTIONS

- Control BT - Off/On/always on/always off
- For define MAC address list only
- Store all MAC addresses of connected device in history

(no possibility to connect to BT device based on certificate, no such devices on the market today)

WIFI SECURITY AND RESTRICTIONS

- Control WiFi - Off/On/always on/always off
- For define MAC address list only
- WiFi with certificate only
- Only for listed WiFI and APN's
- Store all MAC addresses of connected WiFi in history
- integration with CISCO & other Radius systems

NFC SECURITY AND RESTRICTIONS

- Control NFC- Off/On/always on/always off
- NFC with certificate only
- NFC with hardware certificate (YubiKey)

All setup can automatically change based on geolocation and time.

1 APPS LAYER

2 WYSP LAYER

3 DATA CONTAINER LAYER

4 OS LAYER

5 VPN LAYER

6 SIM LAYER

7 **RADIO MODEM LAYER**

8 SECURE BOOT LAYER

9 HARDWARE LAYER

FAMOC FOR **GOVERNMENT**

RADIO MODEM LAYER

GSM SECURITY AND RESTRICTIONS

- GSM voice - on/off
- GSM data - on/off, only on selected APN
- GSM SMS - on/off
- GSM MMS - on/off
- GSM APN operator service - one or two selected APN dedicated for customer
- Voice log - in and out
- SMS & MMS log in and out
- IP address log
- IP connections log

All setup can change based on geolocation, time and event.

1 APPS LAYER

2 WYSP LAYER

3 DATA CONTAINER LAYER

4 OS LAYER

5 VPN LAYER

6 SIM LAYER

7 **RADIO MODEM LAYER**

8 SECURE BOOT LAYER

9 HARDWARE LAYER

FAMOC FOR **GOVERNMENT**

SIM LAYER

SIM CARD SECURITY AND RESTRICTIONS

- Wipe on SIM card change
- SIM card with special customer APN only
- SIM card random PIN force by FAMOC
    - SIM dedicated to one device only
    - no possibility to use SIM in other device

1 APPS LAYER
2 WYSP LAYER
3 DATA CONTAINER LAYER
4 OS LAYER
5 VPN LAYER
6 **SIM LAYER**
7 RADIO MODEM LAYER
8 SECURE BOOT LAYER
9 HARDWARE LAYER

FAMOC FOR **GOVERNMENT**

VPN / MVCN LAYER

FAMOC VPN is a fully on-premise solution available for public & government customers

STRONG ENCRYPTION

VPN - AES 128/192/256
IPsec/IKEv2
MODP2048/3017/4096 for IKE

STRONG AUTHENTICATION

Two-factor authentication using biometry combined with NFC card or other tokens as the 2nd factor

CERTIFICATION-READY

Source code analysis as an option for government customers

1 APPS LAYER
2 WYSP LAYER
3 DATA CONTAINER LAYER
4 OS LAYER
5 **VPN LAYER**
6 SIM LAYER
7 RADIO MODEM LAYER
8 SECURE BOOT LAYER
9 HARDWARE LAYER

FAMOC FOR **GOVERNMENT**

OS LAYER

MOBILE OS SECURITY

- **VPN or MVCN**
- **Data encryption on Phone memory**
- **Data encryption on SD card**
- **Data encryption on SIM***
- **Secure certificate**

- **IPS mobile - process/task control***
- **OS version control - eFOTA, iOS Supervised**
- **OS producer communication restrictions**
  - **Push**
  - **Services**
- **Hardware producer communication**
  - **Samsung KCC / KME**
  - **Apple iOS Supervise mode**
  - **Android Zero Touch**
  - **Other** with cooperation with producer possible some functions

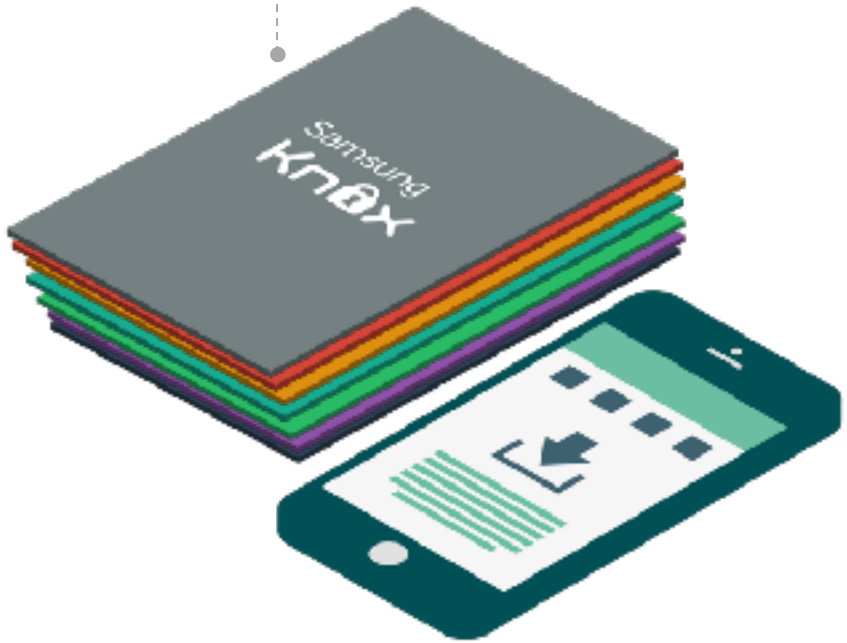
1 APPS LAYER
2 WYSP LAYER
3 DATA CONTAINER LAYER
4 **OS LAYER**
5 VPN LAYER
6 SIM LAYER
7 RADIO MODEM LAYER
8 SECURE BOOT LAYER
9 HARDWARE LAYER

FAMOC FOR **GOVERNMENT**

DATA CONTAINER LAYER

DATA CONTAINER

- Data containers
  - KNOX Workspace
  - Google Workspace
  - Apple iOS in Supervised Mode
- Two factor authentication to device
- Two factor authentication to container
- External hardware based certificate (YubiKey)
- Encrypted internal & external data communication
- Encrypted voice communication
- Encrypted messaging COMMUNICATION
- Hardware producer communication
  - Samsung KME
  - Android Zero Touch
  - Others



FAMOC FOR **GOVERNMENT**

NAVAYO/WYSP LAYER

WHAT IS NAVAYO?

Navayo deliver encrypted data and voice communication based n patented key exchange mechanism and encryption to all those who need discretion on the digital frontlines of the 21st century

NAVAYO BENEFITS

- Complete, secure ecosystem
- Certified hardware based encryption (BSI Common Criteria EAL5+)
- Worldwide patents of the MVCN Technology
- Certification – HW: BSI CC 5+ (done), SW: BSI CC 4+ (in progress)
  Third party symmetric algorithm implementation
- The first hardware encryoted security and privacy system for Android and iOS
- The first independent hardware encrypted security and privacy system for BlackBerry

1 APPS LAYER

2 **WYSP LAYER**

3 DATA CONTAINER LAYER

4 OS LAYER

5 VPN LAYER

6 SIM LAYER

7 RADIO MODEM LAYER

8 SECURE BOOT LAYER

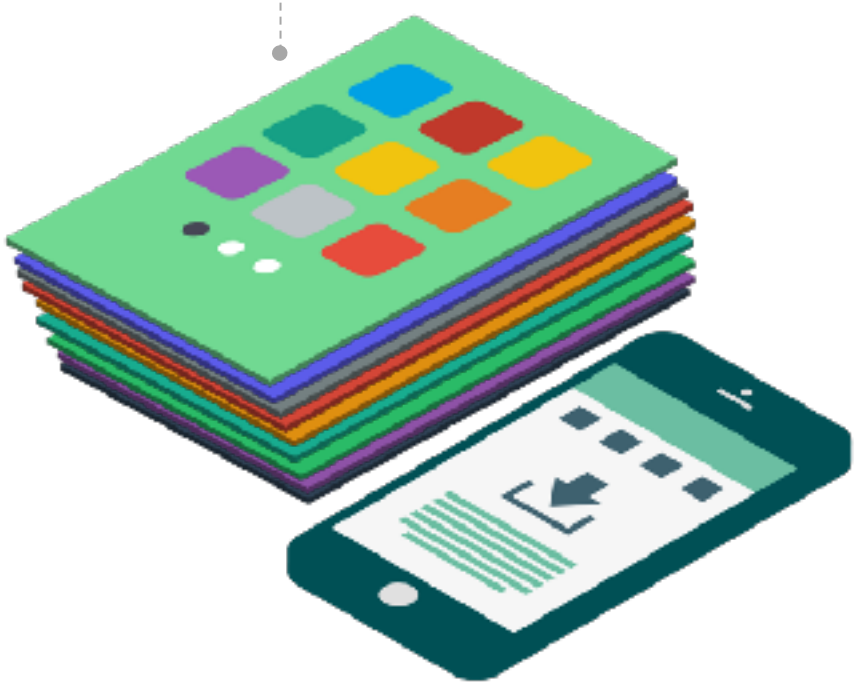
9 HARDWARE LAYER

FAMOC FOR **GOVERNMENT**

APPS LAYER

APPLICATION SECURITY

- **Corporate App Store**
- **App Blacklist**
- **App Whitelist**
- **Application ‚always on' list**
- **Kiosk mode**
- **App Reputation Verification**
- **Secure Browser**
- **Enterprise Wipe**
- Application Process verification (IPS)*



1. **APPS LAYER**
2. WYSP LAYER
3. DATA CONTAINER LAYER
4. OS LAYER
5. VPN LAYER
6. SIM LAYER
7. RADIO MODEM LAYER
8. SECURE BOOT LAYER
9. HARDWARE LAYER

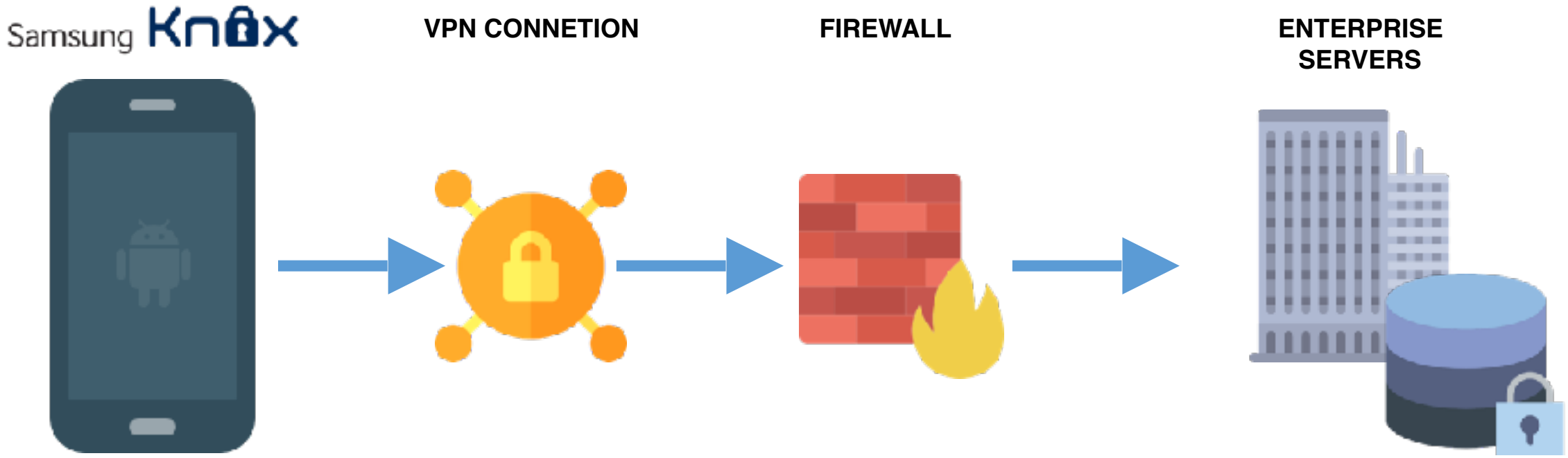
KNOX **MOBILE ENROLLMENT**

Enrolling new devices into your enterprise is a time-consuming process but with **KNOX Mobile Enrollment** IT admins can quickly enroll hundreds of devices into their enterprise MDM at once.

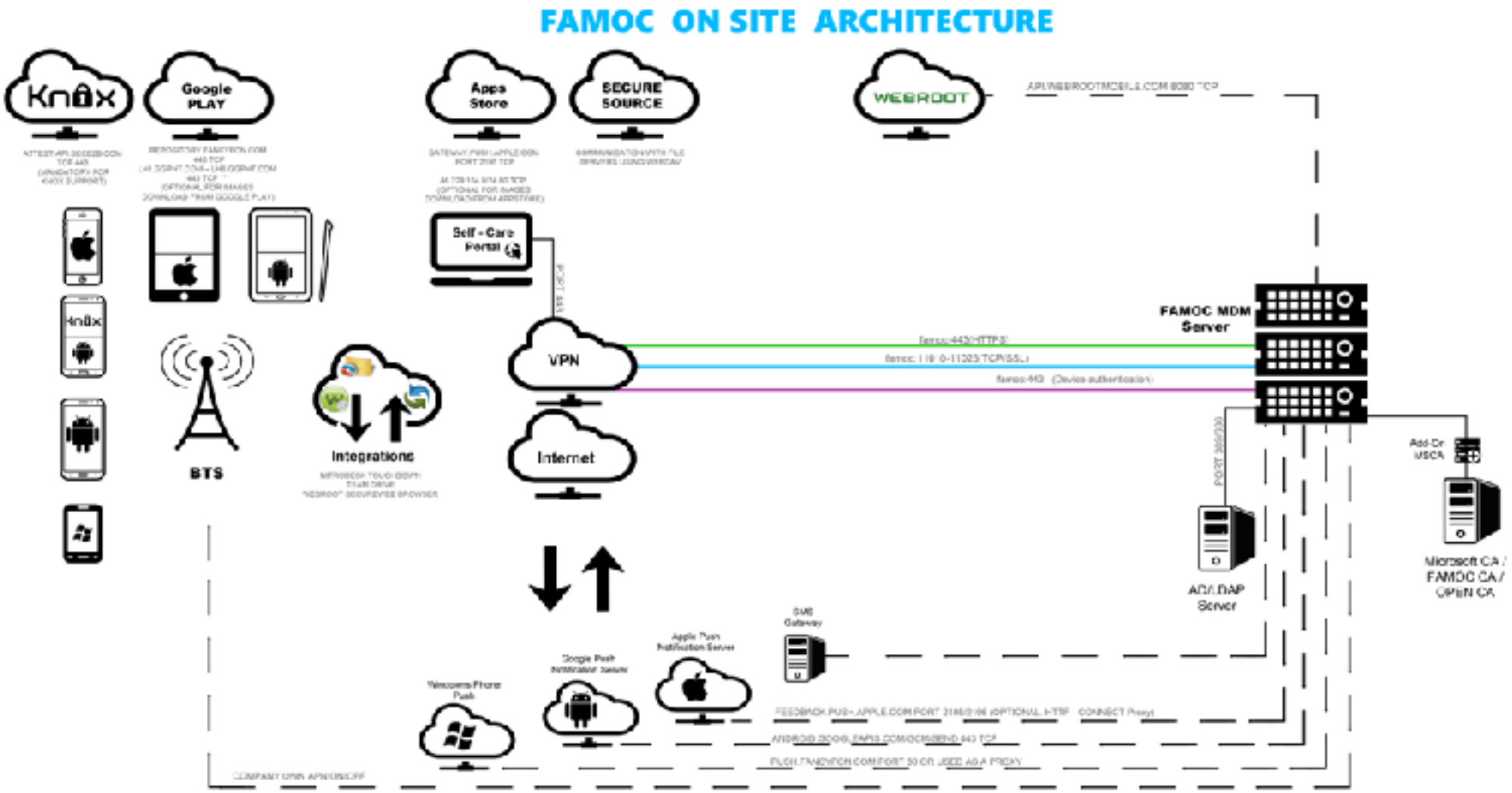
With KNOX Mobile Enrollment you can get devices into your MDM by uploading a spreadsheet or scanning the packaging with the mobile enrollment app

Then just hand the enrolled devices to users, turn them ON, connect to WiFi and mobile enrollment will push all the software to the devices to be installed and configured

FAMOC **VPN GATEWAY**



PRODUCT **ARCHITECTURE**



GOVERNMENT CUSTOMERS

MINISTERSTWO
INFRASTRUKTURY
I ROZWOJU

LOCAL AUTHORITIES AND **STATE FINANCIAL INSTITUTIONS**

NBP Narodowy Bank Polski

THE CENTRAL BANK OF HUNGARY

Diputació de Lleida
municipis, territori i tu

red.es

Ajuntament de Terrassa

BANCO DE LA NACION ARGENTINA

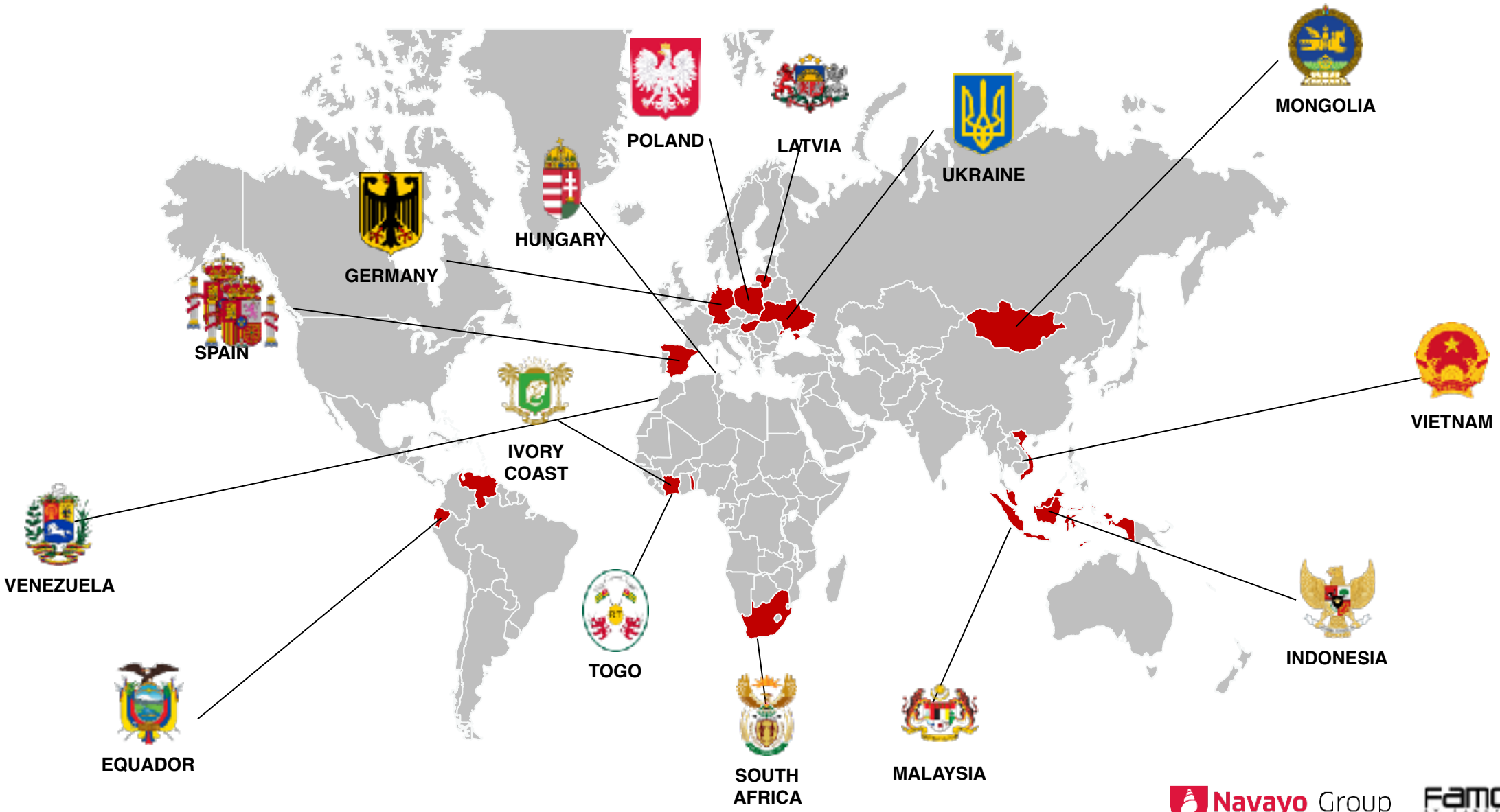
ALILAGUNA

נס-ציונה

Oelde

SAMORZĄD WOJEWÓDZTWA POMORSKIEGO

NAVAYO & FAMOC REFERENCES **BY COUNTRY**



Navayo Group Famoc

FANCYFON'S **UNIQUE DIFFERENTATIORS**

Purchase your own authentication server and create a closed communication system.

INDEPENDENT SOLUTION

OPEN FOR OWN DEVELOPMENT

SELF-PLANNED SECURITY ARCHITECTURE

MOBILE + DESKTOP MANAGEMENT

VPN + MVCN