isss, 9. – 10.4. dubna 2018

TAKTICKÝ KOMUNIKAČNÍ SYSTÉM ATOS HOOX

ATS - TELCOM PRAHA a.s. ®

TELEKOMUNIKAČNÍ SPOLEČNOST

PORTFOLIO SLUŽEB

Základním pilířem služeb je systémová integrace

Vlastníme certifikované týmy lidí

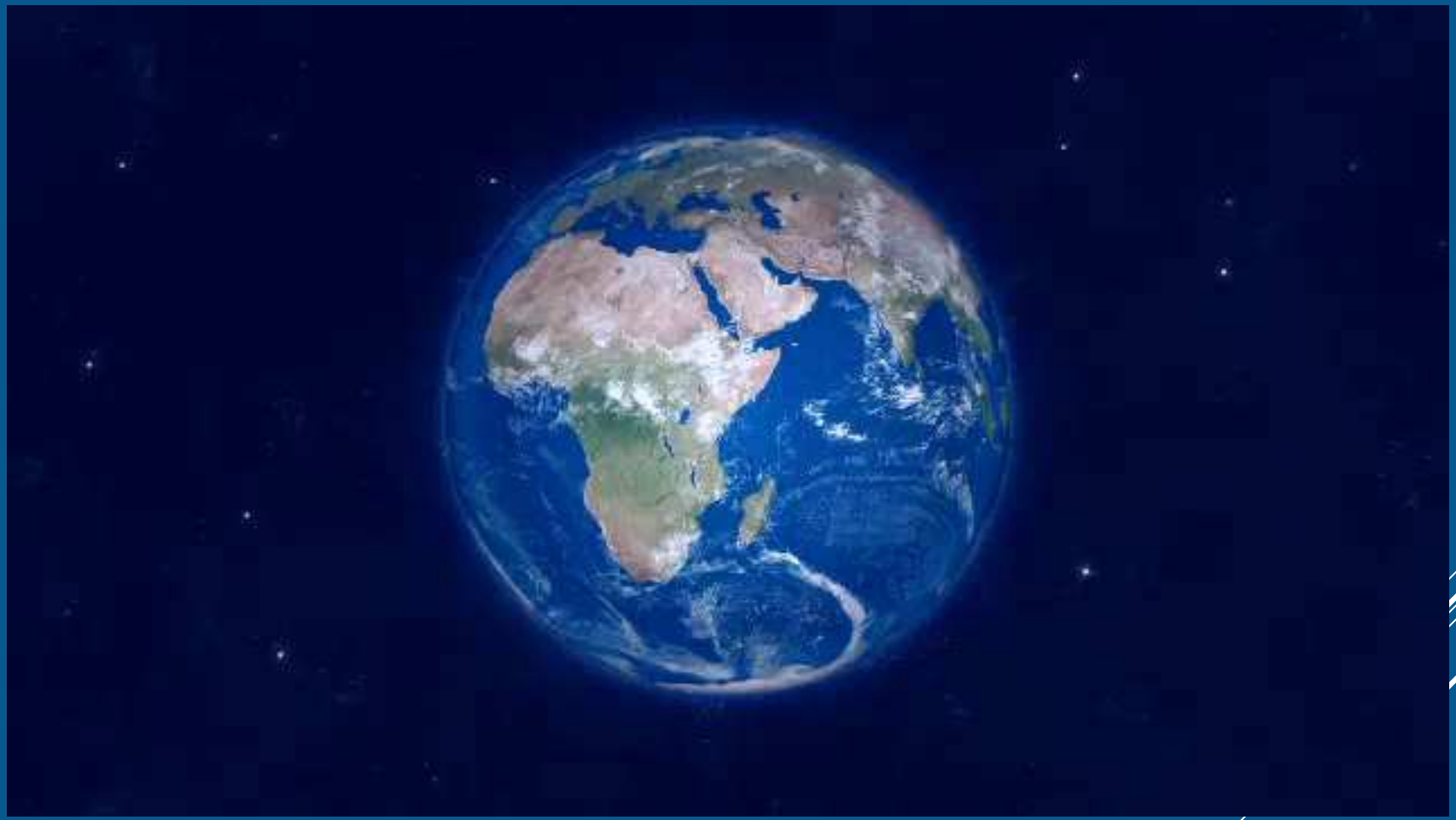
Implementujeme certifikované krypto prostředky

Implementujeme bezpečnostní a legislativní požadavky

Zavádíme procesy prevence a včasné reakce na bezpečnostní hrozby a incidenty v kritické infrastruktuře státu

Budujeme silné partnerství s výrobci bezpečnostních technologií

HOOX FOR MISSION



TACTICAL COMMUNICATION
PMR TO LTE MARKET

MARKET – CHALLENGES

FIELD COMMUNICATIONS FOR HOMELAND SECURITY

Growing threats

x9

Terrorist attacks increase in 15 years

Terrorism threat, bombings

$119 B

Loss from natural disasters

Natural disasters (forest fire, floods, cyclone…)

6700

Killed by technological disasters

Technological disasters (crashes, industrial accidents)

New technologies

Smartphones, IoT, applications…

Emerging new needs

Coordinate
fast and appropriate response in the field

Share reliably
video, images, information and voice, whatever the network conditions

Provide relevant information
on the crisis conditions, updated in near real time

TACTICAL COMMUNICATION – SITUATIONAL ANALYSIS

LEADING USAGE OF PROFESSIONAL MOBILE RADIO (PMR)

PMR is widely used in tactical communications

- **MoI**: police, intervention forces, border guards…
- **MoD**: homeland security & peacekeeping…
- **Other public services**: MoJ, firefighters, medical emergency services,
- **Private services**: transports

PMR offers:

Network availability
Highly resilient network and wide coverage

Confidentiality of voice communication
Private radio network

Critical communication features
Push-to-talk, closed user groups…

BUT … PMR network data sharing capacity is highly restrictive

LTE or LTE over PMR solutions

4G/LTE COMMUNICATION

TO ANSWER CURRENT AND FUTURE OPERATIONAL CHALLENGES

Today	Tomorrow:
▸ Real time position sharing ▸ Communication ▸ Video ▸ Multimedia exchanges ▸ Event management	▸ **Sensors (on human or for environment)** ▸ **IoT** ▸ **Drone control & feedback,** ▸ **Augmented reality** ▸ **Data analytics** ▸ **…**

New usages will guide the migration process from PMR to LTE

The migration path begin today, with first implementations over the world, and will end in 2025-2030

MIGRATION FROM PMR TO LTE
GAINS AND CHALLENGES

Gain #1
Data bandwidth
New usages, real time applications, multimedia, IOT, …

Gain #2
Existing public infrastructure
Fast and cost-effective deployment: LTE-based solution can use existing public networks.

Challenge #1
Cybersecurity
LTE = IP world. Smartphones = mass market products and operating system.
Welcome to cybersecurity threats!

Challenge #2
Network resilience
Public networks are not resilient and doesn't cover all locations.
Private LTE is part of the solution but is not available in all contexts.

Challenge #3
Applications
Business needs of a firefighter are not the same than a border guard or a maintenance technician.

Hoox for mission

Atos highly secure and resilient tactical LTE solution

HOOX FOR MISSION

OVERVIEW

Clear communication with standard phones

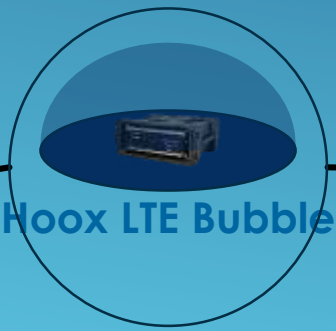
Secure communication with Hoox for business solution

Connection to HQ

Public network

Hoox Smartphone
Secure Android phone with mission-oriented features:
- Push-to-talk
- Blue force tracking

Hoox Hub
Carry-on module ensuring connection to multiple networks



Hoox LTE Bubble

Device-to-device

One single handheld for mission apps and voice

Always-on communication access No voice break

Deployable mission support

CHALLENGE #1: CYBERSECURITY
HOOX FOR MISSION ADDED VALUE

Based on Hoox technologies

- **Secure LTE Bubbles**
- **Secure Terminal & Hub**
  - Secure boot
  - Secure OS
    - Without google services & account
    - Controlled ports
- **Secure Communication**
  - End to end voice encryption
  - Secure conference call
  - Secure instant messages
  - Secure data
- **Secure Apps**
  - Private store, signature mechanism

Additional advantages

- Capacity to integrate local cryptography
- Use of NATO secret Hardware Security module

CHALLENGE #2: NETWORK RESILIENCE
HOOX FOR MISSION ADDED VALUE

On public network

- Optimized communication protocols to allow maximum of service even with a low network signal
- Solutions to improve coverage event on public network

On private network

- Range of Private LTE bubbles adapted at each kind of mission
- Optimized LTE architecture for mission critical contexts
  - Native Network federation
- Separate flows are to allow natively QOS (quality of service) LTE mechanisms

Without network

- Device to device capabilities to keep crucial features event when you have no network

CHALLENGE #3: APPLICATION
HOOX FOR MISSION APPROACH

Hoox for mission brings communication features	• Hoox legacy : secure voice, secure conference, secure group instant messaging with file transfer (WhatsApp like) • Dedicated for H4M : basic Push to talk and blue force tracking	
For advanced needs, we combine Hoox for Mission with	Atos solutions	AUXYLIUM, UNIFY, Bull BMS
	Third party solutions	StreamWIDE, LUCIAD, pushcom, SYSTEMATIC
	Adhoc dev.	Provided by Atos or local partner

Modular equipment

Catalog

HOOX SMARTPHONE (1/2)

What is it?

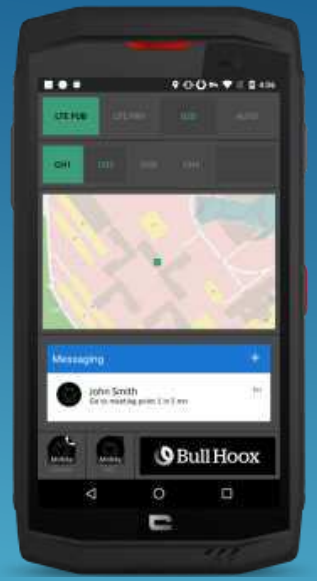
- An Android-based smartphone with **end-to-end security** (device, communication, applications)

Out-of-the-box functions

- Rugged terminal
- Encrypted communications (1to1, conference, message, mission-critical push-to-talk, VPN)
- Push-to-talk and position sharing
- Multiuser with QR code identification
- Can call non-Hoox phones with standard LTE
- Direct access to mission app, private app store

Customer-specific features

- Specific smartphone/tablet
- IMSI catcher detection, IMEI/IMSI lure



High-grade security

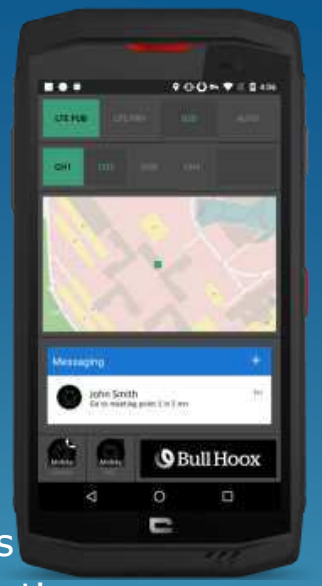
- Highly secured OS based on Android 6+
- Encrypted voice and data communications
- Secure ports for intrusion protection

HOOX SMARTPHONE (2/2)

DATASHEET

Hardware features

Features	Hoox T30
Android version basis	6.0
Screen	5"
Screen resolution	1920x1080
Screen resistance	Gorilla Class 4
Wet touch / gloves	Yes
RAM (GB)	3
ROM (GB)	32
External SD card	Yes
Fingerprint	No
Back Camera	16Mpx
Front Camera	8Mpx
Wireless networks support	2G/3G/4G
Wifi	Wi-Fi 802.11 b/g/n/ac
Bluetooth	v4.1 LE
SIM format	nano
Water resistant	IP67
Audio output	jack 3.5
USB	USB-C
NFC	No
GPS	GPS, A-GPS, Glonass, Beidou
Battery	Non-removable Li-Po 3500 mAh
Dimensions	155.7 x 81.8 x 14.3 mm
Weight	230



Software features

- Secure Terminal
  - Secure boot,
  - Hardened OS,
  - Controlled ports
- Secure Communications
  - Encrypted voice
  - Encrypted messages
  - Encrypted data
- Secure Apps
  - Private store
  - Signature mechanism
- Oriented mission GUI
  - Dedicated interface
  - Basic BFT/PTT

HOOX HUB (1/2)

What is it?

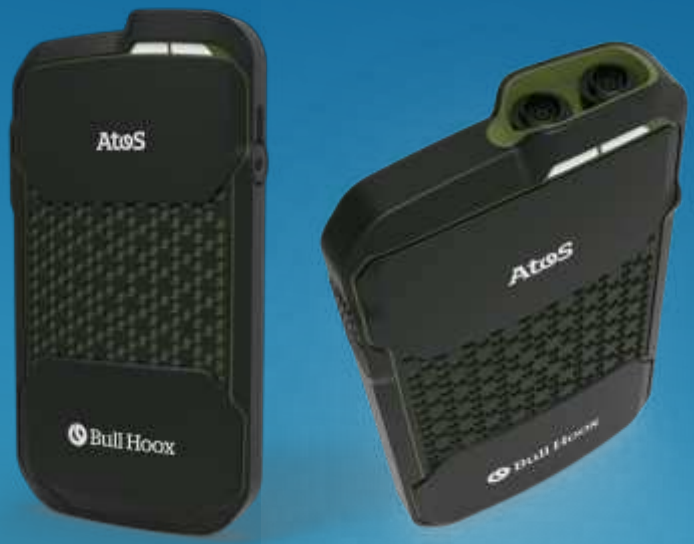
- A small portable multi-channel module that provides **communication resilience** to Hoox Smartphone

Out-of-the-box functions

- Switch between networks with no voice break
  - Large-band LTE (public wideband)
  - Specific-band LTE (e.g. b40, b28)
  - Device-to-device
- Automatic switch – or activated from Smartphone
- LED indicators (battery, network type and quality)

Customer-specific features

- Satellite connection, specific modem
- IMSI catcher detection, IMEI/IMSI lure



Brings strong network resilience

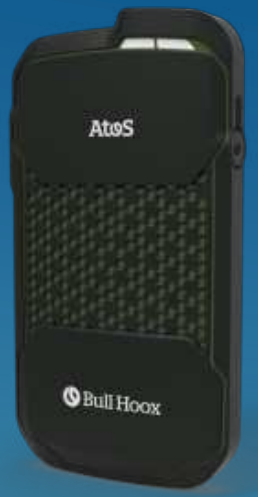
- Ensures access to available networks
- Switches transparently, no voice/data drop
- Rugged physical connections

Same high security as Hoox Smartphone

HOOX HUB (2/2)
DATASHEET

Hardware features

Features	Hoox T30
LTE modem 1	adaptable to public networks 3G/4G
LTE modem 2	adaptable to private LTE network (ie B28, B38, B40, B68 in europe)
D2D Modem	ISM bands
USB 1	micro-USB, power port
USB 2	micro-USB, peering port
Buttons	On/Off, network staus, battery status
Lights	Network status, battery staus
Battery	Removable Li-Po 5000 mAh
Dimensions	154 x 80 x 19 mm
Weight	260g



Software features

- Secure Device
  - Secure boot,
  - Hardened OS,
  - Controlled ports
  - Secure peering
- Resilient communications
  - Automatic switch between Public and private network
  - D2D mode in case of absence of network

HOOX LTE BUBBLE (2/2)

What is it?

- A range of tactical LTE bubbles (man pack, mobile, fixed)

Standard functions

- Man pack and (vehicle) transportable versions can be deployed for the mission
- Works in standalone or in connection with headquarters
- Connected to headquarters via fiber, microwave, public network, satellite
- The smartphones always benefit locally from secure communication features.
- Range: from 1 to 10 km if using Europe emission standards

Man pack

Transportable or fixed

Ensuring LTE resilience and security

- Very high local bandwidth
- Full LTE services to deployed users
- Independence from public network
- 100% access-controlled

HOOX LTE BUBBLE (2/2)
DATASHEET

Hardware features

Features	Hoox B1	Hoox B10
Usage	man pack	transportable, fixed
Bands	700 MHZ PPDR	Standard bands : 400-700-800-900 Mhs On demand bands : 1800-2100-2600 MHz
Channels	1,4-3-5-10 MHz	1,4-3-5-10-20 MHz
Emit Power	2x1W (mimo)	2x20w(mimo)
Consumption	50w	400w
External Port	USB, RJ45	USB, RJ45
Dimensions	310 x 205 x 90 mm	800 x 600 x 400 mm
Weight	7Kg (nude), 10Kg (manpack including battery)	45kg (including casing)
Water resistance	IP 67	IP54
Up and running	< 2 mn	< 5 mn

Software features

- Include Hoox Security Platform for communication encryption
- Automatic network federation between Bubbles

Zoom on security

SECURE COMMUNICATIONS

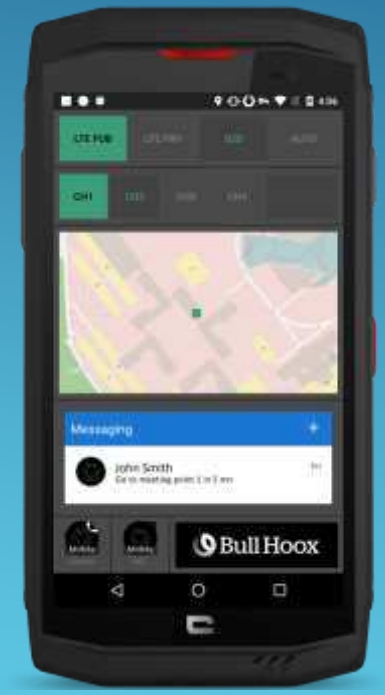
PREVENTION FROM EAVESDROPPING AND INTERCEPTION

- **Two ways to communicate with Hoox:**
  - **Secure communication with other Hoox users**
  - **Standard communication** (standard calls, standard SMS): same risks as with a standard smartphone
- **Hoox secured channel of communication:**
  - **Secure calls or conference calls**: voice calls are encrypted. Signaling uses SIP/TLS and voice data transfer uses SRTP Passthrough protocol (end-to-end encrypted call), 256-bit AES
  - **Instant messaging**: SIP/TLS, 256-bit AES
  - **Data**: all data exchanges (e.g. web browsing and mails) are going exclusively through a VPN. There is an IP tunneling which forces all connections from the mobile phone to the central system through the VPN; TLS.

SECURE CONNECTIONS

PREVENTION FROM OVER-THE-AIR INTRUSION

- All **wireless** features are strictly controlled
- Only fundamental features are kept
- All other functions are removed from the Hoox (not just deactivated)



4G/3G: IP tunneling and no MMS

Totally removed

Audio profile only (for car connection)

Hotspot connection only

No Wi-Fi tethering

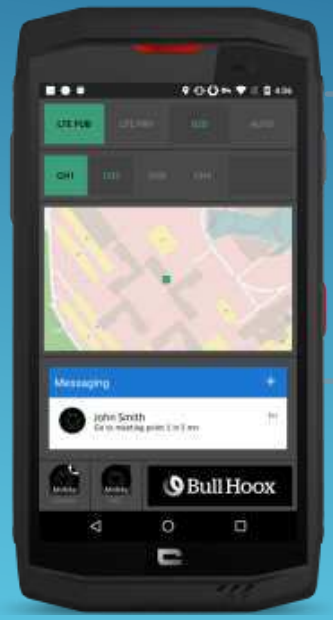
Other profiles removed

PROTECTED DEVICE

PREVENTION FROM EXTRACTION OF INFORMATION

USB

- USB is strictly controlled
- Only fundamental features are kept
  - File transfer (with security code)
  - 4G connection sharing
- All other functions are removed from the Hoox (not just deactivated)



A secure boot

- Data is encrypted
- Prevents from penetrating or changing something in the system

Security code

- After five tries, the Hoox is reset

PRIVATE STORE

PREVENTION FROM UNSAFE APPLICATIONS

- **Hoox smartphones include a private store**
  - **No public store** installed on the Hoox
  - **Only "signed by Atos" applications up for installation**: no other possibility to install an application (i.e. downloading by a file transfer)
- **Atos audits all applications for download in your private store**
  - Security policy compliance
  - Rights and permissions
  - Most inappropriate behaviors are detected (malware, virus, rootkit, unwanted connection to servers etc.)
- **Your own applications for download in your private store**
  - Possibility to **add your own applications** after an Atos audit and test.
  - Available **for your employees only**

FAQ

FREQUENTLY ASKED QUESTIONS NETWORK/LTE BUBBLES

- **Does Hoox for mission work on public network**
  - yes.
  - If you need to go in an uncovered zone or be independent of the telco operator, you need your own network provided by LTE Bubbles.
  - one important thing to mention is that our solution offer the capability to be operated on private and public network simultaneously in order offer the strongest system resilience and availability (network diversity).
- **Which frequencies/standard do we use for LTE bubbles?**
  - We use LTE standard bands and modulation. LTE, Long term Evolution uses the modulation format, OFDM - orthogonal frequency division multiplex, adapted to provide a multiple access scheme using OFDMA and SC-FDMA
  - LTE bands use frequencies between 700 and 2600Mhz. According to customer needs and local regulation (spectrum management) , we can propose the system in various configuration.
- **Which portability for LTE bubbles?**
  - We propose 2 sizes for LTE bubbles
    - Man pack (<10Kg), Transportable (~40 kg)
  - This elements can be integrated in various platform such as vehicles…

FREQUENTLY ASKED QUESTIONS NETWORK/LTE BUBBLES

- **Which range for LTE bubbles?**
  - From 3 to more than 20km, depending of power, frequency band and mast height
- **How do you deal with electronic warfare?**
  - as already mentioned, the system can be operated on 2 networks simultaneously offering, natively, a strong resilience against EW
  - in addition to the "network diversity" capability, system offers a device to device communication service that can be used in case of strong EW environment
  - as an alternative to prevent about being suppressed by electronic warfare solution, we can implement sniffer to detect it
    - a.Mobile device will include detector tool
    - b.Base station equipped with UE modem to detect
    - c.And we can propose to change the freq bandwidth in case of attack

FREQUENTLY ASKED QUESTIONS COMPETITION

- **What added value of Hoox against competition, like BlackBerry?**
  - Blackberry is a competitor on Hoox for business (daily standard communication), not on Hoox for mission (tactical communication)
  - Blackberry is proposed as a service only with limited guaranty to insure end to end security
  - You have to compare the full solution including servers, Mobile Application Management features and communication features. Hoox is providing fully ruggedized Android embedding natively the full features of secure communication (data, voice, IM, …).
  - The HSP (central system) is embedded into LTE bubbles, providing security even in a private LTE network

Ing. Vladimír BRENKUŠ, CISA

GSM: +420 602 226 229

email: brenkus@atstelcom.cz

ATS - TELCOM PRAHA a.s. ®

TELEKOMUNIKAČNÍ SPOLEČNOST