

Nový standard kritické komunikace MCX z pohledu kybernetické bezpečnosti

Řešení pro kritickou širokopásmovou mobilní komunikaci - MCX

Martin Bajer

2.9.2025

MCX

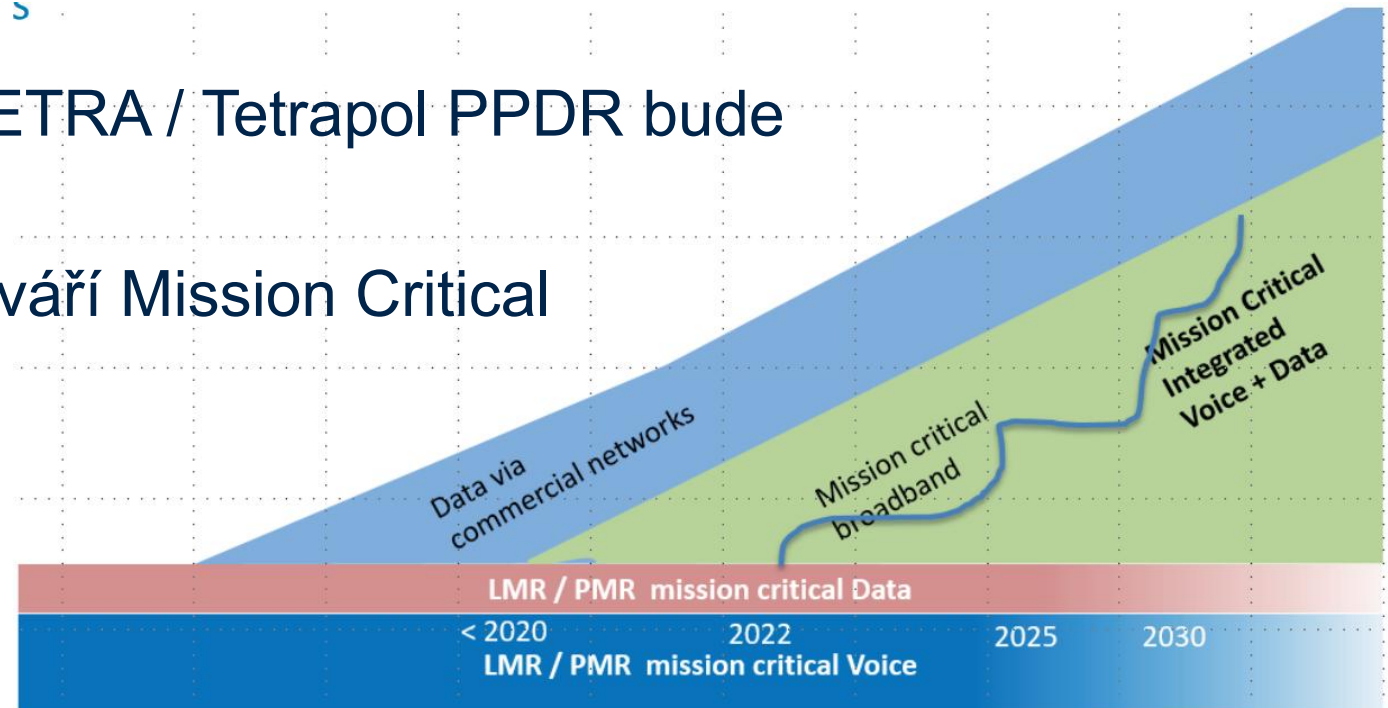
Zatímco tradiční úzkopásmové technologie pozemního mobilního rádia (LMR), jako jsou **systemy TETRA, DMR, P25 nebo TETRAPOL**, byly schopny splnit požadavky na hlasové volání push-to-talk (PTT), **nejsou schopny splnit rychle se měnící potřeby kritické komunikační infrastruktury**.

Služby Mission Critical (MCX) jsou **širokopásmové kritické komunikační aplikace** na základní 4G a **5G infrastrukturu**. Jejich cílem je zejména podpora ochrany veřejnosti a pomoc při mimořádných situacích a katastrofách.

Standardizace služeb MCX byla zahájena v roce 2013, jejím úkolem je definovat, vyvíjet a udržovat technické specifikace pro standardy služeb MCX včetně Mission Critical Push-To-Talk (**MCPTT**), Mission Critical Data (**MCData**) a Mission Critical Video (**MCVideo**).

Kritická mobilní komunikace - PPDR

- Public Protection & Disaster Relief (zkráceně PPDR) je systém ochrany veřejnosti a odstraňování následků živelných pohrom.
- TETRA, Tetrapol, P25, GSM-R se používají pro kritický hlas, ale mají omezené datové funkce.
- Většina národních operátorů TETRA / Tetrapol PPDR bude pokračovat do roku 2025/2030.
- 3GPP od března 2015 (4G) vytváří Mission Critical Specifications – tzv. Releases.
- Železnice přicházejí s řešením nové generace FRMCS postavené na MCX a 5G.



Vlastnosti řešení

Mission Critical Communication & Emergency Services

MESSAGING



Instant Messaging



Multimedia

VoIP & PTT



Push-to-Talk (MCPTT)



VoIP Calls



Call Conferencing



Advanced Telephony

GEOLOCATION



Geolocation



Geofencing



Beacons

VIDEO



Video Streaming



Video Calls



Screen sharing



Video Conferencing

EMERGENCY



Emergency Messages



Emergency Calls



Lone Worker Protection



Ambient listening call

Field Service Management

MY MISSION



Digital Forms



Digital Processes

MY TOOLS



Patrol Routes



Scheduling

API & SDK

API



API

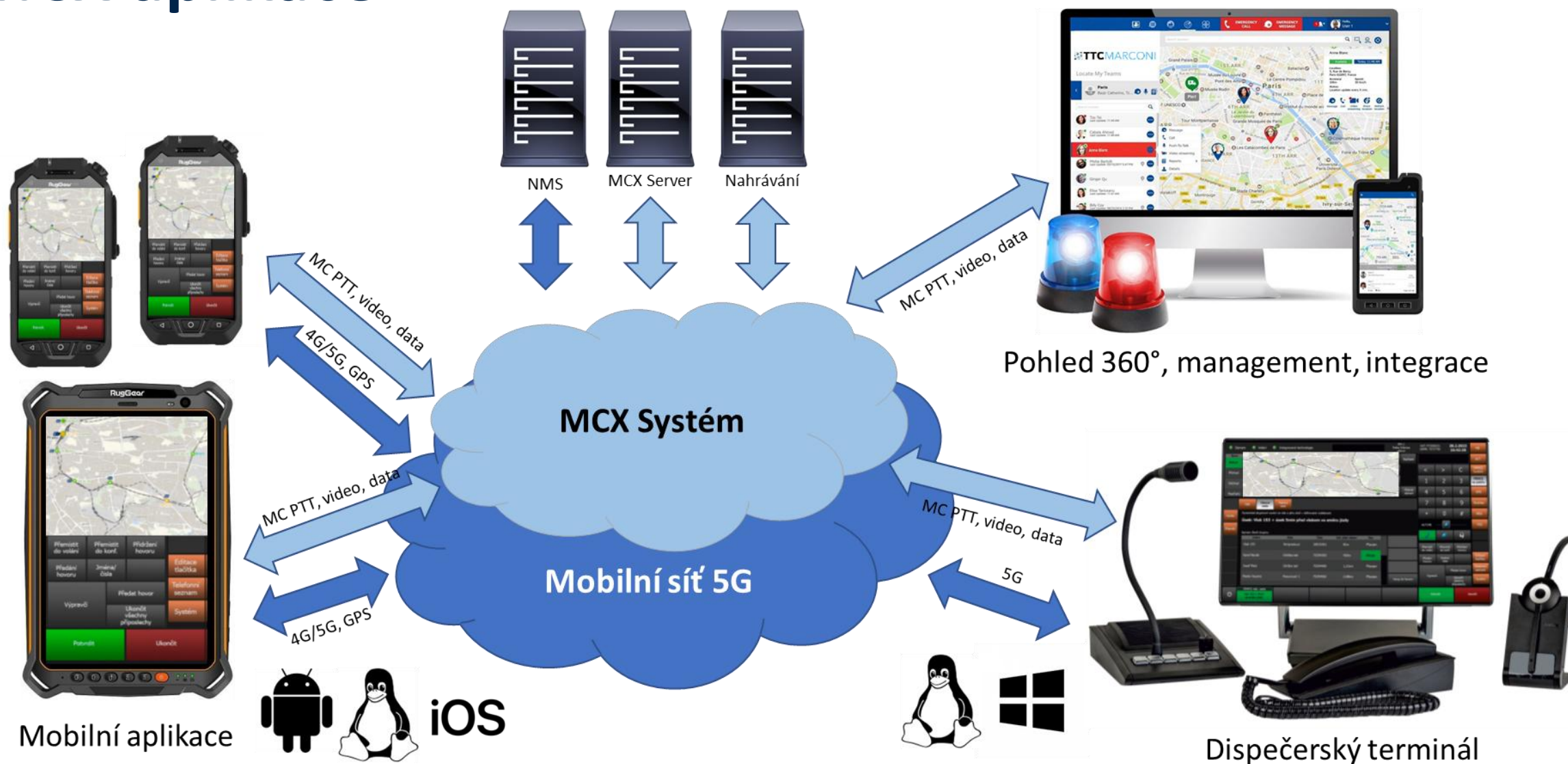
SDK



SDK

MCX aplikace

Program **TREND**



Multi Operator Core Networks – MOCN

- Sdílení RAN (Radio Access Network) s jedním nebo více mobilními operátory
- MOCN je definován v 3GPP TS 23.251 a TS 23.501, poskytuje nejvyšší úroveň zabezpečení, QoS a řízení
- Hlavní výhody MOCN:
 - Významné snížení nákladů (na budování a udržování vlastních rádiových stanic)
 - Zvýšení propustnosti (např. možnost použití kritického videa)
 - Zvýšení odolnosti (záloha v případě výpadku vyhrazené rádiové sítě železnice)
- Dnes se již využívá pro národní sítě kritické komunikace MCX (Finsko, Francie, USA, Jižní Korea...)

Čtyři vrstvy zabezpečení sítě 5G a MCX



Provozní proces

- Bezpečné provozní postupy, např. oddělení povinností, používání oprávnění
- Monitorování bezpečnostního výkonu, správa zranitelností a detekce útoků
- Reakce a obnova po narušení



Proces nasazení

- Návrh sítě s ohledem na bezpečnost a odolnost
- Konfigurace bezpečnostních parametrů, posílení



Proces vývoje produktů dodavatele

- Bezpečné hardwarové a softwarové komponenty
- Bezpečné vývojové procesy
- Správa verzí a bezpečná aktualizace softwaru



Proces standardizace telekomunikací

- Bezpečné protokoly, algoritmy, úložiště

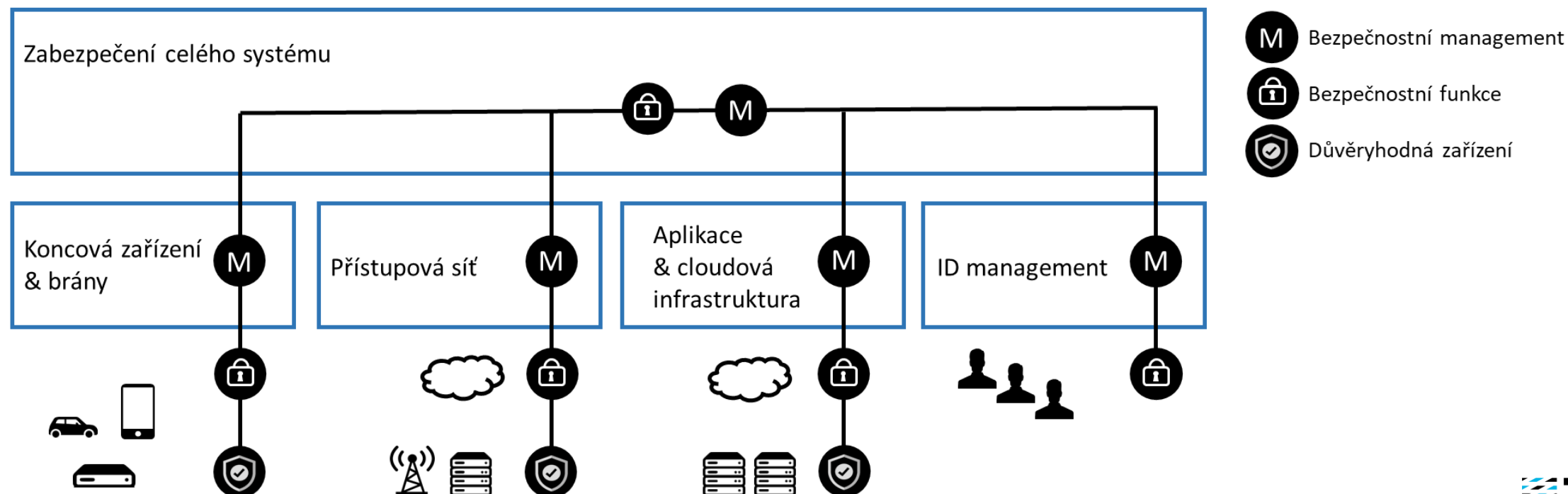
Architektura bezpečnosti v 5G

Zabezpečení v celém systému (horizontální zabezpečení)

- Úroveň sítě, slicing, zabezpečení na úrovni aplikace, ochrana důvěrnosti a integrity

Nasazení funkčních prvků 5G (vertikální zabezpečení)

- NFVi (virtualizované nebo cloudově nativní), funkce založené na zařízeních



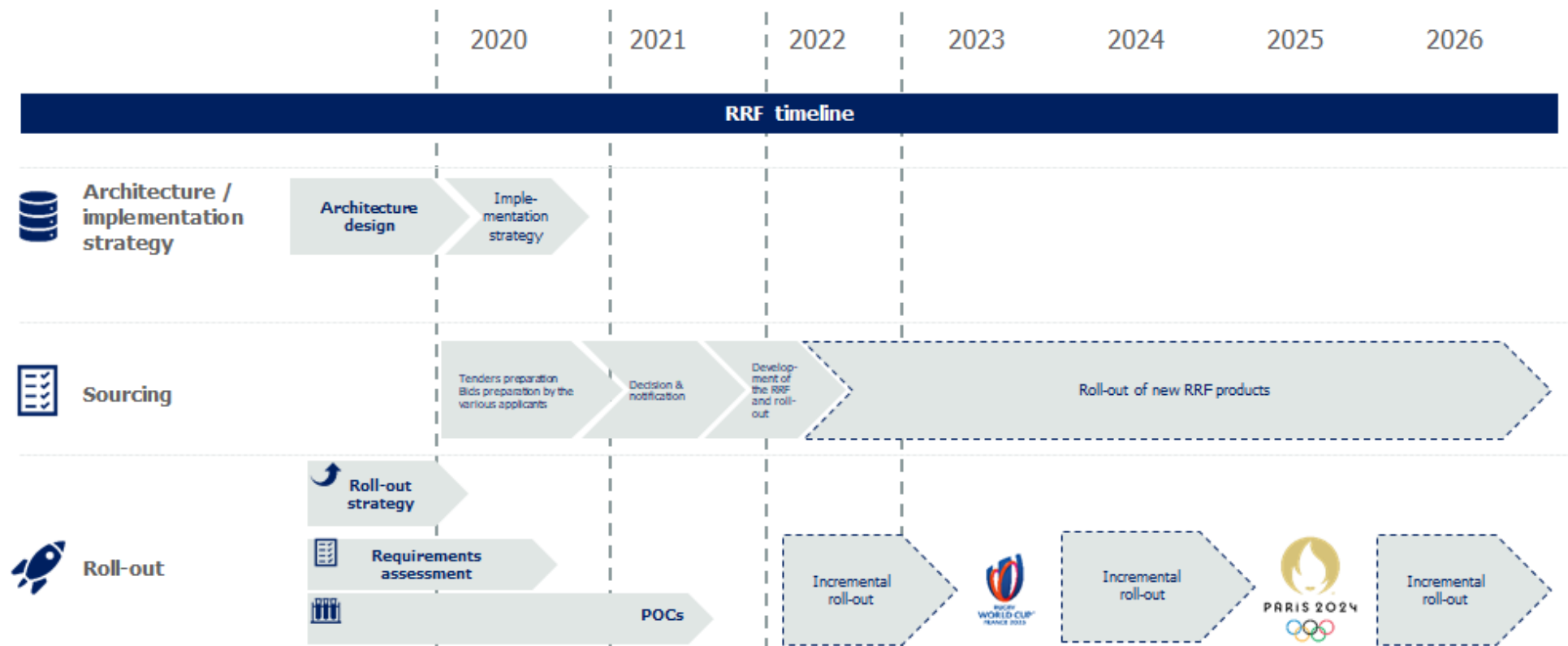
Bezpečnost řešení MCX

- Plně zabezpečené připojení aplikace PTT/serveru PTT přes TLS:
 - SIPS
 - HTTPS
 - Kryptografická sada: TLS 1.2, šifra až AES-256 a hash až SHA-512
- Bezpečná hlasová komunikace pomocí SRTP.
- Volitelně lze integrovat specifické šifrovací moduly.
- Vzdálené vymazání dat z řídicího centra v případě ztráty mobilu.
- Zablokování nebo odebrání přístupu uživatele ke službě.
- Zaměření na zabezpečení citlivých informací zahrnuje vzdálené ukládání aplikačních protokolů pomocí syslog a šifrování všech uložených hesel.
- Veškerá komunikace s externími systémy, jako jsou mapové servery nebo úzkopásmové brány PTT, je šifrována.
- Monitorování a auditování aplikačního serveru proti neoprávněným změnám a konfiguraci.



Nasazování MCX služeb ve světě

- Francie, RRF program (Réseau Radio du Futur Program) - náhrada systému Tetrapol



EUCCS Preparation

- Cílem přípravy EUCCS je pomoci při zavádění systému EU pro kritickou komunikaci (EUCCS) s cílem realizovat novou celoevropskou operační mobilitu: schopnost složek veřejné bezpečnosti:
 - provádět své operace, ať už se fyzicky nacházejí kdekoli a odkudkoli
 - kdykoli potřebují
 - s kýmkoli ve své komunikační skupině
- Složky záchrannářů potřebují lepší technologie, které jsou vhodné pro daný účel, fungují kdekoli, jsou bezpečné, spolehlivé a důvěryhodné. Geopolitické hranice by neměly být omezením
- EUCCS umožní operační mobilitu. Záchranáři budou moci provádět své operace kdekoli a kdykoli potřebují a spolupracovat s kýmkoli by měli.



Děkuji za pozornost

Třebohostická 987/5
100 00 Praha 10
+420 234 052 400
ttdm@ttc.cz