



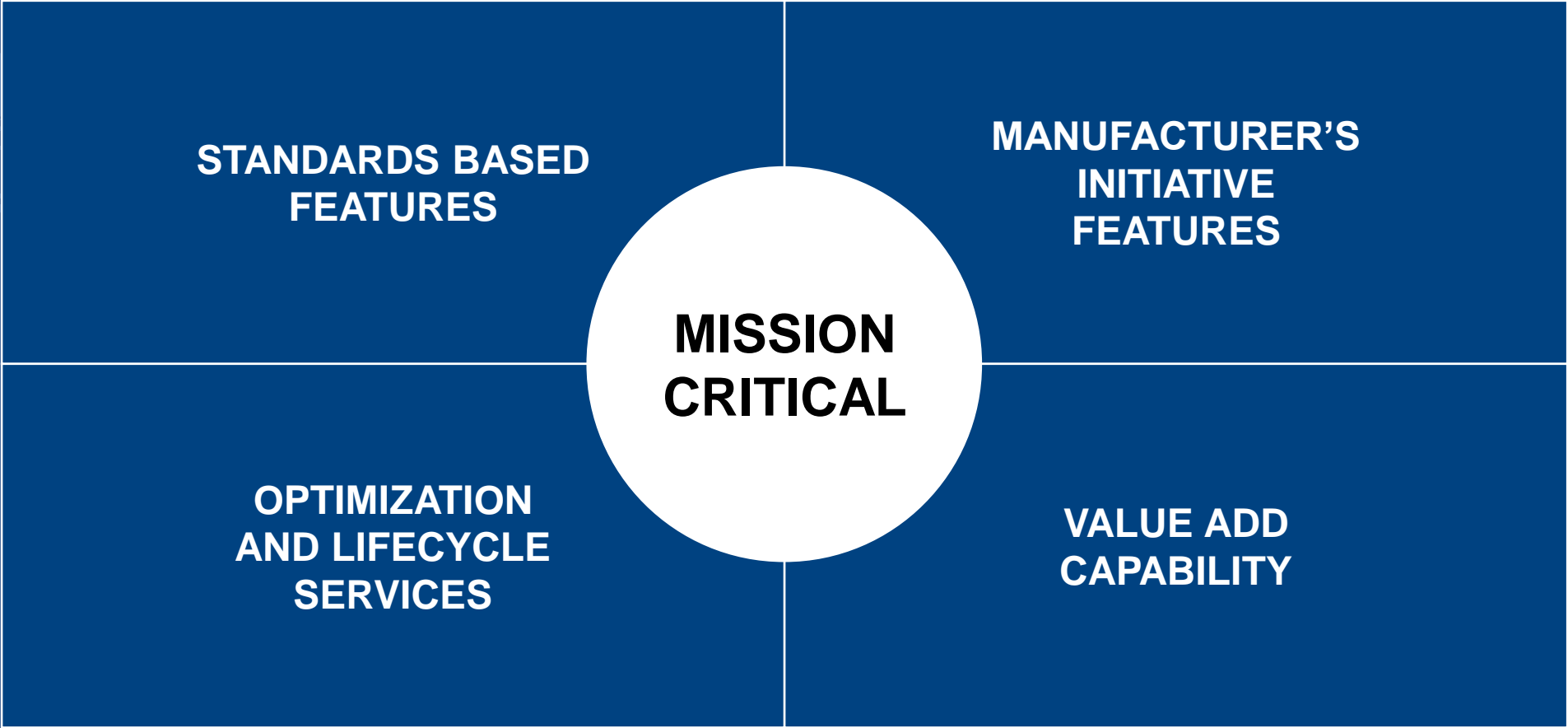
# DIMETRA SECURITY

MISSION CRITICAL  
COMMUNICATIONS



**MOTOROLA** SOLUTIONS

# FOUNDATIONS OF LMR MISSION CRITICAL COMMUNICATIONS



# **DIMETRA MISSION CRITICAL COMMUNICATIONS**



## **STANDARDS BASED FEATURES**

- Fixed Network Trunked
- Integrated voice and data
- Integrated command & control
- Authentication
- Air Interface Encryption
- Packet data
- Direct mode operation
- TETRA Enhanced data
- Inter-system interface

## **MANUFACTURER'S INITIATIVE FEATURES**

- Agency Priority Matrix
- Valid site profiles
- Object call
- Announcement TG

## **OPTIMIZATION AND LIFECYCLE SERVICES**

- Security Update Service
- System Upgrade Agreement
- Migration Assurance Program
- Software Maintenance Agreement

## **VALUE ADD CAPABILITY**

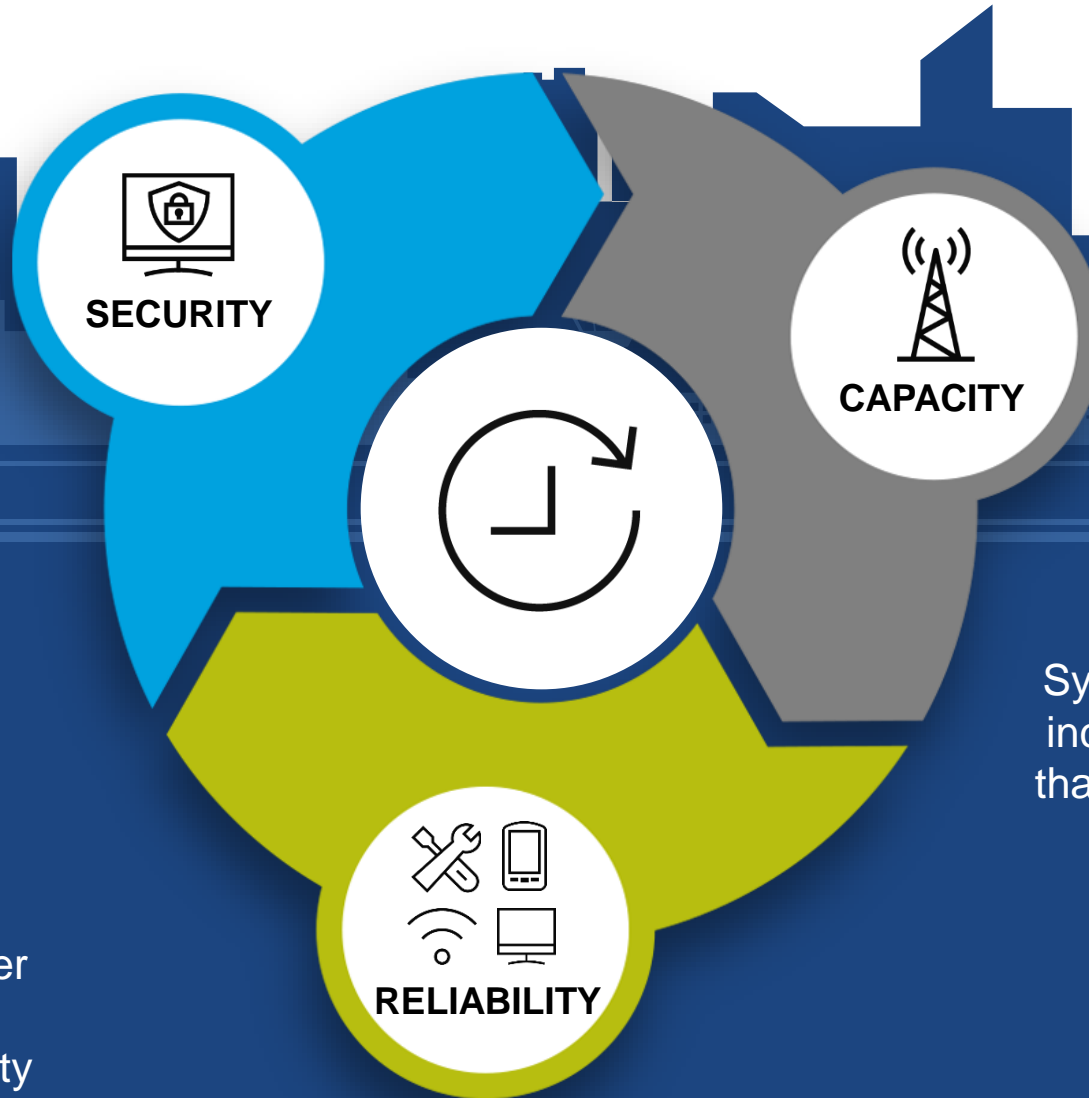
- Agency Priority Matrix
- WAVE PTX
- Advanced Air Interface Encryption (AIE) security (Class 3G)
- End-To-End Encryption (E2EE)
- Cyber Security
- Data Applications
- System Resiliency
- Software Expansions
- Enhanced Command & Control

**DIMETRA**



# MISSION CRITICAL FRAMEWORK

## THREE PILLARS OF MISSION CRITICAL COMMUNICATIONS



### SECURITY

The security and integrity of the system is maintained with an impenetrable layered defence architecture

### RELIABILITY

System is always available no matter what the circumstances due to the unique layered redundancy capability

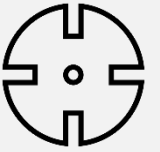
### CAPACITY

Systems able to cope with extreme increases in capacity requirements thanks to best in class features and monitoring capability

ENSURING SERVICES ARE ALWAYS AVAILABLE



# INDUSTRY BEST PRACTICES



## PRIME REFERENCES FOR MOTOROLA SOLUTIONS



- NIST Cybersecurity Framework (CSF)
- NIST 800-53 – Controls
- NIST CSF maps to ISO 27001
- FIPS 140-2



- OWASP - Open Web Application Security Project
- Top 10 Most Critical Web App. Security Risks

## ALSO TAKES INTO ACCOUNT



- CIS - Center for Internet Security (20 Controls and Benchmarks) globally recognized standards and best practices



- ISO 27001 - Specification for an Information Security Management System (ISMS)





# COMPREHENSIVE SUPPORT FOR EVERY PHASE OF THE NIST FRAMEWORK



## AN ORGANISATION-WIDE APPROACH TO SECURITY

Today organisation must adopt a holistic and organisation-wide based approach to security against a recognised international framework.

Motorola Solutions has adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework. NIST focuses on mitigation options, continuous monitoring, diagnosis and remediation.

### CYBERSECURITY FRAMEWORK

### SYSTEMATIC ANALYSIS AND PLAN



#### **IDENTIFY** Assess Risk

- Provide a thorough risk analysis
- Uncover potential vulnerabilities



#### **PROTECT** Develop Safeguards

- Develop policies and procedures
- Implement appropriate access and auditing control



#### **DETECT** Make Timely Discoveries

- Continuous monitoring 24x7x365
- Enable auditing capabilities



#### **RESPOND** Take Action

- Establish a robust response plan
- Create, analyze, triage and respond to detected events



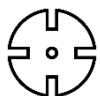
#### **RECOVER** Restore Functionality

- Institute a robust response plan
- Create improvements to prevent future attacks



# COMPREHENSIVE SUPPORT FOR EVERY PHASE OF THE NIST FRAMEWORK

## NIST PRODUCTS AND SERVICES MAPPING



### IDENTIFY

#### Asset Management

- Systems staging centers inventory database
- Open Source Review Board provides approval for use of open source documents

#### Business Environment

- Strategy planning and priorities aligned to support vertical markets

#### Governance

- Governance broad handling Governance, Risks and Compliance by creation of policies, standards and procedures

#### Risk Assessment

- Secure Design Review and Audit
- Vulnerability scanning, remediation and intelligence

#### Risk Management Strategy

- Dedicated team actively monitoring and collecting threat information

#### Supply Chain Risk Management

- Supplier qualification and assessment



### PROTECT

#### Identity Management, Authentication & Access Control Awareness & Training

- Extensive security training

#### Data Security

- Appropriate controls on policies and risk strategy

#### Info Protection & Procedures

- Secure software development lifecycle

#### Maintenance

- Pre-tested Patch and AV updates

#### Protective Technologies

- Common hardening benchmarks



### DETECT

#### Detect Anomalies & Events

- Abuse/Misuse case testing
- Audit logging
- In-field security assessments

#### Security Continuous Monitoring

- Security Operation Center Monitoring
- Anti-malware and event reporting

#### Detection Process

- In-field security assessments



### RESPOND

#### Response Planning Communications

- Coordinated communications

#### Analysis

- Vulnerability investigation

#### Mitigation

- Security Operation Centers and Call Centers can remotely access the supported systems in order to quickly take action

#### Improvements

- SOC incident notification



### RECOVER

#### Assisted System Restoration Recovery Planning

- Assisted system restoration
- Loaner program

#### Improvements






- Lessons learned and Process

#### Communications



# INFORMATION SECURITY DIMETRA FEATURE AND SERVICE ALIGNMENT AGAINST THE NIST

COUNTERING EVOLVING THREATS - MULTI LAYERED DEFENCE

	<div><u>COMMUNICATIONS CONFIDENTIALITY</u><ul style="list-style-type: none"><li>• <u>E2EE Voice, Short and Packet Data</u></li><li>• <u>AIE Cryptographic Separation (GCK)</u></li><li>• <u>Over The Air Re-keying (OTAR)</u></li><li>• <u>IPSEC Link Encryption (SHA-2)</u></li><li>• <u>Air Interface Encryption (AIE)</u></li><li>• <u>Authentication / Mutual Authentication</u></li></ul></div>	<div><u>INTRUSION DETECTION</u></div>		
<div><u>VULNERABILITY SCANNING REMEDIATION</u></div>	<div><u>NETWORK BASED CONTROLS</u><ul style="list-style-type: none"><li>• <u>Perimeter Protection</u></li><li>• <u>Remote Control Site Access Control Lists</u></li></ul></div>	<div><u>UEM NORTH BOUND</u></div>		
<div><u>SECURITY STANDARDS</u></div>	<div><u>IDENTITY AND ACCESS MANAGEMENT</u><ul style="list-style-type: none"><li>• <u>2-Factor Authentication</u></li></ul></div>	<div><u>SYSTEM LOGGING</u></div>		
<div><u>SECURITY BY DESIGN</u></div>	<div><u>HOST BASED CONTROLS</u><ul style="list-style-type: none"><li>• <u>System Hardening</u></li><li>• <u>OS Patching (Windows and LINUX)</u></li><li>• <u>Antivirus and Updates</u></li></ul></div>	<div><u>NOTIFICATION OF UNAUTHORISED ACCESS ATTEMPTS</u></div>	<div><u>VULNERABILITY MANAGEMENT LIFECYCLE (GA – Q2'2021)</u></div>	<div><u>ENHANCED SOFTWARE UPGRADE BACKUP / RESTORE</u></div>
<div> <u>IDENTIFY</u></div>	<div> <u>PROTECT</u></div>	<div> <u>DETECT</u></div>	<div> <u>RESPOND</u></div>	<div> <u>RECOVER</u></div>
<div>ASSESS RISKS</div>	<div>DEVELOP SAFEGUARDS</div>	<div>MAKE TIMELY DISCOVERIES</div>	<div>TAKE ACTION</div>	<div>RESTORE FUNCTIONALITY</div>







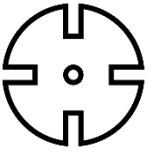
# IDENTIFY

ASSESES RISK

- SECURITY BY DESIGN
- SECURITY STANDARDS
- VULNERABILITY SCANNING  
REMEDATION



# MOTOROLA SOLUTIONS APPROACH TO SECURITY

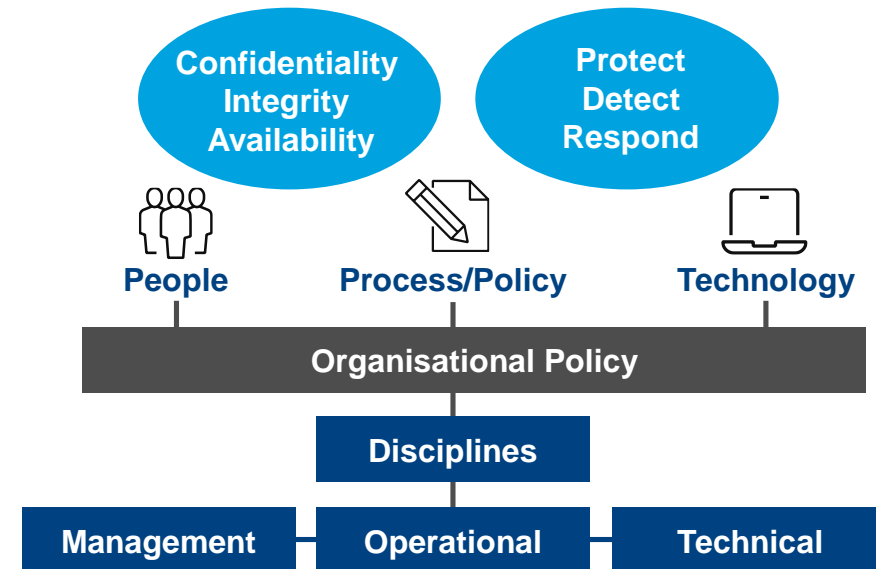


## SECURITY BY DESIGN

- Covers product development, implementation and operational support lifecycle
- Based on three foundational pillars:
  - Confidentiality
  - Integrity
  - Availability
- The pillars are addressed via the application of the following controls (as identified in the NIST Framework):
  - Protect
  - Detect
  - Respond

### Motorola Solutions Cybersecurity Framework: A Holistic, Risk-Based Approach

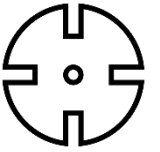
Governance and Oversight Throughout the Product Development,  
Implementation and Operational Support Lifecycle



Holistic Risk Management-based approach  
instead of Check-in-the-Box mindset







# MINIMUM SECURITY STANDARD

## SECURITY BY DESIGN

- The purpose of the minimum security standard is to provide cyber security standards for all of Products and Services developed and sold by Motorola Solutions
- The standard complements Motorola Solutions Products and Services Foundational Cybersecurity Policies by providing an additional level of detail
- The standard focus primarily on the following:
  - **IDENTIFY**
    - Asset Management
    - Vulnerability Management
  - **PROTECT**
    - Delivery of Software Updates
      - Regular
      - Out of band Emergency
    - Access Control
    - Audit Log Generation
    - Boundary / Perimeter Defence
    - Data Protection
  - **DETECT**
    - Malicious Code Protection
  - **RESPOND**
    - Backup / Restore



# VULNERABILITY SCANNING AND REMEDiation



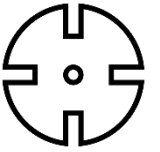
## SECURITY BY DESIGN

- Motorola Solutions has a structured approach to the development of the solutions that it sells, based on the D-Gates process
- Software is developed in 'sprints' of 90 days duration using the SafeAgile methodology, within the various individual software development teams ('box' teams) responsible for particular capabilities e.g. call processing, network management etc
- As part of the development process Motorola Solutions operates a policy of continuous integration and validation
  - Ensures end-to-end traceability from requirements, through design to final verification
  - Validation and verification is carried out at the unit/module, application and system levels
- Credential based security vulnerability scanning is conducted throughout the development process





# THE CYBER SECURITY CHALLENGE



**OUTDATED  
SYSTEMS**



**INCREASING  
COMPLEXITY**



**DWELL TIME:  
access time in  
network undetected**



**BREACHES  
or ATTACKS**

**The Challenge is to stay updated** and current with solutions matching the increasing diversity of threats

**Need a shift to the right** – traditionally focused on **Prevent**; need to enhance with **Detect, Respond** and **Recover**





# PROTECT

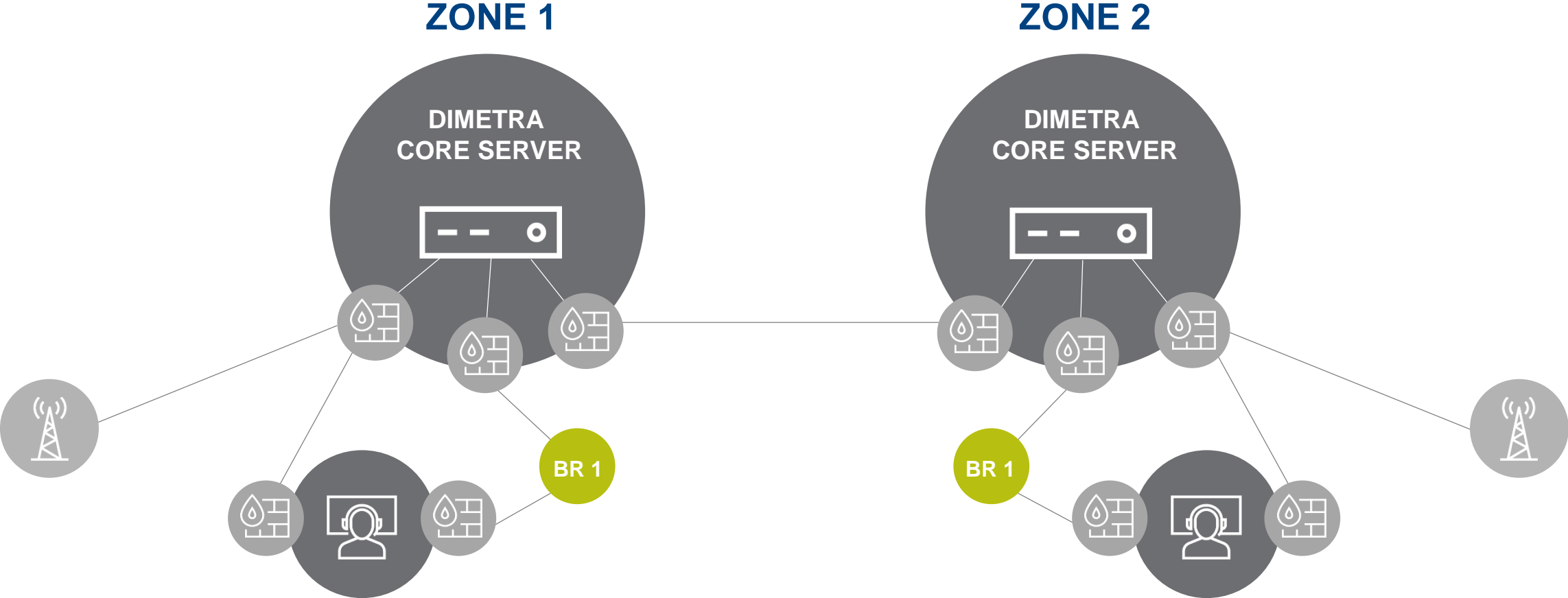
DEVELOP SAFEGUARDS

- HOST BASED CONTROLS
- IDENTITY AND ACCESS MANAGEMENT
- NETWORK BASED CONTROLS
- COMMUNICATIONS CONFIDENTIALITY

# Protection

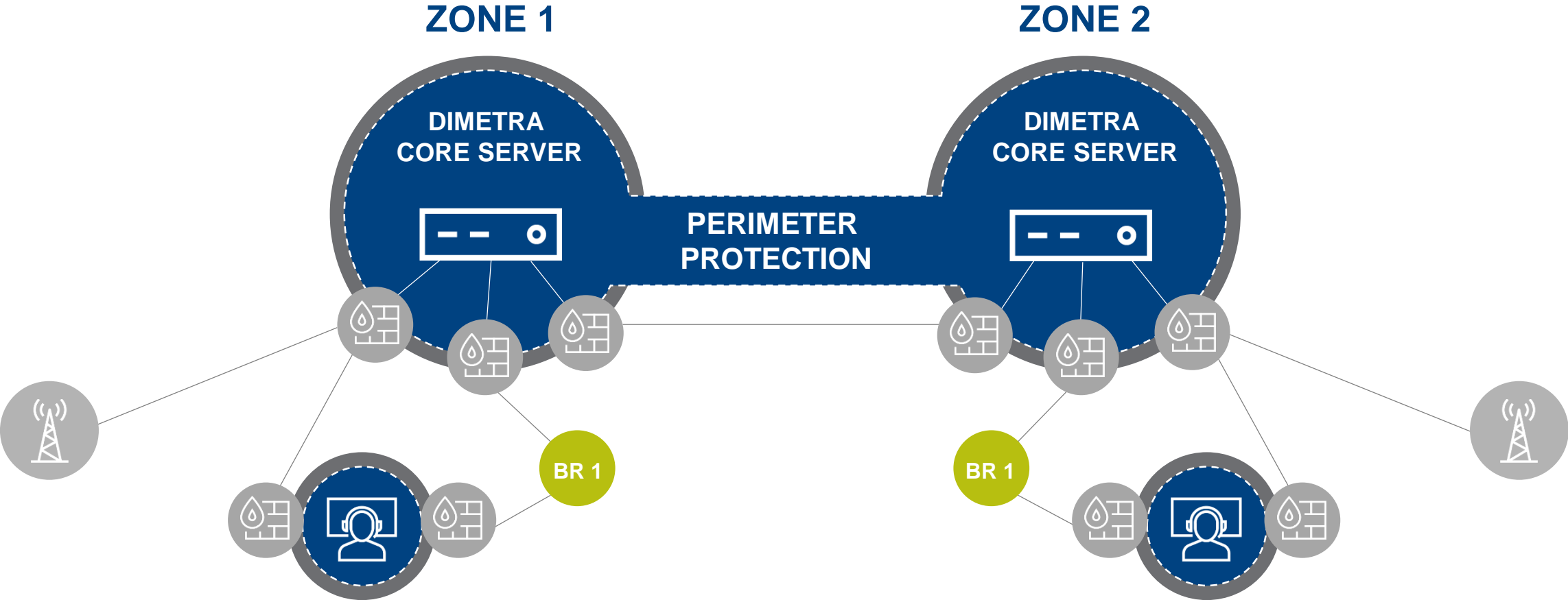


# LAYERS OF NETWORK SECURITY



# LAYERS OF NETWORK SECURITY

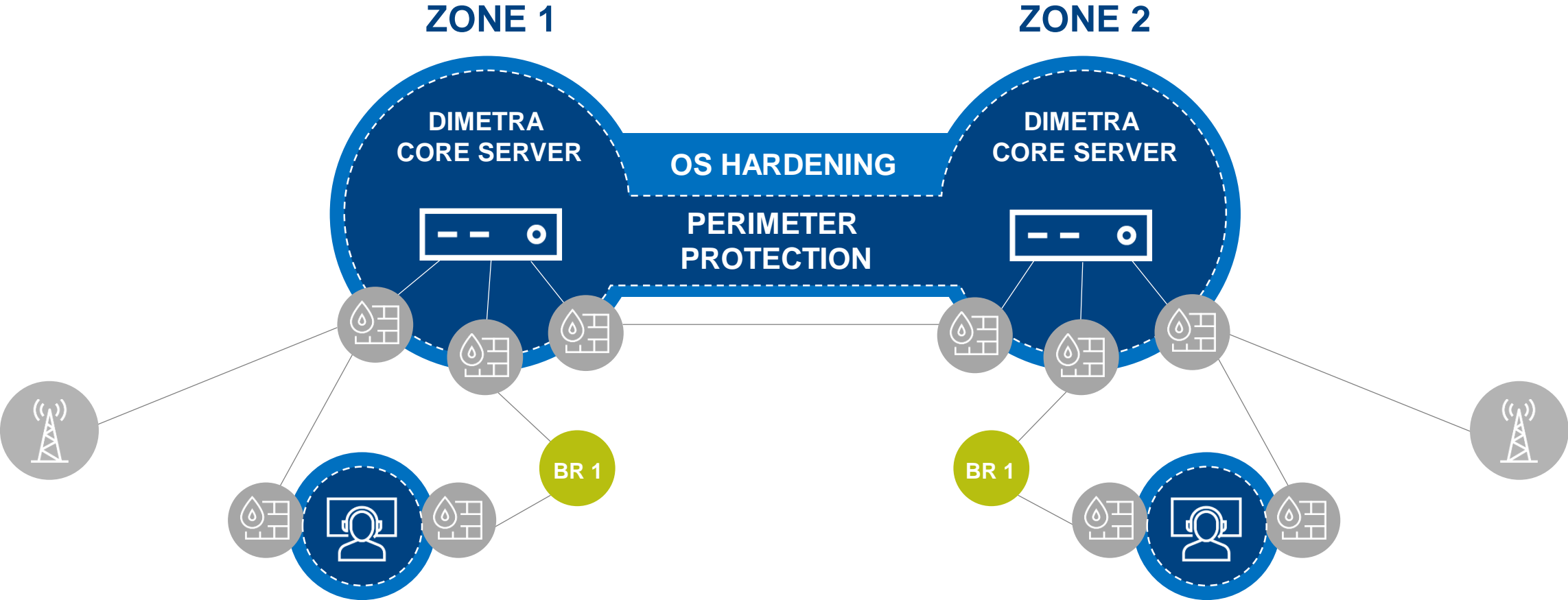
## PERIMETER PROTECTION





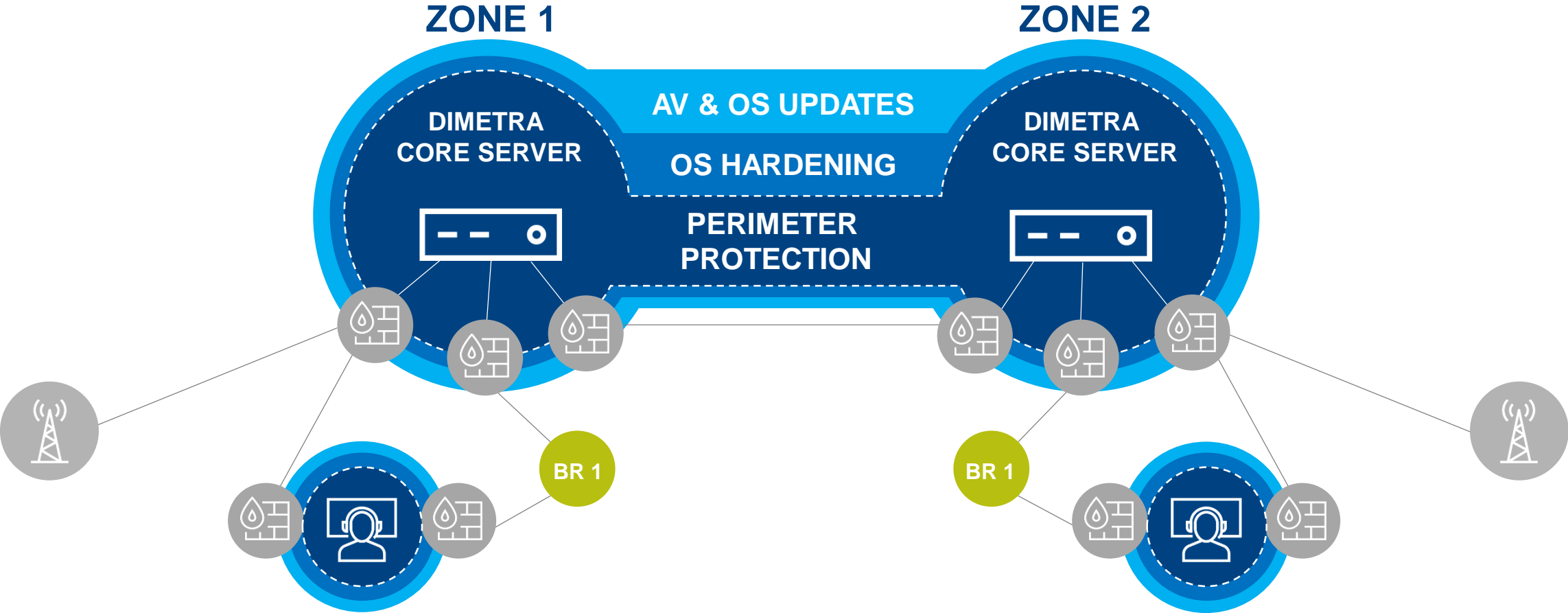
# LAYERS OF NETWORK SECURITY

OS HARDENING



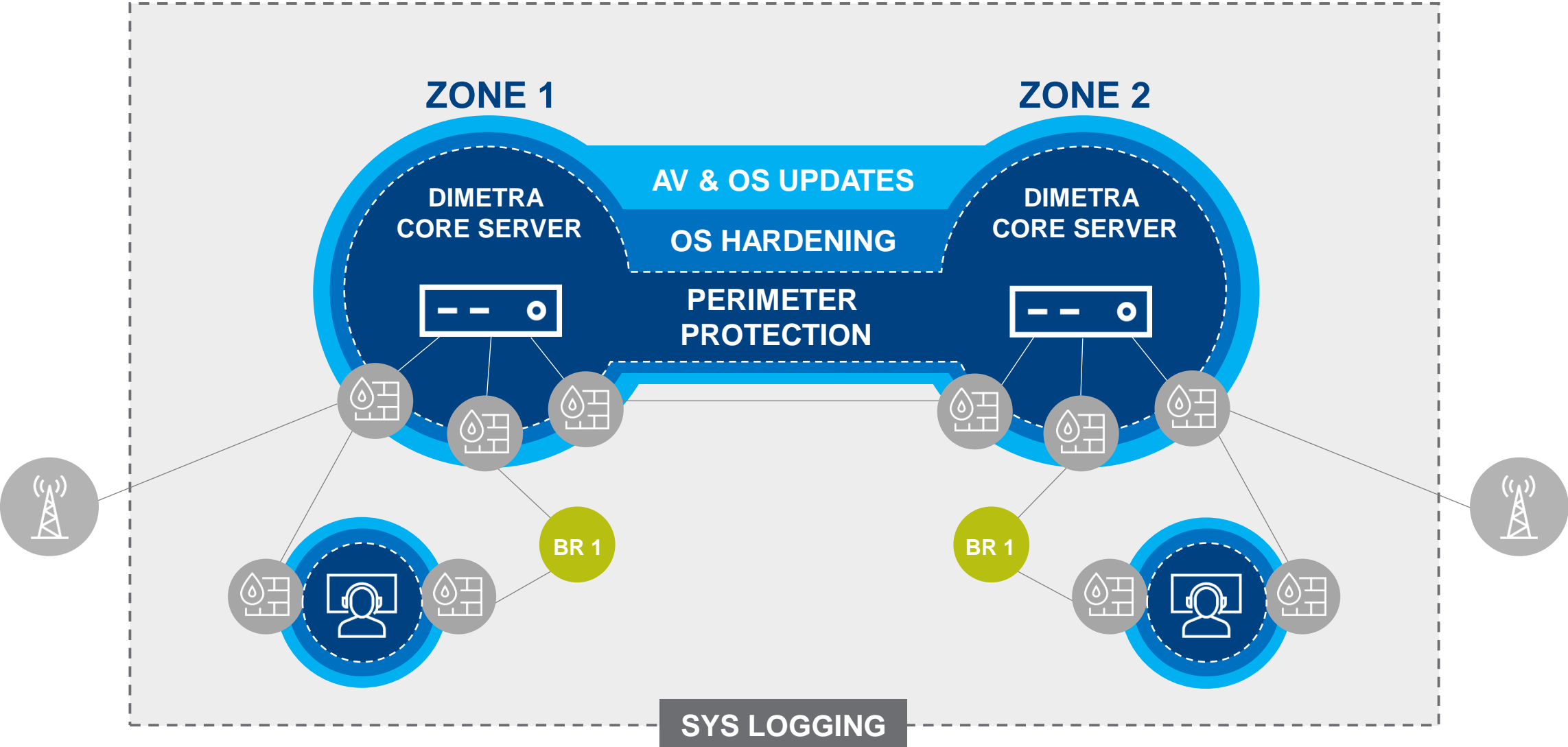
# LAYERS OF NETWORK SECURITY

ANTIVIRUS AND OPERATING SYSTEM SECURITY UPDATES



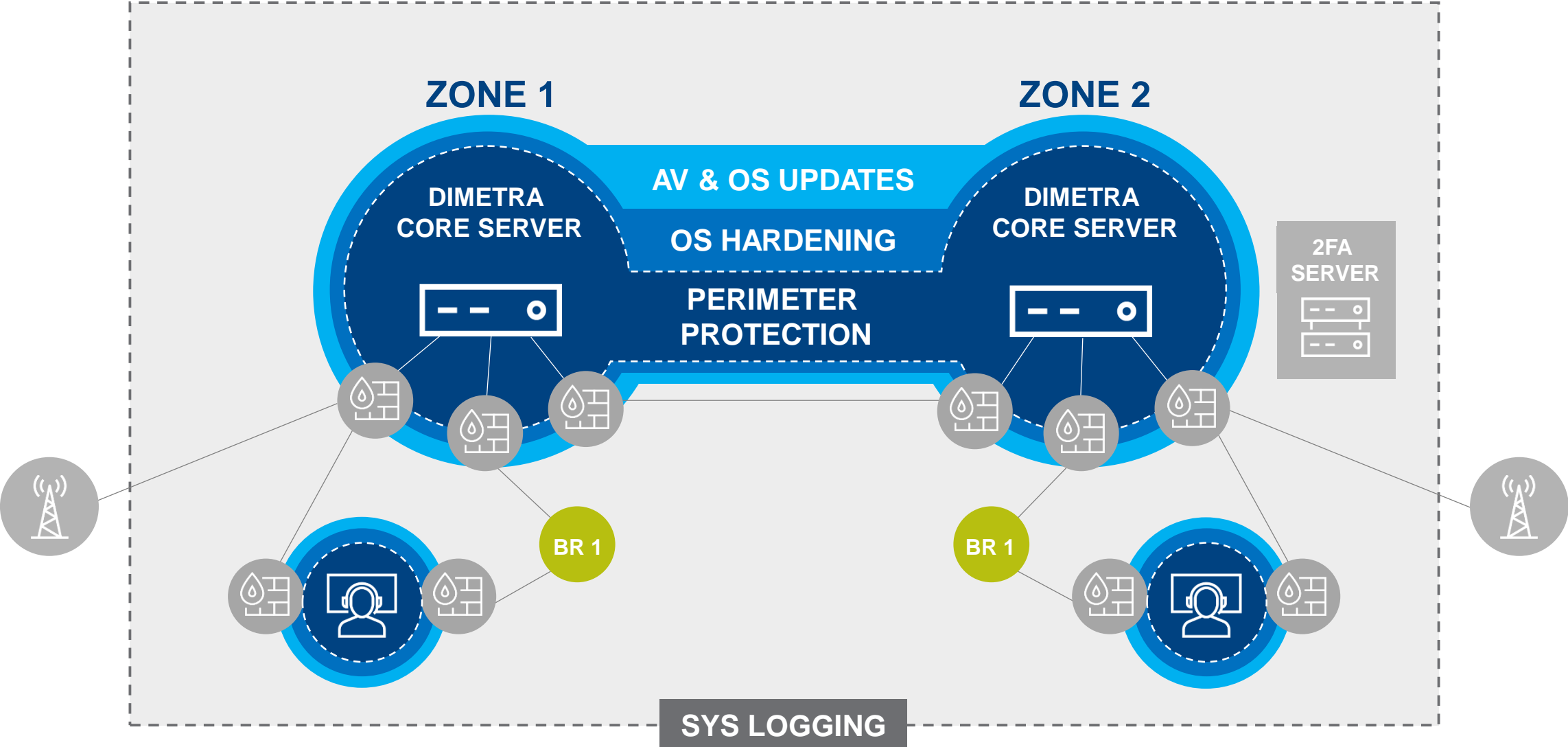
# LAYERS OF NETWORK SECURITY

SYS LOGGING



# LAYERS OF NETWORK SECURITY

## TWO-FACTOR AUTHENTICATION







# HOST BASED CONTROLS

SYSTEM HARDENING

---

OS PATCHING (WINDOWS AND LINUX)

---

ANTIVIRUS AND UPDATES





# HOST BASED CONTROLS

SYSTEM HARDENING

---

OS PATCHING (WINDOWS AND LINUX)

---

ANTIVIRUS AND UPDATES





# SYSTEM HARDENING

- What is hardening?
  - Most operating systems are inherently insecure which leaves them open to cyber attack. The purpose of system hardening is to eliminate as many security risks as possible. This is done by removing all non-essential software programs, services and utilities from them
- Why harden?
  - To help protect DIMETRA from cyber attacks and potential loss of service / disruption to the Users Communications i.e. to protect their 'Life Line'
- Hardening Benchmarks
  - Motorola Solutions adheres to the US Department of Defence Security Technical Implementation Guide's (STIG's) for the hardening of DIMETRA
    - STIG's are guidelines for standardising security within networks, servers and computers
    - When implemented these guides, enhance the security of the software and the, hardware to reduce vulnerability to cyber attack
    - The hardening settings are regularly reviewed in DIMETRA and updated as part of every Major Release (SR) / System Enhancement Release (SER)





# HOST BASED CONTROLS

SYSTEM HARDENING



OS PATCHING (WINDOWS AND LINUX)



ANTIVIRUS AND UPDATES







# OS SECURITY PATCH UPDATES

## WINDOWS AND LINUX

- OS security updates (patches) provided via SUS portal:
  - Windows - Monthly
  - Linux - Quarterly
- Deployed using MotoPatch process
  - Customers needs a valid Security Update Service (SUS) subscription
- Included in all 'service' packages:
  - Essential
  - Advanced
  - Advanced Plus
  - Premier
  - Premier Plus





# HOST BASED CONTROLS

SYSTEM HARDENING



OS PATCHING (WINDOWS AND LINUX)



ANTIVIRUS AND UPDATES





# ANTIVIRUS AND SIGNATURE UPDATES



- The Antivirus / malware protection application (ESET) is hosted on the Core Security Management Server (CSMS)
- Antivirus (AV) updates are provided weekly for Customers download via SUS portal
  - The update AV signatures are distributed to each network component automatically from the PSMS
- Included in all 'service' packages:
  - Essential
  - Advanced
  - Advanced Plus
  - Premier
  - Premier Plus
- ESET can also be used to control and manage the USB ports on any Windows device (e.g. any Server or Workstations) to prevent unauthorised use e.g. it is possible to create a 'White list' of storage devices that can be used
  - 'White lists' can also be created for optical storage devices (CD/DVD/Blu-ray), FireWire storage devices, Imaging devices, USB printers, Bluetooth devices, Memory card readers, Modems and LPT/COM ports





# **IDENTITY AND ACCESS MANAGEMENT**

2-FACTOR AUTHENTICATION



# 2 FACTOR (RSA) AUTHENTICATION



## ENHANCES ACCESS SECURITY

- Uses the RSA application which is hosted on the Performance and Security Management Server (PSMS)
  - Controls access to Windows and Linux application Servers
  - Can also be used for Remote VPN Access (via Service Access Firewall)
- The secure token can be either 'Soft' (for use with a mobile phone) or a physical token

Note, 2 FA can be supported for the Transport devices via the use of RADIUS

### IMPROVED SECURITY

COMBINES  
"SOMETHING YOU KNOW"  
WITH  
"SOMETHING YOU HAVE"

#### CENTRALIZED ACCESS CONTROL MANAGEMENT

Minimizes local amount management



LINUX SERVERS  
SUPPORTED



WINDOWS SERVERS  
SUPPORTED

1



2



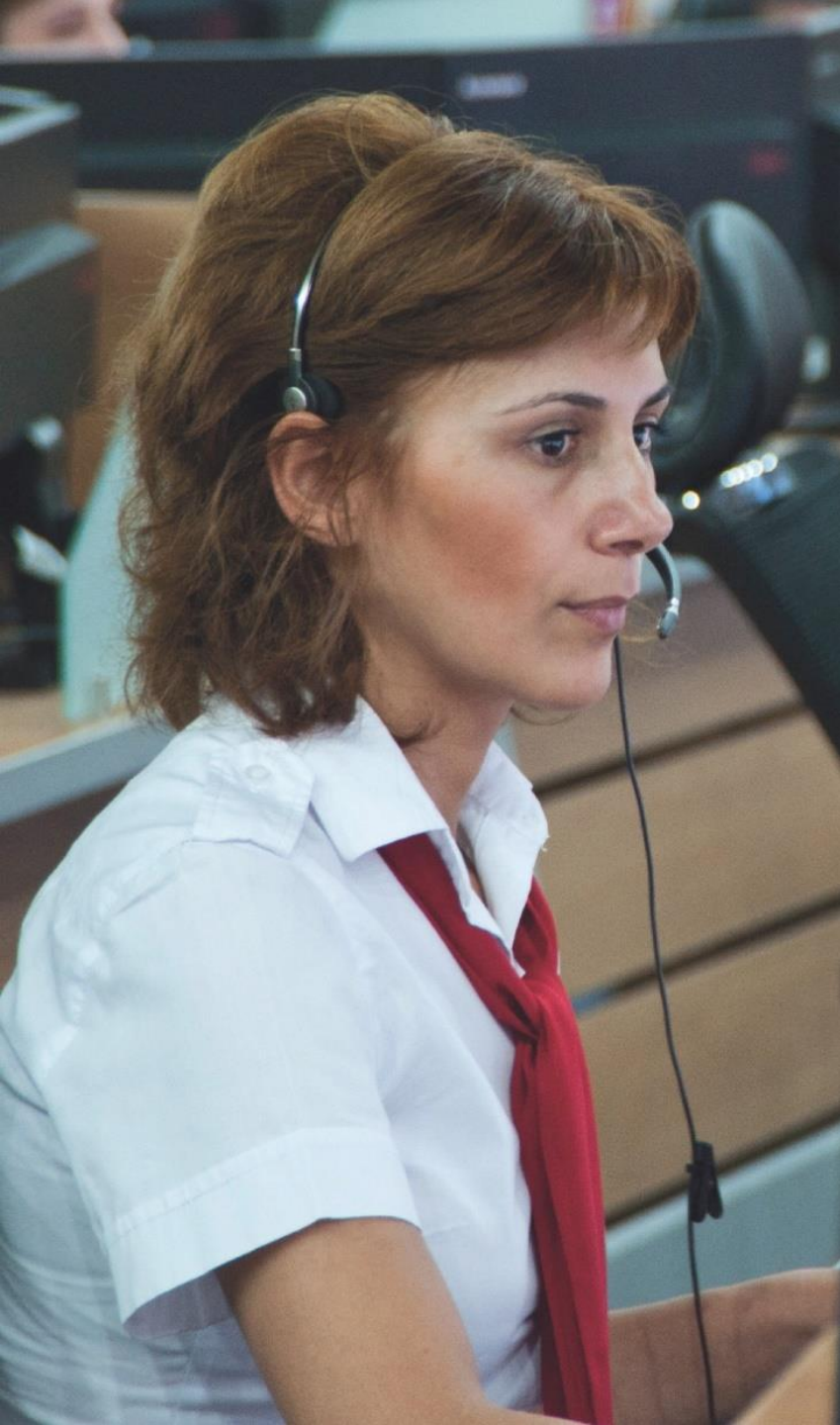
SECURE  
TOKEN  
OR MOBILE  
PHONE



\*\*\*\*\*  
ONE TIME PASSWORD  
WITH 60 SECOND AVAILABILITY







# MCC7500 CENTRALISED ACCOUNT MANAGEMENT & AUTHENTICATION



## ACTIVE DIRECTORY

- Domain Controllers:
  - Handle the 'Active Directory' services for the MCC7500 Console 'Domain'
    - Two Domain Controllers are required for each zone containing MCC7500 consoles
  - Provides centralised Account Management and Authentication of MCC7500 Console Users







# NETWORK BASED CONTROLS

REMOTE CONTROL SITE ACCESS CONTROL LISTS

---

PERIMETER PROTECTION





# NETWORK BASED CONTROLS

REMOTE CONTROL SITE ACCESS CONTROL LISTS

---

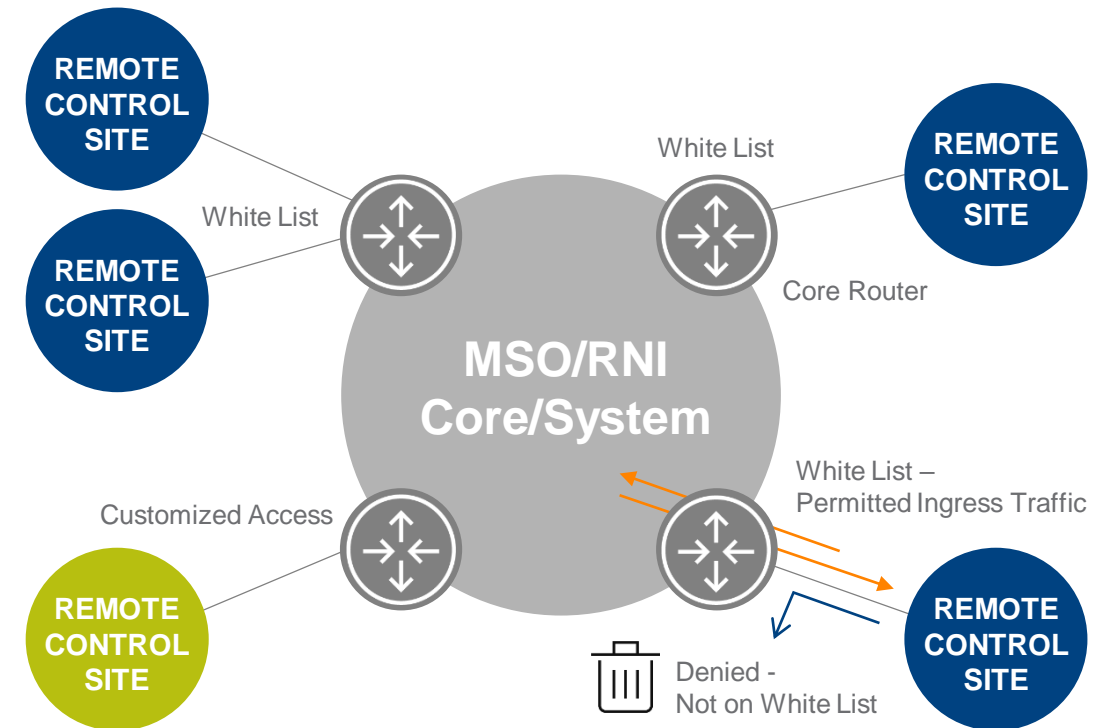
PERIMETER PROTECTION



# MOTE CONTROL SITE ACCESS CONTROL LISTS



- Security enhancement that makes it possible to configure Access Control Lists at the Core Routers enhancing security towards the Mobile Switching Office (Core) from Remote Control Sites
  - Applies packet filtering/firewall functionality at Core Routers using the Transport Network Configuration Tool (TNCT)
  - Configuration of white list for specific protocols/ports per Core Router thus effectively limiting undesirable applications from performing remote access to the MSO





# NETWORK BASED CONTROLS

REMOTE CONTROL SITE ACCESS CONTROL LISTS

---

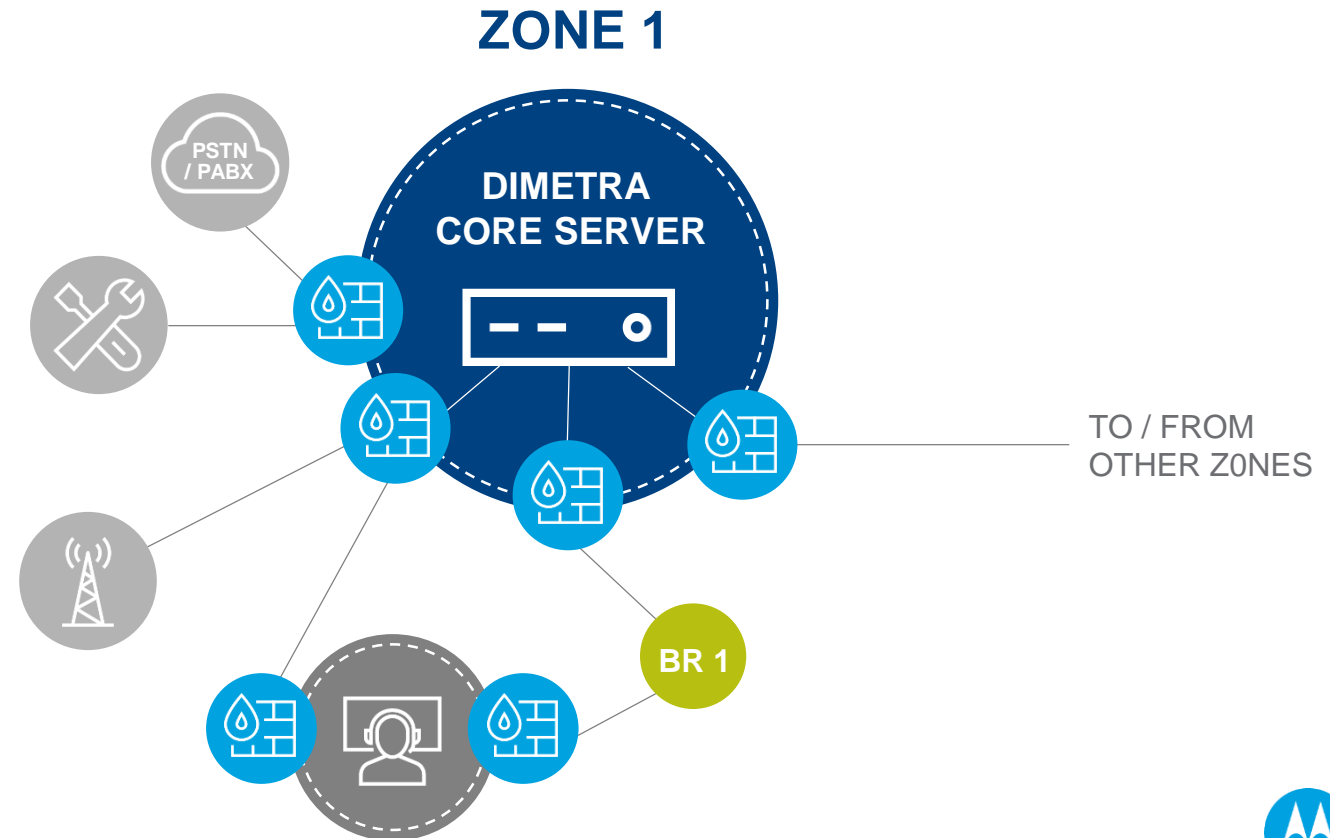
PERIMETER PROTECTION



# PERIMETER PROTECTION



- Backhaul Perimeter Protection is support for systems with Ethernet GBN:
  - Backhaul Firewalls are provided between the Core / Combined routers and the Backhaul switches and between the remote Control site switch and the Ethernet GBN access
  - For MSO redundant Backhaul Firewalls are mandatory
  - For Control Sites redundancy is optional
- Protection is provided towards the Customer Enterprise Network via the provision of the Customer Enterprise Network Interface Barrier (comprises Firewalls and Border Routers and DMZ)





# COMMUNICATIONS CONFIDENTIALITY

THE BASICS OF SECURITY

AUTHENTICATION / MUTUAL AUTHENTICATION

AIR INTERFACE ENCRYPTION (AIE)

IPSEC LINK ENCRYPTION (SHA-2)

OVER THE AIR RE-KEYING (OTAR)

AIE CRYPTOGRAPHIC SEPARATION (GCK)

E2EE VOICE AND SHORT DATA







# COMMUNICATIONS CONFIDENTIALITY

THE BASICS OF SECURITY

AUTHENTICATION / MUTUAL AUTHENTICATION

AIR INTERFACE ENCRYPTION (AIE)

IPSEC LINK ENCRYPTION (SHA-2)

OVER THE AIR RE-KEYING (OTAR)

AIE CRYPTOGRAPHIC SEPARATION (GCK)

E2EE VOICE AND SHORT DATA



# THE BASICS OF SECURITY



## THE CIA TRIAD

**Availability** ensures protection against network interruption.

**Integrity** ensures that data has not been altered in an unauthorized manner.

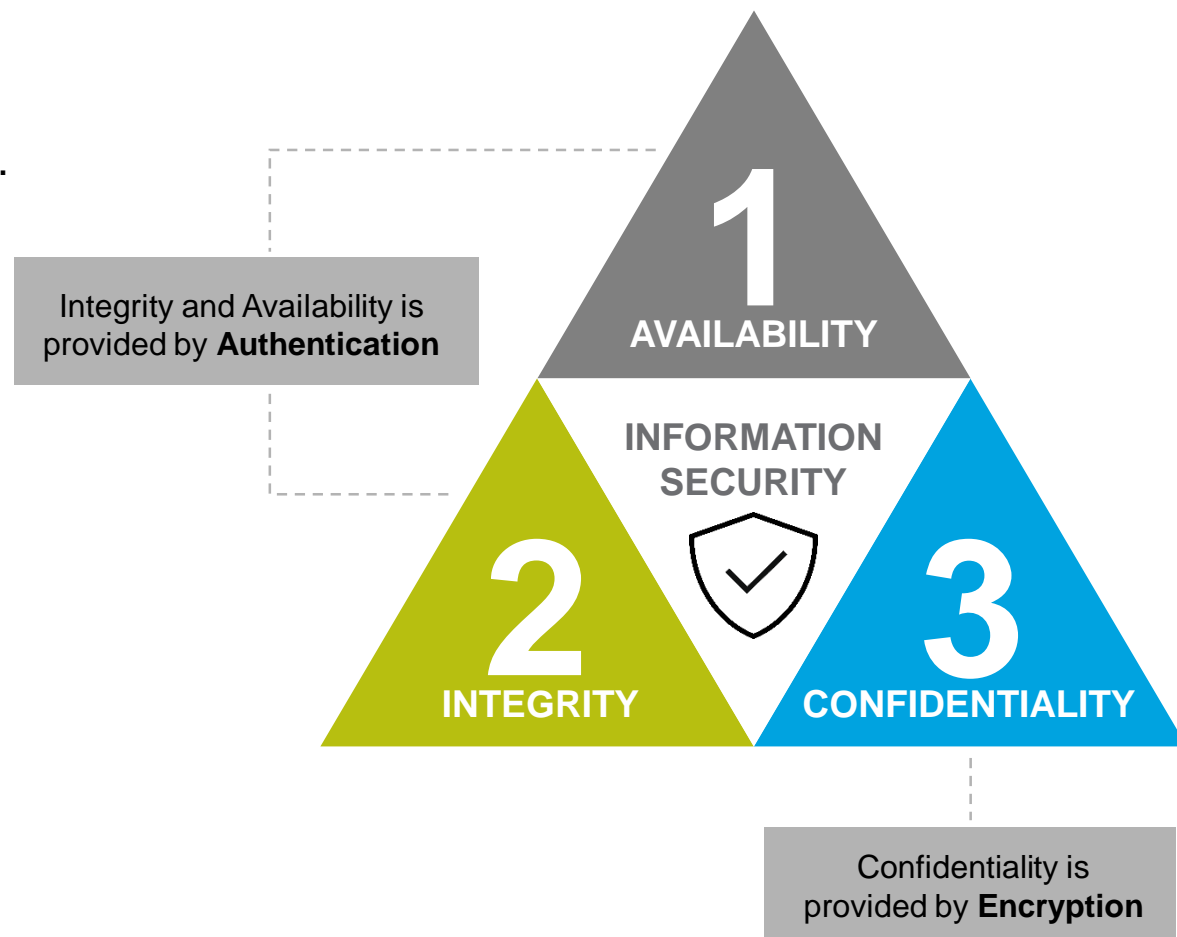
### Protection against:

- Unauthorized modification
- Deletion
- Creation
- Replication

Should also provide an indication of these unauthorized activities.

**Confidentiality** ensures only authorized users should have access to the information being exchanged.

- Eavesdropping
- Interception of radio path or network





# COMMUNICATIONS CONFIDENTIALITY

THE BASICS OF SECURITY

---

AUTHENTICATION / MUTUAL AUTHENTICATION

---

AIR INTERFACE ENCRYPTION (AIE)

---

IPSEC LINK ENCRYPTION (SHA-2)

---

OVER THE AIR RE-KEYING (OTAR)

---

AIE CRYPTOGRAPHIC SEPARATION (GCK)

---

E2EE VOICE AND SHORT DATA



# AUTHENTICATION



## FUNDAMENTAL SECURITY SERVICE IN TETRA

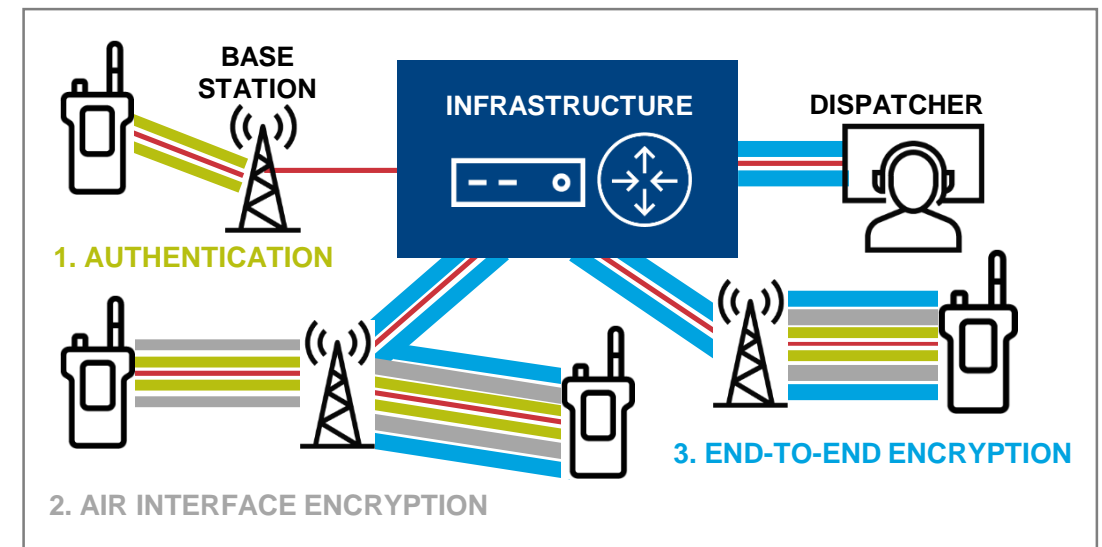
Foundation for a secure distribution channel

OTA SERVICES: KEY MGMT, ROTATION, ZEROIZE ETC

END-TO-END ENCRYPTION

AIR INTERFACE ENCRYPTION (AIE)

(MUTUAL) AUTHENTICATION



No Authentication = No AIE, E2EE or OTA Service





# AUTHENTICATION



## FUNDAMENTAL SECURITY SERVICE IN TETRA

### General

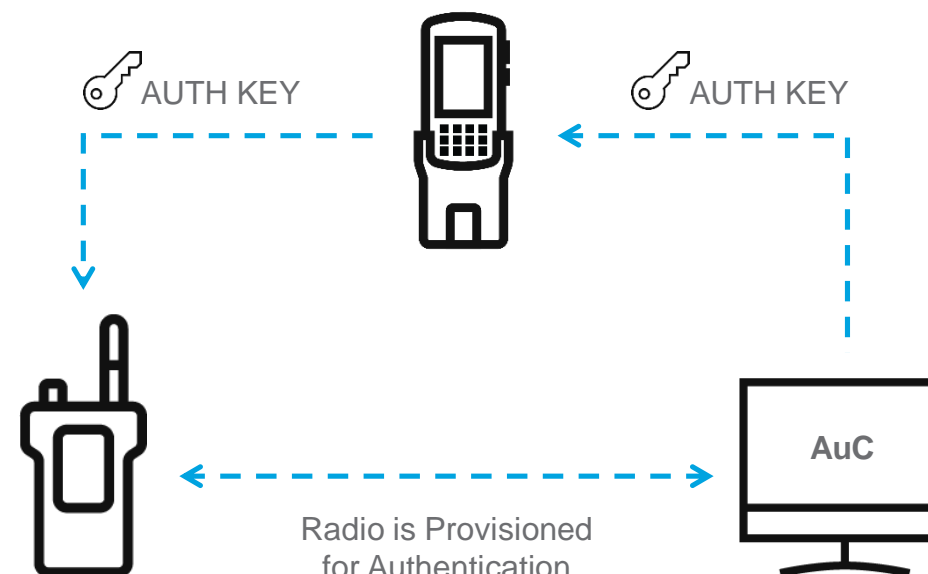
The process of 2 parties participating in communication, **proving** they are who they say they are.

### In TETRA

Authentication is used to ensure only valid subscribers have access to the system.

The authentication in TETRA is based on proving knowledge of the same **secret (K)** shared between a subscriber and the authentication centre (AuC).

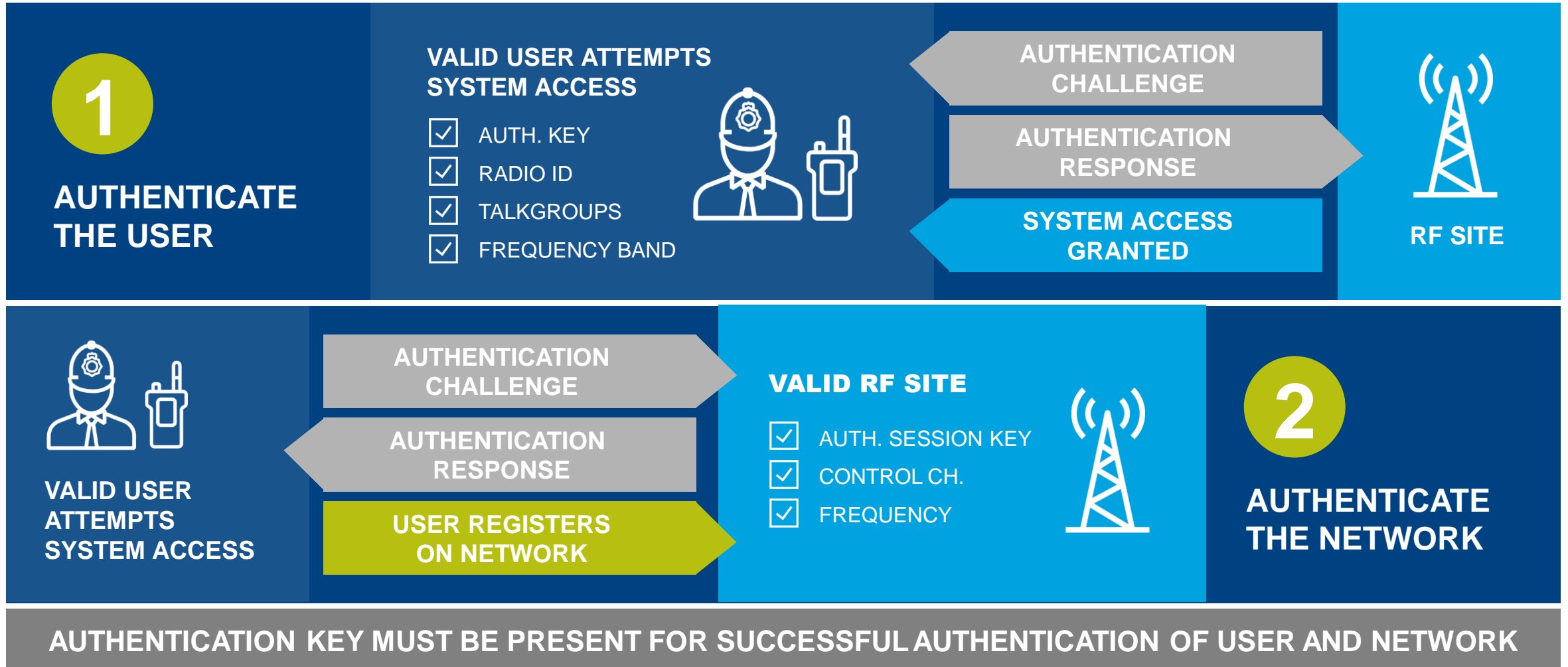
With that shared secret in both endpoints, the subscriber will be able to successfully authenticate into the network when challenged.



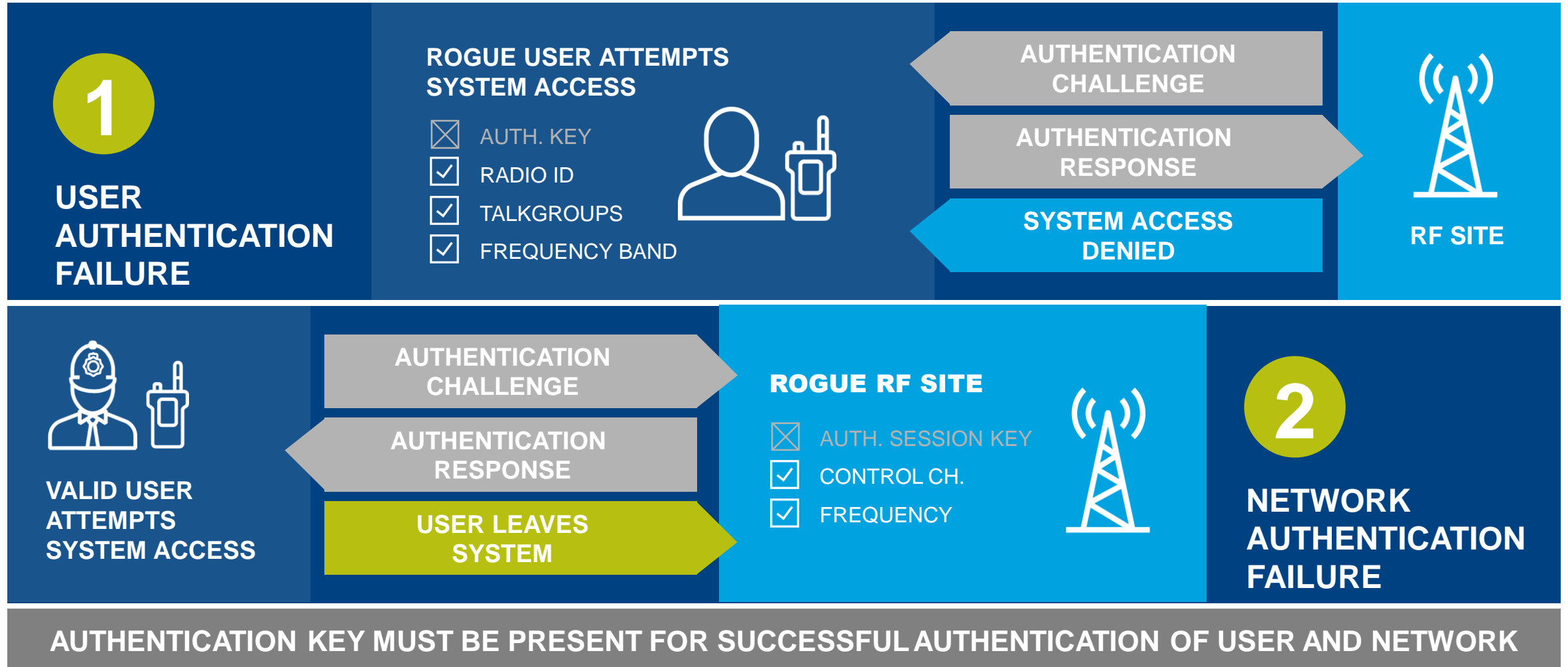
Provisioning for Authentication



# MUTUAL AUTHENTICATION FOR COMMUNICATIONS INTEGRITY



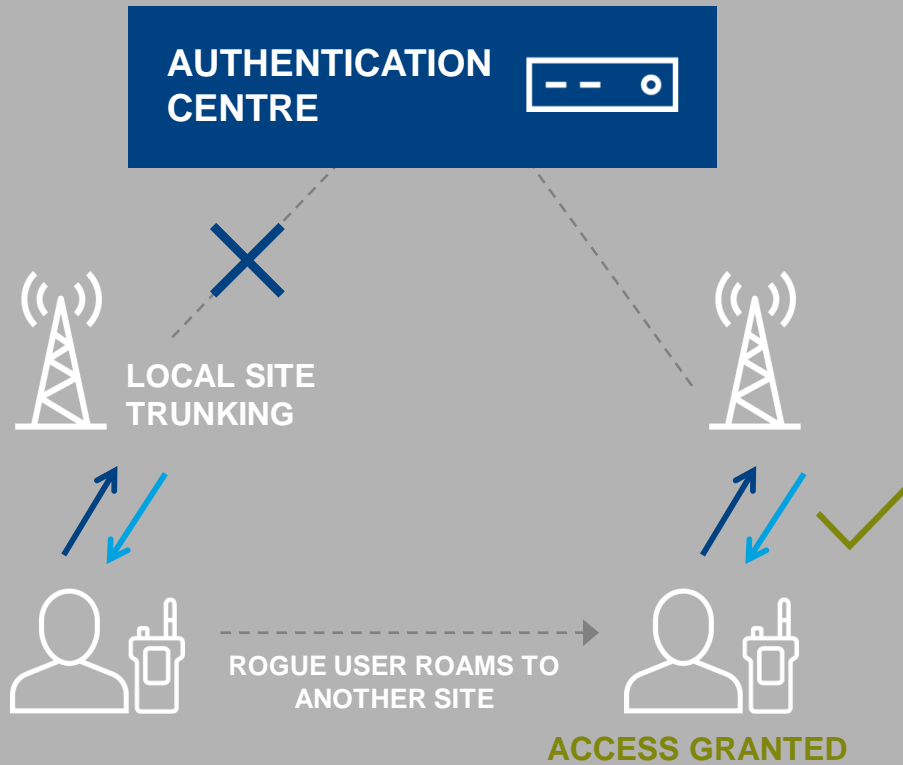
# MUTUAL AUTHENTICATION FOR COMMUNICATIONS INTEGRITY



# WHY AUTHENTICATION ON ROAMING IS CRITICAL

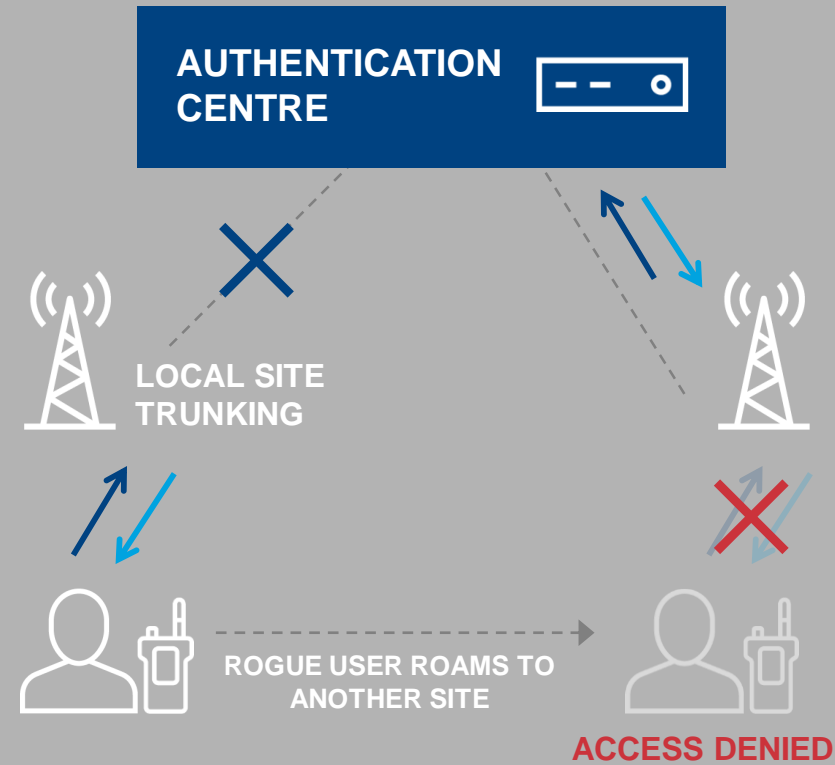


## WITHOUT AUTHENTICATION ON ROAMING



ACCESS GRANTED TO UN-AUTHENTICATED ROGUE USER

## WITH AUTHENTICATION ON ROAMING



ACCESS DENIED TO UN-AUTHENTICATED ROGUE USER





# COMMUNICATIONS CONFIDENTIALITY

THE BASICS OF SECURITY

---

AUTHENTICATION / MUTUAL AUTHENTICATION

---

AIR INTERFACE ENCRYPTION (AIE)

---

IPSEC LINK ENCRYPTION (SHA-2)

---

OVER THE AIR RE-KEYING (OTAR)

---

AIE CRYPTOGRAPHIC SEPARATION (GCK)

---

E2EE VOICE AND SHORT DATA





# ENCRYPTION



## THE BASICS

Encryption is the method by which plaintext (e.g. voice or location) is converted into ciphertext that can only be decoded by another entity if they have access to a decryption key.

In cryptography, a key is a random string of bits created explicitly for encrypting and/or decrypting data. The longer the key, the harder it is to find the right key using brute force.

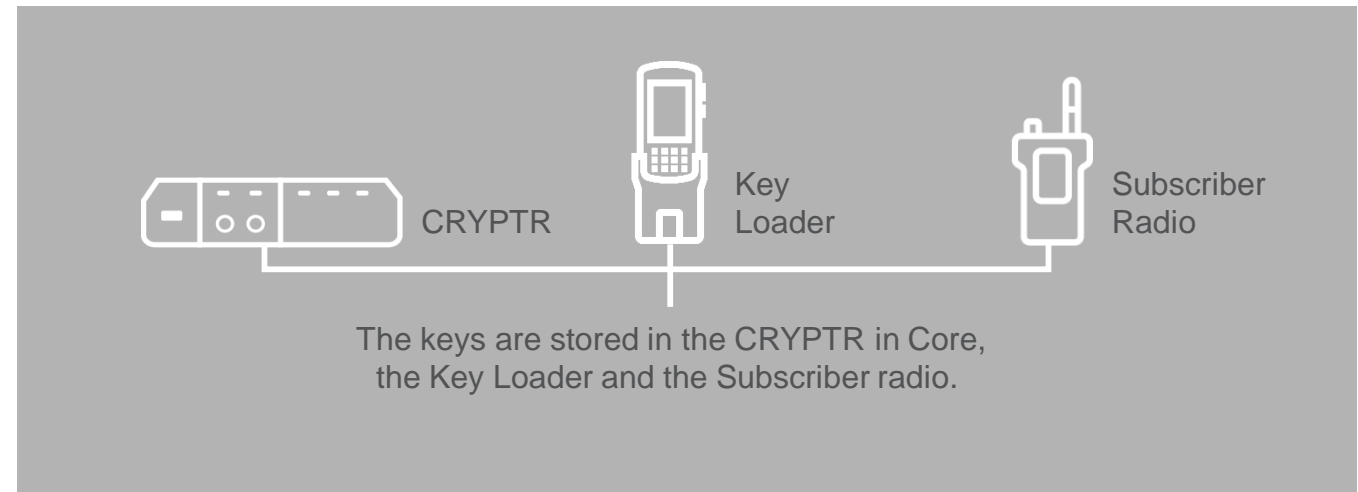
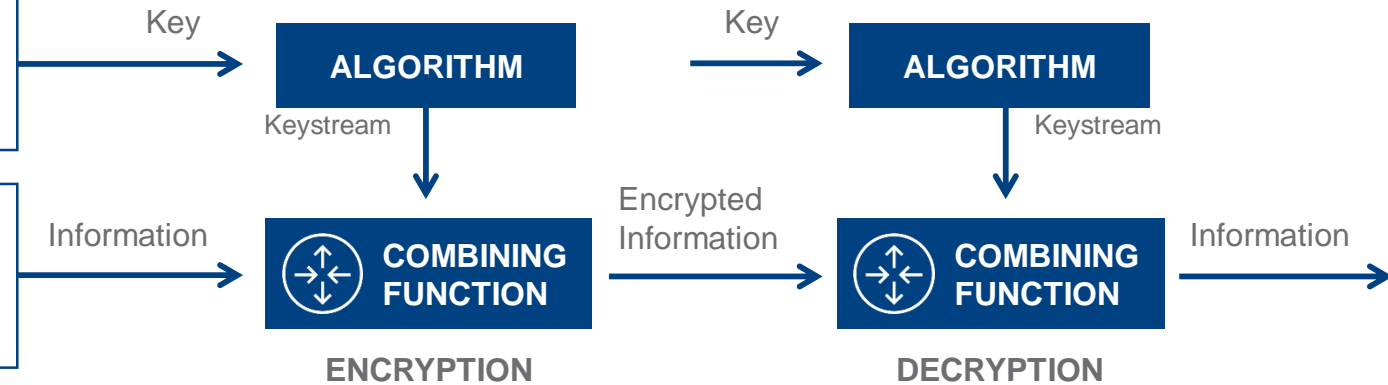
TETRA security features are based on Symmetric Encryption.

- Same key for both encrypting and decrypting data
- Key is known as a shared secret

### Challenge

Finding an efficient and secure method to agree upon, exchange and store this secret key. Key should only be known to the communicating parties but otherwise kept secret.

- Key Variable Loader 4000
- Key Management Facility



# AIR INTERFACE ENCRYPTION (AIE)



## PROTECTING CONFIDENTIALITY

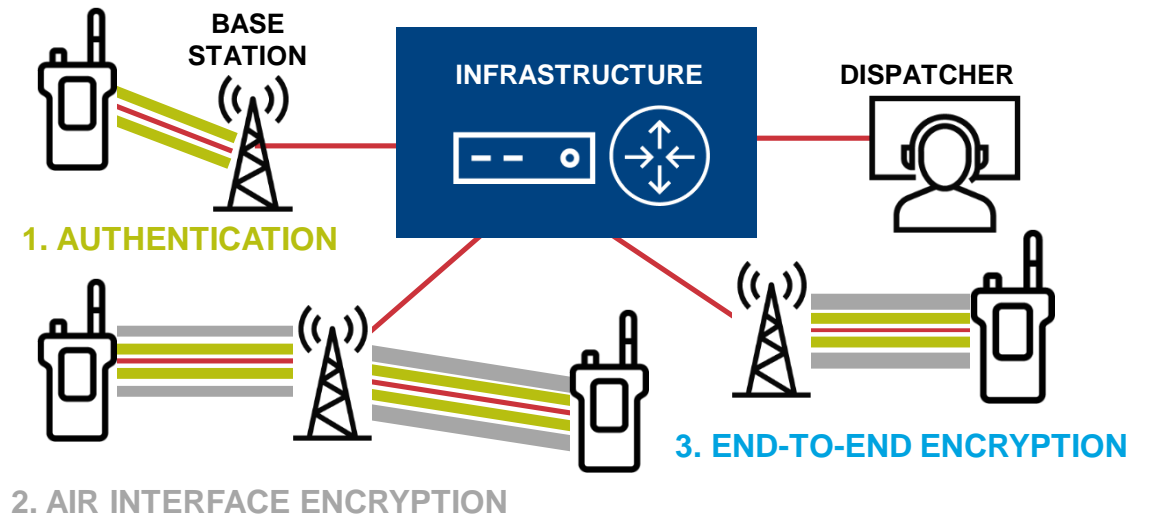
### AIR INTERFACE

- All of the signaling and traffic between the subscriber and the base station
- Also known as the radio link

Since anyone could listen to air channels during the communication of MS and BTS, it is important to encrypt information transmitted over the air.

### AIR INTERFACE ENCRYPTION (AIE)

- Protects voice
- SDS (short data services e.g. location, text)
- Packet data transmissions
- Signaling



The TETRA standard supports four AIE TETRA Encryption Algorithms (TEAs)

- TEA1 (intended for general use)
- TEA2 (restricted to use by Schengen / EU countries)
- TEA3 (intended for general use)
- TEA4 (not supported by Motorola Solutions)

There are differences in the intended use and the exportability of equipment containing these algorithms.

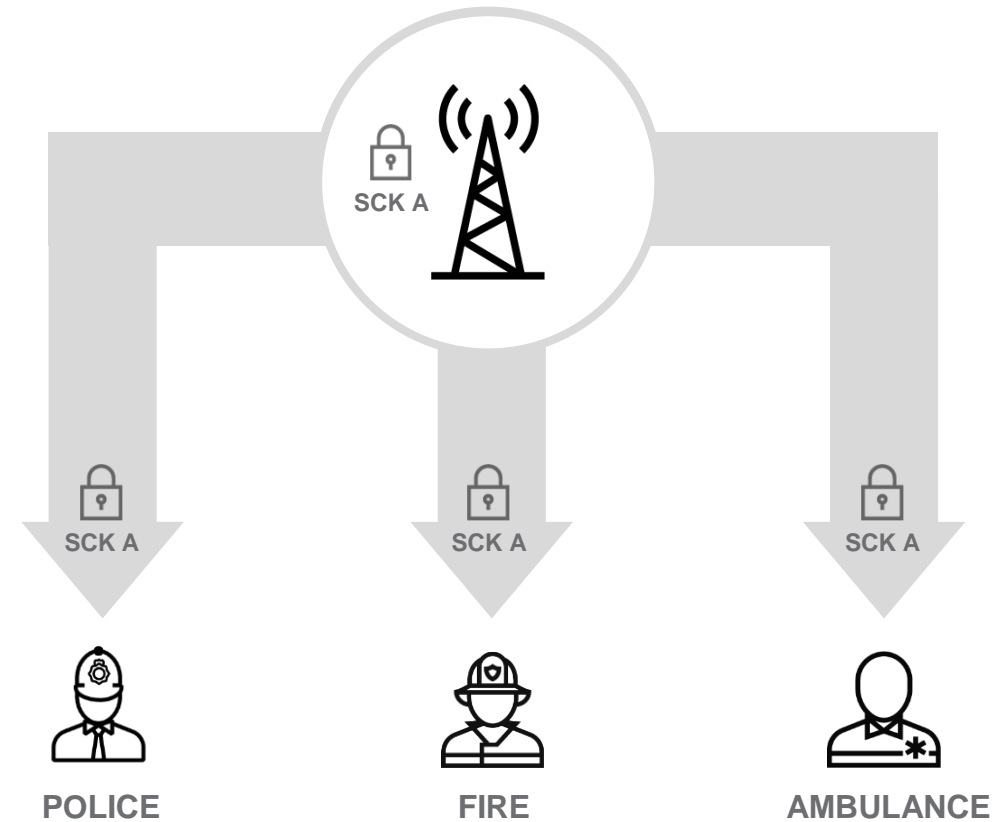


# CLASSES OF AIE



## Static Cipher Key (SCK)

- System Wide
- Manually or system generated
- Max of 32 keys shared between TMO and DMO
- Key life = 6 months (max recommended)
- Changed / updated via OTAR



# CLASSES OF AIE

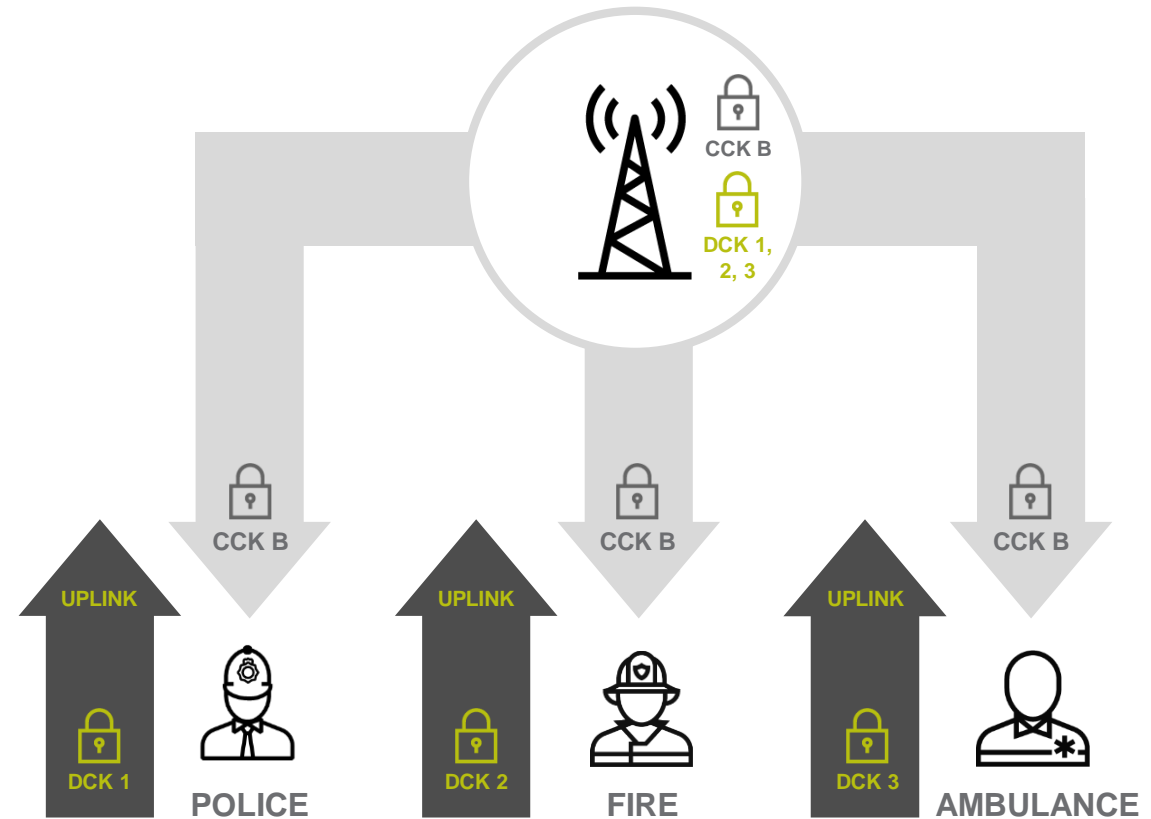


## Common Cipher Key (CCK)

- System Wide
- System generated, unlimited number of keys
- Key life = 24 hours (max recommended)
- Changed / updated via OTAR

## Derived Cipher Key (DCK)

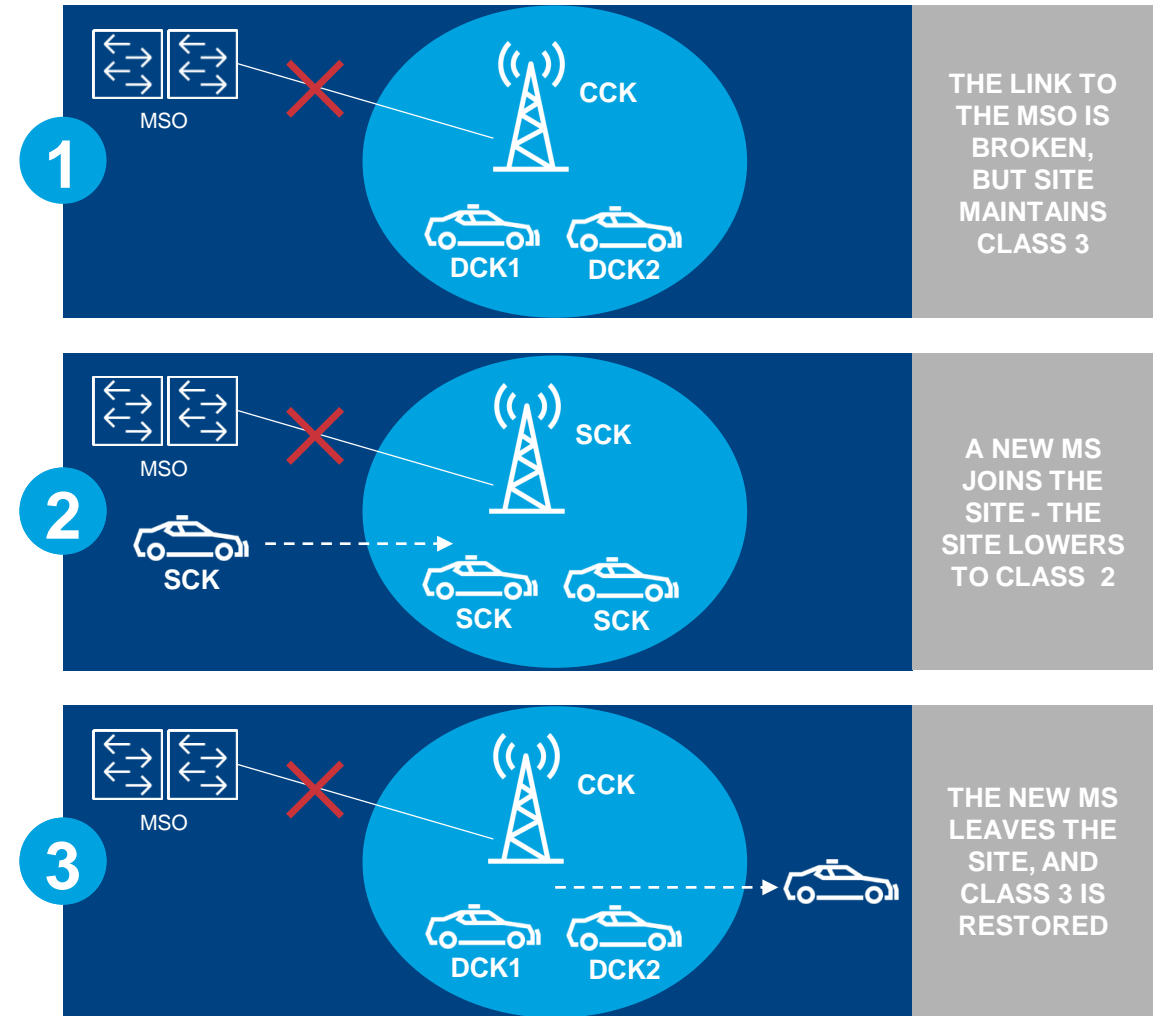
- Unique to each User
- Derived during authentication
- Key life = Last successful authentication



# SECURITY IN FALLBACK MODES



- Whilst base station is connected to the MSO, it operates in Class 3 with dynamic keys – individual DCK and CCK for identity encryption and for group calls
  - DCK is derived by the mutual authentication process
- When the base station is disconnected from the switch, it maintains Class 3 using the DCK derived from the last authentication
- If a new MS joins the site – and so cannot be authenticated – the base station falls back to Class 2 (SCK)
  - Implicit authentication of new MS by knowledge of the correct SCK
- Fallback is seamless – takes place during calls in progress without calls dropping
- If that MS leaves, and the base station has DCKs for all other MSs, the base station will revert to Class 3 – seamlessly
- The highest security possible is maintained in all conditions







# COMMUNICATIONS CONFIDENTIALITY

THE BASICS OF SECURITY

---

AUTHENTICATION / MUTUAL AUTHENTICATION

---

AIR INTERFACE ENCRYPTION (AIE)

---

IPSEC LINK ENCRYPTION (SHA-2)

---

OVER THE AIR RE-KEYING (OTAR)

---

AIE CRYPTOGRAPHIC SEPARATION (GCK)

---

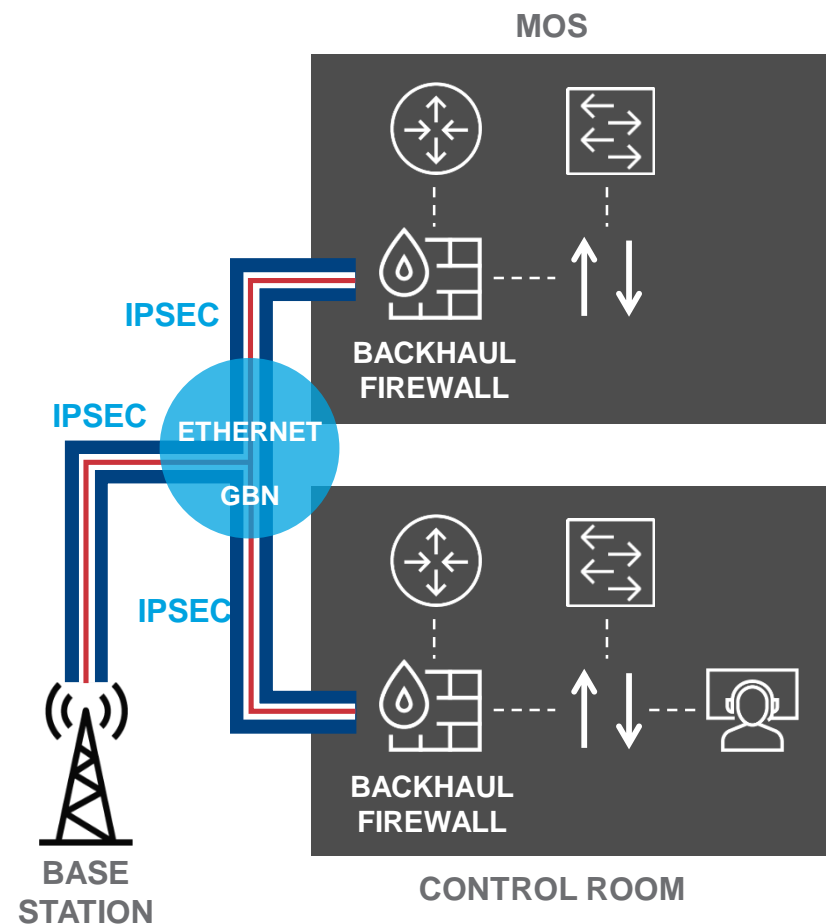
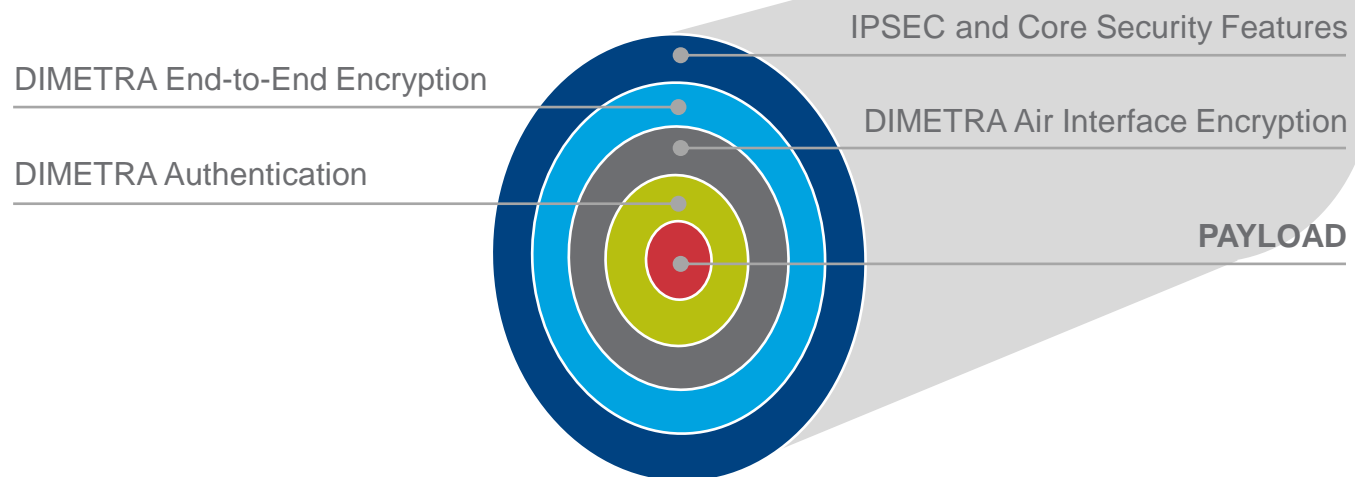
E2EE VOICE AND SHORT DATA



# IPSEC LINK ENCRYPTION (SHA-2)

## Key Benefits

- Enhanced security on backhaul links
- Take advantage of lower cost public networks without sacrificing link security.





# COMMUNICATIONS CONFIDENTIALITY

THE BASICS OF SECURITY

---

AUTHENTICATION / MUTUAL AUTHENTICATION

---

AIR INTERFACE ENCRYPTION (AIE)

---

IPSEC LINK ENCRYPTION (SHA-2)

---

OVER THE AIR RE-KEYING (OTAR)

---

AIE CRYPTOGRAPHIC SEPARATION (GCK)

---

E2EE VOICE AND SHORT DATA



# ENHANCING SECURITY WITH OVER THE AIR RE-KEYING (OTAR)



WITHOUT OTAR = LESS SECURE WITH MANUAL, COSTLY PROCESSES



WITH OTAR = MORE SECURE WITH SIGNIFICANT TIME AND COST SAVINGS



Note: SCK security is essential for subscriber radios working in direct mode, including where TMO coverage is extended using DMO gateways





# COMMUNICATIONS CONFIDENTIALITY

THE BASICS OF SECURITY

AUTHENTICATION / MUTUAL AUTHENTICATION

AIR INTERFACE ENCRYPTION (AIE)

IPSEC LINK ENCRYPTION (SHA-2)

OVER THE AIR RE-KEYING (OTAR)

AIE CRYPTOGRAPHIC SEPARATION (GCK)

E2EE VOICE AND SHORT DATA





# AIE CRYPTOGRAPHIC SEPARATION (GCK)



## Common Cipher Key (CCK)

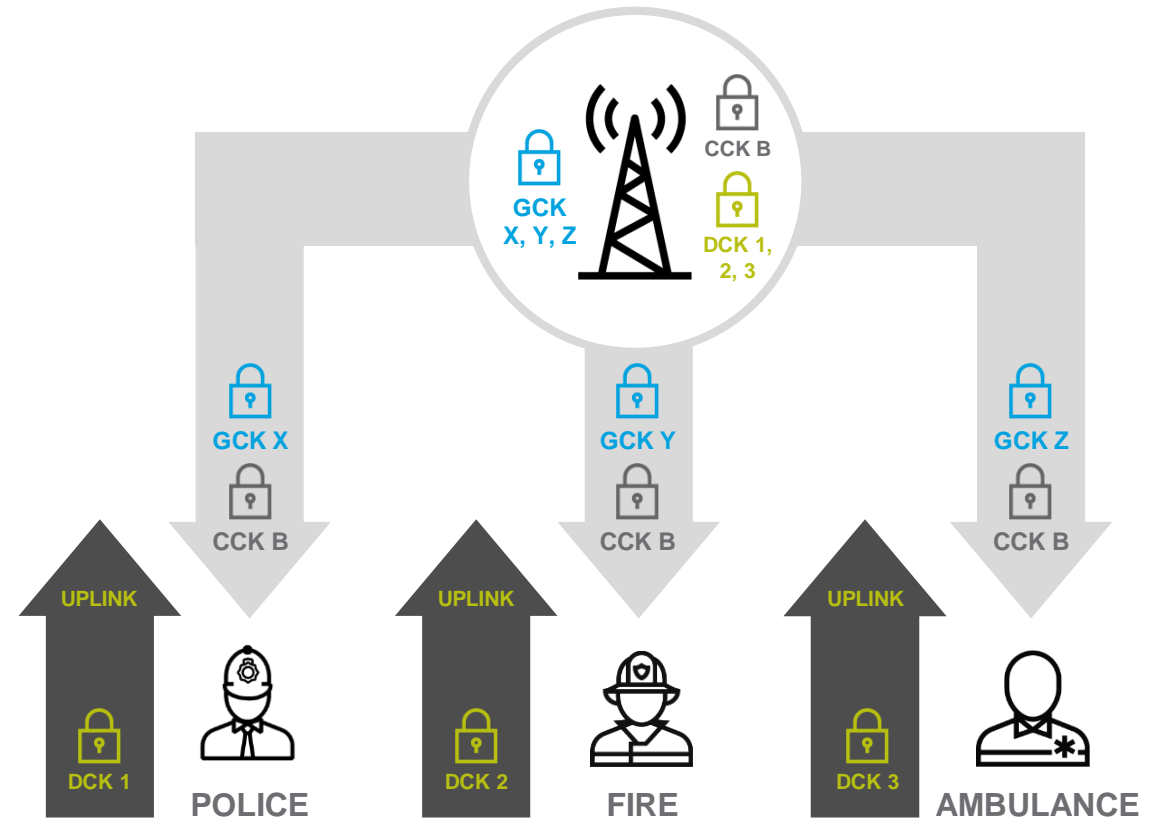
- System Wide
- System generated, unlimited number of keys
- Key life = 24 hours (max recommended)
- Changed / updated via OTAR

## Derived Cipher Key (DCK)

- Unique to each User
- Derived during authentication
- Key life = Last successful authentication

## Group Cipher Key (GCK)

- Crypto Management Group based
- System generated, unlimited keys
- Key life = 3 months (max recommended)
- Changed / updated via OTAR



# MULTI-AGENCY PARTITIONING



## Whole system secured by:

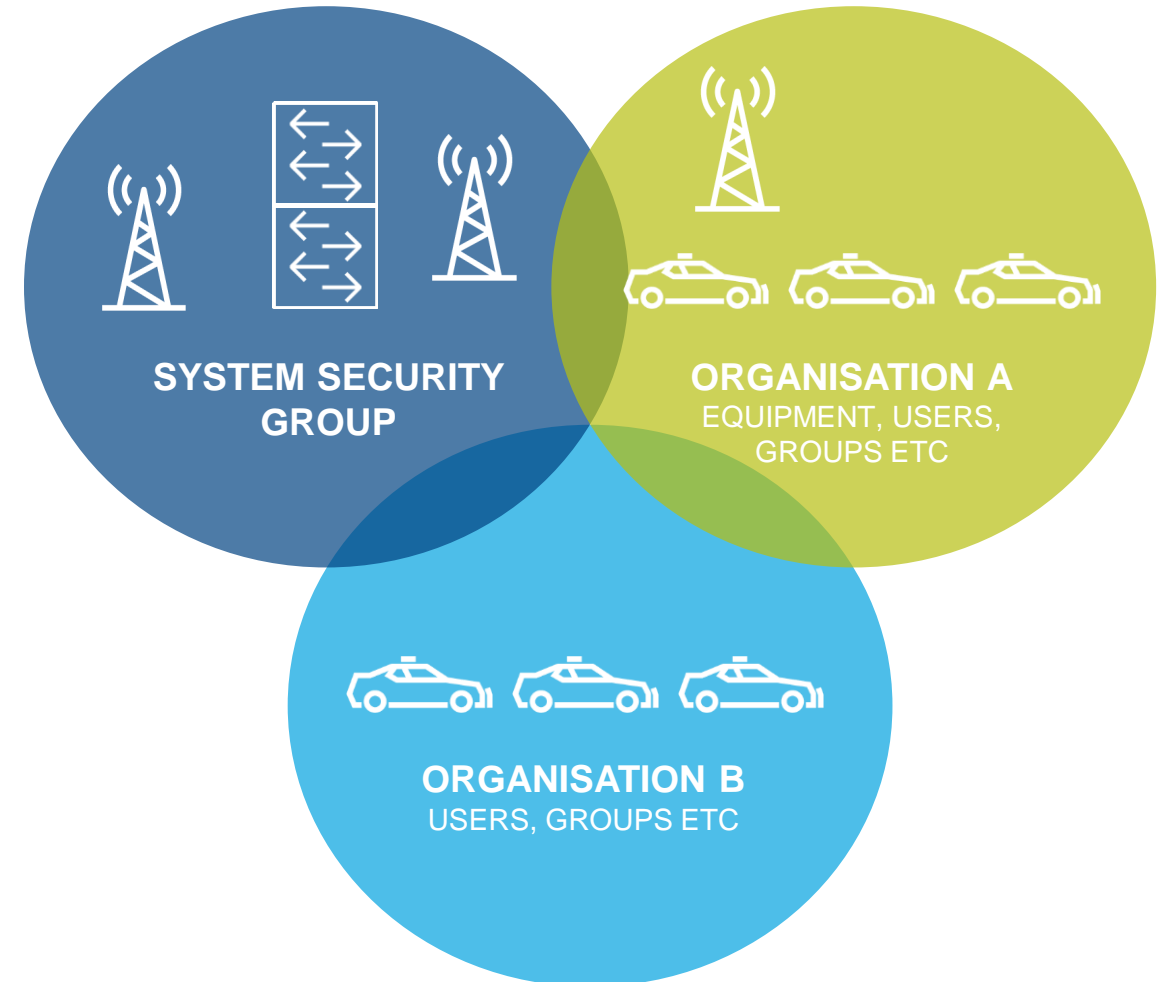
- Mutual authentication
- Class 3 (normal operation – dynamic keys) and Class 2 (fallback – static cipher keys) air interface encryption

## All security parameters are stored centrally for the best protection of all

- Only short term key material is sent to sites

## Security partitioning is built into the network management systems

- Allows different organisations to configure and manage their own subscribers, groups etc
- Equipment can also be managed within security groups
  - e.g. one organisation owns a site, and other organisations cannot manage it
- Separate control rooms, separate logging systems etc





# COMMUNICATIONS CONFIDENTIALITY

THE BASICS OF SECURITY

---

AUTHENTICATION / MUTUAL AUTHENTICATION

---

AIR INTERFACE ENCRYPTION (AIE)

---

IPSEC LINK ENCRYPTION (SHA-2)

---

OVER THE AIR RE-KEYING (OTAR)

---

AIE CRYPTOGRAPHIC SEPARATION (GCK)

---

E2EE VOICE AND SHORT DATA



# END-TO-END ENCRYPTION (E2EE) VOICE AND SHORT DATA

Protects the transmission of the information throughout the network.

- Data is encrypted within the transmitting terminal, and only decrypted within the receiving terminal.

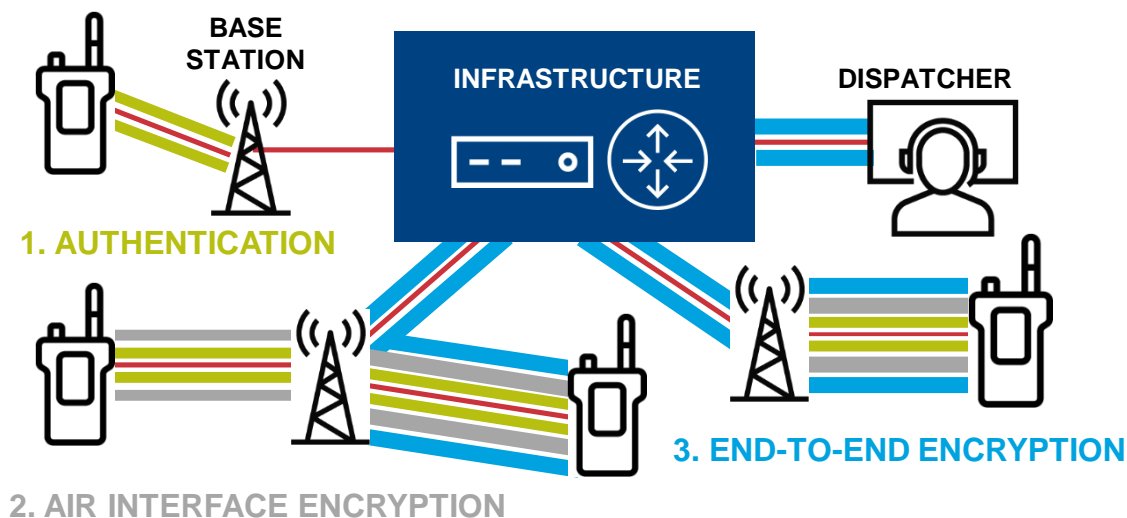
Network is indifferent to what traffic is flowing...  
Clear or encrypted.

## Voice

- Subscriber to subscriber
- Subscriber to dispatch and vice versa
  - MCC7500S | S-DCS

## Short Data

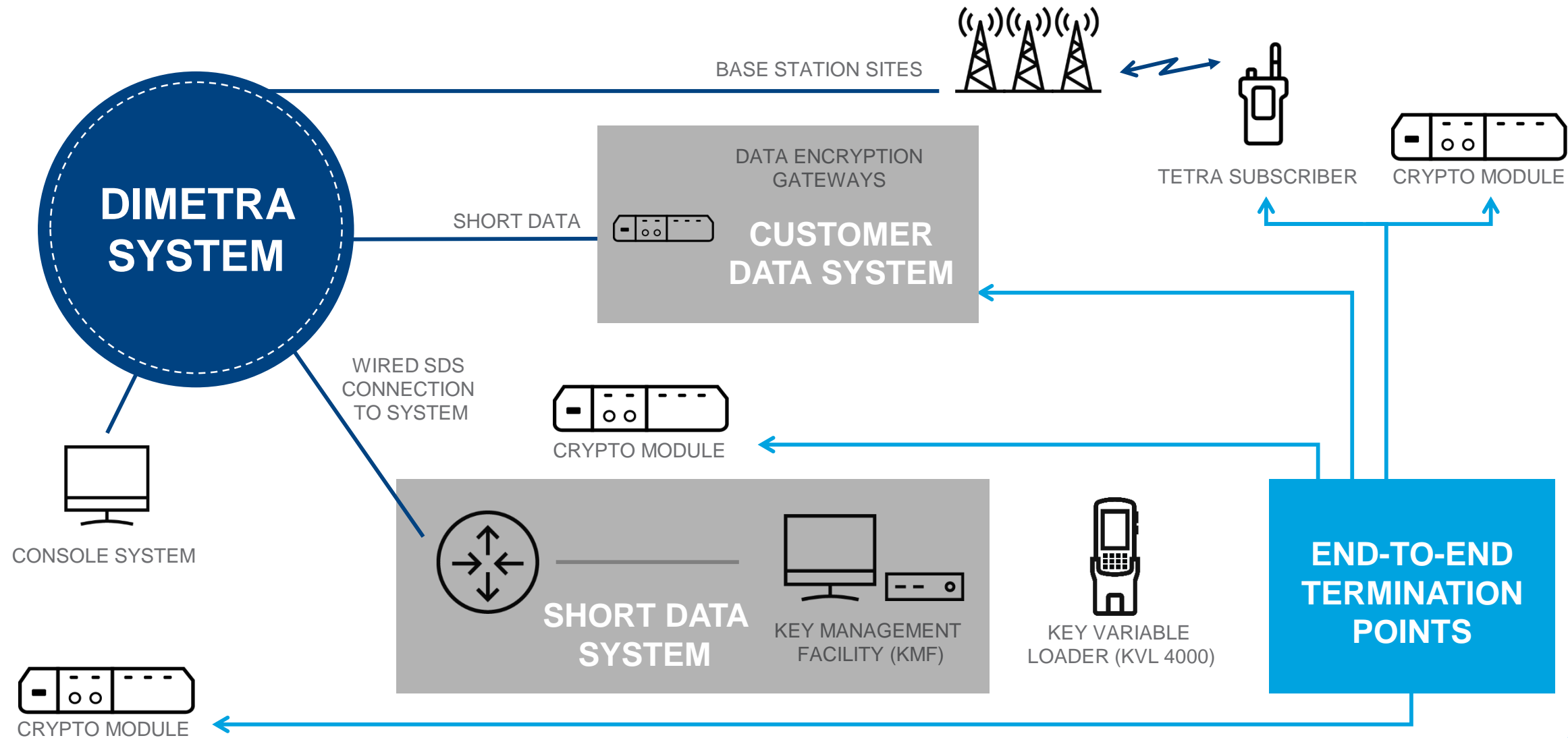
- Device to device
- Device to fixed host and vice versa



The underlying management infrastructure has no ability to decode messages or any access to the end to end keys



# MOTOROLA SOLUTIONS TETRA END-TO-END ENCRYPTION SYSTEM ARCHITECTURE





# MCC 7500 SECURE DISPATCH CONSOLE



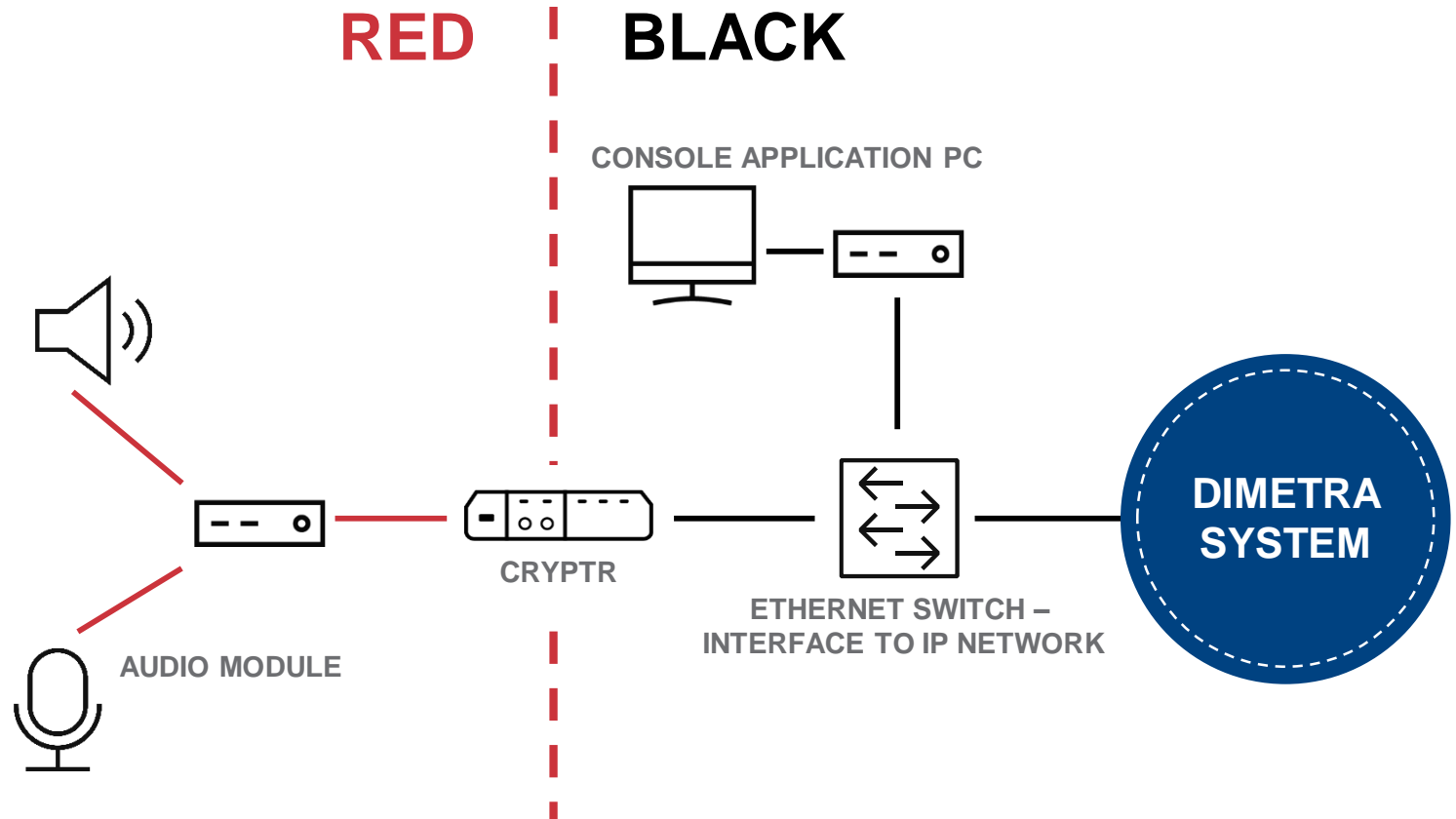
The console architecture maintains a high security separation between sensitive (Red) and non-sensitive (Black) information

The call processing and console application is carried out using a Windows based application

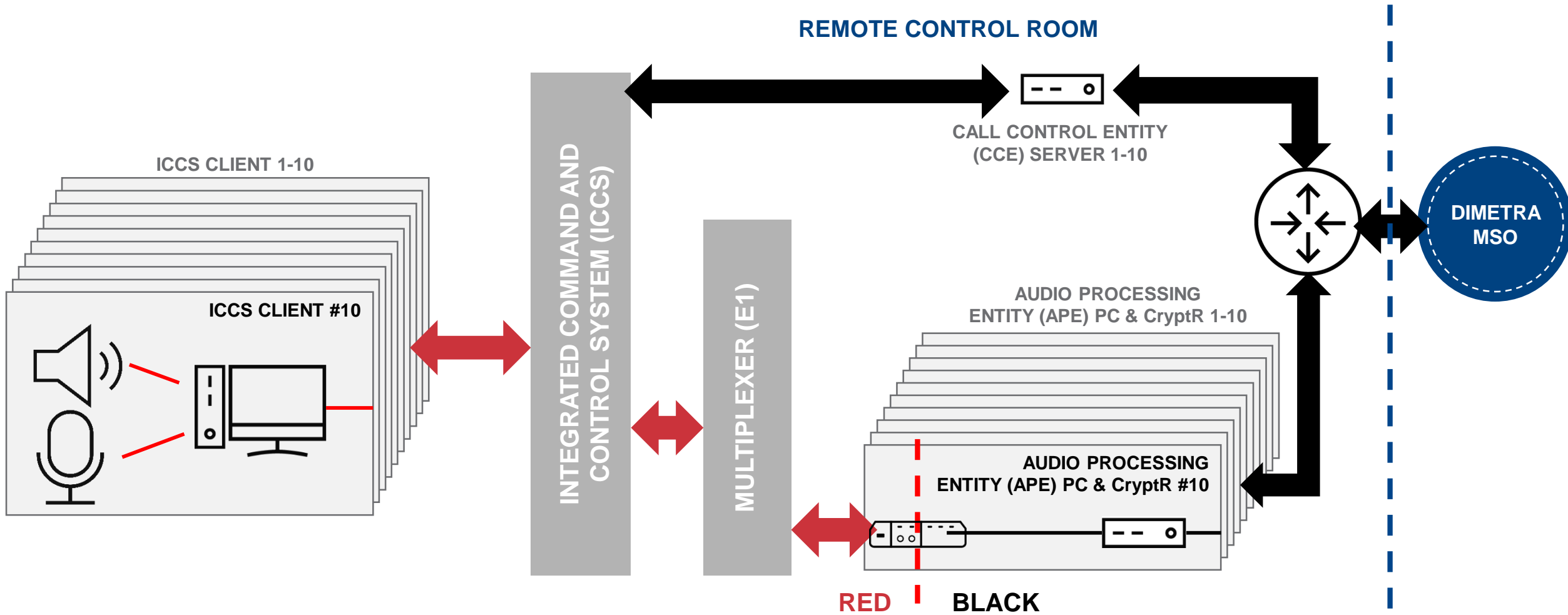
The encryption/decryption is carried out by a separate unit (the CryptR), with separate ports for Red and Black information.

The audio module provides the interface to audio accessories, and incorporates the vocoder, with appropriate audio processing

No danger of information crossing the red/black boundary, for example through Windows etc.



# SECURE DISPATCHER COMMUNICATION SERVER (DCS)

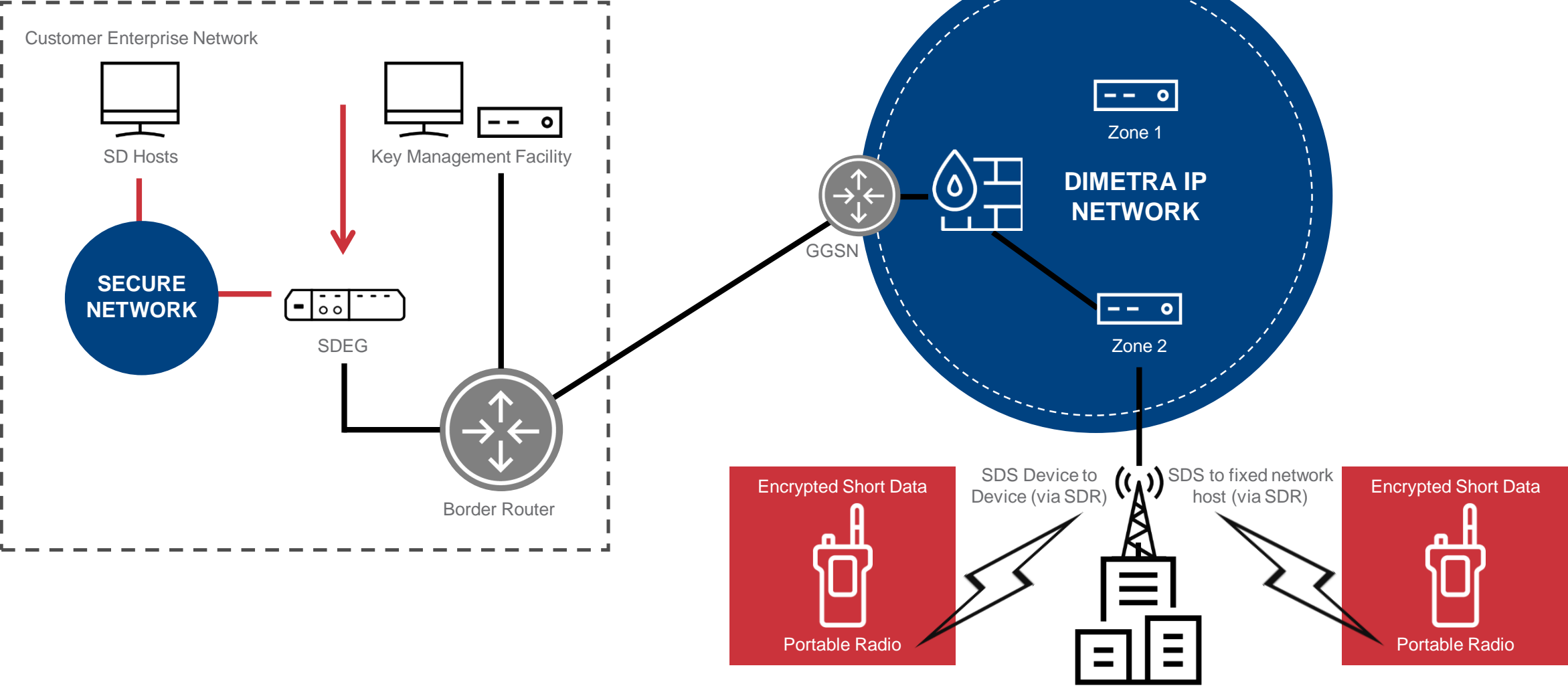


Leverages CCE consolidation, as per 'clear' DCS, however, there is still a 1:1 relationship between the APE PC and the cryptr, reducing space and power when compared to E2EE ICCS GW solution



# SHORT DATA ENCRYPTION GATEWAY (SDEG)

## PROTECTING SHORT DATA SERVICES (SDS)



# MOTOROLA SOLUTIONS KEY MANAGEMENT TOOLS



## THE SOLUTION TO THE KEY MANAGEMENT PROBLEM

### Key management tools consist of:

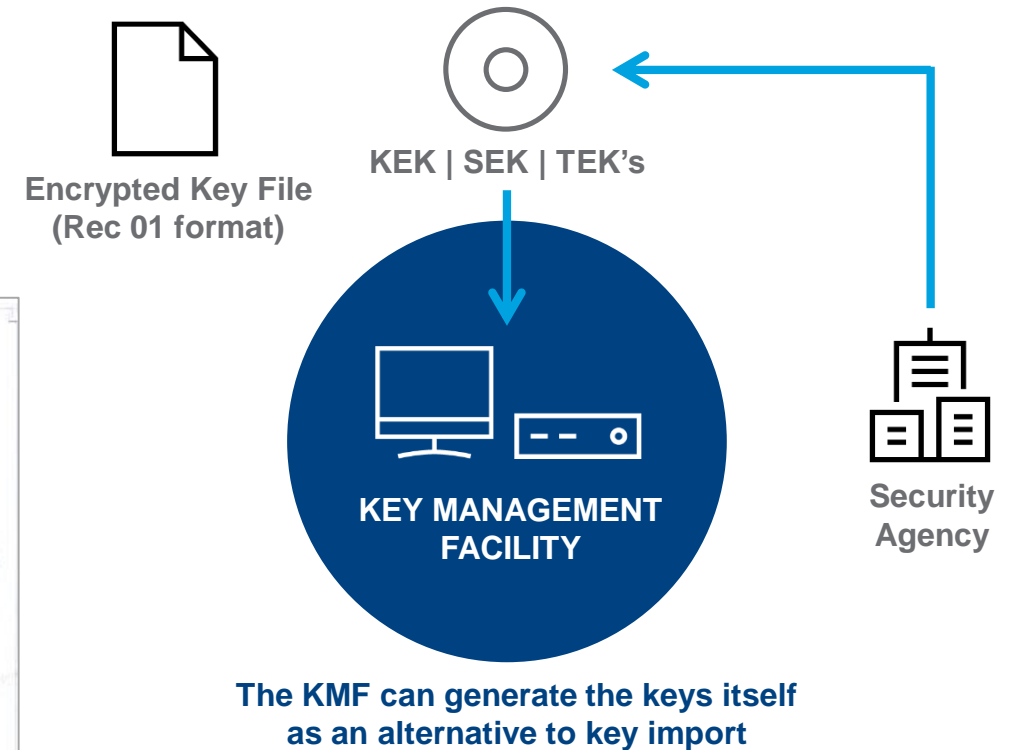
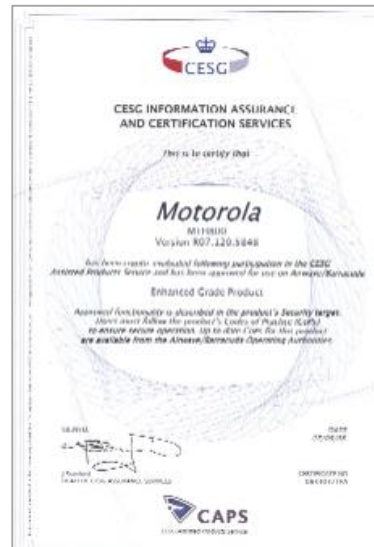
- Hand Held Key Variable Loaders (KVL)
  - Custom designed, rugged key management device
- Key Management Facility (KMF)
  - Central database of key material
  - Co-ordination of KVLs either by direct connection or dial up modem
  - Over The Air Re-Keying (OTAR) from KMF to radios

**All tools are compliant to TETRA MoU SFPG Recommendation 02**



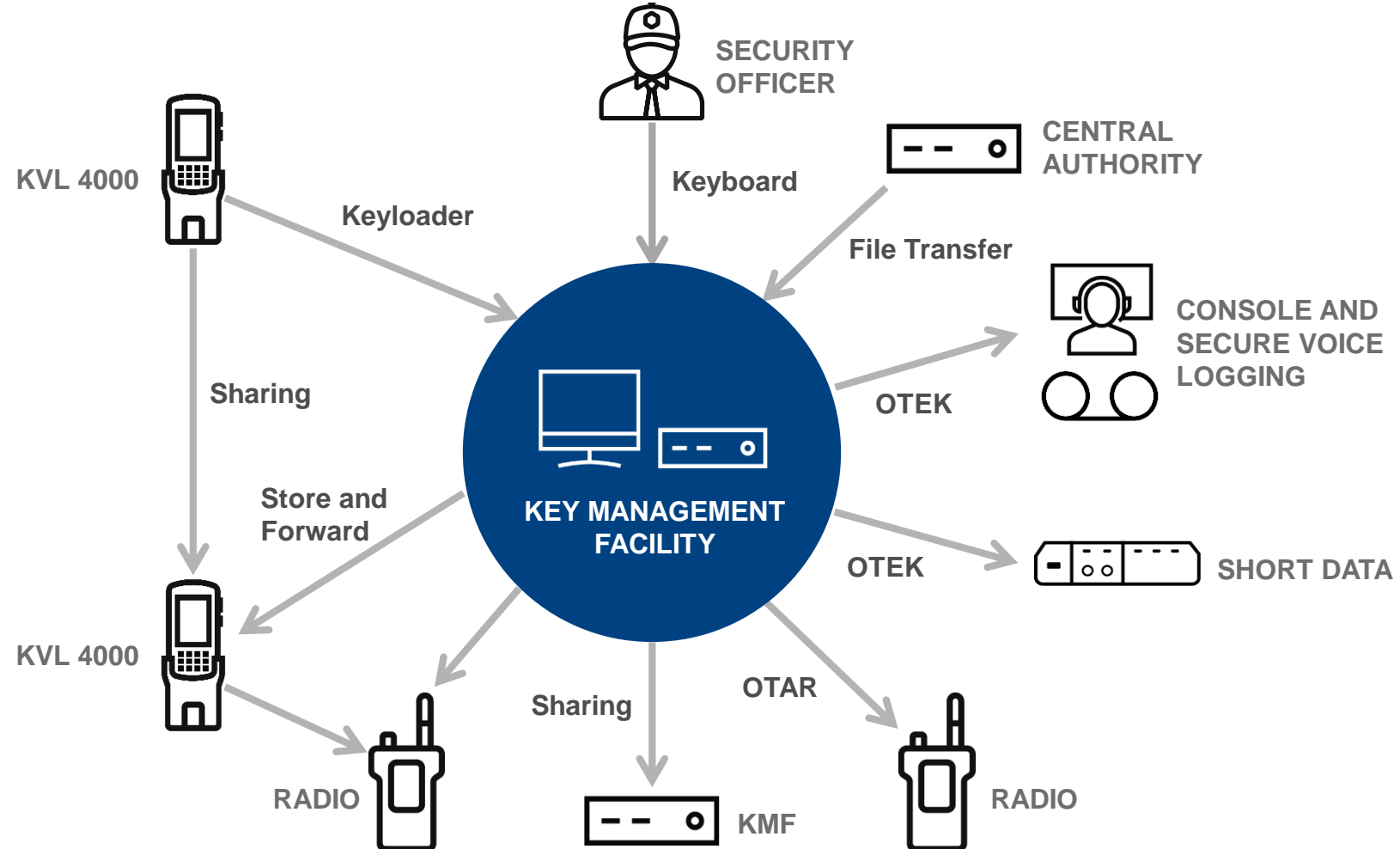
# END TO END KEY GENERATION

- Keys can be automatically generated or imported
- National authority can provide the key material
  - No dependence on Motorola Solutions for keys
- TETRA Security Fraud Prevention Group (SFPG) made a statement that TETRA should use components designed towards FIPS 140-2 (TETRA SFPG Rec.09 document)
  - SFPG standardised key import file format follows SFPG Recommendation 01
  - Keys may also be exported in Recommendation 01 format to allow sharing between user groups
- Motorola Solutions has added support for TETRA to the same hardware cryptopr module that is certified to FIPS 140-2 in the US that is used for P25
- Complete E2E solution components certified to Enhanced Grade by UK Government (CESG)





# A COMPLETE SECURE END TO END ENCRYPTED SYSTEM SOLUTION





# DETECT

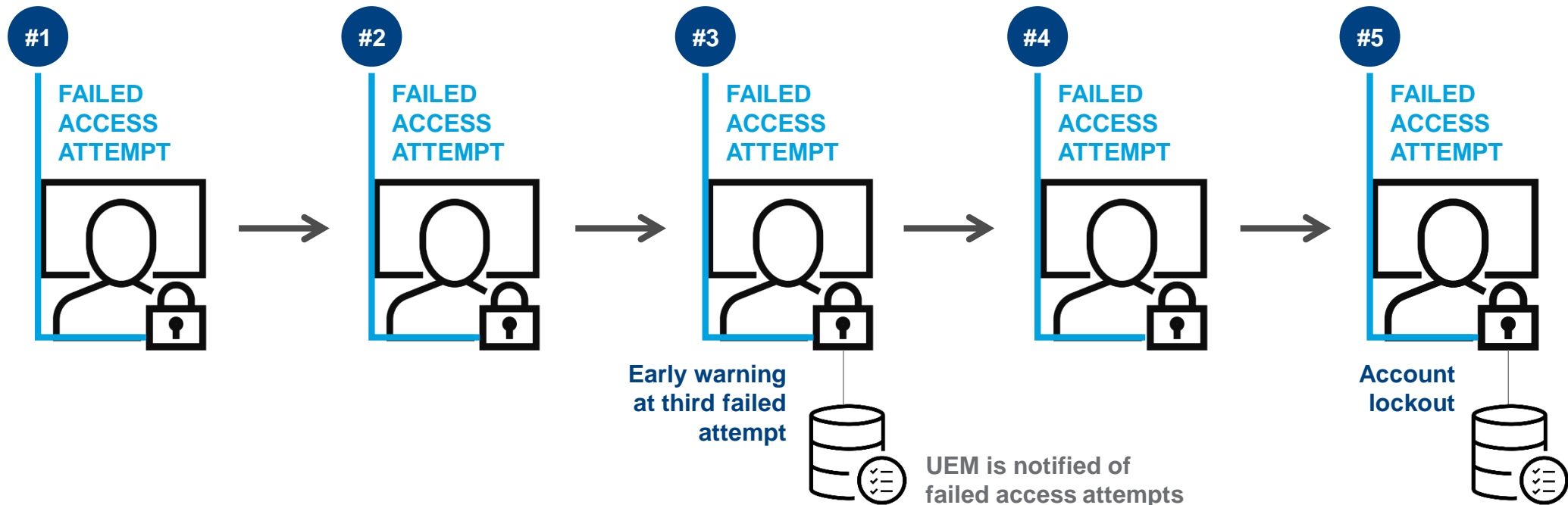
MAKE TIMELY DISCOVERIES

- NOTIFICATION OF UNAUTHORISED ACCESS ATTEMPTS
- SYSTEM LOGGING
- UEM NORTH BOUND
- INTRUSION DETECTION



# NOTIFICATION OF UNAUTHORISED ACCESS ATTEMPTS AT UNIFIED EVENT MANAGER (UEM)

## FOR WINDOWS OS APPLICATIONS



Note, this is supported on all Windows based applications except for Alias Server, PrC, APE and Devices in the Customer Enterprise Network (CEN) or DMZ (e.g. IMW, KMF, etc)



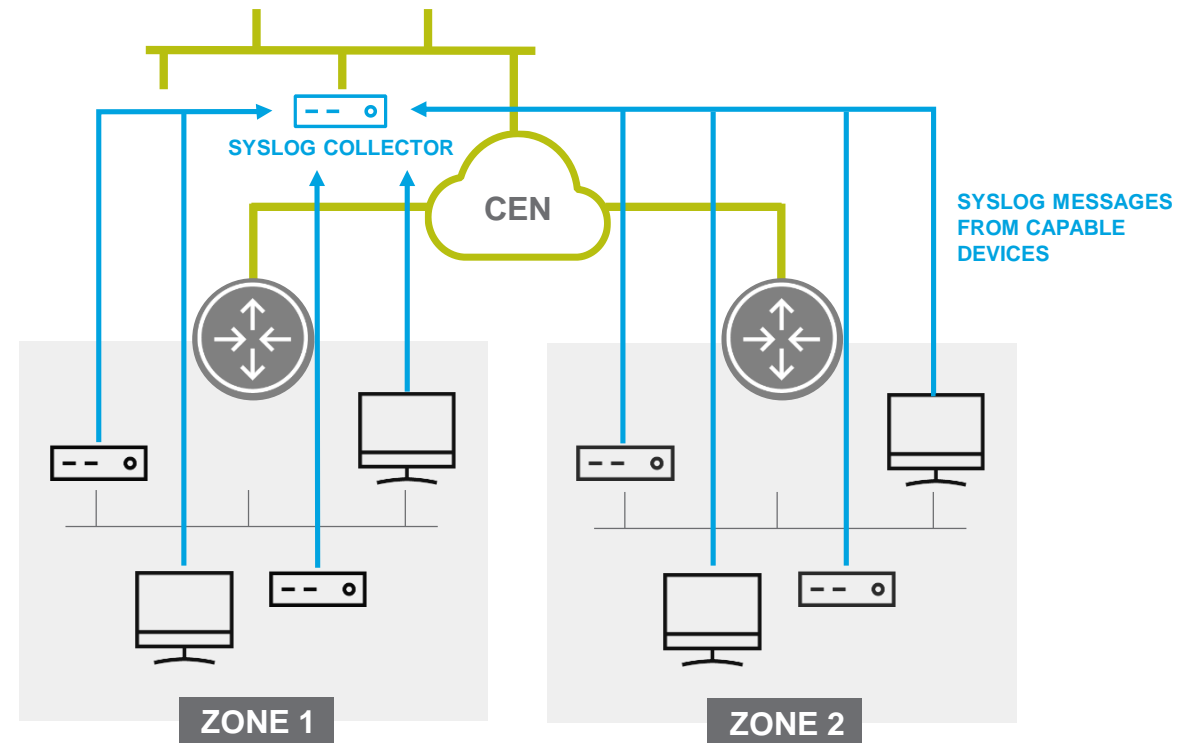


# AUDIT AND EVENT MANAGEMENT

## CENTRALISED EVENT LOGGING (SYSLOG)

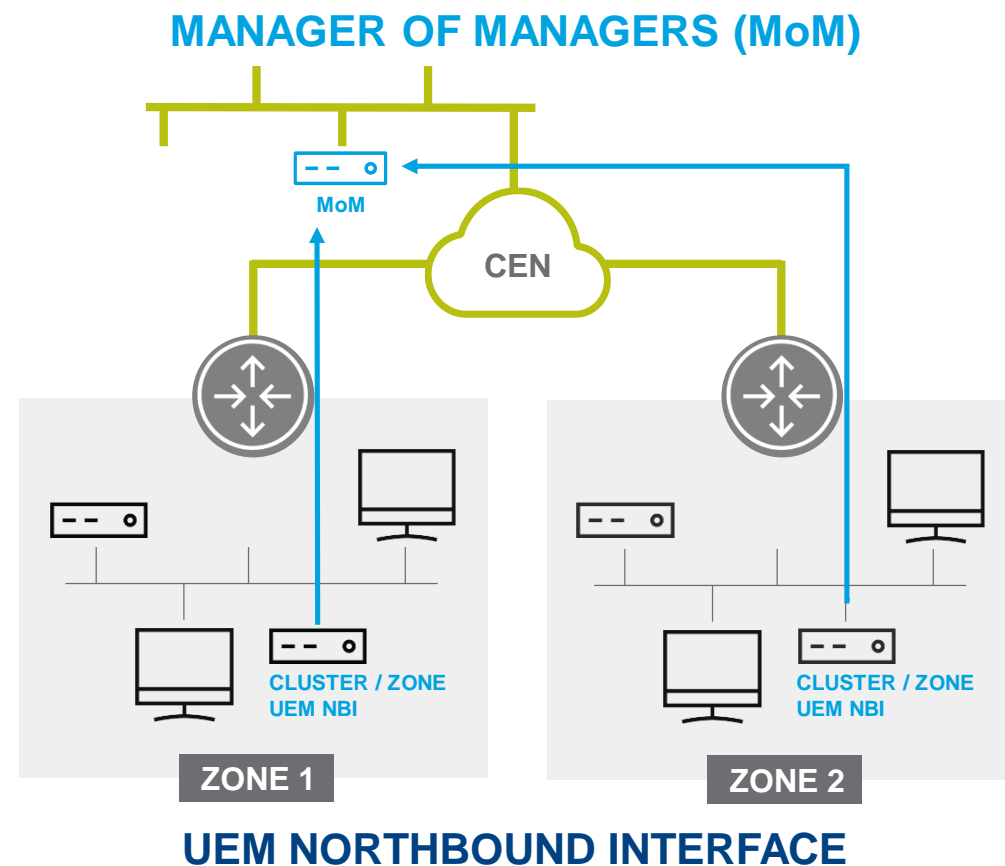
- Logs operating system events on a defined set of devices in the radio access infrastructure; servers, clients, and network transport devices
- Creates evidence of access control, change management, and accountability
- Forwards Syslog records to remote Syslog server outside of the DIMETRA network, in the Customer Enterprise Network (CEN)

## SYSLOG CENTRALISED EVENT LOGGING



# UNIFIED EVENT MANAGER (UEM) NORTHBOUND INTERFACE

- UEM is the primary fault management / troubleshooting tool used in DIMETRA systems
- Includes a North Bound Interface (NBI) so that traps can be sent to external registered managers (e.g. a Manager of Managers (MoM))
- Supports 4 addresses:
  - 2 x Reserved for Motorola Solutions
  - 2 x For Customer use





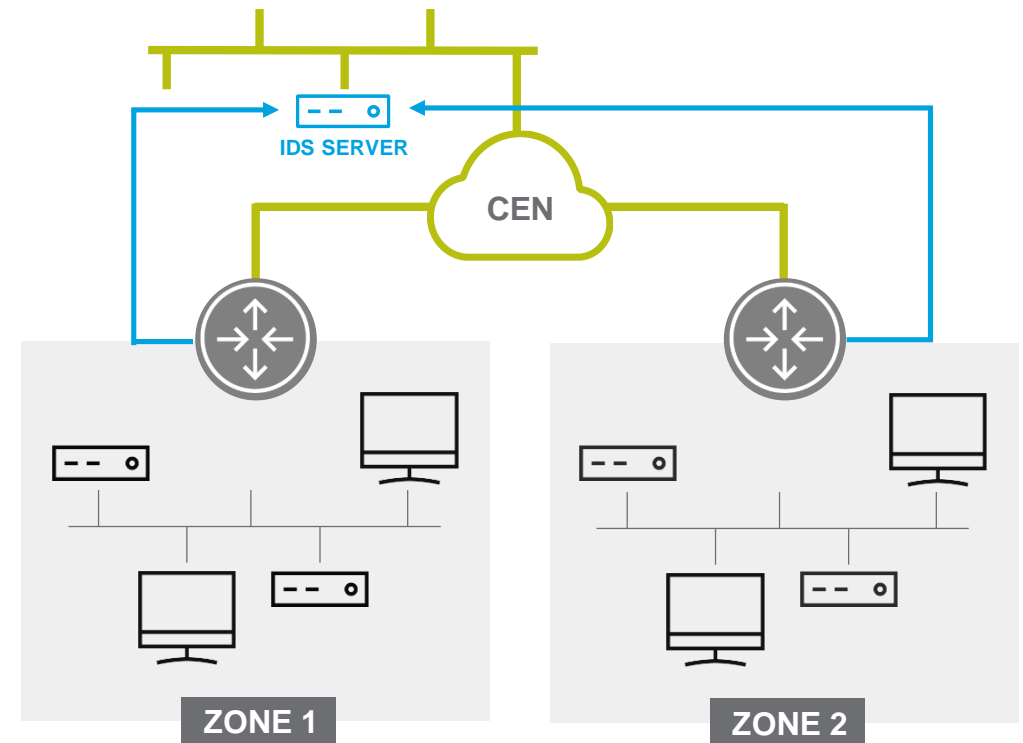
# NETWORK BASED CONTROLS

## INTRUSION DETECTION

IDS in DIMETRA is currently supported via 3rd party solution implementation, either Customer or Project specific

- IDS is supported by placing IDS Sensors in the system
  - Sensors are supported at the Master Site but not remote Control sites
- Monitoring takes place at the DMZ switch
  - The sensor connects to the Mirror port of the switch
  - If Geographically Redundant then monitoring takes place at both locations
  - Monitors all Firewall interfaces connected to the DMZ switch
- The IDS 'Manager' can be deployed in the CEN, if required by the Customer

## INTRUSION DETECTION SYSTEM (IDS)



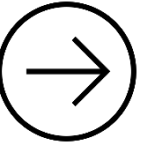


**RESPOND**

TAKE ACTION

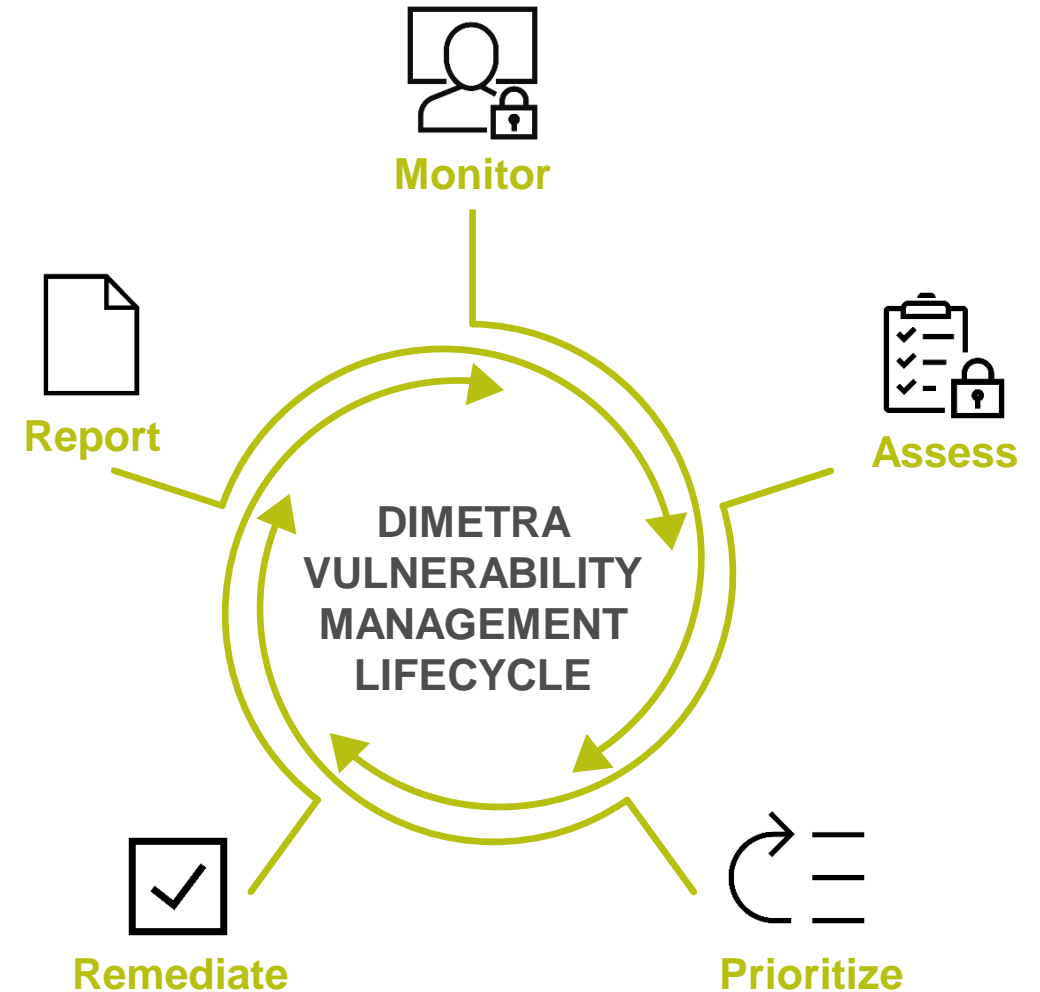


# VULNERABILITY MANAGEMENT LIFECYCLE



Workflow for DIMETRA that enables the continuous assessment of security vulnerabilities and their fix, against pre-defined resolution times, based on the published Common Vulnerability Scoring System (CVSS) severity

- Continuous monitoring of CVSS scores for major / critical DIMETRA components e.g. Operating Systems, 3rd party software, Firewalls, LAN switches, others
- Where a fix(es) is available, validate it. Where not available
  - Assess the impact of the vulnerabilities to DIMETRA (i.e. assessing the severity of vulnerability in the context of DIMETRA, creating a modified / lower severity and a different fix resolution time)
  - Develop fix(es) inline with the pre-defined resolution times. Where these cannot be met, develop appropriate compensating controls and make them available to our Customer(s), whilst the final fix(es) are being developed in parallel
- Fix(es) / compensating controls will be delivered by the most appropriate mechanism e.g. Motorola Solutions Technical Notification (MTN), via 'standard' patching process, Box Release, System Enhancement Release, System Release, etc.
- Continuously tracking and reporting
- **New proposed service – target launch Q2'21**



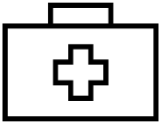




# RECOVER

RESTORE FUNCTIONALITY





# ENHANCED SOFTWARE UPDATE (ESU) BACKUP / RESTORE

## DIMETRA UPDATE AND RECOVERY

- Enhanced Software Update (ESU) is a framework for performing updates to DIMETRA system automatically. It covers:
  - Data backup
  - Data restoration
  - Software upgrades to DIMETRA systems automatically
- The framework is operated from the Upgrade Console with the upgrade software being distributed via the Upgrade Install Server (UIS)
- The backup and restore functionality allows the system applications to be backed-up for later restoration e.g. in the event of application / server failure
  - The backups can be stored on the 'Master UIS' or a designated 'Storage PC' attached to the system
  - Back-ups can be 'on demand' or scheduled to run at regular intervals

Note, it is recommended that the backups taken are exported and stored 'off-site', as per standard IT procedures





A police officer in a dark uniform and a peaked cap with a checkered band is seated in the driver's seat of a vehicle. He is holding a Motorola radio to his mouth with his right hand. The vehicle has yellow and blue reflective stripes. In the background, another officer is partially visible. The entire image is overlaid with a semi-transparent blue filter.

# KEY TAKEAWAYS





## KEY TAKEAWAYS

- We are the only Vendor to offer 3G AIE (GCK)
- We are the only Vendor to offers a comprehensive End-To-End Encryption (E2EE) Voice & Data solution
- We have a class leading Key Management Solution
- Not only do we offer complete protection for over the air communications but we also a complete set of features to provide protection of the network information to guard against cyber attack





A police officer in a dark uniform and cap is standing next to a white police car at night. The officer is holding a radio to his mouth. The car's door is open, and its emergency lights are flashing. The background is dark with some blurred lights from a city street.

# THANK YOU



**MOTOROLA SOLUTIONS**

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2021 Motorola Solutions, Inc. All rights reserved.