tait communications

Managing Encryption

A guide for public safety decision makers

White Paper

CONTENTS

General terms of use for Tait technical documentation. While Tait has taken every care to ensure that the information and contents are correct and up-to-date at the time of printing, the information may contain technical inaccuracies and/or printing errors. Tait does not guarantee the accuracy or correctness of the information. Tait cannot be held liable or responsible for errors or omissions in the contents of the technical documentation. All information contained in the technical documentation is given without warranties or representations, expressed or implied.

Disclaimer. Tait Limited marketed under the Tait Communications brand. Tait Limited expressly disclaims all warranties, expressed or implied, including but not limited to implied warranties as to the accuracy of the contents of this document. In no event shall Tait Limited be liable for any injury, expenses, profits, loss or damage, direct, incidental, or consequential, or any other pecuniary loss arising out of the use of or reliance on the information described in this document.

INTRODUCTION

Secure radio communications are essential for public safety organizations wanting to improve the safety of their staff and the communities they serve. Often crucial and sensitive information may be exchanged by staff using a radio communications network, especially those staff carrying out tactical operations. However, if intercepted by third parties, this information could assist criminal movements or compromise the safety of staff as well as the general public. Hence the reason public safety organizations choose to incorporate encryption into a radio solution.

Encryption in a P25 radio is a service provided to enable secure voice and data communication. A group of radios may be assigned a unique key to allow users to communicate securely. Users of these radios can then send a message which is digitized and encrypted (locked) and can only be decrypted (unlocked) and received by those radio users with the same unique key.

Encryption is commonly believed to be the silver bullet to solving issues with insecure communications. However, investing in encryption is a long-term commitment. Purchasing encrypted radios and keying tools is only the start.

There are a number of threats to any secure radio communications and, perhaps surprisingly, the primary threat to any encryption is not someone guessing or calculating the key. The biggest threat to secure encryption comes internally. In particular, key and radio mismanagement can leave an organization more vulnerable than if they do not have encryption. If encryption is compromised as a result of poor key management procedures it can often lead to a heavily increased workload, result in heavy financial costs or worse: put first responders and the public in danger. Here are some issues for public safety decision makers to consider when assessing the security needs of their radio communications.

SYSTEM SECURITY

LEVEL OF SECURITY

Under-investing in encryption or acquiring the wrong type of encryption tools may mean an organization does not have the level of safe communications needed for front-line staff to carry out their job. Just as important as what is purchased is how the encryption is managed. If an encryption solution does not have allocated resources and the right processes, then the communications may be more vulnerable than if encryption is not used, due to the level of security perceived by radio users. To have good management practices there needs to be an investment of resources and time. So what is the real impact of an encryption solution on a team's budget and workload? Understanding the right encryption tool may save your organization time and money in the long term.

Organizations that require high-level security may need to consider implementing full encryption on all radios; however the goal at all times should be to optimize security, not to maximize it at the expense of operational flexibility. This will also require the right resources to be allocated to rekeying and updating of radios. Any person repairing or programming a radio associated with a highly-encrypted system may need a key filler to load all the keys, as well as access to the UKEK (Unique Key Encryption Key) and OTAR (Over-The-Air Rekeying) details.

Radios with full encryption are likely to also require configuration and testing by technical staff with appropriate security clearances before they are returned to the fleet, meaning valuable radios or vehicles can be out of action in the workshop for longer than necessary. However, if radios can operate on some channels without encryption it means that they can be more easily commissioned and returned to operation after installation, repair or upgrade.

ENCRYPTION CONSIDERATIONS

END TO END

For encryption to be effective, it must secure communications from end to end. Radio users who know their system is not secure will be circumspect in what they say over the air. Users who believe their system is secure are likely to communicate more freely – a major risk if encryption is incomplete by design or procedure.

A commonly overlooked flaw is the playing of speech out of speaker microphones and in-vehicle speakers, or the use in a dispatch center of unencrypted wireless headsets. Encrypted systems must be made secure by design, taking such factors into account, as well as issues such as linking infrastructure and gateways to less secure systems.

MANAGING ENCRYPTION KEYS

With some encryption solutions all key-sets in an entire fleet must be changed at one time – so the need to change one key for one user group monthly mandates the changing of all keys monthly. This is very difficult as it can impose significant demands on system air-time and in turn it becomes difficult keeping all radios up to date. Due to some of these constraints some fleet managers make the decision not to change their keys! Encryption managers should consider how the system supports the changes of keys between different user groups on the system when determining the encryption rules and processes for their organization.

ASSET MANAGEMENT

ISSUING EQUIPMENT

It is important to understand which radio belongs to which individual in your organization. This can be recorded by radio serial number and P25 radio ID. If a radio is lost, dispatch can have that radio inhibited immediately.

Public safety decision makers should consider the operational impacts of the choice between using a pool radio system or personally issuing equipment. Many public safety organizations prefer to issue radios directly to personnel because they are more likely to be better maintained, more quickly reported when lost, easily identified on the system and able to be personalized with specific accessories.

However, it is not uncommon for an additional pool radio system to be utilized. A compromise can be to allocate radios to all users who have highly secure keys and pool only the radios required for low security operations.

When a pool system is used, it is important to detail the radio identity and record the whereabouts and user each shift. This means if an officer reports a radio lost, then it can be easily identified and inhibited or, in the worst case, the loss will be detected by the end of the shift.

This system will also aid a dispatcher who receives an emergency call from an unidentifiable person. The dispatcher can use the radio ID to help identify who the radio was issued to at the start of the shift.

WORKLOADS AND WORKFLOW

A Key Fill Device (KFD) allows an organization's encryption specialists and radio technicians to manage their workflow; making the process of encrypting digital radios as efficient and error-free as possible. The use of such a device for key management is best suited to smaller organizations or tactical teams that can rekey radios by plugging into each individual radio.

If you have determined that key fill devices are the best option for your organization then consider how they will be used. Some will require an encryption expert to be on hand to work the device and distribute the keys. Others may have software features that can allow non-technicians to distribute keys in the field simply or create new random keys or to hold keys temporarily until they can be stored in a key management facility. Not all key fill devices are created equally.

A Key Management Facility (KMF) is a client-server system that enables organizations to deploy, store and manage P25 encryption keys. This is essential for larger organizations that have a large fleet of radios, numerous levels of security or several teams and fleets requiring different encryption. Organizations will be able to rekey radios over the air, stage the rekeying of radios so more secure teams have more frequent rekeying and identify genuine problems without needing to touch the radio.

However, the full benefits of a key management facility will only eventuate if the facility suits the needs of your administrators. A system that is too taxing or not user-friendly may negate any intended benefits. So consider administrators' needs: will they remotely inhibit/zeroize radios, send key updates to specific teams or regions rather than an entire fleet or assign radios to teams? Is it important to have a manageable interface, to be able to filter and track specified radios on screen, or to have a key management facility that can work in unison with a key fill device?

ENSURE THE RIGHT FIT

MATCHING TECHNOLOGY TO THE ORGANIZATION

Matching the encryption tools to the organization's size is beneficial. Organizations that have a high need for encryption will require OTAR on the radios and KMF on the system, which will have an install cost and a run-time cost. If a larger organization only invests in a key fill device then there could be lengthy delays when keying radios.

OTAR is often perceived as the best solution for encryption management as it allows for radios to be reprogrammed while still in the field. However OTAR is not free, not completely automatic and in many cases it is less effective than it could be due to system constraints.

The provision of OTAR on all channels can create two levels of increased workload; commissioning and over-the-air time. For each radio registered on the KMF, it is necessary to load some initial key material and other details into the radio using a key fill device. It is also necessary to load the corresponding data into the KMF before re-keying can operate over the air.

Completely keying a new radio may take a significant amount of system airtime – this depends on how many keys are being deployed and whether they are DES (Digital Encryption Standard) or AES (Advanced Encryption Standard) keys.

The more radios with keys deemed high security, then the greater the burden on OTAR services, and therefore on radio system airtime. Due to the length of airtime a radio may require to rekey, and since voice calls may take priority over any data calls, on some busy systems a KMF may continuously retry to key a single radio but ultimately "give up". This is not because of any product or protocol fault – it is just that the radio and the radio system is working hard on voice calls. This is effectively a mismatch of technology to operating environment.

EQUIPMENT INVESTMENT

For any funding that may be available to purchase encryption-enabled products, check whether there are any technology or compliance requirements. Some funding may specify that a system must have specific encryption, such as AES, or that the encryption must have passed a specific encryption standard such as FIPS 140-2[1] (Figure 1). The easiest way to prevent purchasing the wrong level of encryption is to deal with a manufacturer that offers an entire standards-based encryption suite, including key fill device, key management facility and OTAR-enabled radios that have FIPS 140-2 accreditation.

INTEROPERABILITY

Purchasing radios from one manufacturer does not mean an organization needs to purchase encryption tools from the same vendor or vice versa. Interoperability

Footnote

[1] This indicates that encryption techniques have been analyzed by independent experts and found to be robust. The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards.

among P25 radio manufacturers is becoming more transparent, especially with the launch of the P25 Compliance Assessment Program (P25 CAP), which tests the performance and interoperability of P25 radios and base stations.

Project 25 endorses AES and DES encryption (for purposes of backwards compatibility) and the P25 standards include a standardized key fill interface and a standardized OTAR service which enables interoperability between key management devices and encryption devices produced by different manufacturers. A KMF can be used to rekey radios from any manufacturer that has implemented standards-based OTAR. Encryption managers can check the open standards support and evidence of interoperability of any encryption product being sourced.

PRIVACY VS ACCESS

Privacy laws and obligations can differ between jurisdictions, so it is important to examine whether there are any special laws and requirements that apply to your organization.

Contrary to protecting privacy are the goals of promoting interoperability and organizational transparency. Organizations may find that all their general duties communications must be publicly available to media and other parties. This is one reason to run a dispatch channel in the clear (non-encrypted). Some networks are designed with clear dispatch channels to satisfy such requirements, but have a separate 'inquiries' channel that is always encrypted to ensure there is at least one outlet for secure communications.

CONCLUSION

With so much to consider, encryption may be appearing more like a hindrance than a help. However, when encryption is well managed front-line staff will have the confidence to communicate during operations without the concern that eavesdroppers may be listening in to tactical conversations.

An organization's size, geographic spread, location and security levels will need to be determined even before investing in the right encryption solution. But once that investment is made then there needs to be ongoing resources dedicated to minimize the threat of encryption vulnerability.

While there is a number of issues to be considered, the good news is there are just as many tactics that can be incorporated to successfully manage encryption. With a good plan up front and an appropriate solution, managing encryption effectively will be a worthwhile investment.

THREAT MATRIX

Threat	Impact	Investigate
System security	Interception of communications, impacting officers' and citizens' safety.	▸ Have I got the right technology fit? ▸ Are there "holes" in other areas: people, processes? ▸ How safe are my keys? For example, are they too widely distributed? Or is a common UKEK deploy on all radios?
Level of security	▸ Reduced speed and quality of response. ▸ Teams can't talk. ▸ Wasted dollars on equipment. ▸ Administrative burden (radios/vehicles out of action for longer).	▸ How can I optimize security: not maximize it at expense of operational flexibility? ▸ Do all of my staff need the same kind of encryption?
Encryption considerations	Interception of communications, impacting officers' and citizens' safety.	▸ Is encryption end-to-end, integrated with other equipment and applied to info like vehicle location data? ▸ Does my vendor supply a suite of encryption solutions and valuable systems-based expertise?
Managing encryption keys	▸ Inability to easily update encryption across teams, time and territory. ▸ Encryption cannot be matched to the roles, location and mission of those needing to communicate.	▸ Who needs which level of encryption, for what purpose? ▸ How easy is it for my staff to update encryption to match my dynamic organization?
Asset management	Delayed or limited response to lost and stolen radios.	Can I readily see the disposition of my assets? Can I configure my KMF screen by team or by area to make the fleet information more user-friendly?
Workloads and workflow	▸ Highly trained crypto- specialists could be wasting time programming radios. ▸ Too many radio technicians are being given access to too many keys.	▸ How are my workloads and workflow building to my goal of effective encryption management? ▸ Are the right people doing the right things with the right tools?
Matching technology to the organization	Inappropriate match of technology to requirements may result in a solution that is under- or over-secure.	Can I choose a key provisioning solution that matches the scale, complexity and operational needs of my organization?
Equipment investment	▸ System could contain non-standards based components or proprietary "hooks" that reduce choice and competition.	▸ Will encryption tie me to any particular vendor? ▸ Can my systems accommodate a phased digital upgrade? ▸ Can I get funding for my system?
Interoperability	Lack of coordination across agencies or between different vendors' products, impacting efficiency and officers' and citizens' safety.	▸ Are my vendors participating in the P25 CAP Program? ▸ Are they approved to Federal Information Processing Standard (FIPS) 140-2? ▸ Can a Key Management Facility (KMF) update other manufacturers' radios?
Privacy vs access	▸ Breach of Freedom of Information obligations. ▸ Perceived lack of transparency.	Can I run provide appropriate access to all stakeholders without compromising safety?

GLOSSARY

AES Advanced Encryption Standard: Very secure 256 bit Encryption algorithm. Is now released as FIPS 197

CAP Compliance Assessment Program: The P25 CAP is a partnership of the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), the P25 radio industry, and the emergency response community. The P25 CAP establishes an independent compliance assessment process to ensure communications equipment interoperates, conforms to P25 standards, and meets performance requirements.

DES Digital Encryption Standard: US encryption standard for non-classified text, published as FIPS standard 46-3. 64 bit key (56 bits + 8 parity check bits)

FIPS Federal Information Processing Standards

KEK Key Encryption Key: An encryption key used specifically for the encryption of other keys. A KEK is used whenever secure OTAR messages are transmitted.

KFD Key Fill Device: The generic term used for computing devices that deploy encryption keys to radios using wires (instead of over the air)

KMF Key Management Facility: The generic term used for a computing device that deploys encryption keys to radios over the air (OTAR). Key management facilities will also deploy keys to networked devices using OTAR protocols over Ethernet.

OTAR Over-The-Air Rekeying: Used for encryption key management. General name for the protocol used for rekeying radios over a radio link.

UKEK Unique KEK: When messages are transmitted between a KMF and a radio they are encrypted with a unique KEK. The KEK is unique to that radio and known only by the radio and the KMF.

Author: Simon Britten