

# P25 Encryption Management

Improving radio communications security

Presented by: Simon Britten  
Senior Product Manager – P25  
**Tait Radio Communications**  
[taitradio.com/encryption](http://taitradio.com/encryption)



## **Disclaimer**

Tait Electronics Limited marketed under the Tait Radio Communications brand.

Tait Electronics 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 Electronics 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.

Copyright © 2010 Tait Electronics Limited.  
Not to be reproduced without the permission of Tait Electronics Limited

## Learning objectives

- **Discover why P25 encryption management is so important for public safety**
  - How it will improve the safety and efficiency of front-line staff
- **Understand why you need to manage P25 encryption**
  - The benefits of better encryption management
- **Find the best method of P25 encryption for your needs**



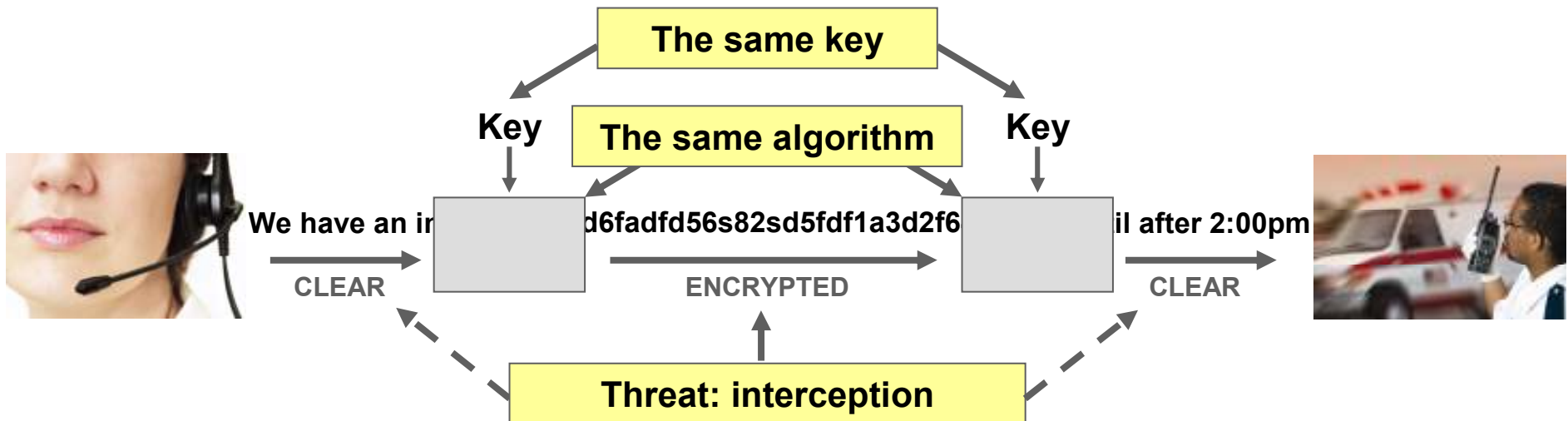
# Agenda

- **Introduction to P25 encryption**
- **What are the threats to your system?**
  - Keeping your fleet secure
  - Dangers of poor asset management
- **P25 encryption management in practice**
  - Case study
  - Encryption components
- **What is the best method for me?**
- **Good P25 encryption management**



# What is P25 encryption?

- Enables secure communication of voice and data between parties across a P25 system
- What is the encryption process?
- Security in these systems is based on keeping the keys secret, not the algorithm secret



## Levels of P25 encryption: DES & AES

- **DES: 56 bit key (secure)**
  - Maintains compatibility with older radios
  - Interoperability (triple DES)
- **AES: 256 bit key (more secure)**
  - Normal choice for most organizations
  - Replacing DES due to regulatory forces (Govt.)
- **How to choose?**
  - Main technological difference: key length
  - Interoperability requirements?
  - External mandates?



# The importance of good practice



## Brazilian banker's crypto baffles FBI 18 months of failure

By [John Leyden](#) • [Get more from this author](#)

Posted in [Enterprise Security](#), 28th June 2010 11:49 GMT

Cryptographic locks guarding the secret files of a Brazilian banker suspected of financial crimes have defeated law enforcement officials.

Brazilian police seized five hard drives when they raided the Rio apartment of banker Daniel Dantas as part of Operation Satyagraha in July 2008. But subsequent efforts to decrypt files held on the hardware using a variety of dictionary-based attacks failed even after the South Americans called in the assistance of the FBI.

The files were encrypted using Truecrypt and an unnamed algorithm, reportedly based on the 256-bit AES standard.

Source: The Register [http://www.theregister.co.uk/2010/06/28/brazil\\_banker\\_crypto\\_lock\\_out/](http://www.theregister.co.uk/2010/06/28/brazil_banker_crypto_lock_out/)  
Reproduced with permission

# Why is P25 encryption needed?

- **Essential feature for organizations needing secure communications**
- **Increased safety and efficiency of public safety personnel**
- **To ensure voice transmissions are accessed only by authorized personnel**





# What are the threats to your system?

- **Interception due to:**
  - Poor system design
  - Poor radio procedure
  - Lost radios / unknown lost radios
- **Lack of operability or interoperability**
  - System too secure
  - Mismatched encryption algorithms

**Encryption management is the solution**



# Keeping a fleet secure

- **Good asset management:**
  - Control of physical assets (radios)
- **Solution components:**
  - Key Fill Device (KFD)
  - Key Management Facility (KMF)
  - Over-The-Air Rekeying (OTAR)



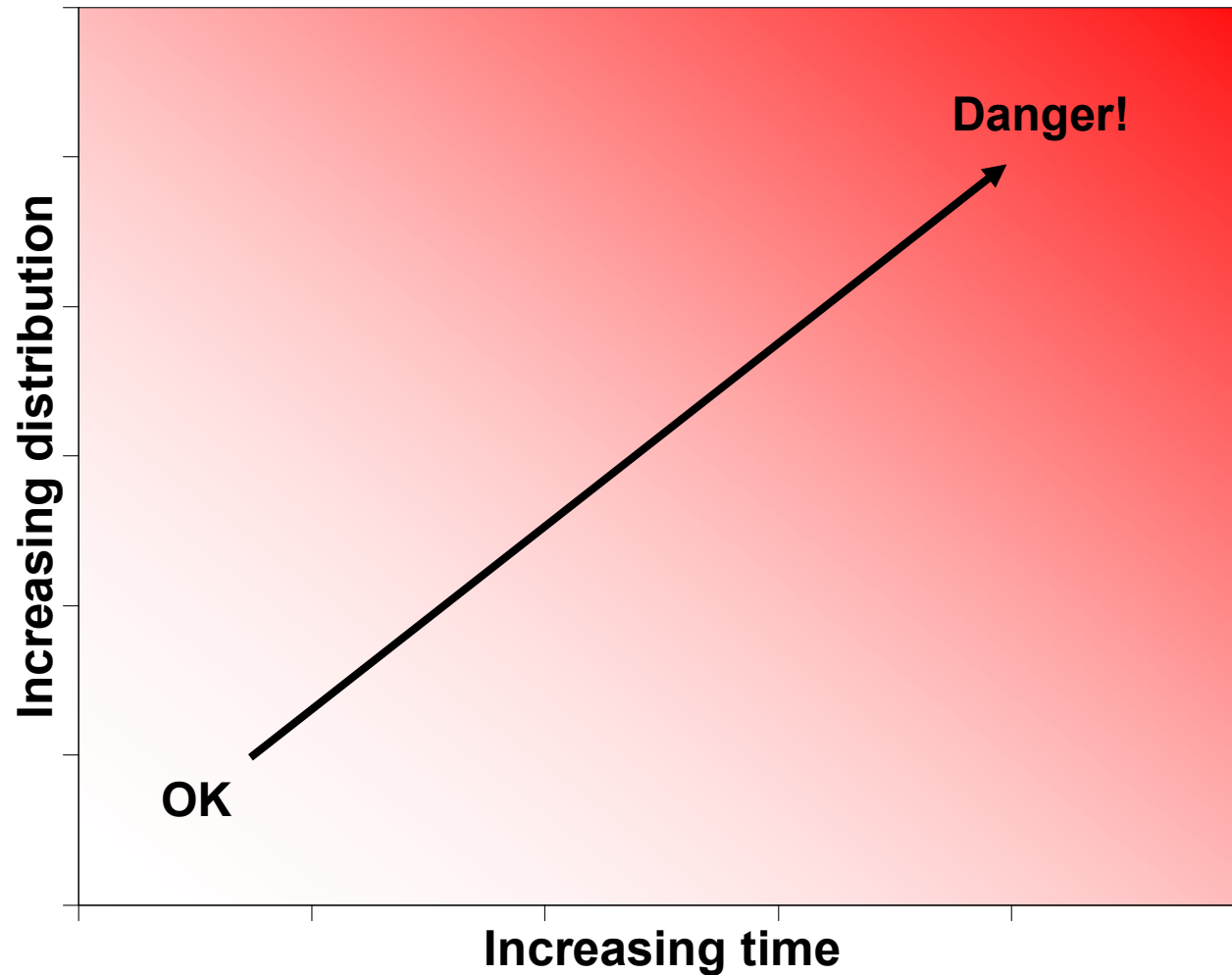
## Poor asset management: the dangers

- Information and lives can be compromised
- Financial loss
- Increased work load

Mismanagement will leave you just as vulnerable as if you did not have encryption at all



# Increasing key usage = decreasing security

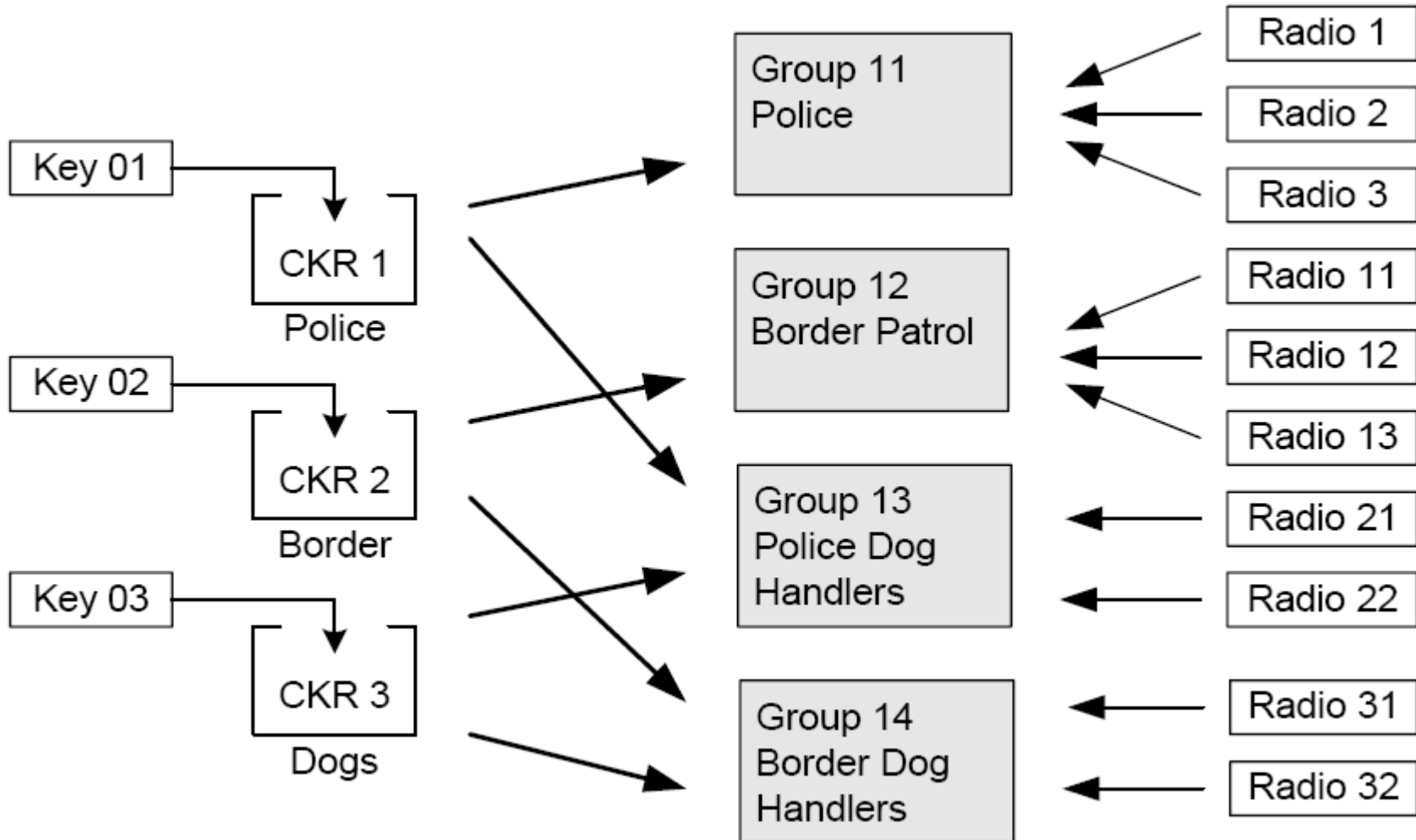


# P25 encryption management in practice

- Not all keys need to be as secure as each other

Channel Type	Frequency of Rekeying					
	Per Operation	Daily	Weekly	Monthly	Annually	Never?
Chat	[Shaded]					[White]
Dispatch	[Shaded]			[White]		
Private Information	[Shaded]					[White]
SWAT	[Shaded]		[White]			
Surveillance	[Shaded]					[White]
Special Operations	[Shaded]	[White]				

# P25 keys, CKRs, groups, radios



## Case study:

	Zone A	Zone B	Zone C	Zone D	Zone E	Zone F
	Patrol		Tactical	Investigations	Interagency	Municipal
Channel 1	DISPATCH1	BORDER	TAC1	VICE	INTER1	PARKING
Channel 2	DISPATCH2	MARINE1	TAC2	INTEL	INTER2	WASTE
Channel 3	ENQUIRIES	MARINE2	TAC3	DRUG1	NRTH1	WORKS
Channel 4	TRAFFIC	GANGS	TAC4	DRUG2	NRTH2	WATER
Channel 5	INFO	EVENT2	DOGS1	ROBERY	SOUTH	AIRPORT
Channel 6	EVENT1	EVENT3	DOGS2	HOMICD	INTER2	ROADS

Team	CKR	CommonKey	IntelKey	PD Key	Inv_Key	Tac_Key_1	Tac_Key_2
		CKR101	CKR102	CKR103	CKR104	CKR105	CKR106
General Duties		Yes					
DogSquad		Yes		Yes		Yes	Yes
SWAT		Yes		Yes		Yes	Yes
Investigators		Yes		Yes	Yes	Yes	Yes
Drug Squad		Yes			Yes		
Undercover		Yes	Yes	Yes			
Municipal Workers							

General Duties	DogSquad	SWAT	Investigators	Drug Squad	Undercover	Municipal Workers
Radio1001	Radio1095	Radio1350	Radio1501	Radio1007	Radio1812	Radio2001
Radio1002	Radio1096	Radio1351	Radio1502	Radio1428	Radio1025	Radio2002
Radio1003	Radio1158	Radio1176	Radio1503	Radio1429	Radio1048	Radio2003
Radio1004	Radio1175	Radio1804	Radio1504	Radio1430	Radio1123	Radio2004
Radio1005			Radio1748			Radio2005
Radio1006						Radio2006
etc...						etc...

Key Name	CKR	Crypto-Period			
		Monthly	6 Monthly	BiAnnual	Never
CommonKey	CKR101				Yes
IntelKey	CKR102	Yes			
PD Key	CKR103			Yes	
Inv Key	CKR104		Yes		
Tac Key 1	CKR105		Yes		
Tac_Key_2	CKR106		Yes		

## P25 key-filling: Key Fill Device

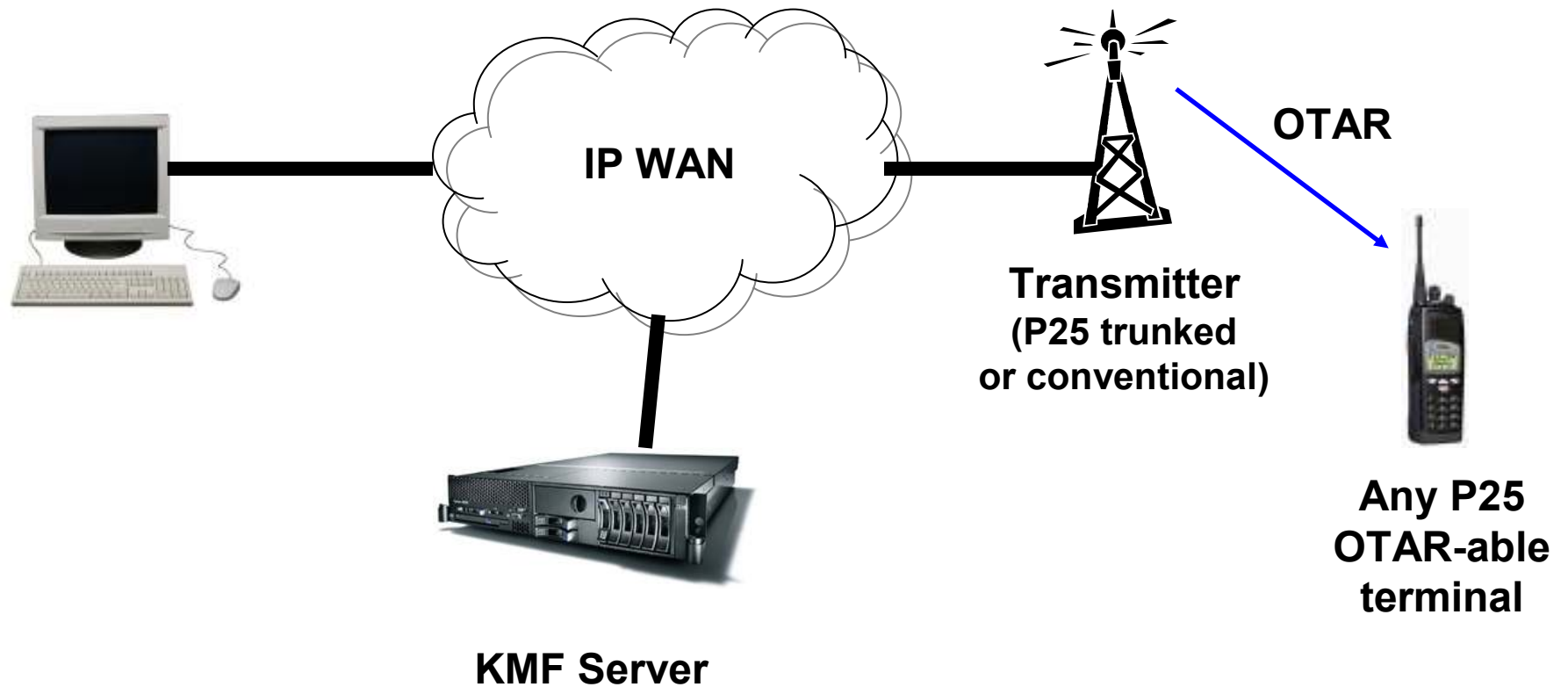
- Hand held device used to deploy keys to a radio using wired protocol
- This is the easiest and simplest means of securing a small radio fleet
- Used to program radios with UKEK and radio identity information
- Can be used to program radios with traffic keys
- P25 standards include a standardized key fill interface

Great for small fleets and deploying keys in the field





# P25 key-filling: remote control



## P25 key-filling: Key Management Facility

- Centralized, client-server type system
- Manages radios, groups and keys in a fleet over-the-air
- Use to inhibit and un-inhibit radios

### Major KMF features:

- Quickly identify and respond to genuine radio problems
- Deployment of keys to radios
- Understand the currency of your fleet
- Rekey as required

**Great for large fleets and deploying keys via OTAR**



## P25 key-filling: Over-The-Air Rekeying

- **Fast and efficient way of sending new keys to all radios within a defined group**
- **Requires:**
  - OTAR software in subscribers
  - A Key Management Facility (KMF)
  - Good encryption management planning
- **Benefits of OTAR: more efficient use of your money and time**
  - Scheduled key updates
  - Responsiveness to lost / stolen radios
- **P25 standards provide a standardized OTAR service**



## What's the best method for me?

- **KFD**
  - Simplest and easiest to get running
  - Ideal for smaller fleets
  - Limited control over who gets which keys
- **KMF and OTAR**
  - Centralized encryption management
  - Highly optimized for large fleets
  - Total control over all key management and group membership
  - Rapid response to lost / stolen radios



# Good P25 encryption management

- **Secure radio system**
- **Increased staff security**
- **Efficient use of staff time**
- **Reduced threat of eavesdropping**
- **Less equipment maintenance**
- **Long term investment and money saver**



# Any questions?



# Thank you



[taitradio.com/encryption](http://taitradio.com/encryption)