

## Technical brief: End-to-end security for software radio

Founded in 1979, IPL has a long history of successfully delivering excellent value consultancy and end-to-end software-intensive solutions to both the public and private sectors.

IPL's consultancy is renowned for its quality and value. Our consultants are talented and independent-minded individuals with extensive industry experience. We consistently exceed our clients' expectations through a combination of imaginative thinking, managerial and technical expertise and many years of systems engineering experience.

IPL's track record in end-to-end software solutions development is exceptional. Our proven development methodology allows us to cut through technical complexity, manage risk and completely focus on delivery. We consistently deliver reliable, efficient and accurate systems to a precise schedule.

IPL is an ISO9001:2000/TickIT registered company having a permanent workforce of 240, revenues of ca. £21M p.a. and 40,000 sq ft of secure office space in central Bath.



### TETRA Crypto key management in software defined radio

#### TETRA

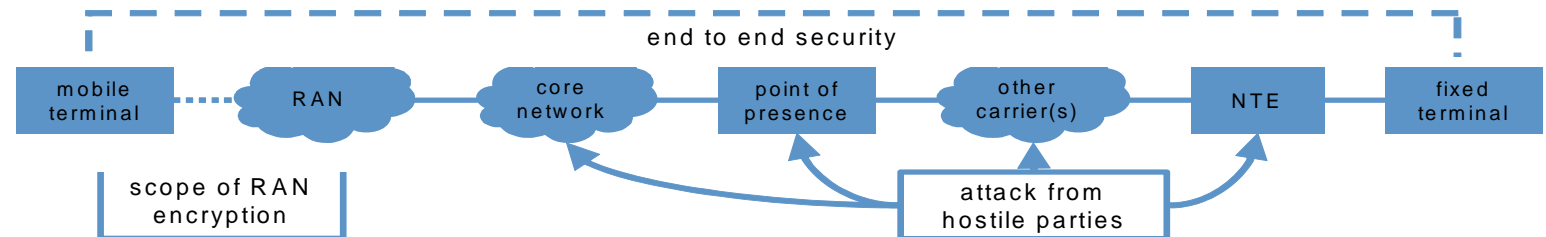
TETRA (TErrestrial Trunked RAdio) is the leading standard for digital professional mobile radio. It is used by emergency services both in the UK and around the world. While TETRA is similar to GSM in using FDMA and TDMA in the radio layer, TETRA is superior to GSM in a number of respects. TETRA provides voice and data communications with levels of resilience and availability that GSM can't match. TETRA offers group calling and direct mode operation, service features that are specific to the emergency services. Group calling means that one user (for example, a police dispatcher) can simultaneously speak to a group of mobile users. Direct mode operation means that users can call each other directly, without having to go via any fixed network infrastructure. This feature allows TETRA to support users in extreme situations where normal mobile networks cannot be relied on to reach.

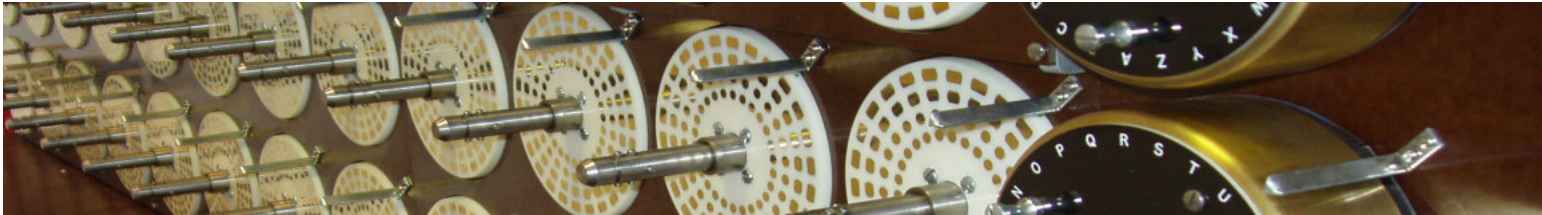
TETRA originates from the TETRA MoU organization, and is standardized through ETSI.

#### End-to-end security

While TETRA, like GSM, provides security in the radio access network through encryption and authentication systems, TETRA user data travels unencrypted across the core network. This makes TETRA unattractive to some specialist users who have extremely demanding information security requirements: for example, in covert military and anti-terrorist operations. End-to-End Network Security is designed to provide the highest possible level of information security, and to counter a new generation of complex threats.

In particular, end-to-end encryption addresses these concerns by encrypting data within the transmitting terminal, and only decrypting it within the receiving terminal(s). The plain text user data is never exposed within the infrastructure, and the infrastructure cannot get the keys with which to recover it.





## E2eS for TETRA

The TETRA end-to-end encryption enhancement (specified in TETRA MoU SPFG Recommendation 02 and related documents) adds end-to-end traffic data confidentiality to the system.

The system uses a two key hierarchy where each mobile device holds a single Key Encryption Key (KEK). The KEK is used to protect Traffic Encrypting Keys (TEKs), which are downloaded into the mobile devices in a 'sealed' format.

Clearly, the integrity of the system depends critically on the management and distribution of the KEKs, which have to be loaded locally into the TETRA mobile.

## Why IPL?

IPL has special expertise in the the crypto key management technology that controls the generation, storage and distribution of the KEKs for TETRA. This fits naturally with our strong background in crypto systems, our outstanding real time software engineering capability, and our defence-grade security infrastructure.

## Software defined radio

Software Defined Radio (SDR) is a radio communication technology where components that have historically been implemented in hardware are instead implemented using software in an embedded computing platform. While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics are making practical many processes that were once only theoretically possible.

SDR enables wireless systems to operate a range of airside protocols just by loading different software. Software radios have significant value for the military and security services, where the ability to swiftly change radio protocols can counter a range of 21st-century threats.

## Why IPL?

IPL has specific experience of end-to-end testing and system assurance for SDR, where our thorough, relentless and technically insightful systems testing can make a huge contribution towards field-hardening the systems.



Certificate Number FM 01589

## Contact information

Services Sales  
IPL Information Processing Limited  
Eveleigh House  
Grove Street  
Bath  
BA1 5LR

Tel: +44 (0) 1225 475000  
Fax: +44 (0) 1225 444400  
Email: sales@ipl.com

IPL 001 BRF T 41.1  
Copyright © IPL 2008  
All trademarks acknowledged  
Bombe image adapted from materials  
developed for the Jefferson Institute for  
Lifelong Learning by David Evans