ETSI TR 101 494 V1.1.1 (2000-02)

Technical Report

Terrestrial Trunked Radio (TETRA);
SIM;
Review

Reference
DTR/TETRA-07018

Keywords
PRM, radio, SIM, TETRA

ETSI

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Project Terrestrial Trunked Radio (TETRA).

1 Scope

The present document provides the following:

- a review of the state of the art of smartcards for potential use in TETRA (clause 4); and
- a consideration of areas in which future smartcards used in TETRA terminals may be applied (clause 5);
- a review of the correctness and completeness of ETS 300 812 [1] (clause 6).

ETS 300 812 [1] deals primarily with trunked mode MS operation. For direct mode MS operation further enhancements may be required and are identified in the present document.

The present document will not provide solutions for the technical issues which are identified therein.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ETS 300 812: "Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM - ME) interface".

[2] ETR 295: "Terrestrial Trunked Radio (TETRA); User requirements for Subscriber Identity Module (SIM)".

[3] ETS 300 641: "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.12 version 4.3.1)".

[4] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[5] ETS 300 608: "Digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11 version 4.21.1)".

[6] ISO/IEC 7816: "Identification cards - Integrated circuit(s) with contacts ".

[7] ISO/IEC 8859-1: "Information processing - 8-bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1 ".

[8] ETR 300-3: "Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Designers' guide; Part 3: Direct Mode Operation (DMO)".

[9] ISO 7816-1: "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".

[10] ISO 7816-2: "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts".

[11] ISO 7816-3: "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols".

[12] ISO 7816-4: "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".

[13] ETS 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[14] ETS 300 396-1: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 1: General network design".

3 Definitions, abbreviations and acknowledgements

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

applet: application that can only run in the context of a shell program. Most commonly applets are small applications run within a web browser. Technically an applet does not contain a *main()* routine.

E.164 [4**] :** ITU Recommendation for the presentation of international telephone numbers.

Mobile Equipment (ME): part of the mobile station which interfaces to the SIM card.

Mobile Station (MS): entirety of the equipment needed to communicate with the infrastructure (in trunked mode of operation) or direct with another mobile station (in direct mode of operation).

non-repudiation service: security service that provides protection against false denial of involvement in a communication. (See: repudiation.) A non-repudiation service does not and cannot prevent an entity from repudiating a communication. Instead, the service provides evidence that can be stored and later presented to a third party to resolve disputes that arise if and when a communication is repudiated by one of the entities involved.

repudiation: denial by a system entity that it was involved in an association (especially an association that transfers information) of having participated in the relationship.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
API	Application Programming Interface
CLIP	Calling Line Identity Presentation
DAWS	Digital Advanced Wireless Service
DECT	Digital Enhanced Cordless Telephone
DM-AUTH	DMO Authorization unit (for Managed DMO)
DM-GATE	DMO Gateway (to TETRA V+D)
DM-MS	Direct Mode Mobile Station
DMO	Direct Mode Operation
DM-REP	DMO Repeater
DM-REP/GATE	Combination of DM-REP and DM-GATE
EF	Elementary File
EFT	Electronic Funds Transfer
EMV	Eurocard Mastercard Visa
ETS	European Technical Standard
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile communication
IC	Integrated Circuit
IEC	International Electrotechnical Commission
IMSI	International Mobile Subscriber Identity
IMT2000	International Mobile Telephone 2000 (ITU standards track of 3GPP)
IN	Intelligent Networks
IP	Internet Protocol

IPR	Intellectual Property Right
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ITSI	Individual TETRA Subscriber Identity
JCRE	Java Common Runtime Environment
LAN	Local Area Network
ME	Mobile Equipment
MMI	Man Machine Interface
MS	Mobile Station
MSISDN	Mobile Station international ISDN number
OAP	One-step Approval Process
PC	Personal Computer
PDO	Packet Data Optimized
POS	Point Of Sale
PSTN	Public Switched Telephone Network
RPDI	Radio Packet Data Infrastructure
SDS	Short Data Service
SIM	Subscriber Identity Module
SMG	Special Mobile Group
SMG9	Study group 9 of SMG (responsible for SIM issues)
SNDCP	Sub-Network Dependent Convergence Protocol
SS	Supplementary Service
SwMI	Switching and Management Infrastructure
TETRA	Terrestrial Trunked Radio
TR	Technical Report
URL	Uniform Resource Locator
WAP	Wireless Application Protocol

3.3 Acknowledgements

The following acknowledgements of trademarks are made:

Gameboy	A trademark of Nintendo Corporation
Java	A trademark of Sun
JavaCard	A trademark of Sun
Multos	A trademark of MAOSCO (an industry consortium)
OASOS	A trademark of Keycorp
Windows	A trademark of Microsoft Corporation

4 Overview

4.1 Previous work in TETRA

The current ETS 300 812 [1] defines the interface between the Subscriber Identity Module (SIM) and the Mobile Equipment (ME) for use during the network operation phase of TETRA. In addition it defines those aspects of the internal organization of the SIM which are related to the network operation phase. This is to ensure interoperability between a SIM and an ME independently of the respective manufacturers and operators. The concept of a split of the MS into a separable SIM and ME is described in the User Requirement Specification ETR 295 [2].

The physical SIM described in ETS 300 812 [1] is a removable Integrated Circuit (IC) card. The SIM is an optional device within a TETRA MS. ETS 300 812 [1] does not preclude the implementation of fully functional MSs without a SIM. All references to mobile equipment in ETS 300 812 [1], and in the present document, are to be taken to mean mobile equipment, which have been designed to operate with a SIM.

4.2 Introduction

The base standards for smartcards are ISO 7816-1 [9], ISO 7816-2 [10], ISO 7816-3 [11], ISO 7816-4 [12] from which all operational specifications for smartcards are derived. ISO 7816-1 [9], ISO 7816-2 [10], ISO 7816-3 [11], ISO 7816-4 [12] define the physical nature of the card, the voltage levels at which a card is operated, and the physical interface constraints. Whilst the physical card is defined in a second set of standards bodies (de-facto, de-jure, and industry specific) further define the operation of smartcards within specific industries and associated equipment. ETSI is one of the second set of standards bodies and has developed specifications for GSM and DECT in addition to TETRA.

Telecommunications smartcards fall into two categories:

- Pre-paid subscriber independent telephone cards; and
- Subscriber authorization cards.

4.3 Card operating systems

Computing development has moved since its origins in the early 1940s (Turing and others) from machines being set up to perform one task at a time to the modern expectation of an operating system giving a level of abstraction from the hardware of the computer, and to manage the access of several different applications to that hardware. It can now be safely stated that smartcards have entered this generation. There are several operating systems vying for market share and in this TR we will only look at the development of Sun's Java™ for Cards (JavaCard™) environment as the primary tool for exploring the possibilities of smart cards. Alternative operating systems from card manufacturers and others do exist which provide equivalent functionality. These alternatives include Multos™, Windows for Cards™, and OASOS™.

4.4 Java™ in smart cards

The Java™ programming language offers the attraction of "write once, run anywhere" software. Whilst this is not strictly true where the target environments differ it is attractive in the ability to consider a smart card as an application holder.

Java™ offers a programmer the ability to write applets (small applications) and following the Object Oriented paradigm to inherit methods and data definitions from other (predefined) classes. Java™ although subject to inevitable error through poor implementation offers the security model of all strict object oriented methods by restricting visibility to data through the public interface (in this respect Java™ is more similar to the latest variants of the Ada language than its syntactic cousin C++).

In GSM the attractions of the JavaCard™ have already been examined and the GSM SIM API toolkit has been captured in an API for the JavaCard™ in the ETSI Technical Specification GSM 03.19 (ETS 300 641 [3]).

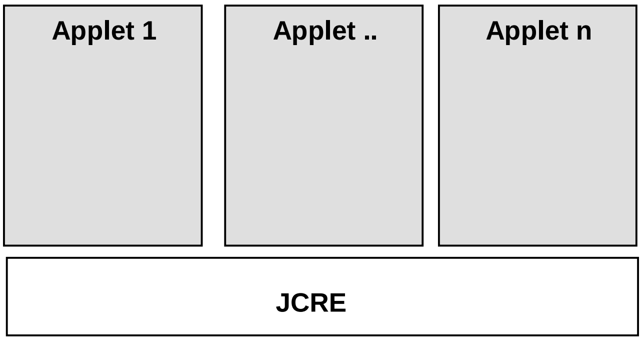

Figure 1: Applets lying over Runtime Environment

In GSM 03.19 (ETS 300 641 [3]) one Applet, set as the default, is the SIM toolkit. In a completely open card environment any applet can be initiated by the Java Common Runtime Environment (JCRE). In an ideal case, say the TETRA case, one applet may be the base TETRA Subscriber authorization applet, the other applets may be TETRA SDS control applets, TETRA Status control applets, WAP capability applets, server applets.

4.5 Radio terminal capability

The TETRA terminal is not specified in any of ETSI's standards. What is specified is the behaviour of the terminal in some specific instances, e.g. authentication and registration. It is quite possible that the TETRA standards are interpreted as a means to provide ubiquitous network access for applications, in other words that TETRA terminals become in part equivalent to the Ethernet cards used in PCs and LAN based devices. What this leads to is a possibility to move away from the mobile telephone look and feel of TETRA terminals towards a family of terminals that offer different forms of MMI.

In essence this means that the enabling data for a terminal, contained in a TETRA SIM, is but a small part of the capability offered by the SIM. For example a web-browser type of MMI may be used over TETRA (using IP and the SNDCP protocols) with the SIM offering basic access to the TETRA network (SwMI or RPDI for PDO/DAWS) and offering in addition a suite of terminal specific applications. Here we need to stargaze a little and consider a move in mobile networking from dumb terminals (the PSTN 'phone), through the client-server model, towards the distributed network, in which each element offers some capability to deliver service (applications). This may be seen as the SwMI/RPDI element offering part of a service, the radio terminal offering some, and the SIM or smartcard offering a final enabling application or data, or service.

In clause 5 some applications which may be enabled by a SIM capable TETRA terminal are considered.

4.6 Future smartcards

Existing smartcards are very largely based upon 8-bit processor technology, and largely (not exclusively) from developments of the 6800 processor series. Memory densities are quite low, operating voltage is high, and the external interface is slow. These factors are unlikely to remain constant and will improve over time. It is already known that 32-bit processors and multi-megabyte memory cards are in development in labs. When this is tied in to the abstractions of hardware possible in well defined operating systems we can expect smartcards to continue to extend the distributed computing model in networks.

The current weakest point of smartcards is their relative lack of robustness for multiple reuse, an example being contact wear, although this is being addressed by manufacturers. This can in part be countered by use of contactless cards but in such cases the radiation of data may be considered an unacceptable security risk. As technologies develop, and in particular when the contact methods improve data transmission rates across this interface, this will allow designers much greater leeway in apportioning subscriber data and subscriber specific applications across the network.

It is suggested in passing in the preceding paragraph that the SIM is part of the network. This is a matter being debated in many circles as the provision of IP as a network protocol in the elements we tend to consider historically as the "core" network, in the access network, and in the access terminals, means that the future model of communication is moving to one in which every network is a network of networks. In such a world the SIM is a network element offering subscriber data services.

5 Applications used in TETRA

NOTE: This clause refers to co-resident application using a common network access protocol in which the card is maintained in the terminal for operation.

In order to move the SIM in the directions suggested in this subclause the matter of SIM ownership has to be determined. A multi-application card will move towards the user as owner. Current single purpose use encourages the service provider to own the card and the data it has stored. This existing model does not encourage the future multi-application card where each application has a different target service provider. Perhaps the best known ownership model that we look to as analogous is the PC model developed by companies such as Microsoft and Apple. In these models the user buys a platform offering computing power and an operating system able to support applications. The user is then able to customize the function of the platform to his personal needs. In other words in the hands of a set of users the same computing platform may be word processor, an accounts station, a graphics workshop, or a design assistant.

5.1 Telephony

Technology independent roaming (migration). This application allows a user addressable identity (say an MSISDN like ITU-T Recommendation E.164 [4] format telephone number) to be dynamically associated with a network layer TETRA or GSM address, i.e. to map the MSISDN to either the ITSI or IMSI. The application also allows generic commands such as registration and authentication to enable technology specific methods and algorithms.

NOTE: Roaming in TETRA refers to intra-network movement between serving base stations, whilst migration in TETRA refers to inter-network movement. In some other mobile systems roaming is used to describe both the intra- and inter-network cases.

5.1.1 TETRA specific telephony

TETRA extends the conventional GSM mobile telephone model to encompass group calls and data services. In order to allow this the subscriber data covers the relation ship of individual to group, and the security features for group calls.

5.1.2 Pre-pay, or non-contractual service

SIM based pre-pay is not straightforward to secure. Future SIM based pre-pay systems are likely to move towards a distributed pre-pay model. Very probably this model will be based upon the Intelligent Network (IN) model with some elements of the transaction model (e.g. user identity, pre-pay scheme variant) retained on the SIM thus allowing SIM roaming to be maintained.

Purely SIM based pre-pay systems offer many opportunities for fraud as the credit information itself has to reside in the SIM. Of itself pre-pay is a service offered for subscribers making use of a network, therefore network based solutions to pre-pay where the SIM holds only the data to allow identification of a pre-pay as opposed to a the credit history or credit standing are likely to maintain a position of preference.

5.2 Terminal and data maintenance

NOTE: Applications in this group do not require the terminal to be connected to the network. This means that if a terminal is powered up but not connected to a network for telephony service it will still be possible to make use of the terminal to maintain data on the SIM.

5.2.1 Phone book maintenance

The user phone book may be updated (entries created, edited, deleted) by the user. Validation rules may be built into the application and network or technology specific parameters assigned to addresses (e.g. priority, scope, area selection restrictions).

5.2.2 Terminal customization

The MMI parameters may be stored and maintained on the SIM card. This will allow users to maintain the terminal look and feel (fonts, shortcut keys, icons, altering tones) when moving from terminal to terminal.

5.2.3 Profile selection

A user may be able to pre-set different terminal parameters as belonging to a profile and to select between profiles. This may allow a user to switch between a "business" profile and a "home" profile set in order to allocate billing or even ring tones. Another option may be to allow terminals and SIMs to be shared amongst closed user groups with each member of the group storing a preferred configuration.

5.3 Financial applications

TETRA (or similar network access methods) may be used to provide access for resident applications such as banking and Electronic Funds Transfer (EFT). In such a SIM based application the communication and financial applications run at the same time (using the multitasking capabilities of the card).

Applications in which POS facilities (e.g. bar code reading and data encoding) are co-resident with the TETRA network access to allow various forms of remote inventory and billing functions. Such facilities may be provided in parallel with EFT services.

5.4 Terminal location

Applications in which the SIM offers an enabling platform to bring network access (through TETRA) and location systems together to report location to the TETRA infrastructure.

5.5 Vehicle based systems

A TETRA terminal may be integrated into an intra-vehicle network offering communication capability of the local network to the wide area that will allow remote interrogation of diagnostic data. In emergency services vehicles such capability may be required as part of a non-repudiation service.

5.6 Voice recognition parameters

Many hands free devices require trained voice recognition. Whilst it may not be feasible to host a voice recognition application in full on a SIM it may be possible to store the training parameters on the SIM for transfer between terminals.

When coupled to voice recognition in a terminal the form of the man-machine interface may be allowed to develop towards a speaker/machine transportable voice command suite.

5.7 Miscellaneous

The items in this subclause may not be practical in existing SIMs but are given for consideration of future development.

5.7.1 Entertainment systems

Games such as those already extant on GSM terminals may be stored on the SIM. This may be used for marketing. Nintendo Gameboy™ like games may be traded in this way.

5.7.2 Memo recorder

Short voice messages may be stored on the SIM and played back using SIM resident applications (or applets).

5.7.3 Micro-browsers and micro-servers

If a Java™ device is used as the basis of the SIM it may be possible to use a micro web server application to host and offer the display of data using micro-web browsers either as applets on the SIM or terminal. Storing data in a class structure may offer more efficient data packing than that offered by byte-aligned file based structures.

In addition the SIM may be used to store URLs for the browser in a similar manner to the "favourites" and "bookmarks" of commercial browsers.

5.7.4 Auto-completion

This is a feature familiar to users of many PC software products in which the text entered in short hand form by the user is completed to a meaningful phrase.

6 Detail review of ETS 300 812

6.1 Introduction

It has been noted in the course of review of, and implementation of practical SIM card based upon, edition 1 of ETS 300 812 [1], that there are a number of errors (technical or editorial), conflicts (both internal and with other IC card specifications), and missing parts. This subclause identifies the errors, ambiguities and those additions required to make ETS 300 812 [1] more complete as a second edition.

These changes and modifications are essential to allow a SIM option to exist in the TETRA market. Failure to implement the changes in this subclause may indirectly lead to closure of a standard TETRA SIM on the market.

6.2 Editorials

Table 1: Editorial errors found in ETS 300 812 [1]

Where	Comment
Clause 5.7 Baud rate	Should read…'The baud rate for all communications shall be as defined in GSM 11.11 (ETS 300 608 [5])….'
Clause 6.2 file identifier	Should read… '2F' = EF under a MF '6F' = EF under a DF
Clause 8.1 & Clause 9.2.1 SELECT	There are references to INCREASE command, which is not used in TETRA. These need to be removed
Clause 8.17.4 TA71 algorithm	Should read…. Output to EF: MGCK (to EF_{MGCK})
Clause 9.3 coding of access conditions	Should read ' … on bytes 9, 10 and 11 of the response…'
Clause 10.2 Contents of the EFs at MF level	Should read… 'There are three EFs at MF level'
Clause 10.2.1 Card identifier	Should read… 'EF_{ICCID} (Card Identifier)
Clause 11.5.1 Username request	Should read '… procedure with EF_{UNAME}.
11.7.1 Dialling numbers	Should read '…and also to EF_{FDN},…'

6.3 Conflicts

Table 2: Conflict errors found in ETS 300 812 [1]

<table>
<tr><th>Where</th><th colspan="3">Comment</th></tr>
<tr><td>Clause 7.4, Table 2</td><td colspan="3">Level 5 is used by TETRA for AUTI however in GSM this is reserved for ADM.
Is this access condition really needed? With the advancement made with TETRA security has this become obsolete or is there another method to protect the data?</td></tr>
<tr><td>Clause 9.2 Coding of commands</td><td colspan="3">The following instruction codes already exist:
'76' Lock command already defined in EN726 part 7
'22' already defined in ISO/IEC 7816 [6]
'58', '5A', '5C' and '5E' already defined in EN726 part 7</td></tr>
<tr><td rowspan="5">The following EFs are out of alignment with the current version GSM 11.11 (ETS 300 608 [5])</td><td><b>EF</b></td><td><b>TETRA</b></td><td><b>GSM 11.11 (ETS 300 608 [5])</b></td></tr>
<tr><td>EF_{PHASE}</td><td>'6F06'</td><td>'6FAE'</td></tr>
<tr><td>EF_{AD}</td><td>'6F32'</td><td>'6FAD'</td></tr>
<tr><td>EF_{LP}</td><td>File size: 1 – n
Length: 1
M/O: M</td><td>File size: 2n
Length: 2
M/O: O</td></tr>
<tr><td>EF_{SPN}</td><td>ID: '6F14'
SPN-coding: ISO 8859-1 [7]</td><td>ID: '6F46'
SPN-coding: GSM03.38</td></tr>
<tr><td>There is no need to specify an EF_{CHV}</td><td colspan="3">The preferred method is to hand over the specification of this file to the smartcard manufacturers
The required procedures for CHV verification are implemented in the command VERIFY CHV, there is no direct access of the ME to this file required and therefore EF_{CHV} should be removed from the specification</td></tr>
<tr><td colspan="4">NOTE: ETS 300 812 [1] was based on an early version of GSM11.11 and one of the main aims of EPT.7 at that time was to remain compatible with GSM11.11. This would make co-existence on a multi-application card easier.</td></tr>
</table>

6.4 Additions

In light of changes to ETS 300 392-7 [13] in which TETRA security is now based upon a class then the SIM needs to reflect this. This involves extension of the file EF_{SEC} as shown in table 3.

Table 3: Modifications to file EF_{SEC}

Name	Length	Coding	Notes
Mutual authentication flag	1	0	Not required
		1	Required
Authentication flag	1	0	Not required
		1	Required (note)
Security class	2	00	Class 1
		01	Class 2
		10	Class 3
		11	Reserved
NOTE: If security class 3 then this bit shall be set to 1.			

Support of DMO in the SIM as described in ETS 300 812 [1] is restricted to support of some of the security functions. Full support of DMO is required to cover the following DMO variants (see also ETS 300 396-1 [14] and ETR 300-3 [8]):

- DM-MS;
- DM-REP;
- DM-GATE;
- DM-REPGATE; and
- DM-AUTH.

Edition 1 of ETS 300 812 [1] does not contain an elementary file to hold the subscriber's telephone number as either an MSISDN as per GSM, or as international number in ITU-T Recommendation E.164 [4] format. This may inhibit the support of SS-CLIP (Supplementary Service - Calling Line Identity Presentation).

6.5 Support of evolving IC technologies

As smartcard technology evolves we need to ask some questions regarding the technology specified for the TETRA SIM. These should include:

- Do we wish to maintain alignment to GSM 11.11 (ETS 300 608 [5]) in release 3 (the core specification for smartcards in GSM)?
- Do we wish to allow application co-existence on a 'SIM' card?
  - If yes, how much do we address this in edition 2 of ETS 300 812 [1]?

7 Conclusions and recommendations

7.1 Recommendation #1

To modify ETS 300 812 [1] to a second edition based upon the content of clause 6 of the present document. This work to be completed for submission to the ETSI One-step Approval Procedure (OAP) procedure in Q1 2000.

This work to be done within EPT.7.

7.2 Recommendation #2

To investigate with other forums and card issuing organizations the ownership model for SIM cards to allow a user to have multiple applications resident on a personal card. This is analogous to the PC ownership model in which the user and owner of the PC is free to load and run applications of his choice subject to license conditions of the software publisher.

This investigation should be done in close collaboration with SMG9, ISO, EMV, and evolving groups including 3GPP and IMT2000. In some instances close collaboration with legal advisers may be required to ensure IPR and data privacy legislation is respected.

This work is required to validate the market and technologies for a multi-application card, where each application is targeted to a different organization. For example financial applications aimed at the banking sector may have different requirements than those in the telecommunications sector.

This work to be started as soon as possible within EPT.7.

7.3 Recommendation #3

It is required to investigate the level of support required for compatibility with other standards published by other forums and standards bodies. This to cover amongst other things:

- Variable supply voltage (5V, 3V, 1.8V cards);
- Bootstrap procedures; and
- Alphabet selection (i.e. encoding of digits and letters as either 7, 8, 15, or 16 bits).

This work to be co-ordinated with other card standards development forums and organizations. It is likely that TETRA will only be required to observe and recommend adoption of standards developed by these and other bodies.

This work to be started as soon as possible in parallel to recommendation #2 with EPT.7 representing TETRA.

7.4 Recommendation #4

Following on from recommendations #2 and #3 to develop a new standard for TETRA SIM. This to develop an object model for a TETRA SIM application (or applet) as suggested in clause 4.

It is suggested that this work be started by EPT.7 immediately following submission of draft ETS 300 812ed2 as per recommendation #1 to OAP.

7.5 Recommendation #5

Methods of using a SIM in a live environment are not discussed in ETS 300 812 [1]. This in particular covers such issues as key management and distribution, and partitioning of storage space to optional elements such as user updateable phone books. It is recommended that EPT.7 in close collaboration with EPT.6 and EPT.1 prepare extensions to the TETRA designer's guide (ETR 300-3 [8]) suggesting methods of addressing these issues. This work should start in 1999 aiming for completion in the second quarter of 2000.

7.6 Conclusion

The current edition of ETS 300 812 [1] is invalid without the changes outlined in clause 6.

Further, it is shown that whilst making these changes and publishing a valid edition of ETS 300 812 [1] the smartcard technologies are moving towards a point where even that will be valid for only a short, although unassessed, period. Therefore given that EPT.7 has a duty to ensure that TETRA is able to profit from advances in technology it should undertake such work as is required to publish appropriate standards to capitalize upon such advances.

History

Document history		
V1.1.1	February 2000	Publication