A Study on Implementation Aspects of Galileo Conditional Access Service

Stig F. Mjølsnes
SINTEF Telecom and Informatics

March 10, 2000

SINTEF Technical Report STF40 F00045, Trondheim,15 May 2000.

Contents

Acronyms

CAS	Controlled Access Service
DAB	Digital Audio Broadcasting
DVB	Digital Video Broadcasting
GNSS	Global Navigation Satellite Service
GPS	Global Positioning System
MEO	Medium Earth Orbit
MPEG	Moving Picture Expert Group coding standard
NIM	Navigation Subscriber Identity Module
OAS	Open Access Service
PPS	Precise Positioning Service
PVT	Position, velocity and time
SIM	Subscriber Identity Module
SPS	Standard Positioning Service
UMTS	Universal Mobile Telecommunications System

Chapter 1

Introduction

1.1 Background

> Galileo will provide, as a minimum, three-dimensional positioning over landmasses, accurate to better than 10 metres horizontally. Galileo will provide a universal indepedent time reference on a global basis, similar to what the GPS system currently offers. Moreover, the Galileo system is scheduled to make commercially available value-added services, such as integrity, accuracy and availability certification, and support various "location-aware" network services and terminals.

According to current reports (Conclusion from [5]), a core Medium Earth Orbit constellation is considered to be the most cost-effective and technically proven approach for the initial deployment and provision of a basic service. The constellation needs to be fully integrated into a cohesive Trans-European position and navigation network. Adequate long-term spectrum allocation and full interoperability and compatibility with GPS are said to be critical.

A good level of security and a controlled access signal are also key features. This report investigates some of these challenges in a commercial environment. We limit the scope to the civil and commercial operation, leaving out the military/national concerns and control requirements.

The system comprises a central control unit that among other nodes connects through some terrestrial network to a satellite uplink node, and of course the downlinks of the navigation satellites to the mobile terminal receivers. The system can be broken down into the following segments:

- ground and control segment
- command and control communication links

- space segment
- navigation signal
- user segment

The report is mainly occupied with the access control mechanisms for the navigation signals from the MEO broadcast satellite constellation and the user segment. The proposals have consequences for the design of the other segments though.

1.2 Method, Objectives and Scope

Galileo is an initiative of the European Commission. This study is a contribution to the complementary development program of ESA named GalileoSat.

The specific documents and meetings of the Galileo project available in this study have been References [5, 4, 6, 7, 8]. Professor Børje Forssell has been actively involved in the project work, by supplying litterature [1] and knowledge on GNSS, by several internal discussion events by responding to questions, ideas and proposals, an by commenting on this report. In addition, I found References [2, 3] helpful in understanding GPS technology. My collegue Knut Grythe validated the feasibility of the spread spectrum structure proposal of Section 4.6.

The ESTEC Statement of Work stated the following study objectives:

> The implementation of the controlled access, in particular for the very large number of commercial users will require certain provisions with regard to frequencies, signal structures and most importantly, access control. Relevant experience exists with broadcasting satellite systems but can not be directly scaled to the Galileo system. The primary objective of this exploratory study is to describe in outline one or two concrete implementation techniques, building on that existing experience but matching it to the specific needs and constraints of satellite navigation.

Two task descriptions were listed:

1. Assessment of Requirements and Initial Review of Implementation Schemes. The output of this task will comprise:
   - Listing of principle requirements, as seen from the controlled access viewpoint. This list shall not only include the technical requirements but also comprise all other requirements as relevant for the implementation of commercial services.

- Listing of the specific navigation boundary requirements as relevant for controlled access.
- Preliminary listing of potential candidate implementation schemes.

The results of this task are described in Chapters 2 and 3 in this report.

2. Elaboration of at least two alternative Implementation Techniques. The output of this task shall [...] concentrating on the driver requirements and on the identified implementation solutions.

   The results of this task are described in Chapters 3 and 4 in this report.

Chapter 2

Security Issues

2.1 The Galileo System

2.1.1 Levels of Service

Currently, the requirement is that Galileo shall provide three levels of service:

1. Open Access Service (OAS). A service to the mass market. The satellite position messages are freely available, with better than 10 meters 95 % accuracy. Universal access to a basic signal for mass-market applications.

2. Controlled Access Service 1 (CAS1). A certifiable service. A certified satellite navigation message service with commercial added value compared to level 1. Guaranteed availability and accuracy with liability cover in case of system failure.

3. Controlled Access Service 2 (CAS2). Safety of life and security-related services. A certified satellite navigation message service with added value to aviation, transport and community-critical and safety-of-life operations such as police, fire-, search- and rescue brigades etc.

Service level two and three must only be available in return for payment, hence some sort of cryptographic techniques must be applied to limit the signal access only to eligible parties. Several commercial models for service access payment can be envisioned, the subscription model being probably the most immediate and relevant.

2.1.2 Security

The Technical Approach

This report is focussed on the information security of the downlink channels carrying navigation messages that shall be access controlled within three levels of service. We start out by assuming the standard cryptographic threat models of passive and active attacks, that is, the signals can be tapped, generated, modified or deleted without physical restrictions. This leads to consider the basic information properties of

confidentiality: only authorized users can acquire the information,

authenticity: the recipients can verify the origin and integrity of the information,

required of the communication channel.

Access control theory models the access problem as a triple (S, O, R), where S is the set of subjects, O is the set of objects, and R is the set of access rights or operations defined on the objects. This can be depicted as an access matrix coordinating subjects and objects, and with entries being subsets of R. Examples of fundamental access rights of information objects are *Read* and *Write*.

The satellite channel is a broadcast channel, each satellite covering a fourth of the earth's surface at any time. Protecting access to information objects on an open communication channel available for both passive tapping and active attacks can only be done by cryptographic techniques. Restricting *read* access can be done by cryptographic coding, hence creating confidentiality. Restricting *write* access is done by authentication coding, hence creating verifiable integrity and origin of data.

The information objects are primarily the navigation data and ranging signal in our context here, but must also include the access rights themselves, in the representation of cryptographic keys. The cryptographic key management is the mechanism for implementing the access rules.

The concept of a *reference monitor* in access control theory is an abstraction that is postulated to control all accesses from subjects to objects according to the rules of the access control policy and the specific access rights granted. Basic security properties for a reference monitor are:

- Enforcing a complete separation between subjects and objects, so that it is always invoked,
- Complete and correct operation according to access control rules/policy.

- Tamperproof functionality.

As it is an abstraction, a reference monitor is not necessarily implemented by a single piece of hardware and software. In a distributed system, it rather represents the collection of access control devices.

The basic idea is to design an access policy model and implement that by protecting the information by encryption such that only eligible users can gain access to the navigation information and value/added messages, that is, being able to decode and interpret such messages.The informational authentication and integrity property, that is, security against sender impersonation ("spoofing") can be solved with public-key techniques of one-way hash function and digital signatures on the dataframes, where copies of the system's public key reside in the mobile receiver terminals, encapsulated by the smart card chips.

A first solution sketch entails distinguished public keys associated with subscriptions in the form of smart cards attached to the the mobile receiver terminals. The service access right, the smart card, and the subscribing person are linked by some kind of identity verification, such as password or biometrics. The subscription roster will be maintained in a key management center in the master control.

Security Requirements

The following is a very short list of security requirements that have been excerpted and condensed from available documents and interpreted into my own nomenclature. This list is far from exhaustive and complete as it stands now.

The *Navigation Service Provider's* requirements include:

Access structure: The access control policy, which addresses the availability, integrity and confidentiality of the navigation information should be based on the three access classes OAS, CAS1 and CAS2, as previously described in some detail. The access classes should be well separated (frequency or code structure) because of service denial by (local) signal jamming, which carries implications to the signal structure.

Unanticipated access right modifications: It must be possible to modify or revoke user (group) access rights on short notice (hours), globally or conditioned on geographical location. In particular, it should be possible to turn navigation service which is normally freely available into a controlled access service, either on a global basis or on a regional basis.

Open design: According to best practice, commercial security must not be based on obscurity of design or implementation, because experience shows that eventually this will become a weak mechanism of security. Hence, it must not be possible to break the security of the system by reverse engineering of security algorithms and protocols. Security assumptions relying on obscurity of implementation will exclude technologies like software radio.

The *User's* requirements include:

Authenticity of data: It should be able to authenticate the data provided by the satellites such that the user can verify the origin, integrity and timeliness of the data in real-time.

Authenticity of ranging signal: It should be able to detect unauthorized modification and other forms of misuse and interference with the ranging signal in real-time.

Availability: The navigation service should be available to the user according to the assigned access rights, or else exceptions and discontinuities must be notified.

Non-repudiation of service: The user should be able to prove to a third party whether he received the certified navigation service as provided.

2.2 The GPS architecture

This study started out by looking into the GPS architecture and technical solutions. The GPS background is relevant because it is the most advanced extant navigation system, and Galileo is being positioned as a future alternative to GPS. The Precise Positioning Service is most relevant in our context.

The access control of GPS PPS The Precise Positioning Service (PPS) of GPS is access controlled by the US military, and access is conditioned on DoD-authorization. The access mechanism is by symmetric encryption of the spread spectrum code, denoted the P-code, the encrypted result denoted the Y code. Each satellite transmitter uses a unique P-code. The access is conditioned on the availability of a correct decryption key in the receiver terminal.

Highly likely, the cryptomechanism is a streamcipher constructed by components of linear feedback shiftregisters combined in a non-linear manner, the

output being a bitstream satisfying good cryptographic pseudonrandomness properties. This cryptographic pseudorandom bit stream is added (XOR) to the spread spectrum code.

The encryption key granularity appears to be very coarse in the GPS. The same key instance is employed for all P-code and satellite. The access control policy distinguishes user groups by nation or collection of nations. Further information (probably classified) is needed in order to reliably sketch how the key distribution system is implemented. Apparently the cryptoperiod is about one year, so the receiver keys are renewed each year, probably by manually swapping tamper-resistant modules in the receiver device.

The navigation message of GPS is divided into twenty-five frames of 1500 bits each. Each frame divides into five subframes. Each subframe begins with a telemetry 30-bit word and a hand-over 30-bit word. The channel capacity is 50 bps, thus a subframe is received every 6 seconds. It takes 12.5 minutes to receive the complete navigation message.

The hand-over word (HOW) contains a time-of-week count (TOW) of 17 bits, which indicates the number of epochs (timeunits) since start-of-week, which is Saturday midnight (UTC(US)). The spreading code P has a cycling time of 267 days, but only 7 days are spent in each satellite before reset. The bit-length is $1/10.23$ μs. Each satellite uses a distinct part of the total bit-cycle. The TOW (Z-count) is a reference for where to start using the P-code for decoding of the next subframe. Of course, this cannot be read from the PPS, but is taken from the open SPS signal, for which the short spreading code is fixed and well-known. Hence the name "hand-over-word".

At the time of writing, the GPS design decision of making the spreading code distinct from the cipher stream/code is unclear, but could be due to a trade-off between security and hardware cost and complexity.

Chapter 3

Scenarios

3.1 Some Analogies

We observe the analogy between the problems posed by this navigational information channel and other systems, such as commercial satellite based video broadcasting. Similar to GPS, satellite pay-TV distribution is traditionally based on a one way broadcast mode of communication. The emerging convergence and integration of digital communication technology mainly based on packet-switched two-way computer networks, notably Internet technology, certainly will make an impact on the modes of operation for typical stand-alone broadcast systems as well. Already, GPS-functionality merges with mobile cellphones, and MPEG satellite decoder boxes include telephone network modems. Actually, the GPS system has already moved toward this by obtaining improved accuracy by employing differential signals from terrestrial networks.

The unidirectional mode assumed of the downlink satellite communication could be enhanced with bidirectional satellite communication from the mobile navigation terminal. It is even more reasonable to introduce bidirectional channels by mobile cellular networks when available, that is, combine the Galileo navigational information channel with mobile access to terrestrial communications, such as UMTS with internet services. This will introduce quite a large degree of freedom with respect to value-added services that will be supported by public-key based interactive cryptographic protocols implementing the access control policy. This architecture will provide a much stronger and more flexible access control security than ever be possible within the constraints of a "one-way" channel to the navigation terminal. The technical arguments for this will be presented further in Chapter 4.

The commercial success of the GSM is very well established by now.

We note the similarity between the subscription model and user roaming techniques of digital mobile telephone systems like GSM and UMTS, and a subscription model applicable to a Galileo system with regional access control. The GSM is in many aspects an open system, with respect to network operators, to value-added service providers, and to equipment suppliers. The merge between handheld computers and mobile telephones is happening within the GSM. With the GSM, normally the user will hold a subscription with one of his local GSM operators. In principle, the user is able to roam through the realm covered by any other GSM operator, supported by the mechanism of visiting location registers and secure authentication service. Unfortunately, the GSM system specification did not enter sufficiently into the challenges of automated clearing mechanisms of operators, nor did the standardisation process foresee the potential of other payment mechanism than the subscription model with its postpayment. The unexpected popularity of the prepaid "cash" SIMs shows now that much is left to be gained within this area. Within a dynamic marketplace of communication services, where value-added services will come and go, the mechanisms of open digital cash payments will be indispensable to cost-effective network services. Micropayments could be applicable to Galileo service as well. Limiting payments merely to a subscription model will effectively be a "low-pass filter" on service developments.

Common to both a pay-TV system and UMTS is the utilization of a personalized token, currently with the physical design denoted a smart card. The current formfactor of a plastic card is inherited from the banking industry, and directly adopted in the telecom industry. However, alternatives to cards exist. The essential property of this security component is copy-protection, implemented by tamper-resistant hardware and secure software. The small computing device, its content and computing behaviour are associated with access rights, hereby obtaining conditional access to the system services. I find it pertinent to propose the use of smart card in the mobile receivers, analog to subscription cards utilized in the telecommunication systems of DVB and GSM/UMTS. Furthermore, this could be combined with public-key based cryptographic key distribution by the satellite broadcast channel, very well inspired by the current digital payTV distribution.

3.2 Security-relevant Characteristics

Three significant characteristics or aspects have been identified to have major impact on the design constraints relevant to security and controlled access.

The *first and foremost* is the existence and capacity of a *bidirectional*

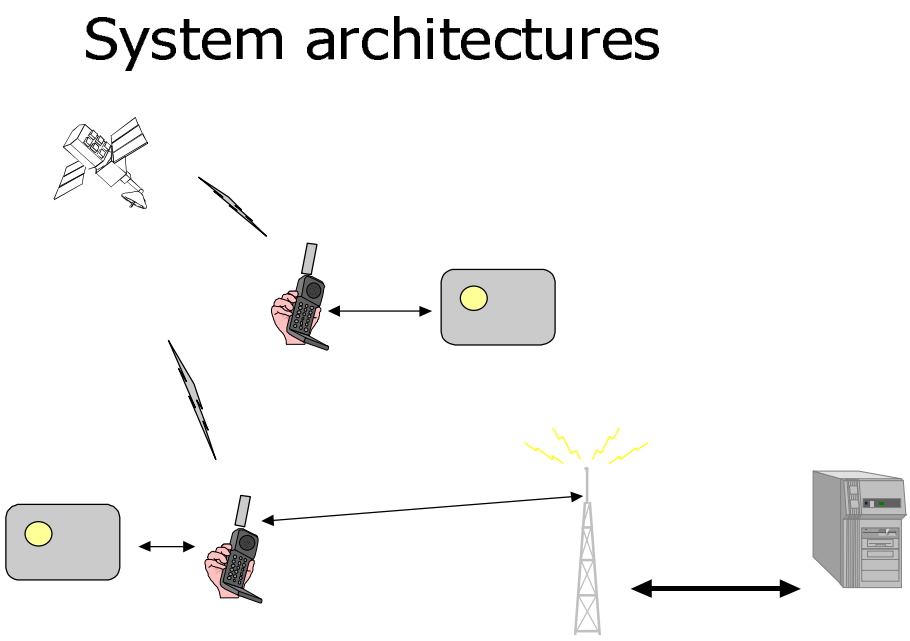

Figure 3.1: Architectural scenarios may span from "satellite only" to complete integration with client – server interaction support with auxiliary networks.

data communication channel between the receiver terminal and the system. Actually, the scenario description in the following sections has been split in two according to this aspect. As will be shown, the bidirectional channel is important for the security of

- key distribution efficiency,
- piracy control,
- flexibility in implementing geographical access control policy, and
- integration of payment and service access.

As a consequence, the availability and capacity of this bidirectional channel will be a major force in the rapid development of location-aware value-added services based on Internet-technology. For instance, both DVB, DAB and other standardized network technologies are heftily looking for a "return channel". For DVB, the threat and activity relating to commercial piracy of subscription smart cards is a driving force behind this search. The current version of GSM subscription cards has also been hacked to some extent, but the impact is much less because of bidirectional data channel available between the mobile terminal and the service provider. Most modern cryptographic protocols assume a bidirectional channel of some sort.

The *second* aspect concerns the concept of subscription *roaming*, similar to "visiting location" service available in GSM. A similar notion of "realm access policy" could be enforced by the smart card, or a combination of smart card and a interactive network service. The GPS differential system is considered to be a first generation of such services.

The *third* aspect is the access control mechanism support of a variety of payment options and tariffs. Payment is "the other side of the coin" of a commercial access control system, and provisions for completely digital payment functionality are mandatory for future digital services. An integrated approach to digital payment systems will carry implications to the access control system, both at the user terminal level and the system management level. It will impact the level of smooth service integration and combination. Unfortunately, this report does not venture into the technical challenges of this third aspect, but is listed in further work activities of Chapter 5.

It becomes clear that the Galileo system could span access control mechanisms from

a) Offline with physical predistribution of smartcards, update over satellite.

b) Something in between, "preauthorization" online via Internet

c) Realtime online client-server mode of operation, where for instance system integrity and monitoring data simply are protected by server access via some mobile radioacess network.

The next two sections discuss these scenario categories in more detail.

3.3 Unidirectional Satellite Only System

3.3.1 Alternative Design Strategies

At least two basic design strategies for access right maintenance exist in a unidirectional communication service setting. The main design decision seems to be whether the service feed is turned off at the service provider end or at the user's side.

Currently, in most practical solutions, granting access rights involves assigning cryptographic keys, put them into use at the sender's side, and distribute them by some carrier instrument as smart cards to the users. When it comes to modification or revocation of granted access rights, we are left with many options open.

Active authorization: The approach favored in this report is to "turn off" the signal service at the sender (service provider) side, simply by renewing the cryptographic keys used by the sender. The general reason for this is the great dynamic advantages that this security management approach creates. The revocation effect will be immediate on the recipient side without any need for extra signalling or acknowledgement. However, the efficiency gained by this mechanism of access right revocation must be balanced against the cost of key renewal management needed for the continued service to eligible users. This approach is further elaborated in Section 3.3.2 for the unidirectional scenario, and in the context of a bidirectional communication system in Section 3.4.

Active deauthorization: An alternative approach is to (attempt to) "turn off" the signal service at the recipient end. This is the technical approach recommended in Ref [10]. The key distribution and authorization are carried out by the personalization and distribution of the smart cards to the subscribers. Modification and revocation of access rights are signalled to the receiver and interpreted by the smart card as a "turn yourself off" message. Actually, a combined enable and disable scenario is presented in Ref [10] too. Anyway, one fundamental security assumption of this approach is that the "off message" is processed by the smart card, and that the smart card cannot be controlled by the user/subscriber because of tamper-resistance.

The approach of active authorization requires that the authorization must be renewed by a synchronized update of keys. This approach of deactivation requires that the authorization revocation message must be synchronized with the user being "on-line". None of the approaches are feasible with the fundamentally "asynchronous listening" receiver. Both alternatives therefore require continuous "carroussell" broadcasting of messages until satisfying high likelihood for receivers being online is reached. The "activate" solution requires a list of activation messages, the "deactivate" solution requires a list containing deactivation messages. Several schemes of carrying out the "turn-off" service at the recipient end can be sketched:

- A "synchronized" revocation will destroy the very intention, because now the user will know when to shut down the receiver listening.
- Continous broadcasting of the deactivation message over time is already discussed.
- Delayed until the next renewal period of access right grant, but this is very close to a variation of the "activation" approach.
- Providing a "local expiration time" in the smart card, relying on the feed of correct UTC time into the smart card. But on closer inspection, it can be realized that this is a variation of the "activation" approach too.

Nevertheless, both approaches need some scheme for updating access keys, at least in the long run. It could be argued that this can be done by distributing replacement cards, relying on physical means of distribution outside the Galileo system. Or it can be argued that this should be done by a the presumably cheaper and faster method of digital distribution. It can also be argued that break-tolerance must be part of the design criteria. Therefore, the *active authorization* becomes the recommended design approach for the long term view.

3.3.2 Scenario Discussion

This scenario is very similar to satellite pay-TV broadcast system. The navigation messages broadcasted from the satellites are protected according to a three-level access control hierarchy by appropriate frame/message encryption. Each subscriber holds a Navigation Identity Module (NIM)(for instance realized by a smart card). The NIM stores among other data, the secret key data specific to each instance and subscriber of the NIM. This device separation between the hardware keeping the subscriber-specific data

and algorithms and the general part of the receiver terminal has been successfully introduced and run in the marketplace both by GSM operators and pay-TV operators. It is considered an essential part of the key distribution solution in the consumer mass-market. In this way, the receiver terminal hardware and the subscriber's access rights can have a totally independent distribution and sale.

The communication is unidirectional from the ground control segment to the users via the navigation satellite system. The asynchrony of users implies that the key distribution be carried out in cycles continuously, socalled carousel broadcast mode. Two solutions can be imagined here. Either the source is the ground stations which continuously use the uplink to transponders in each satellite. Or intermediate storage mounted in the satellite is used, and so will enable a better exploitation of the uplink capacity. The observation is that a trade-off exists here between storage, uplink capacity and time delay of key distribution.

The main advantage of this solution is that necessary and sufficiant signals are carried within the satellite system, thus creating total independence of other communication systems. One drawback is the non-optimal use of bandwith for key distribution. Another drawback is that the lack of a "security return channel" creates great opportunities for "piracy", because there is no way to know that a key has been compromized within the system as such. Greater tamper-resistance of the NIM hardware results in higher cost of the access control system.

The key distribution protection should be done by public-key cryptography, where the secret key of the subscriber is stored in the smart card. The corresponding public-key of the subscriber is used by the system operator to protect the service-keys. The service-keys protects the relevant data of the navigation message. The cryptographic synchronization of the data channel is by a self-synchronization mode of operation, such as Cipher Feedback mode or similar. The technical issues are dealt with in more detail in Chapter 4.

The User Environment: With respect to consumers, the hypothesis put forward here is that this user environment for commercial services will turn out to be similar to satellite-distributed pay-TV systems currently operating. Even the nature and motivation of attacks against the access control can be said to be very similar in consumer relations. For instance, the real-time service of getting access to an important football-match by video can be related in importance to real-time navigation requirements of locating a restaurant or the optimal route out of a traffic jam. Changing encryption key in the middle of the match is the tactics against pirate viewers currently played by

DVB access control operators. Therefore the attack incidents that take place in the DVB industry should present a relevant basis for threat analysis in a satellite only system for navigation service. More serious applications,like emergency calls with automatic position reporting, is definitely outside the analogue claimed here, but belong to public services without access control.

The security environment, as perceived by the satellite pay-TV distributors is characterized as follows:

- No feedback on who or how many are using the service.
- No direct way of detecting misuse.
- The user has direct interest in security break because he escapes payment.
- Misuse are not perceived as criminal by the users.
- High volume makes it economically very interesting to break.
- The system management is vulnerable to intentional "human errors" by insiders.

Satellite DVB system: The access control authorization centre of satellite-based pay-TV manages one or more authorization servers. An authorization server contains the database of subscribers and their assigned access rights. The input to this server basically comes from the card issuers, where the subscriber's identity information is collected. The authorization centre connects to other servers, such as banks, retailing, and content providers. Also, input is received directly from the users via a TCP/IP return path normally carried by the phone network. The set-top decoder box is equipped with a telephone modem for this purpose. User input could be subscription requests, queries, payment transactions, user authorizations, or reconfiguration of the decoder. The output from the authorization server destined for the uplink to the satellites contains cryptographic keying data and user authorizations. Subscriber authorizations/rights are continously multiplexed into the uplink stream, and should be received by the decoders and loaded into the corresponding smart cards.

The keying data is used in the uplink station to encrypt the MPEG stream (60 Mbps) with the current encryption keys. The encryption algorithms are standardized in the industry, but restricted by ETSI custodian. The argument for not using publicly available algorithms and protocols claims that this procedure increases the security of the access control against smart card piracy attacks. My remark is that time and again (Sky, DMAC, DVD

and soon (?) MPEG) this has turned out to be not only a bad assumption for mass market consumer appliances, by underestimating the cleverness and craft of reverse engineering. But this industry custody security assumption seems to influence design decisions for the rest of the security system in the wrong directions. Note that these remarks apply to world-wide consumer markets with high service affinity.

Conceptually, it is possible to group access rights geographically in this scenario, simply by leaving essential parts of the PVT computation to the protected hardware of the smart card. The idea is to let the smart card be enabled/authorized to do only computations related to a predefined geographically area. If positions are outside this area, the card computer will simply discard the request.

The main disadvantages suggested for this scenario are:

- The carousel mode of key distribution and update will not scale well in the consumer mass market, and is non-optimal considering overall communication cost.
- Nonauthorized (piracy) use of the service is hard to control and contain, where piracy smart cards cannot easily be identified within the system.
- A geographic access policy will probably create quite a complex key management system.
- All value-added service creation has to be communicated via the Galileo satellites.

3.4 Bidirectional System

Now we add a "return channel" to the navigation system. Two main scenarios can be envisioned, distinct on whether the interactive channel is "off-satellite" by one or more auxiliary networks, or "on-satellite". Both scenarios open for the "pull" modell of key-distribution for access authorization, The user, whenever necessary, will request a valid decryption key representing an access right directly from a subscriber management system. This approach will be communication optimal with respect to key distribution, because keys will be communicated only when requested. Obviously, this is not the case in the carousel mode of a unidirectional system. The log-on time will be dependent on the access and response time of the key distribution server.

On-satellite: This is a system integrated approach (on-satellite), where the idea is to equip the Galileo satellites with bidirectional communication facilities for access to key distribution and other service management. This implies that the terminals must be equipped with, at least low-rate, satellite commmunication transmitters for uplink communication.

Cellular networks: A system convergent approach is to exploit the availability of another network, for instance mobile cellular systems such as GSM/UMTS or satellite networks. The availability of mobile communicators and data access terminals in safety-critical applications is highly likely, and presents additional value-added system potentials, such as client-server computing. This will create security management possibilities similar to what exist in GSM and UMTS and similar.

The computing requirements of the receiver terminals could be offloaded by providing a sort of client – server computation by the auxiliary network. Hence the power requirement of battery-operated equipment could be reduced and being made light-weight. The sharing of processing and database functions between the mobile GPS receiver/processor (the client) and the local or remote infrastructure (the server) will enable an excellent platform for access control services, which now will reside with the interactive server.

Furthermore, a terrestrial cellular network can easily support and enable a truly localized navigation service provision. Special navigation services may only be available in selected cells. The access control can be based on physical cells and fixed network addresses. The combination of Galileo for outdoor navigation with picocell structures for indoor and dense building areas appears to be a promising integration of network technologies. The access control to the commercial services will be verified in the interaction between the smart card of the receiver, the input data received from the Galileo satellites, and the local access control service. The next step toward a roaming service should be easy, based on emerging solutions in mobile networks.

Multiapplication smart cards: Smart cards today are security parts of "closed systems" where the issuer is equal to or closely associated with the service provider. The user ends up with a card for each service. The reason for this is rooted in the security and technical management architecture of the systems. The problems with usability, management cost, and service flexibility are clearly acknowledged, and the industry is trying hard to move towards solutions based on multiapplication/service cards. The forces against this are at least threefold: All service providers want to be in control of the

card and their branding, the sharing of resources and smart card creates new security problems not solved yet, and the general task of revenue clearing among the service providers requires established infrastructure cooperations. This problem will not show up for a "closed" unidirectional Galileo system, where a centralized/hierarchical subscriber organization can be set up for Europe or world-wide. The problem will emerge as soon as the commercial navigation service is to be integrated with another service, say cellular phone service. How many card slots will be available? Or how can the Galileo commercial service access be put on and securely managed on for instance USIM (The subscriber cards for UMTS). Or the other way around, how can the Galileo card accomodate for more security applications? These are vital questions to the implementation of access control in Galileo.

Chapter 4

Technical Challenges and Solutions

This chapter identifies and discusses several technical challenges and constraints posed by the proposed system.

4.1 Overview

The security requirements of the ground and control segment can be met with wellknown mechanisms of link and end-to-end security of confidentiality and authentication. A system for operation command and control, needed for instance in emergency situations, must be developed. It might be interesting to have a closer look on the problem of verifiable sharing of operational control of the system among the member countries. Nevertheless, the main technical challenges of security will probably not be found in this task, where well understood techniques can be employed to the computer-based operation and management of a distributed communication system. The main focus is the problem of access control on the satellite broadcast down-link for positioning service, and this chapter will enter into more technical detail of some issues of this design problem.

4.2 Management of Conditional Access

Access control could be based on several conditions, such as geographic area of subscription (Lat,long), time of subscription (Expires end of ..) , service level etc.

The dynamic management of a subscriber database will include operations and procedures for

1. new users
2. update users
3. delete users
4. modify access rights
5. and so on.

The very large scale of the system, both in the number and variety of users, and it the global coverage, advice employment of a distributed database system.

The initial access rights must be pre-distributed in a separate system "off-line" in a unidirectional communication systems. Exchange either with identity or payment or both are done "off-line", or via an auxiliary networked service.

In a bidirectional communication system, access rights can be booted and communicated directly to the receiver terminal if a universal digital payment system service exists. Continuous monitoring and control of access rights can be done.

4.3 Security Break Tolerance

The trust relation between issuer of the access right and the holder of the access right is asymmetric; the issuer does not trust the holder not to bring the keys to the knowledge of a third parties. Hence the need for the service provider to issue a "tamper-resistant" storage and computation device. In practice, a smartcard or similar.

However, commercially available tamper-resistant hardware can be broken if sufficient reverse engineering resources are put on the job, so we need "break-tolerance" built into the system, thereby avoiding totally breakdown of correct access control if a break should occur. A trade-off exists between cost and tamper-resistance.

Example: The message m is encrypted under key k giving $E_k(m)$. Every person that possesses access right to m is given the key k. If k or some bits of k are disseminated/leaked/published, then the correctness of the access control mechanism breaks down immediately, at least in principle.

Break tolerance can be alleviated by a more elaborate key distribution system. Let k_i be assigned to authorized person P_i. The message is encrypted under key k_i giving $E_{k_i}(m_i)$. Then only P_i has access to m_i. However, if

for all i and $j, m_i = m_j = m$, that is, the message sent to all P_i is the same, then for any i, a leak of k_i will result in total breakdown of the correctness of the access control mechanism.

In principle, with no return channel from the mobile terminal to the system, there is no evidence signalled that that a key k_i should be revoked. In practice, the pirate $\tilde{P}_i$ has a key distribution problem of its own if he wants to "resell" the access rights. The simplest thing for $\tilde{P}_i$ to do is to simply "billboard"/publish k_i, but this will reveal which key is broken, so the compromized key can be revoked by the key management system. Neither will it generate any direct revenue stream.

If k_i is revoked, then k_{i+1} can be found and published. Another approach is to reduce the cryptoperiod of k_i, that is , frequent renewal of the k_i value. This puts some more effort in the redistribution game of the intruder $\tilde{P}$, in particular if it is a "commercial redistribution".

4.4 The Key Hierarchy

The most natural solution to the above stated problem is a cryptographic protection hierarchy of three key levels. Let us call the first level the *subscriber keys*. According to normal use of public-key cryptography, a subscriber s will associate with a public key $K(s)$ and a corresponding secret key $k(s)$. They are long-term key information associated with each subscriber or user. The secret key is stored securely in tamper-resistant hardware (), the public key is stored with the key distribution system. These individual keys are generated and predistributed "off-system" using some form of trusted electronic token. For simplicity it is named a smart card.

The next level will be the *accessgroup keys*. Accessgroup keys will be assigned and distributed to eligible subscribers, protected by individual public subscriber keys. An access group i will be assigned an access group key $k_g(i)$, where a subscriber s to access group i will receive the key distribution message $E_{K(s)}(k_g(i))$.

Access right keys will be protected by access group keys. An access right j is assigned to an access group i by encrypting the access right key $k_r(j)$ under the access group key $k_g(i)$. The resulting message $E_{k_g(i)}(k_r(j))$ is broadcasted and received by all NIMs. However, only the members of the access group determined by the access group key are able to access the protected access right key.

The fourth protection level is the navigation data itself. Navigation data is protected by an access right key. Navigation data m is broadcasted as $E_{k_r}(m)$, hence can be accessed if and only if an access right is held, repre-

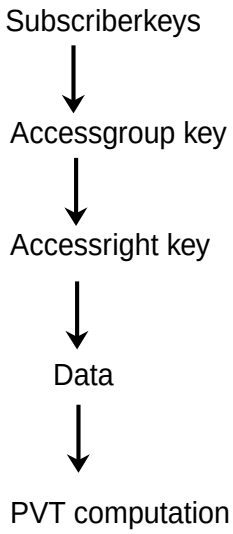

Figure 4.1: The proposed cryptographic key hierarchy for the access system. The arrows can be interpreted as "protects and accesses".

sented by the access right key.

The range measurements and PVT computations cannot be carried out without the correct reception of the actual navigation data. These data are protected by the access right key.

The general concerns of this distribution are:

- The authenticity of the key messages
- Synchronization and error propagation
- Cryptoperiods and key revocation techniques, in particular in relation to the message key.

A basic assumption for the application of the proposed key hierarchy is the following: The service access of the user expires unless renewal messages of some sort are received. The proposal is to achieve this by "enabling communication". Unless a correct and authentic message containing a valid access right is received by the smart card within some deadline, the service becomes unavailable. A simple mechanism implementing this would be according to some pseudorandom sequence generated by a keyed one-way function, but the best solution is to use the key distribution of the access right and user group keys. When the satellite changes encryption key, a "non-enabled" smart card simply cannot do its message decryption task because the new key instance is not replaced by the previous one

Consideration on which keys should be specific to each satellite and which keys could be systemwide keys are left open here.

4.5 Key Distribution

Given the general scheme of the key hierarchy in the previous section, the next challenge is to investigate how the cryptographic keys can be distributed in the system, projecting the message complexity that the hierarchy implies for the Galileo system. This cannot be definitely answered before the channel and signal architecture are available. On the other hand, the key distribution is of fundamental importance to the flexibility of the access control, and therefore to the viability of the commercial exploitation of the system. Hence the key distribution complexity must be a determining factor in the design of the system.

Each subscriber will possess a subscriber key pair, the secret key "imprinted" in the smart card. Of course, the number of keys will increase linearly with the number of subscribers, say n. The distribution is by personalizing the smart card and secure physical transfer to the subscriber. Efficient procedures for this issuing already exists commercially today.

Even so, new concepts of signed applets downloadable by the owner of the smart card are being purported by Microsoft, Sun and others. This will create an opportunity for a totally new way of organizing "the booting" of security applications involving smart cards. For instance, the user will be able to download a Galileo subscription "cardlet" and mount this on his or her card. The underlying assumption is that the navigation service provider is able to rely on trusted public-key infrastructure already in operation, say by the Internet.

The initial access group keys k_g can be distributed with the issuing and transfer of the smart card, but distribution by communication should be available in order to create a economic and flexible distribution system. The number of messages needed for a full update of one access group key is linear in the number of group members, and so is in the order of n. How frequently these messages have to be distributed and renewed depends on the validity period duration set by the subscription service. There are various methods of key generation schemes that will handle smooth overlapping of validity periods.

Example: Say 10^5 users must have their parameter update within 10 minutes, where the individual distinguished user parameters are of length 10^4 bits. (Currently, this can likely be reduced to a fourth or fifth, but one should be

conservative and provide for more taking into account the expected life-cycle of Galileo to be 15-20 years.) This results in a 1 Mbps data rate.

A preliminary estimate of the user population tells 10^7 subscribers of CAS1, and 10^5 subscribers of CAS2 [9]. This needs further evidence, and is in particular crucial to the system dimensioning in the unidirectional key distribution system.

Thus a fundamental problem formulation with respect to key and parameter distribution is which model to go for:

1. A **pull model**, where users pull new keys (asynchronously) from the system database as necessary. This is optimal with respect to communication and scales well on a distributed system basis.

2. A **push model**, where keys, certificates and other parameters are broadcasted on a revolving basis ("carousel mode"), to all users whether they need it or not. This is best suitable for a closed system with a priori knowledge of the maximum number of users.

The best solution for a global Galileo system will be in accordance with a pull model. The optimal way is to let this key distribution be determined by "user pull" via auxiliary bidirectional networks (Internet technology). This will accomodate the asynchronicity of the users. Personal computers and mobile communicators already come standard equipped with smart card readers. GSM terminals are on the market now with dual slots for smart cards, enabled for WAP based applications.

The access right key distribution aggregates only a few messages, proportional to the product of the number of access groups and the number of access right types used in the system. A first estimate would be less than 100. If these messages could be satellite broadcasted more or less continuously on a revolving basis then the start asynchronicity of the users/receivers will probably result in an acceptable average waiting time to service access. Nevertheless, the access right keys should be made available by an auxiliary network as well in order to accomodate time-critical applications. The validity period of the access right keys could be a multiple of the satellite upload rate, determined by the fastest required renewal frequency of the access rights.

We need to identify user requirements that put constraints on the solution for key distribution mechanisms for access control, such as

- Acceptable "Log-on" time
- Resynch-time with key renewal

- Other system parameter updates.

Probably, the system is planned to have a lifecycle of $15 - 20$ years, which requires careful attention to the scalability with respect to users and service providers. The dimensioning of channel capacity for distribution of access group keys is of immediate concern.

4.6 Signal Structure

According to preliminary design documents, Galileo is proposed to have four satellite downlink broadcast carriers and probably not any uplink channels from the mobile terminals, although this might change in future specifications and developments. The channel rate of the navigation messages is proposed to be 1500 bps.

A signal design based on spreading code phase measurements requires a distinction between the channel providing the ranging (R-channel) and the acquisition channel (A-channel), because in order to synchronize efficiently to the current state/position in a *cryptographic* spreading sequence of the ranging channel, some information about system time, shift register states etc. are needed up front. (This must be done even for a long noncryptographic spreading codes.) The necessary "access" data must either be received by some acquisition channel or internally computed.

It follows that this information must be established *prior to* using the ranging channel, hence the ranging channel itself cannot be used to transmit the necessary synchronization data. In principle, there exists several possible sources of approximate synchronization information that needs to be input to the demodulator.

The receiver, when already having access to the cryptographic key and time-count, can carry out a search for the correct state by means of correlation techniques between the approximately known position in the sequence, and the incoming signal. If the time-count is not kept, it can be manually input based on synchronization information received somehow outside the system. Or, more efficiently, it can be acquired from another communication channel made available.

This synchronization data acquisition channel could employ spread spectrum modulation, so that the very same channel could provide some means of ranging measurements too. Apparantly we have now entered into some kind of circular thinking. Why is it easier to synchronize the receiving end of this channel? Of course, the trick normally done with the spread spectrum channels is that the spreading code applied is short and publicly available, so that it can be predistributed and embedded into the receivers. Hence the

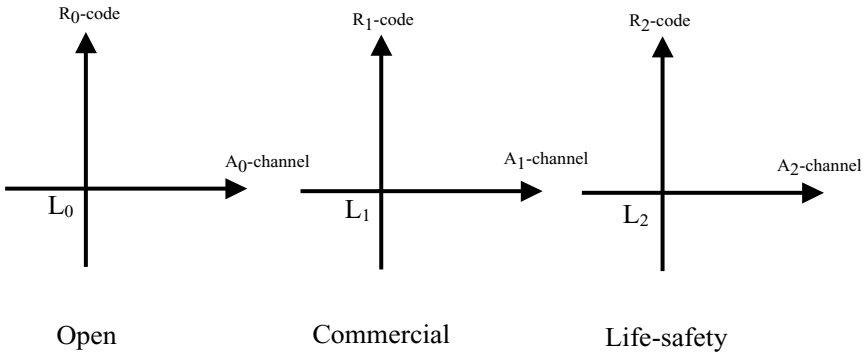

Figure 4.2: The signal structure proposal. The access structure classes of Open, Commercial, and Life-safety is assigned a separate carrier band each. Each carrier band provides two channels, one data channel (A-channel), and one ranging channel based on spread cipher.

correlation technique can be applied successfully in short time without extra input.

Imagine a single carrier L_0 with two "orthogonal" channels, one for data and one for ranging. See Figure 4.2. The channel orthogonality is achieved with the channel codes employed. Despreading of the ranging channel R is dependent on the synchronization data to be received by the data channel A. If the synchronization data provided over the A-channel is encrypted, the access to the crypto-key will control the access to high-precision pseudoranging and coded jamming.

Assume that the key hierarchy described in the previous section is applied. The access right key k_r, which indirectly enables the pseudorange measurements, is distributed on the A-channel. This key gives access to the necessary and sufficient synchronization and ephemeris data, also distributed on the A-channel.

The "handwaving" claim here is that a spreading code based on a strong cryptographic sequence (non-cycling spreading code) will be orthogonal with high probability to a short cycling Gold-code. Conversely, we can achieve channel code orthogonality (with high probability) by employing a spreading cipher for the ranging channel. The A spreading code possesses important cross-correlation properties that can be utilized in the receiving end, in spite of the short length of the code. The ranging channel utilizes a very much longer spreading code, such that it will not recycle. Any strong cryptographic pseudorandom bitsequence can be used as a spreading code because it will, among other characteristics, satisfy the correlation properties necessary for a

good spreading code. Being a cryptographic bitsequence, it is indistinquishable from a uniformly distributed random sequence.

Now assume three independent carriers L_0, L_1, L_2 with the characteristics described above. Assign one to the open access navigation service, assign the second one to the commercial service, and the third one to life-and-safetyservice. The following advantages can be observed:

1. Access control can easily be imposed on the open access signal L_0, if so required.

2. The commercial service can be improved by phase-signal measurements on both L_0 and L_1.

3. The Life-Safety signal will be independent of both the open and the commercial, but could improve its precision by access to combined measurements on both L_0, L_1 and L_2.

4. Using a single carrier for the open access makes the receiver as cheap as a GPS-receiver, the extra modulation/coding is a matter of software.

5. A variety of flexible access control policies can be realized with the independence of service carriers.

The bandwidth at two carrier frequencies are suggested to be 4 MHz with a capacity of 1500 bps, whereas the third bandwidth is suggested to be 20 MHz. The chipping rate will be different for P_0, P_1 and P_2 according to available bandwidth.

4.7 Crypto Synchronization

Another technical challenge for broadcast satellite systems is the synchronization of the cryptographic generators at sender and receiver sides. Either some self-synchronization mode of the crypto pseudorandom generator is used, however, this will create bit-error propagation in the receiver. Or a Vernam-mode (no feedback) is used, then resynchronization is needed whenever the receiver is turned on, or regains a lost downlink signal. If the error-rate is kept low by error-correcting codes, then the most reasonable solution is a self-synchronization mode of decryption.

In GPS, quite a lot of communication capacity is used for fast synchronization of bit-generators for the spreading code and the crypto bit stream. Every subframe (length 300 bits) of the navigation message contains a 30 bit

handover word, that is, 10% of the channel capacity is spent for the purpose of acquiring the PPS.

A viable alternative is to employ self-synchronizing generators. The disadvantage of this type of generator is the error-propagation effects. This is probably the reason why GPS designers selected to use a standard streamcipher mode, where error-propagation is zero.

The error-rate can be reduced by employing forward error-correcting codes. This is used in GPS, but only for the decrypted message content.

Actually, the signal structure proposal in this report must use a self-synchronizing mode of encryption. The receiver terminal must be able to read the data on the acquisition channel as soon as possible after power-on or reset. This will happen totally asynchronous between the satellite system and each user. The user can decrypt and access the navigation data only if a valid decryption key can be used, *and* the receiving ciphergenerator can be set to the same state as the transmitting ciphergenerator.

The standard mode of operation for this situation is called *cipher feedback mode* (CFB). The cipher feedback mode can be adapted to work on one bit at a time, or longer symbols or blocks. An error in the received bitstream will propagate into subsequent bits being received and decrypted, The length of this error-propagation depends on the symbol length and the length of the shiftregister containing the cipher feed-in. After the last bit-error received has been shifted out of the register, then the ciphergenerator will enter correct state and output correct data. The same argument applies if the receiver is reset and the register initially set to all zero.

This mode of encryption will be a large problem if the error-rate of the data channel is high, the result being that the receiver must discard most of the received data. Good forward error-correcting codes must be used to alleviate this problem. Several structures for this seems possible, for instance:

1. Data — FEC — Encrypt — Spread —
2. Data — Encrypt — FEC — Spread —
3. Data — FEC — Spread — Encrypt — FEC —
4. Data — Combine encrypt&spread — Convolutionalcode — Channelcode

Which structure is best in the Galileo system has not been investigated.

4.8 Mechanisms Supporting Signal Liability

The notion of *guaranteed safety-critical performance* of the navigation service must be sustained by some organizational and economic *liability*. This liability requirement should be supported by technical verification mechanisms because it is a potential source of dispute between the service provider and the user.

Let us assume that some incident or accident occurs. The user could claim that the positioning services/signal was not available or did supply misleading data. If the navigation service provider acknowledge this claim and accept the liability, then no problem of dispute will arise. If not, a dispute will probably arise, which could be settled easily if technical evidence is available.

A user claiming the unavailability of the neccessary signals and data can be supported if independent monitoring is taking place in the vicinity. A claim ascertaining the reception of insufficient or faulty data could also be supported by such third party monitoring. However, it could very well be the case that the actual receiver was in error, for instance that it was turned off, not properly configurated/adjusted, or similar circumstances. Therefore, the user must provide some evidence or proof that the signal was received timely indeed. The detailed construction of a cryptographic verification mechanism for this use needs further study. One direction will likely include the use of a one-way function with input time and sequence numbers.

4.9 Spreading Cipher

Using a cryptographic bit sequence as a spreading code appears to me a new problem formulation previously not raised in the open research community, and so this question will be pursued further elsewhere. Obviously, classified knowledge exists because the mechanism is applied in GPS.

The mechanism of encrypting the spreading code, as introduced into GPS, is directed at the threat of active disruption, for instance replay of a signal already transmitted. The claim is that the signal achieves "anti-spoofing" properties. More precisely, one achieves *signal authentication* of the ranging channel by employing a symmetric cipher. The claim states that encryption of the spreading code makes the signal more robust against deceptive signal modification attack, such as intentional signal jamming. "Signal processing gain is retained in spite of the precence of a coded jammer." Deception jamming is a technique in which an adversary generates or replays one or more of the satellite ranging codes, navigation data signals, and carrier frequency

Doppler effects with the intent of deceiving a victim receiver [2].

Recall that the GPS data rate is 50 bps, the encryption rate is 500 000 bps, and the spreading code rate is 10.23 Mbps. If the main security concern is for the authenticiy of the source data, then it is very inefficient to encrypt the channel code in this respect. Obviously, this is not a sufficient requirement. Probably, the reason for using distinct rates for the cryptographic sequence and the spreading code sequence is one of economy of design and implementation, trading off security.

Hence the spreading cipher mechanism is not employed for restricting "read access" to the navigation signal. The "read" access control to precision ranging measurements is carried out by encrypting the data necessary for the PVT computations, for instance some (or part) of the ephemeris parameters. This is termed "Selective Availability" in GPS lingo.

The threat of signal impersonation and interference is perceived to be realistic according to available documents. Authentication by public-key techniques does not require cryptographic secrecy (in the classical sense) at the receiver end. In other words, the authentication service could be made available to all, or on some differential basis, with little extra cost. This is relevant to for example the aviation sector demands, because it does not require access to a secret key, only a public key. An observation made at Estec Signal Workshop [11], is that we cannot achieve "antispoofing" with asymmetric keys. Unfortunately, public key techniques cannot possibly be used to generate spreading cipher because despreading activity of the receiver requires essentially the same capabilities as the sender. This requirement simply does not match the asymmetric properties of public-key systems.

The immediate implication is that any user that holds a legitimate receiver with an authorized smart card is, in principle, able to spoof the navigation signal because he can, for instance, delay and retransmit the signal with a better S/N so that the receivers will lock onto this instead of the original navigation signal. Normally, it is not commercially feasible to screen and classify users, so the service provider cannot assume trusted users. Thus by this thinking, any normal user is now potentially enabled to carry out signal spoofing. Introducing extra tamper-resistance probably will not be viable in a commercial setting.

4.10 Trusted Computer Token

Smart cards are readily available technology that satisfies the demands of high-volume mass market applications. The most important functionality of a smart card, which basically is a microcontroller glued to a plastic card, is to

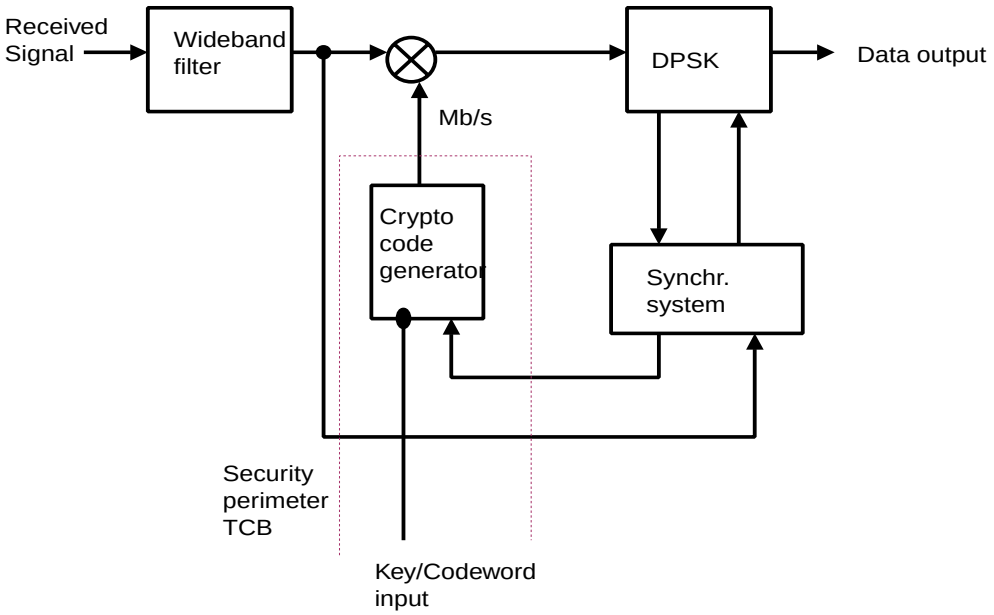

Figure 4.3: Cryptographic direct-sequence system with binary phase demodulation

function as (part of) the Trusted Computing Base in the system. The trusted computer must be able to protect stored data, such as cryptokeys, so that it is impossible for nonauthorized to read, write or modify the protected data. Further, the trusted computer must be able to perform the computations where secret keys and data are part of the input, in such a way that it is impossible for non-authorized to inspect, influence or modify the protected computation. This put forth the requirement of *tamper-resistant hardware*.

By making this distinction between the terminal/receiver as such, and the trusted computing module, it becomes practical to personalize the trusted computing module independent of the rest of the receiver. Thus separating the customer management from the manufacturing process.

Currently, the smart card is the most popular formfactor of a Trusted Computer Token, and is expected to be applied in quantities of billions in the coming years. The GSM and UMTS developments have made the smart card a vital part of the mobile telecommunication business. Several other formfactors than the smart card are available though, which provide a better and more robust encapsulation. For instance, the unavailability of a constant power supply makes the card microcontroller vulnerable to physical attacks of reverse engineering. For the implementation of active tamper-resistance, various electronic sensor and alarm technologies can be added to the encapsulation, thus providing for a total erasure functionality.

It is very important to note the implications of *ranging signal authentication* with respect to the smart card. The decryption facility must be part of the despreading operations, with high speed requirements. For GPS, the P-channel demodulator must operate at the chipping rate of 10.23 MHz. Current smart card technology cannot support such high-speed stream computations. After despreading, the processing rate per satellite seldom will exceed 1 kHz, typically in the order of 200 Hz. The navigation process in a GPS receiver seldom exceeds 1 Hz, even for high dynamic applications [2].

The smart card ISO standard today is half-duplex input/output with datarates restricted to about $5 - 50$ kbps, and likely this will not change in the near future. If public-key based authentication cannot be used because of inefficiency at high chippingrates, then the symmetric keys and computations must be performed by the smart card. The consequence is that the current smart card technology is not sufficient to implement the Trusted Computer Token. On the other hand, this could be turned into an opportunity for Europe to move ahead by developing more advanced tamper-resistant computer hardware for high volume manufacturing, useable both in Galileo receivers, mobile devices, and more.

Several types of attacks are possible. Cryptoanalytical attacks that break the cipher algorithm will imply that all smart card must be exchanged for new ones with stronger cipher algorithms. Other attacks will try to read out the secret keys. There are physical reverse engineering attacks on the VLSI circuitry. And there are potential electrical attacks, like voltage, current and clock tampering, trying to achieve some unexpected circuit behaviour. And there are logical attacks breaking some assumptions about the communication protocols. Normally, smart card hacking is not easy and cheap. In fact, well equipped labs are used in an organized way in the pay-TV business.

The race between the makers and the breakers results in the need for continuously exchanging old technology smart cards with better tamper-resistant technology at a reasonable pace. This fact must be carried in the system management plans, which should find a balance between level of tamper-resistance, cost, and functionality.

4.11 Side-information Effects on Access Control

It is important that the security analysis of the acess control mechanisms and system designed for Galileo make the assumption that one or more "independent" monitoring networks will be available to users and could be used in

attacks on the security. It is very likely that, for instance, dedicated amateurs enter to organize a worldwide monitoring network coordinated and provided by Internet services, if such a service will provide added value to such a group. This type of coordination could provide a very strong informational side-channel with respect to the security of the access control mechanisms employed in the Galileo system.

4.12 Alternative Commerce Transactions

The subscriber model is mostly equivalent to a prepaid service. We should go on thinking about other modes of payment, such as pay-on-demand/cash and postpay/creditcard schemes, and the implications to the access control system model. At least, this will be realistic in a two-way communication with the mobile terminal.

Chapter 5

Conclusions

This final chapter lists the main conclusions and propositions of this report, and wrap up with a list of a few technical issues that are important to pursue.

5.1 Main Propositions

Overall feasibility: It is technically feasible to implement a commercial access control in Galileo. Cryptographic coding techniques with key distribution are essential for realizing the access control for the navigation broadcast channels.

Essential design aspects: The three most significant aspects to successful commercial access control design in the Galileo context are considered to be:

1. The existence and capacity of a bi-directional data communication channel, to effectively enable:
   - Efficiency of key distribution/management.
   - Location-aware access rights.
   - Effective piracy and attack control.
   - Complete integration of payment and service access.
2. Roaming and visiting location service.
3. An integrated approach to digital payment service.

Experience baseline: Both the access control technology and user environment of satellite DVB systems, and the access control technology and user environment of cellular mobile networks are directly relevant for the Galileo design.

Personalized user devices: The access control will require personalized navigation receivers, including tamper-resistant storage and computing for secret keys and computations. Smart card technology present itself as a natural European solution in this respect, in particular in combination with GSM and UMTS terminals. Form factors other than "plastic card" should be looked into, in view to increase the tamper-resistance, for instance by using in-built power-supply to tamper-detecting sensors.

Cryptographic mechanisms: Authenticity requirements should be based on public-key techniques. Encryption should be based on a hybrid approach for efficiency reasons.

Key distribution and management: The key distribution and management complexity must be a determining factor in the system design. Key distribution by broadcast satellites (unidirectional on-satellite key-distribution) will not scale well with increasing subscribers/users, nor with respect to service provision. Hence it is not recommended for the commercial navigation service. The user should be enabled to pull the keys of one or more auxiliary networks, such as UMTS, on demand. The key distribution and management system must:

- Serve in a commercial environment, accordingly, only public-key based distribution techniques can offer sufficient efficiency, flexibility and scalability.
- Provide sufficient flexibility to accomodate a variety of access policies with respect to content, levels and geographical areas.
- Commercial access should be based on public-key techniques according to a distributed pull model realized by auxiliary mobile networks.

Realms of access: Geographically conditioned access control to navigation services is feasible within the scope of the technical recommendations of this report.

Value added services: The most powerful, viable and secure access control is based on client-server shared computations via cellular packetswitched networks.

5.2 Technical Challenges for Further Study

The following areas of technical challenges are identified as a result of the work reported:

Digital payment integration: An integrated approach to digital payment. systems will carry implications to the access control system, both at the user terminal level and the system management level. It will have a large impact on the level of smooth service integration and combination.

Optimal key hierarchy and distribution: Overall and detailed design of the key generation, distribution, renewal and revocation mechanisms of the key management system.

Spreading cipher properties: Characterizing the security properties of the mechanism of spreading cipher, and investigate its implementation complexity, in particular at the receiver side. Investigation of technical feasibility for implementation in smart card technology high rate despreading of spreading cipher channel code.

Cryptosynchronization : The selection of an adequate architecture for the introducton of error correction mechanisms in the data channel to allow good synchronization of the encrypted channel.

Liability mechanisms: Cryptographic verification mechanisms supporting and assuring signal liability in a multiparty setting.

Bibliography

[1] Børje Forssell. Radionavigation Systems. Prentice Hall,1991.

[2] Kaplan (Ed.). Understanding GPS Principles and Applications. Artech House Publishers, 1996.

[3] Special Issue on GPS. Proceedings of IEEE, January 1999.

[4] GNSS 2 FORUM Working Group 3 On Security and Defence Considerations. Final Report 27/11/98

[5] Galileo. Involving Europe in a New Generation of Satellite Navigation Services. Brussels 9 February 1999.

[6] Informational meeting: Security issues in Galileo communication. Beaulieau, DG VII on 17 March, 1999, Brussels.

[7] Intermediate meeting at ESTEC. 9 November 1999.

[8] GNSS-2 Comparative System Study Final Presentation. ESTEC, 7 December 1999.

[9] Rafael Lucas. Email communication, December 1999.

[10] GNSS/2 Specific Aspects Associated with the Controlled Access Service. GNSS-2 Comparative System Study Phase II. 30 November, 1999.

[11] ESA Galileo Signal Workshop. Estec, 27th January 2000.