ELECTRONIC TAGGING (PSE) AND MOBILE ELECTRONIC TAGGING (PSEM) DEVICES

Security Target Lite Common Criteria
Assurance level EAL2+
Standard Qualification

Version 1.0 of December 9th 2011

G4S MONITORING TECHNOLOGIES LTD
4 Dominus Way
Meridian Business Park
Leicester LE19 1RP United Kingdom

Table of Contents

Index of illustrations

Index of tables

References

Reference	Document
[CC]	Information technology - Security techniques - Evaluation criteria for IT security, version 3.1, revision 3. – Part 1: Introduction and general model, ref. ISO/IEC 15408-1:2009. – Part 2: Security functional requirements, ref. ISO/IEC 15408-2:2009 – Part 3: Security assurance requirements, ref. ISO/IEC 15408-3:2009
[ANSSI_AUTH_STD]	Rules and recommendations relating to selecting and dimensioning authentication mechanisms, version 1.0 of 13 January 2010.
[ANSSI_CRYPTO_STD]	Rules and recommendations relating to selecting and dimensioning cryptographic mechanisms, version 1.20 of 26 January 2010.
[ANSSI_GESTION_CLES_STD]	Rules and recommendations relating to managing keys used in cryptographic mechanisms of standard robustness, version 1.10 of 24 October 2008.
[ANSSI_QS_STD]	Qualification process of a security product - standard level - version 1.2 of 18 mars 2008
[FSP]	ADV_FSP.2 Functional Specification, Placement sous surveillance électronique (PSE) et de placement sous surveillance électronique mobile (PSEM), Ref. ADV_FSP.2
[ST]	Cible de sécurité, Dispositifs de placement sous surveillance électronique (PSE) et de placement sous surveillance électronique mobile (PSEM), version 1.2, September 5th 2011.

Glossary

Glossary compiled from the Common Criteria [CC]:

Term	Definition
CC	Common Criteria [CC]
OSP	Organisational Security Policy: System security policy in which the target of evaluation (TOE) is used.
SOF	Strength Of Function: The level of intrinsic strength of a function in the face of "brute force" type attacks. This level should not be confused with the level of overall strength of the TOE (defined by the AVA_VLA component), which takes into account attacks that alter or bypass functions of the TOE.
ST	Security Target: this document
TOE	Target Of Evaluation: this is the product or system for which this security target constitutes the specification for the purposes of the evaluation.
TSF	TOE Security Functions: Subset of the product or system to be evaluated, in which the security functional requirements described in chapter 5.1 of this document are implemented.

Acronyms

The following acronyms compiled from the Common Criteria [CC] are used in this security target:

Acronym	English	French
CC	Common Criteria	Critères Communs
EAL	Evaluation Assurance Level	Niveau d'assurance de l'évaluation
IT	Information Technology	Technologie de l'information
OSP	Organisational Security Policy	Politique de sécurité de l'organisation
PP	Protection Profile	Profil de protection
SF	Security Function	Fonction de sécurité
SFR	Security Functional Requirement	Exigence de sécurité fonctionnelle
SFP	Security Function Policy	Politique de la fonction de sécurité
SOF	Strength Of Function	Résistance des fonctions
ST	Security Target	Cible de sécurité
TOE	Target Of Evaluation	Cible de l'évaluation
TSP	TOE Security Policy	Politique de sécurité de la cible d'évaluation
TSF	TOE Security Functions	Fonctions de sécurité de la TOE

The following acronyms that are not compiled from the Common Criteria [CC] are used in this security target:

Acronym	English
APN	Access Point Name
FEROS	Fiche d'Expression Rationnelle des Risques et Objectifs de Sécurité.
GPS	Global Positioning System
GSM	Global System for Mobile Communications
LBS	Location-Based Service
PRNG	Pseudo-Random Number Generator
PSE	Placement sous Surveillance Electronique
PSEM	Placement sous Surveillance Electronique Mobile
RTC	Réseau Téléphonique Commuté

Naming convention

S.	TOE sensitive services (chapter 3.1.1).
B.	TOE sensitive property items and sensitive property protected by the TOE (chapter 3.1.2).
H.	Hypotheses relating to the TOE environment (chapter 3.2).
M.	Threats to the TOE, its sensitive property items or the sensitive property it protects (chapter 3.3)
P.	Organisational security policies (chapter 3.4).
OT.	The security objectives for the TOE (chapter 4.1).
OE.	The security objectives for the TOE environment (chapter 4.2).
F.	TOE Security functions 6.1)

1 Introduction

This document is the “Lite”’ version and courtesy translation of Security Target [ST].

1.1 Document identification

Title	Security Target Lite – Electronic tagging (PSE) and Mobile Electronic Tagging (PSEM) devices
Version	1.0
Author(s)	Yann Tourdot, Oppida
Date	December 9th 2011
Product name	PSE PSEM
Product version	9
Common Criteria	Common Criteria for Information Technology Security Evaluation, version 3.1 revision 3, July 2009 (ISO/IEC 15408:2009).
Assurance level	Evaluation Assurance Level 2 (EAL2+) supplemented by components ALC_FLR.3, ALC_DVS.1 and AVA_VAN.3 in accordance with standard qualification [ANSSI_QS_STD].

This document constitutes the security target for electronic tagging (PSE) and mobile electronic tagging (PSEM) devices.

The TOE is a product that allows checking that a person - the subject - complies with the curfew scheme he/she is placed under. Failure to comply with this curfew scheme on the part of the subject results in an alarm being fed back to the remote monitoring centre.

This document specifies the security requirements from a functional point of view and in terms of evaluation tasks that the product being assessed (Target of Evaluation, hereinafter "TOE") needs to fulfil in order to handle potential threats during operation.
The security target also indicates to what extent the product under evaluation meets these requirements.

1.2 Section breakdown

Chapter 1 contains the introduction to the document.
Chapter 2 describes in natural language the services provided by the product being assessed (TOE) as well as its architecture.
Chapter 3 specifies the planned operational conditions for the product being assessed, especially threats which the product will be exposed to.
Chapter 4 indicates the security objectives to be attained by the product and by its operational environment in particular countering any identified threats.
Chapter 5 provides details of security requirements to be complied with in order to attain these security objectives: functional requirements and assurance requirements.
Chapter 6 lists the functionalities available in the product being assessed to meet functional requirements and the measures implemented to meet assurance requirements.
Chapter 7 shows whether the product being assessed also claims compliance with the requirements specified in a protection profile (PP).

Chapter 8 comprises all the justifications ensuring in particular that the security objectives and security requirements cover threats fully or that functional requirements are covered by the product functionalities.
Chapter 9 includes the security target annexes.

1.3 Compliance with Common Criteria

This document conforms with Part 2 of Common Criteria version 3.1 revision 3 extended with security functional requirements FCP_CMP.1 et FPT_EMSEC.1 and strictly conforms with Part 3 of Common Criteria version 3.1 revision 3 [CC].

2 Description of the TOE

This chapter specifies the logical and physical scope of the target of evaluation (TOE).

2.1 Overview

2.1.1 Description of elements

- **The electronic tag** (TOE): is crimped by an agent from the prison administration to the subject's ankle. The electronic tag can be removed without damage, and any damage results in an alarm being fed back to the remote monitoring centre application. Kevlar strips are included in the electronic tag in order to prevent removal of the tag through stretching. In addition optical fibres run through the tag so that any physical deterioration (cutting etc.) to the electronic tag can be detected. The tag's electrical battery is non rechargeable. Under normal operation it will last 12 months and in sleep mode 5 years. The electronic tag is waterproof and can work under water to a depth of 5 metres.
- **The monitoring unit** (TOE): can be fixed (when PSE) or mobile (when PSEM)[1]. In the case of PSEM, the subject can for instance wear the mobile monitoring unit on his/her belt. In the case of PSE where the monitoring station needs to be fixed, the latter is fitted by the prison administration at the premises (one or more addresses) where the subject is under home curfew. In the case of PSEM the mobile monitoring unit has a GPS receiver which enables it to determine his/her geographical location.
- **The docking station** (TOE): is used in PSEM mode only. It enables charging of the electronic battery of the mobile monitoring unit.
- **The key fob** (TOE)**:** is used by a prison administration agent only during the initialisation phase, when an electronic tag to be associated with a monitoring unit. The key fob is kept by the prison administration and is used to send signals to the electronic tag and to the monitoring unit to be initialised indicating that the initialisation phase can be completed. Initialisation of an electronic tag and of a monitoring unit can only be carried out in the presence of a prison administration agent who carries a key fob.
- **The fitting and installation tool** (TOE)**:** is used by a prison administration agent only during the initialisation phase when an electronic tag can be associated with a monitoring unit. It is used to send signals to the tag to be initialised making it switch from "non initialised" to "initialised" status.
- **The diagnostic tool** (TOE): is used by a prison administration agent in the initialisation or operational phases. It allows various operations to be carried out on the TOE: obtaining information on TOE elements (serial number, battery status, software version, etc.) and configuration operations to be performed for certain TOE elements (RTC & GSM configuration, etc.).
- **The remote monitoring centre** (outside TOE): is an information system hosting "the remote monitoring centre application" (see definition below) [of the] applications that allow remote administration of the TOE.
- **The remote monitoring centre application** (outside TOE) is an application hosted at the remote monitoring centre which enables the TOE to be administered remotely.

[1] The term "monitoring unit" can refer interchangeably to the fixed or the mobile monitoring unit when the adjective "fixed" or "mobile" is not specified.

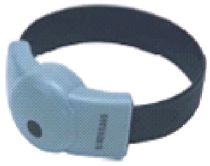

Figure 1 : Electronic tag

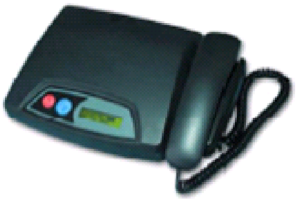

Figure 2 : Fixed monitoring unit

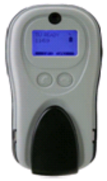

Figure 3 : Mobile monitoring unit

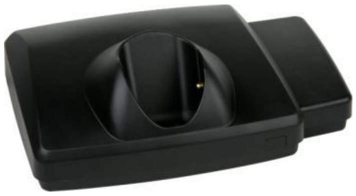

Figure 4 : Docking station

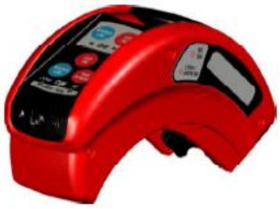

Figure 5 : Fitting and Installation Tool

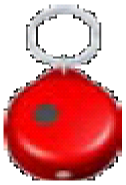

Figure 6 : Key Fobs

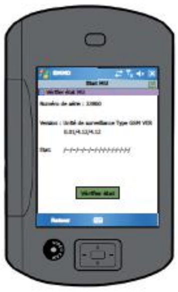

Figure 7 : Diagnostic tool

2.1.2 Description of flows

The flows implemented by the TOE, according to the mode of use (PSE or PSEM) are represented in figure 8 (PSE) and figure 9 (PSEM).

Note: For reasons of readability of Figure 8 and Figure 9 below, several interfaces of the same type may be represented for a single TOE element. In reality, no two elements of the TOE will have the same type of interface any longer.
For example, in Figure 8, two infrared interfaces are represented for the fitting and installation tool, while in reality it only has one infrared interface.

- **Flow in PSE mode**

[Figure 8 is not provided in the sanitized version of
the Security Target in order to protect proprietary information]

Figure 8 : Interfaces and flows implemented by the TOE in PSE mode

- **Flow in PSEM mode**

[Figure 9 is not provided in the sanitized version of
the Security Target in order to protect proprietary information]

Figure 9 : Interfaces and flows implemented by the TOE in PSEM mode

- **Summary of flows**

[Figure 10 is not provided in the sanitized version of
the Security Target in order to protect proprietary information]

Figure 10 **: Table of flows implemented by the TOE**

2.1.3 Description of phases

The life cycle of the TOE has two phases: one initialisation phase and one operational phase. It is imperative that the initialisation phase is completed before the operational phase.

- **Initialisation phase**

The initialisation phase enables an electronic tag to be associated with a monitoring unit.

In PSE mode:

- several electronic tags can be associated to the same fixed monitoring unit,
- a single electronic tag can be associated to several fixed monitoring units.

In PSEM mode:

- an electronic tag can only be associated to a single mobile monitoring unit,
- a mobile monitoring unit can only be associated to a single electronic tag.

It is possible to combine the PSE and PSEM modes. A subject's electronic tag can thus be associated with one (or several) fixed monitoring unit(s) (PSE) and only one specific mobile monitoring unit (PSEM). The combination of both PSE and PSEM is rare.

The initialisation phase is performed by a prison administration agent in the subject's home(s). The prison administration agent responsible for initialisation has a key fob that signals his presence and provides authentication via radio frequency to the fitting and installation tool (flow 1) and the monitoring unit (flow 2). The initialisation phase therefore requires the presence of the key fob i.e. of the prison administration agent. The fitting and installation tool authenticates itself to the monitoring unit (flow 4) via infrared.
Then the fitting and installation tool initialises the electronic tag via infrared (flow 3) and radio frequency (flow 5) and makes it switch from "non initialised" condition to "initialised" condition. The electronic tag then sends messages via radio frequency to the monitoring unit (flow 6).
The diagnostic tool is used by a prison administration agent and allows access (read) to certain information concerning certain TOE elements (serial number, battery status, etc.) or to modify (write) the configuration of certain TOE equipment (RTC & GSM configuration, etc.). The diagnostic tool allows access to the configuration of the monitoring unit (flow 8), the configuration of the docking station (flow 11) and the configuration of the fitting and installation tool (flow 7).
The diagnostic tool also allows access to the configuration of the electronic tag, using the fitting and installation tool to communicate indirectly with the electronic tag. The diagnostic tool communicates with the fitting and installation tool (flow 7), which in turn communicates with the electronic tag (flow 3). Then the electronic tag communicates with the fitting and installation tool (flow 5), which then communicates with the diagnostic tool (flow 7).
The diagnostic tool also allows the key fob's configuration to be accessed. For this, the diagnostic tool uses the fitting and installation tool to communicate indirectly with the key fob. First, the diagnostic tool communicates with the fitting and installation tool (flow 7), which then communicates with the key fob (flow 13). Then the key fob communicates with the fitting and installation tool (flow 1), which then communicates with the diagnostic tool (flow 7).

[Figure 11 is not provided in the sanitized version of
the Security Target in order to protect proprietary information]

Figure 11 : TOE in initialisation phase

- **Operational phase**

The operational phase requires imperatively that the initialisation phase has been performed first. In operational phase the TOE can be used in two modes: PSE and PSEM.

2.1.4 Description of modes of use

- **PSE Mode**

The electronic tag sends messages to the fixed monitoring unit via radio frequency at regular intervals (flow 6). These messages contain amongst others the electronic tag status (open, electrical battery status etc). In the event of messages of presence sent by the electronic tag not being detected, the mobile monitoring unit generates an event. Non-detection of presence messages is only effective during the home curfew period.

The fixed monitoring unit generates events from messages sent by the electronic tag (flow 6). The monitoring unit temporarily and securely stores the events it generates then sends them to the remote monitoring centre application (flow 15, 16).The flows between the fixed monitoring unit and the remote monitoring centre can be initiated by the fixed monitoring unit in real time or in delayed time. There is a complimentary regular flow between the remote monitoring centre application and the fixed monitoring unit which is initiated by the remote monitoring centre application.

The fixed monitoring unit determines whether or not the subject complies with the curfew scheme based on the curfew scheme the unit contains, its time of reference.

From the remote monitoring centre, the remote monitoring centre application can administer (flow 15, 16) the TOE configuration (modification of security attributes of my TOE) and retrieve the events generated by the TOE (flow 15, 16).

[Figure 12 is not provided in the sanitized version of
the Security Target in order to protect proprietary information]

Figure 12 : TOE in operational phase, PSE mode of use

- **PSEM Mode**

The electronic tag sends messages to the mobile monitoring unit via radio frequency at regular intervals (flow 6). These messages contain amongst others the electronic tag status (open, electrical battery status etc). In the event of messages of presence sent by the electronic tag not being detected, the mobile monitoring unit generates an event.

The docking station also generates events that it stores temporarily in a secure manner then sends to the mobile monitoring unit via infrared (flow 7).

The mobile monitoring unit temporarily stores in a secure manner events sent by the electronic tag (flow 6) and the docking station (flow 10) and also generates events. The monitoring unit sends all the events it stores to the remote monitoring centre application (flow 15). The flows between the mobile monitoring unit and the remote monitoring centre application can be initiated by the mobile monitoring unit in real time or in delayed time. There is a complimentary regular flow between the remote monitoring centre and the mobile monitoring unit, which is initiated by the remote monitoring centre application.

The mobile monitoring unit has a GPS receiver that enables its geographical location to be determined and to synchronise its reference time daily (flow 14). In the event that no GPS signal is received, the mobile monitoring unit is geolocated using LBS. LBS geolocation is outside the scope of the evaluation.

The mobile monitoring unit can determine whether or not the subject is complying with the curfew scheme based on the curfew scheme it contains, its reference time and its geographical location, determined with the aid of its GPS receiver.

From the remote monitoring centre, the remote monitoring centre application can administer (flow 15)) the TOE configuration (modification of security attributes of my TOE) and retrieve the events generated by the TOE (flow 15).

[Figure 13 is not provided in the sanitized version of
the Security Target in order to protect proprietary information]

Figure 13 : TOE in operational phase, PSEM mode of use

2.2 Scope of the evaluation

Evaluation is limited to the following equipment:

- The electronic tag
- The fixed monitoring unit
- The mobile monitoring unit
- The docking station
- The key fob
- The fitting and installation tool
- The diagnostic tool

The TOE security functions are implemented by hardware and software.

The following are excluded from its scope:

- The remote monitoring centre, its applications (in particular the remote monitoring centre application) and the information system that hosts it
- The communication networks GSM, RTC that provide communication between the TOE and the remote monitoring centre
- The GPS geolocation signals sent by the GPS satellites and received by the mobile monitoring unit (PSEM)
- The LBS geolocation information for the mobile monitoring unit (PSEM))
- The Key Creation Centre in charge of managing the TOE's cryptographic keys.

2.3 TOE physical interfaces

The TOE external physical interfaces illustrated in Figure 8 are:

- For the electronic tag:
  - The infrared interface
  - The radio frequency interface
- For the fixed monitoring tool:
  - The infrared interface
  - The radio frequency interface
  - The GSM interface
  - The RTC interface
- For the mobile monitoring tool:
  - The infrared interface
  - The radio frequency interface
  - The GSM interface
  - The GPS interface
- For the docking station:
  - The infrared interface
  - The radio frequency interface
- For the key fob:
  - The infrared interface
  - The radio frequency interface
- For the fitting and installation tool
  - The infrared interface
  - The radio frequency interface

2.4 Roles

For the TOE to function in its operational phase, the roles described below are required. These are "logical" roles that are assigned or not to different physical persons depending on the organisational security policy that implements the TOE.

Remote monitoring centre application

The remote monitoring centre application enables the TOE to be administered via the communication networks (GSM, RTC) and to be supervised i.e. to receive the events generated and sent by the TOE via the communication networks (GSM, RTC).

Subject

The subject is the person who is subject to the curfew scheme and wears an electronic tag. He/she must be able to have access to certain events generated by the TOE.

Note: The distinction between a "central administrator" role at the remote monitoring centre, which would have read/write rights for the TOE's security configuration, and a "central supervisor" role at the remote monitoring centre, which would have read only rights for the events generated by the TOE is not made by the TOE. Indeed the TOE only acknowledges one role at the remote monitoring centre i.e. the "remote monitoring centre application" which has reading/writing rights with respect to the TOE security configuration and the events generated by the TOE. The possible management of the "central administrator" or "central supervisor" roles must be carried out by the "remote monitoring centre application".

Prison administration agent

The prison administration agent is responsible for crimping the electronic tag onto the subject's wrist or ankle. He is responsible for installing the fixed monitoring unit at the subject's home(s). The prison administration agent uses the fitting and installation tool during the initialisation phase of the TOE and has the key fob. He also uses the diagnostic tool.

Local supervisor

The local supervisor is a person from the prison administration who has a key fob and who uses the diagnostic tool to perform certain TOE element supervisory operations (reading of certain parameters) locally.

Local administrator

The local administrator is a person from the prison administration who has a key fob and who uses the diagnostic tool to perform certain TOE element administration operations (reading and writing of certain parameters) locally.

2.5 Services provided by the TOE

If a service supplied by the TOE only applies to one particular mode of use of the TOE (PSE or PSEM) then this is stated explicitly in a note. In the absence of a note, the service is offered by the TOE in both TOE modes of use (PSE and PSEM).

2.5.1 Initialisation service

This service is provided by the fitting and installation tool and the prison administration agent's key fob. The association between the monitoring unit, the electronic tag and the docking station (in PSEM mode only) is made at the remote monitoring centre. The prison administration agent's key fob must be in close proximity to the electronic tag, the monitoring unit and the fitting and installation tool in order to carry out the initialisation phase. The fitting and installation tool activates the electronic tag.

The initialisation service is provided by the following TOE elements:

☑ Electronic Tag
☑ Key fob
☑ Monitoring Unit
☑ Diagnostic tool
☑ Docking station
☑ Fitting and installation tool

2.5.2 Service for detecting any attacks on the TOE hardware and software integrity

This service is provided only by the TOE elements that are handed to the subject as follows: the electronic tag, the monitoring unit, the docking station (PSEM).
Any breach of the physical or logical integrity of one of the elements of the TOE is detected and leads to a high priority event being generated and sent to the remote monitoring centre application.

For the electronic tag:

- Kevlar strips are included in the tag in order to prevent removal of the tag through stretching.
- Optical fibres are embedded in the plastic material that the tag is made from and run through the tag so that any physical deterioration of the tag (cutting etc.) can be detected.

For the monitoring unit:

- The monitoring unit has a single special rivet and no other fastening. The rivet has to be tampered with in order to open the casing and a new rivet needs to be used in order to close it again.
- An opening detector in the monitoring unit enables any opening being detected.

For the docking station (PSEM mode only):

- The docking station has a single special rivet and no other fastening. The rivet has to be tampered with in order to open the casing and a new rivet needs to be used in order to close it again.
- An opening detector in the monitoring unit enables any opening being detected.

The service for detection of breaches of hardware and software integrity of the TOE is provided by the following TOE elements:

☑ Electronic Tag	☑ Monitoring Unit	☑ Docking station
☐ Key fob	☐ Diagnostic tool	☐ Fitting and installation tool

2.5.3 Subject geolocation service

This service is provided by the monitoring unit and the electronic tag whatever the TOE mode of use (PSE or PSEM). There are two modes of use for the TOE. The subject wears an electronic tag which is attached to his/her body and communicates with the monitoring unit.

In PSE mode the monitoring unit is fixed which means that the subject is close to the fixed point representing the fixed monitoring unit.

In PSEM mode, when the mobile monitoring unit is not docked in the docking station, the subject is in proximity to a mobile point representing the mobile monitoring unit. The two-dimensional coordinates of this mobile point are determined by the mobile monitoring unit which is equipped with a GPS receiver. When the mobile monitoring unit is docked in its docking station, the subject is in proximity to a fixed point representing the docking station (the mobile monitoring unit being docked in the docking station) the subject is therefore geolocated thanks to the docking station.

In PSEM mode, in the event that GPS signals are not received, the mobile monitoring unit is geolocated using LBS. LBS geolocation is outside the scope of the evaluation.

The subject geolocation service is provided only in PSEM mode by the following TOE elements:

☑ Electronic Tag	☑ Monitoring Unit	☑ Docking station
☐ Key fob	☐ Diagnostic tool	☐ Fitting and installation tool

2.5.4 Service for verification of compliance with curfew scheme

This service is provided by the electronic tag and the monitoring unit whatever the TOE mode of use (PSE or PSEM). This service makes it possible to check whether the subject is complying with the curfew scheme he/she is subject to.

Failure to comply with this curfew scheme on the part of the subject results in a high priority event being generated and sent to the remote monitoring centre application.

Verifying compliance with the curfew scheme takes three parameters into account:

- Geolocation of the subject (PSE or PSEM)
- Monitoring unit reference time
- Curfew scheme which the subject is placed under

The service for verification of compliance with the curfew scheme is provided by the following TOE elements:

☑ Electronic Tag
☐ Key fob
☑ Monitoring Unit
☐ Diagnostic tool
☑ Docking station
☐ Fitting and installation tool

2.5.5 Provision of a reliable time source

This service is provided by the monitoring unit whatever the TOE mode of use (PSE or PSEM). Time is a necessary element used by the service for verification of compliance with the curfew scheme. The curfew scheme can indeed be associated with certain date zones, time periods etc. during which the subject's presence is forbidden/compulsory. For this reason the TOE must have a reliable time source.

The monitoring unit reference time is synchronised with each communication with the remote monitoring centre application. The source of this synchronisation varies depending on the mode of use of the TOE. In PSE mode, the fixed monitoring unit synchronises itself against the reference time provided by the remote monitoring centre application. In PSEM mode, the monitoring mobile unit synchronises itself using GPS signals.

The provision of a reliable time source is provided by the following TOE elements:

☐ Electronic Tag
☐ Key fob
☑ Monitoring Unit
☐ Diagnostic tool
☐ Docking station
☐ Fitting and installation tool

2.5.6 Event generation service

This service is provided only by the TOE elements that are handed to the subject i.e. the electronic tag, the docking station(PSEM) whatever the TOE mode of use (PSE or PSEM).

The TOE elements generate and send events with different priority levels to the remote monitoring centre application. The only element of the TOE able to communicate with the remote monitoring centre application is the monitoring unit. Therefore the latter temporarily stores in a secure manner the events generated by the other elements of the TOE (electronic tag, docking station etc) before forwarding them to the remote monitoring centre application.

The TOE associates a priority level to each event that it generates. These can be "high", "medium" or "low" as described in [FSP]. Generally, the "high" priority events concern non-compliance with the curfew scheme which the subject is placed under.

If communication between the TOE and the remote monitoring centre application is possible through the GSM or RTC communication networks (in PSE mode only), "high" priority events will be transmitted immediately by the TOE to the remote monitoring centre application. If not, the TOE stores them temporarily until communication between the TOE and the remote monitoring centre is possible.

The "medium" or "low" priority events are regularly sent by the TOE to the remote monitoring centre application.

As with all communications between the TOE and the remote monitoring centre, sending of events to the remote monitoring centre application is always initiated by the TOE. No communication between the TOE and the remote monitoring centre application is initiated by the remote monitoring centre application. The communication service between the TOE and the remote monitoring centre is described in chapter 2.5.9.

The event generation and sending service is provided by the following TOE elements:

☐ Electronic Tag
☑ Monitoring Unit
☐ Docking station

☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

2.5.7 Central administration service

This service allows the TOE to be administered by the remote monitoring centre application via the communication networks (GSM, RTC). Administration of the TOE involves being able to view/modify the TOE security configuration (curfew scheme, TOE reference time, etc.), and read and delete the events generated by the TOE.

The administration service is provided by the following TOE elements:

☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

2.5.8 Local supervision and administration service

This service makes it possible for certain TOE elements to be supervised and administrated locally. These local supervision and administration services allow certain configuration elements of certain TOE elements to be read (local supervision) or written (local administration). Local supervision and administration of the TOE are performed by a local supervisor and a local administrator respectively, using the diagnostic tool, which communicates either directly with the TOE element to be administrated (monitoring unit, docking station, fitting and installation tool), or indirectly, via the fitting and installation tool with the TOE element to be administrated (electronic tag, key fob). Annex three of chapter 9.1 provides the operations that can be performed and the corresponding TOE element(s) for each profile (local supervisor or local administrator).

The local supervision and local administration services are provided by the following TOE elements:

☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

2.5.9 Communication service with the remote monitoring centre application

This service enables the TOE to communicate with the application of the remote monitoring centre via the communication networks (GSM, RTC). Communications between the TOE and the remote monitoring centre application are always initiated by the TOE, no communications between the TOE and the remote monitoring centre application are initiated by the remote monitoring centre application.
Communication between the TOE and the remote monitoring centre application enables the TOE to receive updates to its security attributes (curfew scheme, reference time, etc.) and to send the events that it generates.

The communication service with the remote monitoring centre application is offered by the following TOE elements:

☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

2.6 Evaluation platform

The TOE must be evaluated:

- In both phases - initialisation and operation

- In both modes of use: PSE and PSEM.

The architectures of the evaluation platform are those represented in:

- the Figure 11 (initialisation phase)
- the Figure 12 (operational phase, PSE mode)
- the Figure 13 (operational phase, PSEM mode)

3 TOE security environment

This chapter explains the security aspects of the environment in which it is planned to use the TOE.

3.1 Sensitive services and property of the TOE

3.1.1 Sensitive services of the TOE

Sensitive services provided by the TOE have the following suffix:

S.BR.	when they concern the electronic tag
S.US.	when they concern the monitoring unit
S.SA.	when they concern the docking station
S.PC.	when they concern the key fob
S.OM.	when they concern the fitting tool
S.OD	when they concern the diagnostic tool

- **Sensitive services provided by the electronic tag**

S.BR.SERVICES
Sensitive services provided by the electronic tag
Protection: availability, integrity.

- **Sensitive services provided by the monitoring unit**

S.US.SERVICES
Sensitive services provided by the monitoring unit
Protection: availability, integrity.

- **Sensitive services provided by the docking station**

S.SA.SERVICES
Sensitive services provided by the docking station
Protection: availability, integrity.

- **Sensitive services provided by the key fob**

S.PC.SERVICES
Sensitive services provided by the key fob
Protection: availability, integrity.

- **Sensitive services provided by the fitting tool**

S.OM.SERVICES
Sensitive services provided by the key fob
Protection: availability, integrity.

- **Sensitive services provided by the diagnostic tool**

S.OD.SERVICES
Sensitive services provided by the diagnostic tool
Protection: availability, integrity.

3.1.2 TOE sensitive property

The sensitive property items generated / handled / stored by the TOE have the following suffix:

B.BR.	when they concern the electronic tag
B.US.	when they concern the monitoring unit
B.SA.	when they concern the docking station
B.PC.	when they concern the key fob
B.OM	when they concern the fitting tool
B.OD	when they concern the diagnostic tool

If a sensitive property item only exists when the TOE is used in a particular mode (PSE or PSEM), this is stated explicitly in a note. Where this is not specified the sensitive property item exists in both modes of use of the TOE i.e. PSE and PSEM.

- **Cryptographic keys**

B.CLES_CRYPTOGRAPHIQUES
Each element of the TOE contains symmetric keys used for the ciphering and authentication of data. Symmetric keys are used either to cipher data or to authenticate data.
Protection: confidentiality.

- **Identification data**

B.DONNEES_IDENTIFICATION
The identification data serve to identify each TOE element in a unique way. The identification data correspond to a serial number generated and integrated by the manufacturer into the TOE elements. These identification data are non-modifiable and are stored in the TOE elements.
Protection: availability, integrity.

- **Sensitive property items of the electronic tag**

B.BR_EVENEMENTS
The information (electronic tag status: cut etc.) sent at regular intervals by the electronic tag to the monitoring unit. Thanks to this information sent regularly by the electronic tag, the monitoring unit can generate events in case of problem (if the electronic tag has been cut for instance).
Protection: availability, integrity.

- **Sensitive property items of the monitoring unit**

B.US.EVENEMENTS
The events generated by the monitoring unit and sent to the remote monitoring centre application. The monitoring unit is able to temporarily store the events it generates from the information sent by the electronic tag as well as the events sent by the docking station (PSEM only).
Protection : availability, integrity.

B.US.TEMPS_REFERENCE
Monitoring unit reference time. This reference time for the monitoring unit is a necessary element for verification of compliance with the curfew scheme on the part of the subject.
Protection: availability, integrity.

B.US.POLITIQUE_ASSIGNATION

Curfew scheme which the subject is placed under This scheme defines the allowed and forbidden places for the subject as well as any time periods associated with these places. The curfew scheme is stored in the monitoring unit and can be updated from the remote monitoring centre application.
Protection : availability, integrity.

- **Sensitive property items of the docking station**

B.SA.EVENEMENTS
The events generated by the docking station and sent to the mobile monitoring unit. The docking station is able to temporarily store the events that it generates.
Protection : availability, integrity.
Note: As the docking station is only available in PSEM mode, this sensitive property item only exists in PSEM mode.

3.2 Hypotheses

The following hypotheses have the suffix:

H.CT. when they concern the remote monitoring centre or the remote monitoring centre application (CP)
H.AP. when they concern the Prison Administration (PA)
H.RC. when they concern the Communication Networks (CN)
H.MT. when they concern the TOE electronic hardware (TH)

If a hypothesis does not apply to the whole TOE but only to one of its elements (electronic tag, monitoring unit, docking station, key fob, fitting and installation tool) then this is stated explicitly in a note. Unless specified otherwise the hypothesis applies to the whole of the TOE.

If a hypothesis only applies to one particular mode of use of the TOE (PSE or PSEM) then this is stated explicitly in a note. Unless specified otherwise the hypothesis applies to both TOE modes of use i.e. PSE and PSEM.

3.2.1 Hypotheses relating to the cryptographic key generator

H.GENERATION_CLES_CRYPTOGRAPHIQUES

The cryptographic keys stored in the TOE elements in order to ensure the confidentiality and authenticity of communications between the elements, or to ensure the confidentiality and authenticity of communications between the TOE and the remote monitoring centre application, are generated by trusted personnel, on secure premises, using a FIPS-140 certified generator.

3.2.2 Hypotheses relating to the remote monitoring centre and the remote monitoring centre application

H.CT.TEMPS_REFERENCE_FIABLE

The remote monitoring centre application has a reliable time source. In PSE mode, the remote monitoring centre's time source is used to synchronise the TOE's reference times via the communications networks (GSM/RTC). In PSEM mode, the TOE synchronises its reference time using GPS signals.

Note: In PSE mode, the only element of the TOE that synchronises its reference time in relation to the reference time of the remote monitoring centre application is the fixed monitoring unit. In PSEM mode, the only element of the TOE that synchronises its reference time using GPS signals is the mobile monitoring unit.

H.CT.COM.INTER_TOE_PROTECTION

The remote monitoring centre application protects the confidentiality and authenticity of the data that it sends to the TOE via the communication networks (GSM/RTC). The remote monitoring centre application must verify the authenticity of the data it receives from the TOE via the communication networks. The remote monitoring centre application must detect the replay of the data it receives from the TOE via the communication networks. The remote monitoring centre application must detect the deletion of the data it transmits to the TOE via the communication networks.

Note: The only element of the TOE that communicates directly with the remote monitoring centre application is the monitoring unit.

H.CT.DETECTION_PERTE_COMMUNICATION

The remote monitoring centre application detects loss of a communication link (GSM/RTC) between the remote monitoring centre application and the TOE.

Note: The only element of the TOE that communicates directly with the remote monitoring centre application is the monitoring unit.

H.CT.PERSONNEL

The remote monitoring centre has non hostile personnel, with appropriate training and with all the necessary operational documentation available.

H.CT.PROTECTION_CLES_CRYPTOGRAPHIQUES

The remote monitoring centre application protects the confidentiality of the cryptographic keys used by the remote monitoring centre application in order to ensure the confidentiality and authenticity of communications with the TOE.

Note: The only element of the TOE that communicates directly with the remote monitoring centre application is the monitoring unit.

3.2.3 Hypothesis relating to the prison administration

H.AP.SECURITE_STOCKAGE

The prison administration stores the TOE securely on its premises in order to prevent any hardware or software tampering during storage.

H.AP.ALIMENTATION_ELECTRIQUE

The prison administration supplies a TOE to the subject whose elements that are not fitted with a rechargeable battery will be able to operate throughout their normal period of use.

Note: The only element of the TOE handed to the subject which does not have a rechargeable battery is the electronic tag. This hypothesis only applies therefore to the electronic tag.

H.AP.PERSONNEL

The prison administration has non-hostile, appropriately trained personnel with all the necessary configuration and operation documentation made available to them.

H.AP.PLACE

The prison administration makes the subject aware of the value of the various parts of the TOE, informs him/her of the conditions of use of the TOE and of the precautions to be taken.

H.AP.EFFACEMENT_CLES_CRYPTOGRAPHIQUES

Using overloading the prison administration deletes the TOE's cryptographic keys contained in the diagnostic tool in a secure manner in the event that the tool is scrapped.

3.2.4 Hypothesis relating to communication networks between the TOE and the remote monitoring centre

H.RC.DISPONIBILITE_CAPACITE_RESEAUX

The communication networks (GSM/RTC) that provide communication between the TOE and the remote monitoring centre application operate correctly and are dimensioned correctly.

Note: The only element of the TOE that communicates directly with the remote monitoring centre application is the monitoring unit.

3.2.5 Hypothesis relating to the TOE hardware

H.MT.FONCTIONNEMENT_CORRECT

The hardware which makes up the TOE (electronic components etc.) have not broken down and are operating correctly throughout their normal period of use.

3.3 Threats

A threat is the combination of a potential attacker, a method of attack and a targeted property item.

The threats listed below have the suffix:

M.ELT.	when they directly affect the elements of the TOE
M.COM.GPS.	when they directly affect the TOE GPS communications (PSEM only)
M.COM.INTRA_TOE.	when they directly affect communications between the elements of the TOE.
M.COM.CT.	when they directly affect communications between the TOE and the remote monitoring centre application.

If a threat does not affect the whole of the TOE but only one of its elements then this is stated explicitly in a note. Unless otherwise specified the threat applies to all the elements of the TOE.
If a threat only applies when the TOE is used in a specific mode (PSE or PSEM) then this is stated explicitly in a note. Unless otherwise specified the threat applies to both modes of use of the TOE i.e. PSE and PSEM.

3.3.1 Profile of attackers

Potential attackers are:

- The subject
- An outsider with malicious intent who tries to harm the subject or the system as a whole.

3.3.2 Level of attackers

Attackers are physical persons with basic level attacking potential i.e. ill-intentioned persons with the skills and resources of an informed user.

3.3.3 Threats to TOE elements

M.ELT.ALIMENTATION_ELECTRIQUE

An attacker runs down the non rechargeable electric battery of one the TOE elements (through abnormal use of the element for example) so that the element can no longer provide its services.

Property items under threat: Availability of sensitive services provided by the electronic tag (S.BR.SERVICES).

Note: This threat only affects the electronic tag which is the only element of the TOE handed to the subject that does not have a rechargeable electric battery.

M.ELT.PIEGEAGE_MATERIEL_FABRICATION

An attacker with physical access to the TOE during its manufacture modifies or installs an electronic component able to alter its normal operation, to divulge or amend the data it stores or handles.

Property items under threat: Integrity and availability of all sensitive services provided by the TOE. Availability, integrity and authenticity of all sensitive property items contained in the TOE.

M.ELT.PIEGEAGE_MATERIEL_LIVRAISON

An attacker with physical access to the TOE during delivery to the prison administration modifies or installs an electronic component able to alter its normal operation, to divulge or amend the data it stores or handles.

Property items under threat: Integrity and availability of all sensitive services provided by the TOE. Availability, integrity and authenticity of all sensitive property items contained in the TOE.

M.ELT.PIEGEAGE_MATERIEL

An attacker with physical access to the TOE modifies or installs an electronic component able to alter its normal operation, to divulge or amend the data it stores or handles.

Property items under threat: Integrity and availability of all sensitive services provided by the TOE. Availability, integrity and authenticity of all sensitive property items contained in the TOE.

M.ELT.PIEGEAGE_LOGICIEL_FABRICATION

An attacker with logical access via one of the interfaces of the TOE during its manufacture modifies or installs software able to alter the TOE's normal operation, to divulge or amend the data it stores or handles.

Property items under threat: Integrity and availability of all sensitive services provided by the TOE. Availability, integrity and authenticity of all sensitive property items contained in the TOE.

M.ELT.PIEGEAGE_LOGICIEL_LIVRAISON

An attacker with logical access via one of the interfaces of the TOE during delivery to the prison administration modifies or installs software able to alter the TOE's normal operation, to divulge or amend the data it stores or handles.

Property items under threat: Integrity and availability of all sensitive services provided by the TOE. Availability, integrity and authenticity of all sensitive property items contained in the TOE.

M.ELT.PIEGEAGE_LOGICIEL

An attacker with logical access via one of the interfaces of the TOE modifies or installs software able to alter the TOE normal operation, to divulge or amend the data it stores or handles.

Property items under threat: Integrity and availability of all sensitive services provided by the TOE. Availability, integrity and authenticity of all sensitive property items contained in the TOE.

M.ELT.ACCES_ILLICITE_AUX_DONNEES

An attacker with logical access via one of the interfaces of the TOE accesses the data it stores or handles in read or write mode.

Property items under threat: Integrity and availability of all sensitive services provided by the TOE. Availability, integrity, confidentiality, authenticity of all the sensitive property items contained in the TOE.

M.ELT.CANAUX_AUXILIAIRES

An attacker with physical and/or logical access to the TOE carries out non-invasive attacks via auxiliary channels in order to access the cryptographic keys stored in the TOE elements.

Property items under threat: Integrity and availability of all sensitive services provided by the TOE. Availability, integrity, confidentiality, authenticity of all the sensitive property items contained in the TOE.

3.3.4 Threats to communications

- **Threats to communications between the TOE elements**

M.COM.INTRA_TOE.ALTERATION

An attacker alters messages exchanged between the different elements of the TOE.

Property items under threat: The authenticity of the sensitive property items exchanged between the elements of the TOE.

M.COM.INTRA_TOE.DENIS_DE_SERVICE

An attacker prevents any communication from taking place between the different elements of the TOE.

Property items under threat: Availability of all sensitive property items exchanged between the elements of the TOE.

M.COM.INTRA_TOE.SUPPRESSION

An attacker prevents communication of some messages only between the different elements of the TOE.

Property items under threat: Availability of all sensitive property items exchanged between the elements of the TOE.

M.COM.INTRA_TOE.REJEU

An attacker replays some of the messages exchanged between the different elements of the TOE.

Property items under threat: All the sensitive services and property items of the TOE.

- **Threats to communications between the TOE and the remote monitoring centre application**

M.COM.CT.ALTERATION

An attacker alters messages exchanged between the TOE and the remote monitoring centre application.

Property items under threat: The authenticity of all the sensitive property items exchanged between the TOE and the remote monitoring centre application.

M.COM.CT.DENIS_DE_SERVICE

An attacker prevents any communication from taking place between the TOE and the remote monitoring centre application.

Property items under threat: The availability of all the sensitive property items exchanged between the TOE and the remote monitoring centre application.

M.COM.CT.SUPPRESSION

An attacker prevents communication of some messages between the TOE and the remote monitoring centre application.

Property items under threat: The availability of all the sensitive property items exchanged between the TOE and the remote monitoring centre application.

M.COM.CT.REJEU

An attacker replays some of the messages exchanged between the TOE and the remote monitoring centre application.

Property items under threat: All the sensitive services and property items of the TOE.

3.4 Organisational security policy

3.4.1 Cryptography

P.ANSSI.MECANISMES_CRYPTO

The cryptographic mechanisms implemented in the TOE must comply with ANSSI requirements for the standard qualification level [ANSSI_CRYPTO_STD].

P.ANSSI.GESTION_CLES_CRYPTO

The cryptographic key handling procedures used by the TOE must comply with ANSSI requirements for the standard level [ANSSI_GESTION_CLES_STD].

P.ANSSI.AUTHENTIFICATION

The authentication mechanisms implemented by the TOE must comply with ANSSI requirements for the standard level [ANSSI_AUTH_STD].

3.4.2 Qualification standard

P.ANSSI.QUALIFICATION_STANDARD[3]

The TOE is assessed on the basis of the Common Criteria [CC] for an EAL2 assurance level supplemented by the ALC_FLR.3 and AVA_VAN.3 components in accordance with the qualification process for a standard level security product [ANSSI_QS_STD].

3.4.3 Security services provided by the TOE

The [FEROS] document defines 89 security objectives to be achieved for the overall system. The overall system is made up of the following four subsystems: subject's device, remote monitoring centre, GIPSE, central offices.
The TOE corresponds to the "subject's device" in the [FEROS] document. For this reason only those security objectives relating to the subject's device from [FEROS] (Chapter 3.2.1 of [FEROS] entitled "Objectifs de sécurité du dispositif du placé" [Security objectives of the subject's device]) have translated into organisational security policy in this security target[4].
The security targets from [FEROS] relating to other subsystems (remote monitoring centre, GIPSE, central offices) are therefore included in this security target of the security objectives for the TOE environment.

P.INTEGRITE_PHYSIQUE_LOGIQUE

Security objective no 1: The device must have a significant level of resistance and emit an alarm in the event of cutting being detected.
Security objective no 2: It must not be possible to clone the tag or be able to remove it without triggering an alarm. Since this is a fundamental security objective, it is requested that the device be subjected to significant tests within the framework of a COMMON CRITERIA evaluation.

[3] The Evaluation Assurance Level (EAL) 2+ is no more compliant with the standard qualification process [ANSSI_QS_STD]. More details in [ST].

[4] The French prison administration has requested that the security objectives from [FEROS], relating to the subject's device and bearing the numbers 6, 10, 13 and 18 be removed from the security target as they are not adapted to the current organisation.

Security objective no 3: It must not be possible for the subject to modify the operating parameters of his device, and an attack on one of the components of the device (memory, etc.) must trigger an alarm.

Security objective no 4: The device (PSEM) must indicate to the subject that he/she must recharge the batteries by emitting an audible alarm and displaying a message clearly showing the operating time left for the mobile unit.

Security objective no 5: A fault of one part of the device must result in an alarm being sent to the remote monitoring centre, with the exception of the module which serves to emit the alarms. In the event that the device has two types of connection (GSM and RTC for example), the operating module must emit the alarm to the remote monitoring centre.

Note: Security objectives No. 1, 2 and 3 of P.INTEGRITE_PHYSIQUE_LOGIQUE only apply to the electronic tag.

P.INTALLATION_PLACE

Security objective no 7: The subject must be clearly informed, on the handover of the device, of the necessity of connecting the fixed part of the device to the mains.

Security objective no 8: The subject must be made aware of the value of the different parts that make up his device and make sure he does not lose the mobile part for instance.

Security objective no 9: The personnel responsible for fitting the subject's device and for configuring it must be correctly trained. Tests must be specified to verify that everything is operating correctly.

P.PERTE_COMMUNICATION

Security objective no 11: The messages and alarms transmitted between the device and the remote monitoring centre must be correct. In the event of malfunctions (bugs) or interference causing an alteration in the messages, mechanisms (integrity locking or other) would have to make it possible to detect this alteration. It must be impossible to modify geolocation messages regarding the subject under PSEM and alarms of subjects under PSE and PSEM, both statically by attacking the memory of the casing, and dynamically during the sending of these messages. In particular, messages relating to the subject's location must be protected against any modification or alteration, even in the event of the malfunction of the casing, so that the subject cannot dispute alarms due to geolocation.

Security objective no 12: It must not be possible to listen in to the communications between the various parts of the device, and between the device and the remote monitoring centre. It is therefore desirable to encrypt the exchanges.

P.FABRICATION_DEVELOPPEMENT

Security objective no 14: The element or elements made available to the subject must have a unique identifier. In the event that the device is made up of several parts, it must not be possible to obtain a part of the device directly from the supplier of the hardware.

Security objective no 15: All of the built-in software must be tested and the code must be re-read in order to check that there are no hidden functions which make it possible to listen in to communications between the various parts of the device, and between the device and the remote monitoring centre. Within the framework of the (CC) evaluation, proof of the software architecture must be provided.

Security objective no 16: The device must observe the regulations in force and must not be sensitive to electromagnetic radiation. If the subject were to be in a situation where there was an abnormal level of radiation (close to an aerial, for example), a message could be displayed in order to inform him of the interference.

Security objective no 17: The casing must withstand temperatures of between -20°C and + 50°C. Furthermore, the subject must be informed that he/she must not expose the device to a source of abnormal heat.

4 Security objectives

The security objectives reflect the stated intent and are likely to counter all the threats identified and to cover all the organisational security policies and the hypotheses identified.

If a threat does not affect the whole of the TOE but only one of its elements then this is stated explicitly in a note. Unless otherwise specified the threat applies to all the elements of the TOE. If a security objective only applies to a particular mode of use of the TOE (PSE or PSEM), this is stated explicitly in a note. Unless otherwise specified the security objective must apply to both TOE modes of use.

4.1 Security objectives for the TOE

4.1.1 Protection of communications between elements of the TOE

OT.COM.INTRA_TOE.PROTECTION

The TOE must protect the confidentiality and authenticity of the data it sends between its elements. The TOE must verify the authenticity of the data it receives from its elements. The TOE must detect replay of data it receives from its elements. The TOE must detect deletion of data it sends to its elements.

4.1.2 Protection of communications between the TOE and the remote monitoring centre

OT.COM.INTER_TOE.PROTECTION

The TOE must protect the confidentiality and authenticity of the data it sends to the remote monitoring centre application. The TOE must verify the authenticity of the data it receives from the remote monitoring centre application. The TOE must detect replay of data it receives from the remote monitoring centre application. The TOE must detect deletion of data it sends to the remote monitoring centre application.

4.1.3 Remote administration

OT.ADMINISTRATION

The TOE must allow the remote monitoring centre application, located at the remote monitoring centre, to administer it via the GSM or RTC communication networks. The remote monitoring centre application must identify and authenticate himself to the TOE in order to access administration functions.

4.1.4 Physical resistance

OT.RESISTANCE_TEMPERATURES

The TOE must be able to operate correctly at temperatures between -20° C and 50°C.

Note: This TOE security objective only applies to the electronic tag.

OT.RESISTANCE_EAU

The TOE must be waterproof and work properly under water to a maximum depth of 5 metres.

Note: This TOE security objective only applies to the electronic tag.

4.1.5 Resistance to cloning

OT.RESISTANCE_CLONAGE

The TOE must prevent any cloning of any or part of its elements as well as of the data they contain.

4.1.6 Compliance with curfew scheme

OT.RESPECT_POLITIQUE_ASSIGNATION

The TOE must enable establishing whether or not a subject is complying with the curfew scheme he/she is placed under. The TOE must generate and issue an event to the remote monitoring centre application in the event of non compliance with this curfew scheme.

OT.TEMPS_REFERENCE_FIABLE

The TOE must have a reliable time source.

4.1.7 Protection of subject's identity

OT.PROTECTION_IDENTITE_PLACE

The TOE must protect the subject's identity. It should not be possible to determine the identity of a subject by listening to data exchanged between the TOE elements or between the TOE and the remote monitoring centre application. The remote monitoring centre application must not be able to determine the subject's identity either.

4.1.8 Information to the subject

OT.DOCUMENTATION_PLACE

The TOE must be given to the subject with documentation that clearly indicates conditions of use of the TOE (connecting the fixed monitoring unit to the mains etc.), precautions to be taken (exposure to temperatures, water, be careful not to lose the mobile monitoring unit etc.), the different messages that can be displayed by the monitoring unit, their meaning and the procedures to follow for each message.

4.1.9 Detection of abnormal events

OT.DETECTION_COUPURE_BRACELET

The TOE must be able to detect when the electronic tag has been cut and send an alarm to the remote monitoring centre application.

OT.DETECTION_RETRAIT_BRACELET

The TOE must prevent the removal of the electronic tag without cutting (through stretching for instance).

OT.DETECTION_OUVERTURE

The TOE must detect any opening of its elements.

OT.DETECTION_MODIFICATION_DONNEES

The TOE must be able to detect any modification of the data it stores and send an alarm to the remote monitoring centre application in the event of these data being modified.

OT.DETECTION_BATTERIE_FAIBLE

The TOE must monitor (rechargeable or non rechargeable) battery level of its elements. In PSEM mode, the mobile monitoring unit should warn the subject when its battery level is critical and indicate the remaining operating time. In PSEM mode, the mobile monitoring unit should inform the subject, by way of a comprehensible message, when the battery is charging.

Note: The mobile monitoring unit (PSEM mode of use) has a rechargeable battery. The electronic tag does not have a rechargeable battery. The fixed monitoring unit (PSE mode of use) does not have a rechargeable battery and must be powered continually.

OT.DETECTION_PANNE

The TOE must be able to detect any fault of all or part of its elements (electronic tag, monitoring unit) and send an alarm to the remote monitoring centre application. If the TOE has several communication links (GSM, RTC), it must choose automatically the means that will allow it to effectively feed the alarm back to the remote monitoring centre application.

OT.DETECTION_PERTE_COMMUNICATION_INTRA_TOE

The TOE must be able to detect the loss of a communication link between its own elements.

OT.DETECTION_PERTE_COMMUNICATION_CT

The TOE must keep the subject clearly and continuously informed of the quality of the communication links (GSM, RTC) between the monitoring unit and the remote monitoring centre application. In the event of non-availability of one of the links, the TOE must warn the subject via an audible signal and a clear message.

OT.DETECTION_PERTE_COMMUNICATION_GPS

The TOE must keep the subject clearly and continuously informed of the quality of the GPS communication link between the monitoring unit and the GPS satellites. In the event of non-availability of the link, the TOE must warn the subject via an audible signal and a clear message.

4.1.10 Protection of information handled

OT.PROTECTION_CANAUX_AUXILIAIRES

The TOE must not allow access by auxiliary channels to the cryptographic keys contained in the TOE elements.

4.1.11 Qualification standard

OT.QUALIFICATION_STANDARD

The evaluation level of the TOE must be EAL2 supplemented by the ALC_FLR.3 and AVA_VAN.3 components in accordance with the qualification process for a standard level security product [ANSSI_QS_STD]. The TOE must comply with the [ANSSI_CRYPTO_STD] [ANSSI_GESTION_CLES_STD] and [ANSSI_AUTH_STD] documents respectively for cryptographic mechanisms, cryptographic key handling and authentication mechanisms.

4.2 Security objectives for the TOE environment

The security objectives for the TOE environment below have the suffix:

OE.CT.	when they concern the remote monitoring centre or the remote monitoring centre application (CP)
OE.AP.	when they concern the Prison Administration (PA)
OE.RC.	when they concern the communication networks (CN)
OE.MT.	when they concern the TOE hardware (MT)

4.2.1 Security objectives concerning the cryptographic key generator

OE.GENERATION_CLES_CRYPTOGRAPHIQUES

The cryptographic keys stored in the TOE elements to ensure the confidentiality and authenticity of communications between the elements, or to ensure the confidentiality and authenticity of communications between the TOE and the remote monitoring centre application should be generated by trusted personnel, on secure premises, using an FIPS-140 certified generator.

4.2.2

4.2.3 Security objectives for the remote monitoring centre and the remote monitoring centre application

OE.CT.TEMPS_REFERENCE_FIABLE

The remote monitoring centre application must have a reliable time source. This time source is used to synchronise the TOE's reference times via the communications networks (GSM/RTC).

OE.CT.COM.INTER_TOE.PROTECTION

The remote monitoring centre application must protect the confidentiality and authenticity of the data that it sends to the TOE via the communication networks (GSM/RTC). The remote monitoring centre application must verify the authenticity of the data it receives from the TOE via the communication networks. The remote monitoring centre appli cation must detect the replay of the data it receives from the TOE via the communication networks. The remote monitoring centre application must detect the deletion of the data it transmits to the TOE via the communication networks.

OE.CT.DETECTION_PERTE_COMMUNICATION

The remote monitoring centre application must detect the loss of the communication link (GSM/RTC) between the remote monitoring centre application and the TOE.

OE.CT.PERSONNEL

The remote monitoring centre must have non-hostile personnel who are appropriately trained and have all the necessary operational documentation made available to them.

OE.CT.PROTECTION_CLES_CRYPTOGRAPHIQUES

The remote monitoring centre application must protect the confidentiality of the cryptographic keys used by the remote monitoring centre application to ensure the confidentiality and authenticity of communications with the TOE.

4.2.4 Security objectives for the prison administration

OE.AP.SECURITE_STOCKAGE

The prison administration must store the TOE securely on its premises in order to prevent any hardware or software tampering during its storage.

OE.AP.ALIMENTATION_ELECTRIQUE

The prison administration must provide the subject with a TOE whose elements that are not fitted with a rechargeable battery will continue to operate throughout their period of use.

Note: The only TOE element that does not have a rechargeable battery is the electronic tag.

OE.AP.PERSONNEL

The prison administration must have non-hostile personnel who are appropriately trained and have all the necessary operational documentation made available to them.

OE.AP.PLACE

The prison administration must make the subject aware of the value of the various parts of the TOE, inform him of the conditions of use of the TOE and of the precautions to be taken.

OE.AP.EFFACEMENT_CLES_CRYPTOGRAPHIQUES

Using overloading the prison administration must delete the TOE's cryptographic keys contained in the diagnostic tool in a secure manner in the event of the tool being scrapped.

4.2.5 Security objectives for the communication networks between the TOE and the remote monitoring centre application

OE.RC.DISPONIBILITE_CAPACITE_RESEAUX

The communication networks (GSM/RTC) that provide communication between the TOE and the remote monitoring centre application operate correctly and are dimensioned correctly.

Note: The only element of the TOE that communicates directly with the remote monitoring centre application is the mobile monitoring unit.

4.2.6 Security objectives for the TOE hardware

OE.MT.FONCTIONNEMENT_CORRECT

The electronic hardware of which the TOE is made up (electronic components etc) has not broken down and is operating correctly.

5 Security requirements

5.1 Security functional requirements for the TOE

5.1.1 Summary

Requirements		Descriptions
Class FAU : Audit		
	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit Review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
Class FCP : Curfew Policy		
	FCP_CMP.1	Curfew Policy Compliance
Class FIA : Identification and authenticaton		
	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Class FMT : Security management		
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Class FPR : Privacy		
	FPR_ANO.1	Anonymity
Class FPT : Protection of the TSF		
	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_ITT.1	Basic internal TSF data transfert protection
	FPT_ITT.3	TSF data integrity monitoring
	FPT_PHP.2	Notification of physical attack
	FPT_PHP.3	Resistance to physical attack
	FPT_RPL.1	Replay detection
	FPT_STM.1	Time stamps
	FPT_EMSEC.1	TOE Emanation
Class FCS : Cryptographic support		
	FCS_COP.1	Cryptographic operation
Class FDP : User Data Protection		
	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control

Table 1 : List of selected security functional requirements

All functional requirements for the TOE were extracted from Part 2 of the Common Criteria [CC], except for the functional security requirements FCP_CMP.1 and FPT_EMSEC.1.

Class FCP is not part of Part 2 of Common Criteria [CC] and is dedicated to curfew policy. FCP class contains a single family FCP_CMP (Curfew Policy Compliance).

5.1.2 Detailed functional requirements for the TOE

- **Protection against auxiliary channels**

FPT_EMSEC.1 TOE Emanation

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall not emit [assignment: auxiliary channels] enabling access to [assignment: cryptographic keys contained in the elements of the TOE].

Refinement: This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

- **Time source offered by the TOE**

FPT_STM.1 Reliable time stamps

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

- **Generation of events**

FAU_GEN.1 Audit data generation

Iteration 1: Monitoring unit

Dependencies: FPT_STM.1

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
b) All auditable events for [selection, choose one of: minimum] level of audit; and
c) [assignment: the events described in [FSP]].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: a level of priority (high, medium, low)].

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

Iteration 2: Docking station

Dependencies: FPT_STM.1

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
b) All auditable events for [selection, choose one of: minimum] level of audit; and
c) [assignment: the events described in [FSP]].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: a level of priority (high, medium, low)].

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☐ Monitoring Unit ☑ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

FAU_STG.1 Protected audit trail storage

Dependencies: FAU_GEN.1/Iteration_1, FAU_GEN.1/Iteration_2

FAU_STG1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG1.2 The TSF shall be able to [selection, choose one of: prevent] unauthorised modifications to the stored audit records in the audit trail.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

FAU_STG.4 Prevention of audit data loss

Dependencies: FAU_STG.1

FAU_STG.4.1 The TSF shall [selection: overwrite the oldest stored audit records] and [assignment: generate an event showing that old events have been deleted] if the audit trail is full.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

FAU_SAR.1 Audit review

Iteration 1: Central administration

Dependencies: FAU_GEN.1/Iteration_1, FAU_GEN.1/Iteration_2

FAU_SAR.1.1 The TSF shall provide [assignment: monitoring centre application] with the capability to read [assignment: all events generated by the TOE] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

Iteration 2: Subject

Dependencies: FAU_GEN.1/Iteration_1

FAU_SAR.1.1 The TSF shall provide [assignment: subject] with the capability to read [assignment: mobile monitoring unit battery level] from the audit records.
FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

Note: This requirement only applies to the mobile monitoring unit, and therefore PSEM mode. The events which the subject can have access to in read mode are communicated to him via the mobile monitoring unit screen.

- **Central administration and local TOE supervision and administration functions**

FMT_SMF.1 Specification of management functions

Iteration 1: Central administration

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment:
- Central administration of the monitoring unit:
  - Reading and modification of the monitoring unit reference time,
  - Reading and modification of the curfew scheme which the subject is subject to,
  - Reading and deleting events].

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

Iteration 2: Local supervision

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment:
- Local supervision of the electronic tag

    - Battery level check,
    - Serial number check,
    - Software version number check,
    - Status check
- Local supervision of the key fob:
    - Battery level check,
    - Serial number check,
    - Software version number check,
    - Status check
- Local supervision of the monitoring unit:
    - Serial number check,
    - Software version number check,
    - Battery level check
- Local supervision of the fitting and installation tool:
    - Serial number check,
    - Software version number check,
    - Battery level check].

<u>Refinement :</u> This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

Iteration 3: Local administration

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment:

- Local administration of the monitoring unit (PSE and PSEM):
    - Checking and modification of the GSM configuration data:
        - IP Address
        - APN
        - ID
        - password, port
- Local administration of the monitoring unit (PSE and PSEM):
    - Checking and modification of the RTC configuration data:
        - "data" phone number,
        - "voice" phone number,
        - Emergency Number.]

<u>Refinement :</u> This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☑ Diagnostic tool ☐ Fitting and installation tool

Iteration 4: Initialisation

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment:

- Initialisation:

- Change the electronic tag status
- Starting/stopping the docking station]

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

FMT_MTD.1 Management of TSF data

Iteration 1: Central administration

Dependencies: FMT_SMR.1, FMT_SMF.1/Iteration_1

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear] the [assignment:

- Monitoring unit reference time,
- The subject's curfew scheme,
- The events from the audit log]

to [assignment: remote monitoring centre application].

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

Iteration 2: Local supervision

Dependencies: FMT_SMR.1, FMT_SMF.1/Iteration_2

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: query] the [assignment:

- The parameters of the electronic tag:
    - Battery level check,
    - Serial number check,
    - Software version number check,
    - Status check
- The parameters of the key fob:
    - Battery level check,
    - Serial number check,
    - Software version number check,
    - Status check
- The parameters of the monitoring unit:
    - Serial number check,
    - Software version number check,
    - Battery level check
- The parameters of the fitting and installation tool:
    - Serial number check,
    - Software version number check,
    - Battery level check].

to [assignment: local supervisor].

Refinement : This security functional requirement applies to the following TOE elements:

☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

Iteration 3: Local administration

Dependencies: FMT_SMR.1, FMT_SMF.1/Iteration_3

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify] the [assignment:

- The RTC parameters of the fixed monitoring unit (PSE):
  - "data" phone number,
  - "voice" phone number,
  - Emergency Number.
- The GSM parameters of the monitoring unit (PSE and PSEM):
  - IP Address,
  - APN,
  - ID,
  - password,
  - port.]

to [assignment: local administrator].

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☑ Diagnostic tool ☐ Fitting and installation tool

Iteration 4: Initialisation

Dependencies: FMT_SMR.1, FMT_SMF.1/Iteration_4

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear] the [assignment:

- change the electronic tag status]

to [assignment: prison administration agent].

- **Authentication of the central administration and of the local TOE supervision and administration**

FMT_SMR.1 Security roles

Dependencies: FIA_UID.2/Iteration_1, FIA_UID.2/Iteration_2, FIA_UID.2/Iteration_3, FIA_UID.2/Iteration_4

FMT_SMR.1.1 The TSF shall maintain the roles [assignment:

- remote monitoring centre application,
- subject,
- local supervisor,
- local administrator,
- prison administration agent].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

FIA_UID.2 User identification before any action

Iteration 1: Central administration

Dependencies: No other components.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

Note: The term "user" in this security functional requirement refers to the "remote monitoring centre application" role.

Iteration 2: Local supervision

Dependencies: No other components.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

Note: The term "user" in this security functional requirement refers to the "local supervisor" role.

Iteration 3: Local administration

Dependencies: No other components.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☑ Diagnostic tool ☐ Fitting and installation tool

Note: The term "user" in this security functional requirement refers to the "local administrator" role.

Iteration 4: Initialisation

Dependencies: No other components.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

Note: The term "user" in this security functional requirement refers to the "prison administration agent" role.

FIA_UAU.2 User authentication before any action

Iteration 1: Central administration

Dependencies: FIA_UID.2/Iteration_1

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

Note: The term "user" in this security functional requirement refers to the "remote monitoring centre application" role.

Iteration 2: Local supervision

Dependencies: FIA_UID.2/Iteration_2

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

Note: The term "user" in this security functional requirement refers to the "local supervisor" role.

Iteration 3: Local administration

Dependencies: FIA_UID.2/Iteration_3

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

Note: The term "user" in this security functional requirement refers to the "local administrator" role.

Iteration 4: Initialisation

Dependencies: FIA_UID.2/Iteration_4

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

Note: The term "user" in this security functional requirement refers to the "prison administration agent" role.

- **Protection of communications between elements of the TOE**

FPT_ITT.1 Basic internal TSF data transfer protection

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from [selection: disclosure, modification] when it is transmitted between separate parts of the TOE.

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

FPT_ITT.3 TSF data integrity monitoring

Dependencies: FPT_ITT.1

FPT_ITT.3.1 The TSF shall be able to detect [selection: modification of data, substitution of data, re-ordering of data, deletion of data] for TSF data transmitted between separate parts of the TOE.
FPT_ITT.3.2 Upon detection of a data integrity error, the TSF shall take the following actions: [assignment: generate an event].

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

FPT_RPL.1 Replay detection

Dependencies: No dependencies.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [assignment: electronic tag, monitoring unit, docking station, key fob, fitting and installation tool].
FPT_RPL.1.2 The TSF shall perform [assignment:

- generate an event,
- ignore data with failed authenticity verification]

when replay is detected.

Refinement : This security functional requirement applies to the following TOE elements:

☑ Electronic Tag	☑ Monitoring Unit	☑ Docking station
☑ Key fob	☑ Diagnostic tool	☑ Fitting and installation tool

- **Detection and notification of physical attacks on the TOE elements**

FPT_PHP.2 Notification of physical attack

Dependencies: FMT_MOF.1

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
FPT_PHP.2.3 For [assignment: electronic tag, the monitoring unit, the docking station], the TSF shall monitor the devices and elements and notify [assignment: remote monitoring centre application] when physical tampering with the TSF's devices or TSF's elements has occurred.

Refinement : This security functional requirement applies to the following TOE elements:

☑ Electronic Tag	☑ Monitoring Unit	☑ Docking station
☐ Key fob	☐ Diagnostic tool	☐ Fitting and installation tool

- **Protection of communications between the TOE and the remote monitoring centre**

FPT_ITC.1 Inter-TSF confidentiality during transmission

Dependencies: No dependencies.

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

Refinement : This security functional requirement applies to the following TOE elements:

☐ Electronic Tag	☑ Monitoring Unit	☑ Docking station
☐ Key fob	☐ Diagnostic tool	☐ Fitting and installation tool

FPT_ITI.1 Inter-TSF detection of modification

Dependencies: No dependencies.

FTP_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: [assignment: AES deciphering of data sent by the remote monitoring centre shows loss of authenticity].
FTP_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [assignment: generate an event] if modifications are detected.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

- **Cryptography**

FCS_COP.1 Cryptographic operation

Dependencies: No dependencies.

FCS_COP.1.1 The TSF shall perform [assignment: ciphering, deciphering] in accordance with a specified cryptographic algorithm [assignment: AES-CBC (ciphering), AES-CMAC (authentication)] and cryptographic key sizes [assignment: 128 bits] that meet the following: [assignment: FIPS-197 (AES), FIPS81-2 (CBC), ANSSI referentials [ANSSI_CRYPTO_STD], [ANSSI_GESTION_CLE_STD], [ANSSI_AUTH_STD]].

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

- **Protection of subject's identity**

FPR_ANO.1 Anonymity

Dependencies: No dependencies.

FPR_ANO.1.1 The TSF shall ensure that [assignment: remote monitoring centre application] are unable to determine the real user name bound to [assignment: the subject].

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☑ Docking station
☑ Key fob ☑ Diagnostic tool ☑ Fitting and installation tool

FIA_ATD.1 User attribute definition

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment:

- unique ID of the electronic tag (PSE and PSEM)
- unique ID of the fixed monitoring unit (PSE)
- unique ID of the mobile monitoring unit (PSEM)
- unique ID of the docking station (PSEM)
- unique ID of the fitting and installation tool (PSE and PSEM)
- unique ID of the key fob (PSE and PSEM)
- unique ID of the diagnostic tool (PSE and PSEM)].

Refinement : This security functional requirement applies to the following TOE elements:

☑ Electronic Tag
☑ Key fob
☑ Monitoring Unit
☑ Diagnostic tool
☑ Docking station
☑ Fitting and installation tool

- **Resistance to phenomena**

FPT_PHP.3 Resistance to physical attack

Iteration 1 : Electronic tag, monitoring unit, docking station, key fob, fitting and installation tool

Dependencies: No dependencies.

FPT_PHP.3 The TSF shall resist [assignment:

- temperatures between -20°C et +50°C]

to the [assignment: electronic tag, monitoring unit, docking station, key fob, fitting and installation tool]

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag
☑ Key fob
☑ Monitoring Unit
☑ Diagnostic tool
☑ Docking station
☑ Fitting and installation tool

Iteration 2 : Electronic tag

Dependencies: No dependencies.

FPT_PHP.3 The TSF shall resist [assignment:

- water to a maximum depth of 5 metres]

to the [assignment: electronic tag] by responding automatically such that the SFRs are always enforced.

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag
☐ Key fob
☐ Monitoring Unit
☐ Diagnostic tool
☑ Docking station
☐ Fitting and installation tool

- **Compliance with curfew scheme**

FCP_CMP.1 Curfew Policy Compliance

Dependencies: FMT_MSA.3/Iteration_1

FCP_CMP.1.1 The TSF shall enforce the [assignment: curfew scheme] on [assignment:

Subject:

- the subject

Objects:

- the zones resulting from the curfew scheme under which the subject is placed

Operations:

- subject's presence in or absence from these zones].

FCP_CMP.1.2 The TSF shall enforce the [assignment: curfew scheme] to objects based on the following: [assignment:

Subject:

- the subject. Security attribute: the geographical location of the subject.

Objects:

- the curfew scheme. Security attributes: the curfew scheme, the monitoring unit reference time].

FCP_CMP.1.3 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- The subject must not be in an exclusion zone at the forbidden times.
- The subject must be in an inclusion zone at the compulsory times].

FCP_CMP.1.4 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: end of curfew period].

FCP_CMP.1.5 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: none].

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

FMT_MSA.1 Management of security attributes

Iteration 1: Central administration

Dependencies: FDP_ACC.2/Iteration_1, FMT_SMR.1, FMT_SMF.1/Iteration_1

FMT_MSA.1.1 The TSF shall enforce the [assignment: curfew scheme] to restrict the ability to [selection: change_default, query, modify, delete] the security attributes [assignment:

- The exclusion zones and time periods associated with this zone.
- The inclusion zones and time periods associated with this zone.

to [assignment: remote monitoring centre application].

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

Iteration 2: Local supervision

Dependencies: FDP_ACC.2/Iteration_2, FMT_SMR.1, FMT_SMF.1/Iteration_2

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control policy on local supervision] to restrict the ability to [selection: query] the security attributes [assignment:

- o Local supervision of the electronic tag
  - Battery level check,
  - Serial number check,
  - Software version number check,
  - Status check
- o Local supervision of the key fob:
  - Battery level check,
  - Serial number check,

        - Software version number check,
        - Status check
    - Local supervision of the monitoring unit:
        - Serial number check,
        - Software version number check,
        - Battery level check
    - Local supervision of the fitting and installation tool:
        - Serial number check,
        - Software version number check,
        - Battery level check].

to [assignment: local supervisor].

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☑ Key fob ☐ Diagnostic tool ☑ Fitting and installation tool

Iteration 3: Local administration

Dependencies: FDP_ACC.2/Iteration_3, FMT_SMR.1, FMT_SMF.1/Iteration_3

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control policy on local administration] to restrict the ability to [selection: query] the security attributes [assignment:

- Local administration of monitoring unit (PSE et PSEM) :
    - GSM configuration data :
        - IP Address
        - APN
        - ID
        - password, port
- Local administration of monitoring unit (PSE et PSEM) :
    - RTC configuration data :
        - "data" phone number,
        - "voice" phone number,
        - Emergency Number.]

to [assignment: administrateur local].

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

Iteration 4: Initialisation

Dependencies: FDP_ACC.2/Iteration_4, FMT_SMR.1, FMT_SMF.1/Iteration_4

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control policy on initialisation] to restrict the ability to [selection: query] the security attributes [assignment:

- Electronic tag status]

to [assignment: prison administration agent].

Refinement : This security functional requirement applies to the following TOE elements:

☑ Electronic Tag ☐ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

FMT_MSA.3 Static attribute initialisation

Itération 1: Central administration

Dependencies: **FMT_MSA.1/Iteration_1, FMT_SMR.1**

FMT_MSA.3.1 The TSF shall enforce the [assignment: access control policy on central administration] to provide [selection, choose one of: restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow the [assignment: monitoring centre application] to specify alternative initial values to override the default values when an object or information is created.

Refinement : This security functional requirement applies to the following TOE elements:
☐ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

Iteration 2: Local administration

Dependencies: FMT_MSA.1/Iteration_3, FMT_SMR.1

FMT_MSA.3.1 The TSF shall enforce the [assignment: access control policy on local administration] to provide [selection, choose one of: restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow the [assignment: local administrator] to specify alternative initial values to override the default values when an object or information is created.

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☑ Monitoring Unit ☐ Docking station
☑ Key fob ☐ Diagnostic tool ☑ Fitting and installation tool

Iteration 3: Initialisation

Dependencies: FMT_MSA.1/Iteration_4, FMT_SMR.1

FMT_MSA.3.1 The TSF shall enforce the [assignment: access control policy on initialization] to provide [selection, choose one of: restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow the [assignment: prison administration agent] to specify alternative initial values to override the default values when an object or information is created.

Refinement : This security functional requirement applies to the following TOE elements:
☑ Electronic Tag ☐ Monitoring Unit ☐ Docking station
☐ Key fob ☐ Diagnostic tool ☐ Fitting and installation tool

- **Access control policy**

FDP_ACC.2 Complete access control

Iteration 1: Ccentral administration

Dependencies: FDP_ACF.1/Iteration_1

FDP_ACC.2.1 The TSF shall enforce the [assignment: access control policy on central administration] on [assignment:

Subject :

- Monitoring centre application

Objects :

- Access on central administration].

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

<u>Refinement :</u> This security functional requirement applies to the following TOE elements:

☐ Electronic Tag
☐ Key fob
☑ Monitoring Unit
☐ Diagnostic tool
☐ Docking station
☐ Fitting and installation tool

Iteration 2: Local supervision

Dependencies: FDP_ACF.1/Iteration_2

FDP_ACC.2.1 The TSF shall enforce the [assignment: access control policy on local supervision] on [assignment:

Subject :

- Local supervisor

Objects :

- Access on local supervision].

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

<u>Refinement :</u> This security functional requirement applies to the following TOE elements:

☑ Electronic Tag
☑ Key fob
☑ Monitoring Unit
☐ Diagnostic tool
☐ Docking station
☑ Fitting and installation tool

Iteration 3: Local administration

Dependencies: FDP_ACF.1/Iteration_3

FDP_ACC.2.1 The TSF shall enforce the [assignment: access control policy on local administration] on [assignment:

Subject :

- Local administrator

Objects :
- Access on local administration].

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Refinement : This security functional requirement applies to the following TOE elements:

☑ Electronic Tag
☑ Key fob
☑ Monitoring Unit
☐ Diagnostic tool
☐ Docking station
☑ Fitting and installation tool

Iteration 4: Initialisation

Dependencies: FDP_ACF.1/Iteration_4

FDP_ACC.1.2 The TSF shall enforce the [assignment: access control policy on initialization] on [assignment:

Subject :
- prison administration agent

Objects :
- access on initialization].

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Refinement : This security functional requirement applies to the following TOE elements:

☑ Electronic Tag
☐ Key fob
☐ Monitoring Unit
☐ Diagnostic tool
☐ Docking station
☐ Fitting and installation tool

FDP_ACF.1 Security attribute based access control

Iteration 1: Central administration

Dependencies: FDP_ACC.2/Iteration_1, FMT_MSA.3/Iteration_1

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control policy on central administration] to objects based on the following: [assignment:

Subject:
- monitoring centre application

Objects:
- Access on central administration].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:
- Central administration requests should be authenticated].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: Central administration requests are authenticated].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: Central administration requests are not authenticated].

Refinement : This security functional requirement applies to the following TOE elements:

☐ Electronic Tag	☑ Monitoring Unit	☐ Docking station
☐ Key fob	☐ Diagnostic tool	☐ Fitting and installation tool

Iteration 2: Local supervision

Dependencies: FDP_ACC.2/Iteration_2

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control policy on local supervision] to objects based on the following: [assignment:

Subject:

- Local supervisor

Objects:

- Access on local supervision].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- Local supervision requests should be authenticated].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: Local supervision requests are authenticated].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: Local supervision requests are not authenticated].

Refinement : This security functional requirement applies to the following TOE elements:

☑ Electronic Tag	☑ Monitoring Unit	☐ Docking station
☑ Key fob	☐ Diagnostic tool	☑ Fitting and installation tool

Iteration 3: Local administration

Dependencies: FDP_ACC.2/Iteration_3, FMT_MSA.3/Iteration_2

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control policy on local administration] to objects based on the following: [assignment:

Subject:

- Local administrator

Objects:

- Access on local administration].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- Local administration requests should be authenticated].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: Local administration requests are authenticated].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: Local administration requests are not authenticated].

Raffinement : Cette exigence fonctionnelle de sécurité s'applique aux éléments de la TOE suivants :

☑ Bracelet électronique	☑ Unité de surveillance	☐ Station d'accueil
☑ Porte clé	☐ Outil de diagnostic	☑ Outil de montage et d'installation

Iteration 4: Initialisation

Dependencies: FDP_ACC.2/Iteration_4, FMT_MSA.3/Iteration_3

FDP_ACF.1.1 The TSF shall enforce the [assignment: access control policy on initialisation] to objects based on the following: [assignment:

Subject:

- prison administration agent

Objects:

- Access on initialization].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- Initialization requests should be authenticated].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: Initialization requests are authenticated].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: Initialization requests are not authenticated].

Raffinement : Cette exigence fonctionnelle de sécurité s'applique aux éléments de la TOE suivants :

☑ Bracelet électronique	☐ Unité de surveillance	☐ Station d'accueil
☐ Porte clé	☐ Outil de diagnostic	☐ Outil de montage et d'installation

5.2 Security functional requirements for the TOE environment

5.2.1 Security functional requirements for the remote monitoring centre

FPT_STM.1/CT Reliable time stamps

FPT_STM.1.1 The [monitoring centre application] shall be able to provide reliable time stamps for its own use.

Note: This security functional requirement enables the remote monitoring centre application to have a reliable time source available. In PSE mode the TOE synchronises its reference time against that of the remote monitoring centre application. In GPS mode, the TOE synchronises itself directly via GPS.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: ciphering, deciphering] in accordance with a specified cryptographic algorithm [assignment: AES] and cryptographic key sizes [assignment: 128 bits] that meet the following: [assignment: ANSSI referentials [ANSSI_CRYPTO_STD], [ANSSI_GESTION_CLE_STD], [ANSSIAUTH_STD]].

Note: This security functional requirement enables the remote monitoring centre to protect (in terms of confidentiality and authenticity) data that it sends to the TOE and to verify the authenticity of the data it receives from the TOE.

5.3 Assurance requirements for the TOE

The level aimed at is **EAL2 supplemented** by the ALC.FLR.3 and AVA_VAN.3 components.

The evaluation level fulfils the requirements of the qualification process to "standard" level.

Exigences		Intitulés
Class ADV : Development		
	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Class AGD : Guidance documents		
	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Class ALC : Life-cycle support		
	ALC_DVS.1	Identification of security measures
	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.3	Systematic flaw remediation
Class ASE : Security target evaluation		
	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Class ATE : Tests		
	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Class AVA : Vulnerability assessment		
	AVA_VAN.3	Vulnerability analysis

Table 2 : List of selected assurance requirements

All assurance requirements for the TOE were extracted from Part 3 of the Common Criteria [CC].

6 Summary of TOE specifications

6.1 Security functions

F.ADMINISTRATION_CENTRALE

This security function enables the remote monitoring centre application, located at the remote monitoring centre, to administer the TOE remotely via the communication networks (GSM, RTC). Administration of the TOE involves being able to view/modify the TOE security configuration i.e. being able to view/modify its security attributes. This security function also enables events generated by the TOE to be sent to the remote monitoring centre application via the communication networks (GSM, RTC).

Access to the central administration function of the TOE requires identification and authentication of the remote monitoring centre application by the TOE.

F.ADMINISTRATION_LOCALE

This security function allows a prison administration agent with a diagnostic tool and a key fob read-only access to certain parameters (status, battery level, serial number, etc.) of the TOE elements and write access to certain parameters of the TOE elements ("data" and "voice" telephone numbers of the monitoring unit for GSM communications, etc.).

Access to the TOE local administration function requires identification and authentication of the local administrator.

F.SUPERVISION_LOCALE

This security function allows a prison administration agent with a diagnostic tool and a key fob read-only access to certain parameters (status, battery level, serial number, etc.) of the TOE elements.

Access to the TOE local administration function requires identification and authentication of the local supervisor.

F.INITIALISATION

This security function allows a prison administration agent with a diagnostic tool and a key fob to initialise the TOE elements including changing the status of the electronic tag.

Access to the TOE initialisation function requires identification and authentication of the prison administration agent. This identification and authentication is performed using the key fob.

F.PROTECTION_COM_INTER_TOE

This security function enables the TOE to protect the data exchanged between its own elements in terms of confidentiality and authenticity(remote monitoring centre application). The cryptographic keys that protect the data exchanged between the TOE and its environment (remote monitoring centre application) are also stored in the remote monitoring centre. Communications between the TOE and the remote monitoring centre application are also protected against replay and deletion.

F.PROTECTION_COM_INTRA_TOE

This security function enables the TOE to protect the data exchanged between its own elements in terms of confidentiality and authenticity. Communications between the TOE elements are also protected against replay and deletion.

F.ROLES

This security function enables management of the various roles within the TOE i.e. remote monitoring centre application, subject, local supervisor, local administrator. These roles have different privileges and therefore access different functions.

F.RESPECT_POLITIQUE_ASSIGNATION

This security function enables the TOE to verify that the subject does comply with the curfew scheme which he/she is subject to.

F.TEMPS_FIABLE

This security function enables the TOE to have and provide a reliable time source which is one of the elements required to establish whether or not the subject is complying with the curfew scheme he/she is placed under.

The TOE synchronises its reference time against that of the remote monitoring centre (PSE) or via GPS (PSEM).

F.AUDIT

This security function enables the TOE to generate events and store them temporarily and securely. The events generated each have a level of priority. The events generated are transmitted to the remote monitoring centre application, situated in the remote monitoring centre.

F.DETECTION_PERTE_INTEGRITE

This security function enables the TOE to detect any physical attack such as exposure to abnormal temperatures, TOE elements being opened, electronic tag being cut or removed. The purpose of the TOE is not so much to prevent attacks that affect its physical integrity but to detect them systematically.

F.PROTECTION_IDENTITE_PLACE

This security function enables the TOE to protect the subject's identity. The subject's identity cannot be determined from the data contained in the TOE elements nor from the data exchanged between the TOE elements, nor from the data exchanged between the TOE and the remote monitoring centre.

6.2 Assurance measures

The developer has implemented the following security assurance measures.

CONFIGURATION MANAGEMENT

The developer uses a configuration management system that guarantees integrity of the TOE and of its documentation during development phases.

These measures make it possible to meet class ALC assurance requirements.

DELIVERY AND OPERATION

TOE secure delivery and installation procedures are available.

These measures make it possible to meet class ALC assurance requirements.

DESIGN DOCUMENTS

The developer has technical documentation which describes the TOE design with several levels of refinement (functional specifications, high level design, low level design and source code for cryptographic mechanisms).

These measures make it possible to meet class ADV assurance requirements.

GUIDES

TOE user and administration documentation is available.

These measures make it possible to meet class AGD assurance requirements.

LIFE CYCLE SUPPORT

TOE development is carried out in a secure environment.

There is technical support available that provides corrective and evolutive maintenance of the product.

These measures make it possible to meet class ALC assurance requirements.

FUNCTIONAL TESTS

Intensive functional tests are carried out for all versions of the TOE.

These measures make it possible to meet class ATE assurance requirements.

VULNERABILITY ANALYSIS

All the vulnerabilities known to the developer for this type of product have been taken into account during product development.

These measures make it possible to meet class AVA assurance requirements.

7 Conformity to a protection profile

This security target does not claim conformity with a protection profile.

8 Reasons

8.1 Reasons for security objectives

8.1.1 Summary

		Hypothesis													Threats																	Organisational Security Policy								
		H.GENERATION_CLES_CRYPTOGRAPHIQUES	H.CT.TEMPS_REFERENCE_FIABLE	H.CT.COM.INTER_TOE_PROTECTION	H.CT.DETECTION_PERTE_COMMUNICATION	H.CT.PERSONNEL	H.CT.PROTECTION_CLES_CRYPTOGRAPHIQUES	H.AP.SECURITE_STOCKAGE	H.AP.ALIMENTATION_ELECTRIQUE	H.AP.PERSONNEL	H.AP.PLACE	H.AP.EFFACEMENT_CLES_CRYPTOGRAPHIQUES	H.RC.DISPONIBILITE_CAPACITE_RESEAUX	H.MT.FONCTIONNEMENT_CORRECT	M.ELT.ALIMENTATION_ELECTRIQUE	M.ELT.PIEGEAGE_MATERIEL_FABRICATION	M.ELT.PIEGEAGE_MATERIEL_LIVRAISON	M.ELT.PIEGEAGE_MATERIEL	M.ELT.PIEGEAGE_LOGICIEL_FABRICATION	M.ELT.PIEGEAGE_LOGICIEL_LIVRAISON	M.ELT.PIEGEAGE_LOGICIEL	M.ELT.ACCES_ILLICITE_AUX_DONNEES	M.ELT.CANAUX_AUXILIAIRES	M.COM.INTRA_TOE.ALTERATION	M.COM.INTRA_TOE.DENIS_DE_SERVICE	M.COM.INTRA_TOE.SUPPRESSION	M.COM.INTRA_TOE.REJEU	M.COM.CT.ALTERATION	M.COM.CT.DENIS_DE_SERVICE	M.COM.CT.SUPPRESSION	M.COM.CT.REJEU	P.ANSSI.MECANISMES_CRYPTO	P.ANSSI.GESTION_CLES_CRYPTO	P.ANSSI.AUTHENTIFICATION	P.ANSSI.QUALIFICATION_STANDARD	P.INTEGRITE_PHYSIQUE_LOGIQUE	P.INSTALLATION_PLACE	P.PERTE_COMMUNICATION	P.FABRICATION_DEVELOPPEMENT	P.RESPECT_POLITIQUE_ASSIGNATION
Security Objectives for the TOE	OT.COM.INTRA_TOE.PROTECTION																							X	X	X	X											X		
	OT.COM.INTER_TOE.PROTECTION																											X	X	X	X							X		
	OT.ADMINISTRATION_CENTRALE														X			X			X	X		X	X	X	X	X	X	X						X				
	OT.ADMINISTRATION_LOCALE														X			X			X	X																		
	OT.SUPERVISION_LOCALE														X			X			X	X																		
	OT.INITIALISATION																					X																		
	OT.RESISTANCE_TEMPERATURES																																			X			X	
	OT.RESISTANCE_EAU																																			X			X	
	OT.RESISTANCE_CLONAGE																					X																		X
	OT.RESPECT_POLITIQUE_ASSIGNATION																																							X
	OT.TEMPS_REFERENCE_FIABLE																																							X
	OT.PROTECTION_IDENTITE_PLACE																					X																	X	
	OT.DOCUMENTATION_PLACE																							X	X	X		X	X	X						X	X	X	X	
	OT.DETECTION_COUPURE_BRACELET																	X			X	X														X				X
	OT.DETECTION_RETRAIT_BRACELET_BRACELET																	X			X	X														X				X
	OT.DETECTION_OUVERTURE																	X			X	X														X				X
	OT.DETECTION_MODIFICATION_DONNEES																	X			X	X														X		X		X
	OT.DETECTION_BATTERIE_FAIBLE														X																					X				
	OT.DETECTION_PANNE														X			X			X	X														X		X		
	OT.DETECTION_PERTE_COMMUNICATION_INTRA_TOE																								X	X										X		X		X
	OT.DETECTION_PERTE_COMMUNICATION_CT																												X							X		X		X
	OT.DETECTION_PERTE_COMMUNICATION_GPS																																			X		X		X
	OT.PROTECTION_CANAUX_AUXILIAIRES																						X																	X
	OT.QUALIFICATION_STANDARD					X				X	X					X	X		X	X												X	X	X	X				X	
Security objectives for the environment of the TOE	OE.GENERATION_CLES_CRYPTOGRAPHIQUES	X																																						
	OE.CT.TEMPS_REFERENCE_FIABLE		X																																					X
	OE.CT.COM.INTER_TOE.PROTECTION			X																								X										X		
	OE.CT.DETECTION_PERTE_COMMUNICATION				X																								X									X		X
	OE.CT.PERSONNEL					X																																		X
	OE.CT.PROTECTION_CLES_CRYPTOGRAPHIQUES						X																																	
	OE.AP.SECURITE_STOCKAGE							X										X			X	X																		
	OE.AP.ALIMENTATION_ELECTRIQUE								X						X																									
	OE.AP.PERSONNEL									X																											X			

	OE.AP.PLACE									X																										X				
	OE.AP.EFFACEMENT_CLES_CRYPTOGRAPHIQUES										X																													
	OE.RC.DISPONIBILITE_CAPACITE_RESEAUX											X																X												
	OE.MT.FONCTIONNEMENT_CORRECT												X	X																										

Table 3 : Coverage of hypotheses, threats, organisational security policies by the TOE security objectives for the TOE and the security objectives for the TOE environment

8.1.2 Hypotheses coverage

Coverage justifications are not provided in the sanitized version of the Security Target in to protect proprietary information. Complete coverage justification provided in [ST].

8.1.3 Threat coverage

Coverage justifications are not provided in the sanitized version of the Security Target in order to protect proprietary information. Complete coverage justification provided in [ST].

8.1.4 Coverage of the organisational security policies

Coverage justifications are not provided in the sanitized version of the Security Target in order to protect proprietary information. Complete coverage justification provided in [ST].

8.2 *Reasons for security functional requirements*

8.2.1 Summary

	OT.COM.INTRA_TOE.PROTECTION	OT.COM.INTER_TOE.PROTECTION	OT.ADMINISTRATION_CENTRALE	OT.ADMINISTRATION_LOCALE	OT.SUPERVISION_LOCALE	OT.INITIALISATION	OT.RESISTANCE_TEMPERATURES	OT.RESISTANCE_EAU	OT.RESISTANCE_CLONAGE	OT.RESPECT_POLITIQUE_ASSIGNATION	OT.TEMPS_REFERENCE_FIABLE	OT.PROTECTION_IDENTITE_PLACE	OT.DOCUMENTATION_PLACE[5]	OT.DETECTION_COUPURE_BRACELET	OT.DETECTION_RETRAIT_BRACELET_BRACELET	OT.DETECTION_OUVERTURE	OT.DETECTION_MODIFICATION_DONNEES	OT.DETECTION_BATTERIE_FAIBLE	OT.DETECTION_PANNE	OT.DETECTION_PERTE_COMMUNICATION_INTRA_TOE	OT.DETECTION_PERTE_COMMUNICATION_CT	OT.DETECTION_PERTE_COMMUNICATION_GPS	OT.PROTECTION_CANAUX_AUXILIAIRES	OT.QUALIFICATION_STANDARD
FAU_GEN.1/Iteration_1									X	X				X	X	X	X	X	X	X	X	X		
FAU_GEN.1/Iteration_2									X	X				X	X	X	X	X	X	X	X	X		
FAU_SAR.1/Iteration_1																		X	X	X	X	X		
FAU_SAR.1/Iteration_2																		X	X	X	X	X		
FAU_STG.1									X	X				X	X	X	X	X	X	X	X	X		
FAU_STG.4									X	X				X	X	X	X	X	X	X	X	X		
FCP_CMP.1										X														

[5] Cet objectif de sécurité pour la TOE est couvert par la sélection des composants d'assurance au chapitre 5.3.

FIA_ATD.1											X													
FIA_UAU.2/Iteration_1			X																					X
FIA_UAU.2/Iteration_2					X																			
FIA_UAU.2/Iteration_3				X																				
FIA_UAU.2/Iteration_4						X																		
FIA_UID.2/Iteration_1			X																					
FIA_UID.2/Iteration_2					X																			
FIA_UID.2/Iteration_3				X																				
FIA_UID.2/Iteration_4						X																		
FMT_MSA.1/Iteration_1			X							X														
FMT_MSA.1/Iteration_2					X																			
FMT_MSA.1/Iteration_3				X																				
FMT_MSA.1/Iteration_4						X																		
FMT_MSA.3/Iteration_1			X							X														
FMT_MSA.3/Iteration_2				X																				
FMT_MSA.3/Iteration_3						X																		
FMT_MTD.1/Iteration_1			X																					
FMT_MTD.1/Iteration_2					X																			
FMT_MTD.1/Iteration_3				X																				
FMT_MTD.1/Iteration_4						X																		
FMT_SMF.1/Iteration_1			X																					
FMT_SMF.1/Iteration_2					X																			
FMT_SMF.1/Iteration_3				X																				
FMT_SMF.1/Iteration_4						X																		
FMT_SMR.1			X	X	X	X																		
FPR_ANO.1											X													
FPT_ITC.1		X	X	X	X	X			X	X				X	X	X	X	X	X	X	X	X		
FPT_ITI.1		X	X	X	X	X			X	X				X	X	X	X	X	X	X	X	X		
FPT_ITT.1	X							X	X	X				X	X	X	X	X	X	X	X	X		
FPT_ITT.3	X							X	X	X				X	X	X	X	X	X	X	X	X		
FPT_PHP.2									X					X	X	X	X							
FPT_PHP.3/Iteration_1							X																	

FPT_PHP.3/Iteration_2								X																
FPT_RPL.1	X	X	X	X	X	X			X	X				X	X	X	X	X	X	X	X	X		
FPT_STM.1										X	X													
FCS_COP.1	X	X	X	X	X	X			X	X				X	X	X	X	X	X	X	X	X		X
FPT_EMSEC.1																							X	
FDP_ACC.2/Iteration_1			X																					
FDP_ACC.2/Iteration_2					X																			
FDP_ACC.2/Iteration_3				X																				
FDP_ACC.2/Iteration_4						X																		
FDP_ACF.1/Iteration_1			X																					
FDP_ACF.1/Iteration_2					X																			
FDP_ACF.1/Iteration_3				X																				
FDP_ACF.1/Iteration_4						X																		

Table 4 : Coverage of security objectives for the TOE by the security functional requirements for the TOE

8.2.2 Coverage of objectives for the TOE

Coverage justifications are not provided in the sanitized version of the Security Target in order to protect proprietary information. Complete coverage justification provided in [ST].

8.2.3 Satisfaction of dependencies

- **Satisfaction of dependencies for security functional requirements for the TOE**

Requirements	Dependencies	Effective dependencies	OK/NOK: reasons
Classe FAU : Security Audit			
FAU_GEN.1/Iteration_1	FPT_STM.1	FPT_STM.1	OK
FAU_GEN.1/Iteration_1	FPT_STM.1	FPT_STM.1	OK
FAU_STG.1	FAU_GEN.1	FAU_GEN.1/Iteration_1 FAU_GEN.1/Iteration_2	OK
FAU_STG.4	FAU_STG.1	FAU_STG.1	OK
FAU_SAR.1/Iteration_1	FAU_GEN.1	FAU_GEN.1/Iteration_1 FAU_GEN.1/Iteration_2	OK
FAU_SAR.1/Iteration_2	FAU_GEN.1	FAU_GEN.1/Iteration_1	OK
Classe FMT : Security Management			
FMT_MSA.1/Iteration_1	FDP_ACC.1	FDP_ACC.2/Iteration_1	OK
	FMT_SMR.1	FMT_SMR.1	OK
	FMT_SMF.1	FMT_SMF.1/Iteration_1	OK
FMT_MSA.1/Iteration_2	FDP_ACC.1	FDP_ACC.2/Iteration_2	OK
	FMT_SMR.1	FMT_SMR.1	OK
	FMT_SMF.1	FMT_SMF.1/Iteration_2	OK
FMT_MSA.1/Iteration_3	FDP_ACC.1	FDP_ACC.2/Iteration_3	OK
	FMT_SMR.1	FMT_SMR.1	OK
	FMT_SMF.1	FMT_SMF.1/Iteration_3	OK
FMT_MSA.1/Iteration_4	FDP_ACC.1	FDP_ACC.2/Iteration_4	OK
	FMT_SMR.1	FMT_SMR.1	OK
	FMT_SMF.1	FMT_SMF.1/Iteration_4	OK
FMT_MSA.3/Iteration_1	FMT_MSA.1	FMT_MSA.1/Iteration_1	OK
	FMT_SMR.1	FMT_SMR.1	OK
FMT_MSA.3/Iteration_2	FMT_MSA.1	FMT_MSA.1/Iteration_3	OK
	FMT_SMR.1	FMT_SMR.1	OK
FMT_MSA.3/Iteration_3	FMT_MSA.1	FMT_MSA.1/Iteration_4	OK
	FMT_SMR.1	FMT_SMR.1	OK
FMT_SMF.1/Iteration_1	None	None	OK
FMT_SMF.1/Iteration_2	None	None	OK
FMT_SMF.1/Iteration_3	None	None	OK
FMT_SMF.1/Iteration_4	None	None	OK
FMT_SMR.1	FIA_UID.1	FIA_UID.2/Iteration_1 FIA_UID.2/Iteration_2 FIA_UID.2/Iteration_3 FIA_UID.2/Iteration_4	OK

FMT_MTD.1/Iteration_1	FMT_SMR.1	FMT_SMR.1	OK
	FMT_SMF.1	FMT_SMF.1/Iteration_1	OK
FMT_MTD.1/Iteration_2	FMT_SMR.1	FMT_SMR.1	OK
	FMT_SMF.1	FMT_SMF.1/Iteration_2	OK
FMT_MTD.1/Iteration_3	FMT_SMR.1	FMT_SMR.1	OK
	FMT_SMF.1	FMT_SMF.1/Iteration_3	OK
FMT_MTD.1/Iteration_4	FMT_SMR.1	FMT_SMR.1	OK
	FMT_SMF.1	FMT_SMF.1/Iteration_4	OK
Classe FIA : Identification and authentication			
FIA_ATD.1	None	None	OK
FIA_UAU.2/Iteration_1	FIA_UID.1	FIA_UID.2/Iteration_1	OK
FIA_UAU.2/Iteration_2	FIA_UID.1	FIA_UID.2/Iteration_2	OK
FIA_UAU.2/Iteration_3	FIA_UID.1	FIA_UID.2/Iteration_3	OK
FIA_UAU.2/Iteration_4	FIA_UID.1	FIA_UID.2/Iteration_4	OK
FIA_UID.2/Iteration_1	None	None	OK
FIA_UID.2/Iteration_2	None	None	OK
FIA_UID.2/Iteration_3	None	None	OK
FIA_UID.2/Iteration_4	None	None	OK
Classe FPT : Protection of the TSF			
FPT_STM.1	None	None	OK
FPT_ITT.1	None	None	OK
FPT_ITT.3	FPT_ITT.1	FPT_ITT.1	OK
FPT_RPL.1	None	None	OK
FPT_PHP.2	FMT_MOF.1	None	NOK. Reason for non-satisfaction below
FPT_PHP.3/Iteration_1	None	None	OK
FPT_PHP.3/Iteration_2	None	None	OK
FPT_ITC.1	None	None	OK
FPT_ITI.1	None	None	OK
FPT_EMSEC	None	None	OK
Classe FCS : Cryptographic support			
FCS_COP.1	FDP_ITC.1, ou FDP_ITC.2, ou FCS_CKM.1	None	NOK. Reason for non-satisfaction below
	FCS_CKM.4	None	NOK. Reason for non-satisfaction below
Classe FPR : Privacy			
FPR_ANO.1	None	None	OK
Classe FCP : Curfew Policy			
FCP_CMP.1	FMT_MSA.3	FMT_MSA.3/Iteration_1	OK
Classe FDP : User data protection			
FDP_ACC.2/Iteration_1	FDP_ACF.1	FDP_ACF.1/Iteration_1	OK
FDP_ACC.2/Iteration_2	FDP_ACF.1	FDP_ACF.1/Iteration_2	OK
FDP_ACC.2/Iteration_3	FDP_ACF.1	FDP_ACF.1/Iteration_3	OK

FDP_ACC.2/Iteration_4	FDP_ACF.1	FDP_ACF.1/Iteration_4	OK
FDP_ACF.1/Iteration_1	FDP_ACC.1	FDP_ACC.2/Iteration_1	
	FMT_MSA.3	FMT_MSA.3/Iteration_1	
FDP_ACF.1/Iteration_2	FDP_ACC.1	FDP_ACC.2/Iteration_2	
	FMT_MSA.3	None	NOK. Reason for non-satisfaction below
FDP_ACF.1/Iteration_3	FDP_ACC.1	FDP_ACC.2/Iteration_3	OK
	FMT_MSA.3	FMT_MSA.3/Iteration_2	OK
FDP_ACF.1/Iteration_4	FDP_ACC.1	FDP_ACC.2/Iteration_4	OK
	FMT_MSA.3	FMT_MSA.3/Iteration_3	OK

Table 5 : Satisfaction of dependencies for security functional requirements for the TOE

- **Reasons for non-satisfaction of security functional requirements for the TOE**

Non satisfaction of dependency of FPT_PHP.2 with respect to FMT_MOF.1 :

As shown in the justification for the dependency of FPT_PHP.2 in relation to FMT_MOF.1 in Part 2 of the Common Criteria [CC], FMT_MOF.1 is required for the two following functions:

- management of roles that receive the events generated following detection of a physical attack.
- management of the list of TOE elements that must inform the role(s) in question in the event of detection of a physical attack.

However these two functions are not configurable in the TOE. Indeed this is a behaviour which cannot be configured by the TOE.

Non satisfaction of dependency of FCS_COP.1 with respect to FDP_ITC.1, FDP_ITC.2, FCS_CKM.1:

The TOE's cryptographic keys are a sensitive property item of the TOE (B.CLE_CRYPTOGRAPHIQUES) to be protected, particularly in terms of confidentiality. They are not generated by the TOE but by an FIPS-140 certified pseudo-random generator that is part of the TOE environment, which justifies the non-satisfaction of dependency with respect to FCS_CKM.1. Non satisfaction of dependency with respect to FDP_ITC.1 and especially FDP_ITC.2 is justified because the TOE does not have a secure cryptographic key injection interface.

Non satisfaction of dependency of FCS_COP.1 vis-à-vis de FCS_CKM.4:

The TOE's cryptographic keys are used throughout the life of the TOE to ensure confidentiality and authenticity of the messages exchanged between the TOE elements or between the TOE and the remote monitoring centre application. These keys cannot be changed.

8.3 Reasons for TOE security functions

	Security functions

Security Functional Requirements for the TOE	F.ADMINISTRATION_CENTRALE	F.SUPERVISON_LOCALE	F.ADMINISTRATION_LOCALE	F.PROTECTION_COM_INTER_TOE	F.INITIALISATION	F.PROTECTION_COM_INTRA_TOE	F.ROLES	F.RESPECT_POLITIQUE_ASSIGNATION	F.TEMPS_FIABLE	F.AUDIT	F.DETECTION_PERTE_INTEGRITE	F.PROTECTION_IDENTITE_PLACE
FAU_GEN.1/Iteration_1										X		
FAU_GEN.1/Iteration_2										X		
FAU_STG.1										X		
FAU_STG.4										X		
FAU_SAR.1/Iteration_1										X		
FAU_SAR.1/Iteration_2										X		
FCP_CMP.1								X				
FIA_ATD.1												X
FIA_UAU.2/Iteration_1	X											
FIA_UAU.2/Iteration_2		X										
FIA_UAU.2/Iteration_3			X									
FIA_UAU.2/Iteration_4					X							
FIA_UID.2/Iteration_1	X											
FIA_UID.2/Iteration_2		X										
FIA_UID.2/Iteration_3			X									
FIA_UID.2/Iteration_4				X								
FMT_MSA.1/Iteration_1	X				X							
FMT_MSA.1/Iteration_2		X										
FMT_MSA.1/Iteration_3			X									
FMT_MSA.1/Iteration_4					X							
FMT_MSA.3/Iteration_1	X											
FMT_MSA.3/Iteration_2			X									
FMT_MSA.3/Iteration_3					X							
FMT_MTD.1/Iteration_1	X				X							
FMT_MTD.1/Iteration_2		X										
FMT_MTD.1/Iteration_3			X									
FMT_MTD.1/Iteration_4					X							
FMT_SMF.1/Iteration_1	X											
FMT_SMF.1/Iteration_2		X										
FMT_SMF.1/Iteration_3			X									
FMT_SMF.1/Iteration_4					X							
FMT_SMR.1	X	X	X		X		X					
FPR_ANO.1												X
FPT_ITC.1				X								

FPT_ITI.1				X								
FPT_ITT.1						X						
FPT_ITT.3						X						
FPT_PHP.2											X	
FPT_PHP.3/Iteration_1											X	
FPT_PHP.3/Iteration_2											X	
FPT_RPL.1				X		X						
FPT_STM.1									X			
FPT_EMSEC				X		X						
FCS_COP.1				X		X						
FDP_ACC.2/Iteration_1	X											
FDP_ACC.2/Iteration_2		X										
FDP_ACC.2/Iteration_3			X									
FDP_ACC.2/Iteration_4					X							
FD_ACF.1/Iteration_1	X											
FD_ACF.1/Iteration_2		X										
FD_ACF.1/Iteration_3			X									
FD_ACF.1/Iteration_4					X							

Table 6 : Coverage of the TOE security functions by the security functional requirements for the TOE

9 Appendices

9.1 Annex 1: Local supervision and local administration

Annex 1 is not provided in the sanitized version of the Security Target in order to protect proprietary information.