ELECTRONIC TAGGING (PSE), MOBILE ELECTRONIC TAGGING (PSEM) DEVICES AND VICTIM PROTECTION DEPAR

Security Target [LITE]
Common Criteria Assurance level EAL2+
Qualification Standard

ST LITE Version 3.0 of January 14th 2014

G4S MONITORING TECHNOLOGIES
1 Tiber Way
Meridian Business Park
Leicester LE19 1QP
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
[FEROS]	Review of the PSE and PSEM security needs, version 1.03 of 29 June 2007.
[FSP]	ADV_FSP.2 Functional Specification, for PSE PSEM, Ref. ADV_FSP.2

Glossary

Glossary compiled from the Common Criteria [CC]:

Term	Definition
CC	Common Criteria [CC]
OSP	Organisational Security Policy: Security policy of the system in which the Target of Evaluation (TOE) is operated.
SOF	Strength Of Function: Level of inherent strength of a function faced with "brute force" type attacks. This level is not to be confused with the overall strength level of the TOE (level as defined by the AVA_VLA component) which takes into account attacks that alter or bypass TOE functions.
ST	Security Target: this document
TOE	Target Of Evaluation: this is the product or system for which this Security Target constitutes the evaluation specifications.
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
DEPAR	Dispositif Electronique de Protection Anti Rapprochement
FEROS	Fiche d’Expression Rationnelle des Risques et Objectifs de Sécurité (Rational formulation of security risks and objectives datasheet)
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 (Switched Telephone Network)
VTU	Victim Tracker Unit

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

1.1 Document identification

Title	Security Target Lite Common Criteria: Electronic tagging (PSE) and Mobile electronic tagging (PSEM) devices and Victim Protection (DEPAR)
Version	3.0
Author(s)	Onali Ismail [G4S MTL]
Product	PSE/PSEM/DEPAR
Product version	10
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 qualification standard.

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

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 lite 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 Security Target is compliant Common Criteria Part 2 extended - 3.1 Revision 3 [CC] to include the security functional requirements FCP_CMP.1, FPT_EMSEC.1. This Security Target is also compliant with Part 3 of the 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

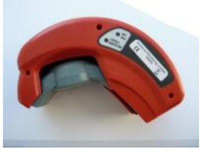
- **The electronic bracelet** (TOE): is crimped by an agent from the prison administration to the subject's ankle. The electronic bracelet cannot be removed without damage, and any damage results in an alarm being fed back to the remote monitoring centre application. Kevlar strips are included in the electronic bracelet in order to prevent removal of the bracelet through stretching. In addition optical fibres run through the bracelet so that any physical deterioration (cutting etc.) to the electronic bracelet can be detected. The bracelet's electrical battery is non-rechargeable. Under normal operation it will last 24 months and in sleep mode 5 years. The electronic bracelet is waterproof and can work under water to a depth of 5 metres but cannot send and receive messages if the depth exceeds 0.5 meters.
- **The monitoring unit** (TOE)**:** can be fixed (when PSE), mobile (when PSEM) or DEPAR VTU (when DEPAR)[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 and DEPAR the monitoring unit has a GPS receiver which enables it to determine his/her geographical location.
- **The home station [PSEM]** (TOE) is used in PSEM mode only[2]. The home station [PSEM] simply provides further range for the detection of the electronic bracelet than the monitoring unit [mobile]. The home station also registers the monitoring unit [mobile] as being home.
- **The key fob** (TOE) is used by a Prison Officer only during the initialisation phase which enables an electronic bracelet to be associated with a monitoring unit. The key fob is kept by the prison administration and is used to send signals to the installation tool and to the monitoring unit to be initialised indicating that the initialisation phase can be completed. Initialisation of an electronic bracelet 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 only during the initialisation phase when an electronic bracelet can be associated with a monitoring unit. It is used to send signals to the bracelet to be initialised making it switch from "non-initialised" to "initialised" status.
- **The diagnostic tool** (TOE) is used by an officer of the prison administration in the initialisation phase or exploitation. It allows you to perform various operations on the elements of the TOE (serial number, battery status, software version, …), perform configuration operations on certain elements of the TOE (configuration of RTC, GSM, …).
- **The home station [DEPAR]** (TOE) is used in DEPAR only. The home station DEPAR is identical to the home station [PSEM]. The home station [DEPAR] simply provides further range for the detection of the electronic bracelet than the DEPAR VTU. The home station VTU can detect

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

[2] The term "home station" can refer interchangeably to the mobile or DEPAR home station. When the adjective “PSEM” or “DEPAR" is not specified.

the subject and alerts the victim via the DEPAR VTU. The home station [DEPAR] also registers the DEPAR VTU as being home.

- **The DEPAR VTU** (TOE) is used in DEPAR only. The DEPAR VTU is identical to the monitoring unit [mobile]. The victim can for instance wear the DEPAR VTU on his/her belt. The DEPAR VTU can detect a nearby subject when not at home. When at home either DEPAR VTU or home station VTU can detect a nearby subject.
- **The remote monitoring centre** (outside TOE) is an information system hosting "the remote monitoring centre application" (see definition below).
- **The remote monitoring centre application** (outside TOE) is an application hosted at the remote monitoring centre which enables the TOE to be administered remotely.

 Figure 1: Electronic Bracelet	 **Figure 2: Fixed monitoring unit**	 **Figure 3: Mobile monitoring unit**
 Figure 4: Home Station [PSEM]	 **Figure 5: Fitting and Installation Tool**	 **Figure 6: Key Fob**
 Figure 7: Diagnostic Tool	 **Figure 8: Home Station [DEPAR]**	 **Figure 9: DEPAR VTU**

2.1.2 Description of flows

The flows implemented by the TOE, according to the mode of use (PSE, PSEM or DEPAR) are represented in figures 10 (PSE), 11 (PSEM) and 12 (DEPAR).

Note: For reasons of legibility figures 10 (PSE), 11 (PSEM) and 12 (DEPAR) below may represent multiple flows of the same type, e.g., multiple RF. In reality, each element of the TOE never has more than one flow type of the same transport medium [e.g., RF, IR etc.,].

- **Flow in PSE mode**

[Figure 10 only available in [ST] in order to protect proprietary information]

Figure 10: Interfaces and flows implemented by the TOE in PSE mode

- **Flow in PSEM mode**

[Figure 11 only available in [ST] in order to protect proprietary information]

Figure 11: Interfaces and flows implemented by the TOE in PSEM mode

- **Flow in DEPAR mode**

[Figure 12 only available in [ST] in order to protect proprietary information]

Figure 12: Interfaces and flows implemented by the TOE in DEPAR mode

2.1.3 Description of phases

The life cycle of the TOE has three phases: one initialisation phase, one operational phase and one refurbish phase. It is imperative that the initialisation phase is completed before the operational phase. At the end of the operating cycle, the components of the TOE are refurbished or disposed.

2.1.4 Initialisation Phase

<Only available in the full ST>

[Figure 14 only available in [ST] in order to protect proprietary information]

Figure 13: TOE in initialisation phase for PSE/PSEM

[Figure 15 only available in [ST] in order to protect proprietary information]

Figure 14: TOE in initialisation phase for DEPAR

- **OPERATIONAL PHASE**

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

- **IN-FIELD UPGRADE**

<Only available in the full ST>

[Figure 16 only available in [ST] in order to protect proprietary information]

Table 15 : Dataflow transmitting in-field upgrade of Firmware

- **Refurbishment**

<Only available in the full ST>

- **Disposal**

Disposal elements of the TOE are within the scope of the evaluation. All devices are securely disposed of using a certified secure disposal service.

2.1.5 Description of modes of use

- **PSE Operational Mode**

<Only available in the full ST>

[Figure 17 only available in [ST] in order to protect proprietary information]

Figure 16: TOE in operational phase, PSE mode of use

- **PSEM Operational Mode**

<Only available in the full ST>

[Figure 18 only available in [ST] in order to protect proprietary information]

Figure 17: TOE in operational phase, PSEM mode of use

- **DEPAR Operational Mode**

<Only available in the full ST>

[Figure 19 only available in [ST] in order to protect proprietary information]

Figure 18: TOE in operational phase, DEPAR mode of use

2.2 Scope of the evaluation

Evaluation is limited to the following equipment:

- The electronic bracelet
- The monitoring unit [fixed]
- The monitoring unit [mobile]
- The home station [PSEM]
- The key fob
- The fitting and installation tool
- The diagnostic tool
- The home station [DEPAR]
- The DEPAR VTU

The TOE security functions are implemented by hardware and software.

The following are excluded from its scope:

- The remote monitoring centre, its applications and the information system that hosts it (monitoring application)
- The communication networks GSM, RTC that provide communication between the TOE and the remote monitoring centre.
- The GPS geo-location signals sent by the GPS satellites and received by the mobile monitoring unit (PSEM/DEPAR).
- The geo-location information of mobile LBS monitoring (PSEM/DEPAR)

2.3 TOE physical interfaces

The TOE external physical interfaces illustrated in Figure 10 are:

- For the electronic bracelet:
  - The radio frequency interface
- For the monitoring unit [fixed]:
  - The infrared interface
  - The radio frequency interface
  - The RTC interface
- For the monitoring unit [mobile]:
  - The infrared interface
  - The radio frequency interface
  - The GSM interface
  - The GPS interface
- For the home station [PSEM]
  - The infrared interface
  - The RF interface
- For the key fob
  - The radio frequency interface
  - The infrared interface
- For the fitting and installation tool (FIT)
  - The infrared interface
  - The radio frequency interface
- For the home station [DEPAR]
  - The radio frequency interface
- For the DEPAR VTU
  - The radio frequency interface

  - The GSM interface
  - The GPS 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 bracelet. He/she must be able to have access to certain events generated by the TOE.

Victim

The victim is the person who is being protected from the subject. The subject must comply to the curfew scheme and wears an electronic bracelet. 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 a right to read/write with respect to the TOE security configuration and a "central supervisor" role at the remote monitoring centre which would only have a right to read in relation to 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. Possible management of the "central administrator" or "central supervisor" roles must be done by the "remote monitoring centre application".

Officer of the Prison Administration

The officer of the prison administration is responsible for setting the electronic bracelet on the wrist or ankle of the person placed. He is in charge of the installation of the monitoring unit in the location (s) of person placed. The prison officer uses the installation tool during the initialization phase of the TOE and has the keyfob. The prison officer also uses the diagnostic tool.

Local Supervisor

The local supervisor is a person of the prison, who has a keyfob and uses the diagnostic tool to perform certain supervisory operations (read some parameters) elements of the TOE locally.

Local Administrator

The local administrator is a person of the prison, who has a keyfob, and uses the diagnostic tool to perform certain administrative operations (reading and writing of certain parameters) elements of the TOE 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, PSEM or DEPAR) then this is stated explicitly in a note. In the absence of a note, the service is offered by the TOE in all TOE modes of use (PSE, PSEM or DEPAR).

2.5.1 Initialisation service

<Only available in the full ST>

The initialisation service is provided by the following TOE elements:

☑ Electronic Bracelet ☑ Monitoring unit ☑ Home Station

☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic 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 bracelet, the monitoring unit and the home station.

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 bracelet:
<Only available in the full ST>

For the monitoring unit [fixed]:
<Only available in the full ST>

For the monitoring unit [mobile] and DEPAR VTU:
<Only available in the full ST>

For the home station:
<Only available in the full ST>

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

☑ Electronic Bracelet ☑ Monitoring unit ☑ Home Station

☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

2.5.3 Subject geo-location service

<Only available in the full ST>

The subject geo-location service is provided only in PSEM or DEPAR mode by the following TOE elements:

☑ Electronic Bracelet ☑ Monitoring unit ☑ Home Station

☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

2.5.4 Service for verification of compliance with curfew scheme

This service is provided by the electronic bracelet and the monitoring unit whatever the TOE mode of use (PSE, PSEM or DEPAR). 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:

- Geo-location of the subject (PSE, PSEM or DEPAR)
- 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 Bracelet ☑ Monitoring unit ☑ Home Station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

2.5.5 Provision of a reliable time source

This service is provided by the monitoring unit [fixed or mobile] or DEPAR VTU whatever the TOE mode of use (PSE, PSEM or DEPAR). 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 or DEPAR mode, the monitoring mobile unit or DEPAR VTU synchronises itself using GPS signals.

The provision of a reliable time source is provided by the following TOE elements:
☐ Electronic Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

2.5.6 Event generation service

This service is provided by either the TOE elements that are handed to the subject or to the victim i.e. the electronic bracelet, the home station whatever the TOE mode of use (PSE, PSEM or DEPAR).
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 bracelet, home station etc) before forwarding them to the monitoring centre application.

The TOE associates each event it creates with a level of priority which can be "high", "medium" or "low." Within ADV_FSP details the type of events which can be generated by the TOE associated priority level. In general, the events of priority "high" mean non-compliance with the policy set to the assignment it is submitted.
If communication between the TOE and monitoring application via communication networks GSM [PSEM, DEPAR) or PSTN (PSE mode only) is possible, the events of priority "high" are immediately transmitted by the TOE to the monitoring application. If communications are lost, the TOE stores

events temporarily until communication between the TOE and the monitoring application is established.
Events priority level "medium" or "low" are regularly transmitted by the TOE to the monitoring application.
As well as all communications between the TOE and the remote monitoring center, sending events to the monitoring application is always initiated by the TOE. No communication between the TOE and monitoring application is initiated by the monitoring application. Service communication between the TOE and the monitoring application is described in section 2.5.9.

The event generation and sending service is provided by the following TOE elements:
☐ Electronic Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

2.5.7 Administration service central

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 Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

2.5.8 Service and local supervision of local administrators

This service allows certain elements of the TOE to be supervised and administered locally. These services and local supervision of local administration can read (local supervision) or write (local administration) configuration elements of the TOE. Local supervision and the local administration of the TOE are performed, respectively, by a local supervisor and a local administrator using the diagnostic tool that communicates either directly with the element of the TOE to administer (unit Surveillance, home station, tool assembly and installation), or indirectly via the tool assembly and installation (electronic bracelet, key chain). Annex 1 to Chapter 9.1 presents, for each profile (local supervisor or local administrator), operations and achievable (s) element (s) relevant for the TOE.
Service and local overview of local administration is provided by the TOE following elements:

☑ Electronic Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic 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 communication between the TOE and the monitoring application is initiated by the monitoring application. Communication between the TOE and monitoring application enables the TOE to receive updates for its security attributes (curfew scheme, reference time etc.) and send the events it has generated.

The firmware found in the Monitoring Units, Keyfob, Electronic Bracelet and Home Station can be upgraded and deployed over the air via in-field upgrade via Leicester only. To achieve this, firmware for the Monitoring Units, Keyfob, Electronic Bracelet and Home Station is securely distributed to in-field Monitoring Units by the Monitoring Application, using flows 15a,b,c and 16 in the TOE.

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

☐ Electronic Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

2.6 Evaluation platform

The TOE must be evaluated:

- In both phases - initialisation and operation
- In all modes of use: PSE,PSEM and DEPAR.

The evaluation platform architectures are as represented in:

- Figure 14: TOE in initialisation phase for PSE/PSEM
- Figure 15: TOE in initialisation phase for DEPAR
- Figure 17: TOE in operational phase, PSE mode of use
- Figure 18: TOE in operational phase, PSEM mode of use
- Figure 19: TOE in operational phase, DEPAR mode of use

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 bracelet
S.US. when they concern the monitoring unit [PSE, PSEM]S.USV. when they concern the DEPAR VTU
S.SA. when they concern the home 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 bracelet**

S.BR.SERVICES
Sensitive services provided by the electronic bracelet
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 home station**

S.SA.SERVICES

Sensitive services provided by the home 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 diagnostic tool**

S.OD.SERVICES
Sensitive services offered 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 bracelet
B.US.	when they concern the monitoring unit [PSE, PSEM]
B.USV	when they concern the DEPAR VTU
B.SA.	when they concern the home 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, PSEM or DEPAR), this is stated explicitly in a note. Where this is not specified the sensitive property item exists in all modes of use of the TOE i.e. PSE, PSEM or DEPAR

- **Cryptographic Keys**

B.CLES_CRYPTOGRAPHIQUES

<Only available in the full ST version>

Protection: confidentiality.

- **Identification Data**

B.DONNEES_IDENTIFICATION
The identification data enable unique identification of each element of the TOE. The identification data correspond to a serial number generated and integrated by the TOE manufacturer. These identification data cannot be modified and are stored in the TOE.
Protection: availability, integrity.

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

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

- **Sensitive property items of the monitoring unit [PSE, PSEM and DEPAR]**

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 bracelet as well as the events sent by the home station
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 home station

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

The victim [DEPAR] is assumed non-volatile or non-hostile and harmless to the TOE.

If a hypothesis does not apply to the whole TOE but only to one of its elements (electronic bracelet, monitoring unit, home station, key fob, fitting and installation tool, diagnostic 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, PSEM or DEPAR) then this is stated explicitly in a note. Unless specified otherwise the hypothesis applies to all TOE modes of use i.e. PSE,PSEM or DEPAR.

3.2.1 Hypotheses relating to the cryptographic key generator

H.GENERATION_CLES_CRYPTOGRAPHIQUES
<Only available in the full ST version>

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 must have a reliable time source. Under PSE mode time source is used to synchronise the TOE's reference times with that of the monitoring application via the communications networks (GSM/RTC). Under PSEM or DEPAR, the TOE's reference times are synchronised with GPS Satellites.

Note: In mode PSE, 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 monitoring unit [fixed]. In mode PSEM or DEPAR, the only element of the TOE that synchronizes its time reference signals via GPS is the monitoring unit [mobile].

H.CT.COM.INTER_TOE_PROTECTION

The remote monitoring centre application must protect the confidentiality and authenticity of the data 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_DONNEES_DEVELOPPEUR

The monitoring application protects the confidentiality of cryptographic keys used by the monitoring application to ensure the confidentiality and authenticity of communications with the TOE. This includes the protection of delivered firmware upgrade during over the air in-field firmware upgrade.

Note: The only part of the TOE communicates directly with the monitoring 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 bracelet. This hypothesis only applies therefore to the electronic bracelet.

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

The prison administration erases securely cryptographic keys contained in the TOE diagnostic tool when disposing of it.

3.2.4 Hypothesis relating to the 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 or DEPAR 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, PSEM or DEPAR) then this is stated explicitly in a note. Unless otherwise specified the threat applies to all modes of use of the TOE i.e. PSE,PSEM or DEPAR.

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

3.3.3 Threats not taken into account

Threats not taken into account are:

- In PSEM or DEPAR mode the threat involving amending the data sent to the mobile monitoring unit by the satellites via GPS signals is not taken into account.
- In PSE, PSEM or DEPAR modes, the threat consisting in using relays or amplifiers between the electronic bracelet and the monitoring unit in order to increase the maximum permissible distance between the bracelet and the monitoring unit is not taken into account.

3.3.4 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 bracelet (S.BR.SERVICES).

Note: This threat only affects the electronic bracelet 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 capable of altering normal operation, disclose or modify the data it stores or handles.

Threatened properties: integrity and availability of all services offered by the TOE sensitive. Availability, integrity, authenticity of all sensitive items contained in the TOE.

M.ELT.PIEGEAGE_MATERIEL_LIVRAISON

An attacker with physical access to the TOE during its 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 attacker firmware capable of altering normal operation, disclose or modify the data it stores or handles.

Threatened properties: integrity and availability of all services offered by the TOE sensitive. Availability, integrity, authenticity of all sensitive items contained in the TOE.

M.ELT.PIEGEAGE_LOGICIEL_LIVRAISON

An attacker with physical access to the TOE or its delivery to the prison administration 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.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 performs non-invasive attacks by auxiliary channels to access cryptographic keys stored in elements of the TOE.

Threatened properties: integrity and availability of all services offered by the TOE sensitive. Availability, integrity, confidentiality, authenticity of all sensitive items contained in the TOE.

3.3.5 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 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 In-Field Upgrade

P.FIELD.UPGRADE

Parts of the TOE [Electronic Bracelet, Home Station, Monitoring Units, KeyFob] firmware can be upgraded over the air using in-field upgrade. This must be upgraded securely.

3.4.3 Standard Qualification [3]

P.ANSSI.QUALIFICATION_STANDARD

The TOE is assessed on the basis of the Common Criteria [CC] for an EAL2 assurance level supplemented by the ALC_FLR.3, ALC_DVS.1 and AVA_VAN.3.

3.4.4 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.

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 bracelet 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.

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: The security objectives 1, 2 and 3 apply only P.INTEGRITE_PHYSIQUE_LOGIQUE electronic bracelet.

P.INSTALLATION_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.

Security Objective No° 9a [DEPAR]: The victim shall be correctly trained on the DEPAR equipment and installation and check the equipment is correctly configured and tested after installation.

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 geo-location 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 geo-location.

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.

P.RESPECT_POLITIQUE_ASSIGNATION

In order to determine whether the person placed respects the assignment policy to which it is subjected, the TOE generates and sends an event to the monitoring application in the event of breach of their policy assignment.

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,PSEM or DEPAR), this is stated explicitly in a note. Unless otherwise specified the security objective must apply to all 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 Secure In-Field Upgrade of Firmware

OT.FIELD.UPGRADE

Parts of the TOE [Electronic Bracelet, Home Station, Monitoring Units, KeyFob] firmware can be upgraded over the air using in-field upgrade. This must be upgraded securely.

4.1.3 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.

4.1.4 Administration central

OT.ADMINISTRATION CENTRALE

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.

4.1.5 Local Administration

OT.ADMINISTRATION_LOCALE

The TOE must allow local administrators equipped with a keyfob, an installation tool and / or a diagnostic tool to read and modify some configuration parameters of some elements of the TOE.

4.1.6 Supervision local

OT.SUPERVISION_LOCALE

The TOE must allow local supervisors equipped with a keyfob, an installation tool and / or a diagnostic tool to read and only read certain configuration of some elements the TOE.

4.1.7 Initialization

OT.INITIALISATION

The TOE must allow prison officials equipped with a keyfob, an installation tool to initialize the electronic bracelet.

4.1.8 Physical resistance

OT.RESISTANCE_TEMPERATURES

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

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

OT.RESISTANCE_EAU

The TOE must be waterproof and work function under water to a maximum depth of 0.5 metres.

Note: This security objective for the TOE applies only to electronic bracelet. The electronic bracelet is waterproof to a depth of 5 meters. Beyond 0.5 meters, the messages sent or received by the electronic bracelet are too attenuated.

4.1.9 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.

4.1.10 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 noncompliance with this curfew scheme.

OT.TEMPS_REFERENCE_FIABLE

The TOE must have a reliable reference time.

4.1.11 Protection of subject's identity

OT.PROTECTION_IDENTITE_PLACE

The TOE must protect the subject/victim identity. It must not be possible to determine the subject's identity through listening to data exchanged between the components of the TOE 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.

4.1.12 Detection of abnormal events

OT.DETECTION_COUPURE_BRACELET

The TOE must be able to detect when the electronic bracelet 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 bracelet 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 the charge level of batteries (rechargeable or non-rechargeable) of its elements [PSEM mobile monitoring unit, DEPAR VTU]warn the subject when the battery level of one of the elements of the TOE has reached a critical level and give a clear indication to the subject/victim of the remaining operating time. The TOE [in mode PSEM or DEPAR] must inform the subject/victim via a clear message when the TOE is currently being recharged.

Note: The mobile monitoring unit (PSEM or DEPAR mode of use) has a rechargeable battery. The electronic bracelet 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 bracelet, 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.

4.1.13 Protection of information handled

OT.PROTECTION_CANAUX_AUXILIAIRES

The TOE shall not be allowed access to cryptographic keys contained in the elements of the TOE auxiliary channels.

4.1.14 Standard qualification

OT.QUALIFICATION_STANDARD

The evaluation level of the TOE must be EAL2 supplemented by the ALC_FLR.3, ALC_DVS.1 and AVA_VAN.3. 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 (RMC) or the remote monitoring centre application
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 (TH)

4.2.1 Security objectives cryptographic key generator

OE.GENERATION_CLES_CRYPTOGRAPHIQUES

<Only available in the full ST version>

4.2.2 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 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.

OE.CT.DETECTION_PERTE_COMMUNICATION

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

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

4.2.3 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 bracelet.

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 and victim 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

The prison administration must delete securely, cryptographic keys contained in the TOE diagnostic tool when disposing of it.

OE.AP.DOCUMENTATION_USER

The Prison Administration must provide documentation to the subject and victim 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.

4.2.4 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.

4.2.5 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	Subset access control
Class FIA: Identification and authentication		
	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 transfer 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 security are extracted from part 2 of the Common Criteria [CC] except FCP_CMP.1 and FPT_EMSEC.1.
The class FCP was specially created as part of this assessment and does not belong to Part 2 of the Common Criteria [CC]. Class FCP (Curfew Policy) relates to compliance with the assignment policy. FCP class contains only one family, FCP_CMP (Curfew Policy Compliance), which defines the rules for determining whether or not the set meets the assignment policy to which it is subjected.

5.1.2 Detailed functional requirements for the TOE

Protection of Axillary Channels

FPT_EMSEC.1 TOE Emanation

FPT_EMSEC.1.1 The TSF shall not emit [assignment : canaux auxiliaires] enabling access to [assignment : les clés cryptographiques continues dans les éléments de la TOE].

Dependencies: No dependencies.

Refinement: This security functional requirement applies to the following TOE elements:
☑ Electronic Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic 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 Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

- **Generation of events**

FAU_GEN.1 Audit data generation

Dependencies: FPT_STM.1

Iteration 1: Monitoring unit

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) All auditable events for [selection, choose one of: minimum] level of audit; and
b) [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 Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

Iteration 2: Home station

Dependencies: FPT_STM.1

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) All auditable events for [selection, choose one of: minimum] level of audit; and
b) [assignment: the events described in the [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 Bracelet ☐ Monitoring unit ☑ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic 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 Bracelet ☑ Monitoring unit ☑ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic 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 Bracelet ☑ Monitoring unit ☑ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

FAU_SAR.1 Audit review

Iteration 1: Administration centrale

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

FAU_SAR.1.1 The TSF shall provide [assignment: monitoring 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 Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

Iteration 1: Curfew Scheme

Dependencies: FAU_GEN.1/Iteration_1

FAU_SAR.1.1 The TSF shall provide [assignment: subject place/victims place] with the capability to read [assignment: batterie de l'unité mobile de surveillance déchargée] 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 Bracelet ☑ Monitoring unit ☑ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

Note: This requirement only applies to the Monitoring Unit [mobile]. The events which the subject can have access to in read mode are communicated to him via the monitoring unit [mobile] screen.

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

FMT_SMF.1 Specification of management functions

Dependencies: No dependencies.

Iteration 1: Central Administration

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
  - Firmware in-field upgrade (this is a security management function)].

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

☐ Electronic Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

Iteration 2: Supervision locale

Dependencies: No dependencies

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

- Supervision local electronic bracelet:
  - Read the battery level
  - Reading the serial number
  - Read the version number of the software
  - Read status
- Supervision local keyfob:
  - Read the battery level
  - Reading the serial number
  - Read the version number of the software
  - Read status
- Supervision of the local monitoring unit:
  - Reading the serial number
  - Read the version number of the software
  - Read the battery level
- Supervision local installation tool:
  - Reading the serial number,
  - Read the version number of the software
  - Read the battery level].

Raffinement : Cette exigence fonctionnelle de sécurité s'applique aux éléments de la TOE suivants :
☑ Electronic Bracelet ☑ Monitoring Unit ☑ Home Station
☑ Keyfob ☑ Installation Tool ☑ Diagnostic 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, PSEM or DEPAR):
  - Reading and editing configuration data GSM:

- IP address
- APN
- Name
- Password, port
- Local Administration of the monitoring unit (PSE, PSEM or DEPAR):
    - Reading and editing configuration data RTC:
        - phone number "data"
        - phone "voice"
        - emergency number

Raffinement : Cette exigence fonctionnelle de sécurité s’applique aux éléments de la TOE suivants :
☐ Electronic Bracelet ☑ Monitoring Unit ☐ Home Station
☐ Keyfob ☑ Diagnostic Tool ☐ 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 status of the electronic bracelet
  - Stop/Start the Home Station
  - Subject place of initialisation
  - Victim place of initialisation

Refinement: This security functional requirement applies to the following TOE elements:
☑ Electronic Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic Tool

FMT_MTD.1 Management of TSF data

Dependencies: FMT_SMR.1, FMT_SMF.1/Iteration_1

Iteration 1: Central Administration

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
- Firmware in-field upgrade (this is a security management function)]

to [assignment: remote monitoring centre application].

Refinement: This security functional requirement applies to the following TOE elements:
☐ Electronic Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

Itération 2: Supervision locale

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 bracelet:
  - Read the battery level
  - Reading the serial number
  - Read the version number of the software
  - Read status
- The keyfob parameters:

  - Read the battery level
  - Reading the serial number
  - Read the version number of the software
  - Read status
- The parameters of the monitoring unit or DEPAR VTU:
  - Reading the serial number
  - Read the version number of the software
  - Read the battery level
- The parameters of the tool assembly and installation:
  - Reading the serial number
  - Read the version number of the software
  - Read the battery level

to [assignment: the local supervisor].

Refinement: This security functional requirement applies to the following TOE elements:
☑ Electronic Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic Tool

Iteration 3: Administration locale

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 parameters of the RTC fixed monitoring unit (PSE):
  - phone number "data"
  - phone "voice"
  - emergency number
- The parameters of the GSM unit (PSE, PSEM or DEPAR):
  - IP address
  - APN
  - ID
  - password
  - Port.]

to [assignment: Local Administrator].

Refinement: This security functional requirement applies to the following TOE elements:
☐ Electronic Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☑ Diagnostic Tool

Itération 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] the [assignment: change status of the electronic bracelet] to [assignment: agent de l'administration pénitentiaire].

- **Authentication of TOE remote central administration, local administration, local supervisor**

FMT_SMR.1 Security roles

Dependencies: FIA_UID.1

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

- remote monitoring centre application,
- subject
- local supervisor
- local administrator
- Prison officer
- Victim].

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 Bracelet
☑ Key fob
☑ Monitoring unit
☑ Fitting and installation tool
☑ Home station
☑ Diagnostic Tool

FIA_UID.2 User identification before any action

Itération 1: Administration central

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 Bracelet
☐ Key fob
☑ Monitoring unit
☐ Fitting and installation tool
☐ Home station
☐ Diagnostic Tool

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

Itération 2: Supervision locale

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 Bracelet
☑ Monitoring unit
☑ Home station

☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic Tool

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

Itération 3: Administration locale

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 Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☑ Diagnostic Tool

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

Itération 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 Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic Tool

Note: The term "user" in this security functional requirement refers to the role of "Prison Officer."

FIA_UAU.2 User authentication before any action

Itération 1: Administration central

Dependencies: FIA_UID.1/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 Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

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

Itération 2: Supervision locale

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 Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic Tool

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

Itération 3: Administration locale

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 Bracelet ☑ Monitoring unit ☐ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic Tool

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

Itération 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 Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic Tool

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

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

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 Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic 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 Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic Tool

FPT_RPL.1 Replay detection

Dependencies: No dependencies.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [assignment: electronic Bracelet, monitoring unit, home station, key fob, fitting and installation tool, DEPAR VTU].
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 Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic Tool

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

FPT_PHP.2 Notification of physical attack

Dependencies: No dependencies

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 bracelet, monitoring unit, home station, DEPAR VTU 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 Bracelet ☑ Monitoring unit ☑ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic 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. [4]

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

☐ Electronic Bracelet	☑ Monitoring unit	☑ Home station
☐ Key fob	☐ Fitting and installation tool	☐ Diagnostic 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 Bracelet	☑ Monitoring unit	☐ Home station
☐ Key fob	☐ Fitting and installation tool	☐ Diagnostic Tool

- **Cryptography**

FCS_COP.1 Cryptographic operation

Dependencies: No dependencies

FCS_COP.1.1 <Only available in the full ST version>

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

☑ Electronic Bracelet	☑ Monitoring unit	☑ Home station
☑ Key fob	☑ Fitting and installation tool	☑ Diagnostic 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, the victim].

Refinement: This security functional requirement applies to the following TOE elements:
☑ Electronic Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic 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 identifier of the electronic bracelet (PSE, PSEM or DEPAR)
- Unique identifier fixed monitoring unit (PSE)
- Unique identifier of the mobile surveillance unit (PSEM or DEPAR)
- Unique identifier of the home station (PSEM or DEPAR)
- Unique identifier of the tool assembly and installation (PSE or PSEM)
- Unique identifier of the keyfob (PSE or PSEM)
- Unique identifier of the diagnostic tool (PSE or PSEM).

Refinement: This security functional requirement applies to the following TOE elements:
☑ Electronic Bracelet ☑ Monitoring unit ☑ Home station
☑ Key fob ☑ Fitting and installation tool ☑ Diagnostic Tool

- **Resistance to phenomena**

FPT_PHP.3 Resistance to physical attack

Dependencies: No dependencies.

Iteration 1: Electronic bracelet, monitoring unit, home station, key fob, fitting and installation tool
FPT_PHP.3 The TSF shall resist [assignment:
- temperatures between -20°C et +50°C]

to the [assignment: electronic bracelet, monitoring unit, home station, key fob, fitting and installation tool] by responding automatically such that the SFRs are always enforced.

Refinement: This security functional requirement applies to the following TOE elements:
☑ Electronic Bracelet ☐ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

Iteration 2: Electronic Bracelet

FPT_PHP.3 The TSF shall resist [assignment:
- water to a maximum depth of 0.5 metres]

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

Refinement: This security functional requirement applies to the following TOE elements:
☑ Electronic Bracelet ☐ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

- **Compliance with curfew scheme**

FCP_CMP.1 Curfew Policy Compliance

Dependencies: : FMT_MSA.3/Iteration

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

Subject:

- the subject

Objects:

- the zones [inclusion for PSE/PSEM and exclusion for DEPAR] 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's 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:

- Under PSE/PSEM the subject must not enter an exclusion zone at the required times.
- Under DEPAR the subject remain in an exclusion zone at the required times.
- Under PSE/PSEM the subject must be in an inclusion zone at the compulsory times
- Under DEPAR the subject must not enter 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_CMP1.5 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 Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

FMT_MSA.1 Management of security attributes

Itération 1: Administration centrale

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

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

- Reference time of the monitoring unit
- Curfew scheme [assignment policy]
- Events

to [assignment: remote monitoring centre application].

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

☐ Electronic Bracelet
☐ Key fob
☑ Monitoring unit
☐ Fitting and installation tool
☐ Home station
☐ Diagnostic Tool

Itération 2: Supervision locale

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

FMT_MSA.1.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions de supervision locale] to restrict the ability to [selection: query] the security attributes [assignment:

- Supervision local electronic bracelet:
  - The battery level,
  - The serial number
  - The version number of the software,
  - The status
- Supervision local keyfob:
  - The battery level,
  - The serial number
  - The version number of the software,
  - The status
- Supervision of the local monitoring unit or DEPAR VTU:
  - The serial number
  - The version number of the software,
  - The battery level
- Supervision local installation tool:
  - The serial number
  - The version number of the software,
  - The battery level].
- to [assignment: the local supervisor].

Refinement: This security functional requirement applies to the following TOE elements:
☑ Electronic Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☑ Fitting and installation tool ☐ Diagnostic Tool

Itération 3: Administration locale

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

FMT_MSA.1.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions d'administration locale] to restrict the ability to [selection: change_default, query, modify, delete] the security attributes [assignment:

o Local Administration of the monitoring unit or DEPAR VTU (PSE,PSEM or DEPAR):
- GSM configuration data:

- IP address
- APN
- Name
- password, port
- Local Administration of the monitoring unit or DEPAR VTU (PSE,PSEM or DEPAR):
- Align RTC Configuration with:
    - phone number "data"
    - phone "voice"
    - emergency number.

to [assignment: Local Administrator].

Refinement: This security functional requirement applies to the following TOE elements:
☐ Electronic Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

Itération 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: politique de contrôle d'accès aux fonctions d'initialisation] to restrict the ability to [selection: change_default, query, modify] the security attributes [assignment:

- The status of the electronic bracelet

to [assignment: agent de l'administration pénitentiaire].

Refinement: This security functional requirement applies to the following TOE elements:
☑ Electronic Bracelet ☐ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

FMT_MSA.3 Static attribute initialisation

Itération 1: Administration centrale

Dependencies: FMT_MSA.1/Iteration_1, FMT_SMR.1

FMT_MSA.3.1 The TSF shall enforce the [assignment: curfew scheme access and control functions at the central monitoring 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: remote 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 Bracelet ☑ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

Itération 2: Administration locale

Dependencies: FMT_MSA.1/Iteration_3, FMT_SMR.1

FMT_MSA.3.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions d'administration locale] 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: administrateur local] 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 Bracelet ☑ Monitoring unit ☐ Home station
☑ Key fob ☑ Fitting and installation tool ☐ Diagnostic Tool

Itération 3: Initialisation

Dependencies: FMT_MSA.1/Iteration_4, FMT_SMR.1

FMT_MSA.3.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions d'initialisation] 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: agent de l'administration pénitentiaire] 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 Bracelet ☐ Monitoring unit ☐ Home station
☐ Key fob ☐ Fitting and installation tool ☐ Diagnostic Tool

- **Access Control Policy**

FDP_ACC.2 Complete access control

Itération 1: Administration central

Dependencies: FDP_ACF.1/Iteration_1

FDP_ACC.2.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions d'administration centrale] on [assignment:

Topic :

- Monitoring application

Objects:

- Access to function at 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 Bracelet ☑ Monitoring unit ☐ Home Station
☐ Keyfob ☐ Installation Tool ☐ Diagnostic Tool

Itération 2: Supervision locale

Dependencies: FDP_ACF.1/Iteration_2

FDP_ACC.2.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions de supervision locale] on [assignment:

Topic:

- Local Supervisor

Object :

- Local supervisor access functions.

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 Bracelet ☑ Monitoring unit ☐ Home Station
☐ Keyfob ☑ Installation Tool ☐ Diagnostic Tool

Itération 3: Administration locale

Dependencies: FDP_ACF.1/Iteration_3

FDP_ACC.2.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions d'administration locale] on [assignment:

Topic :

- Local administration

Objets :

- Access to the function of the local administrator

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 Bracelet ☑ Monitoring unit ☐ Home Station
☑ Keyfob ☑ Installation Tool ☐ Diagnostic Tool

Itération 4: Initialisation

Dependencies: FDP_ACF.1/Iteration_4

FDP_ACC.2.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions d'initialisation] on [assignment:

Topic :
- Prison Officer

Objets :
- Initialisation functions

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 Bracelet ☐ Monitoring unit ☐ Home Station
☐ Keyfob ☐ Installation Tool ☐ Diagnostic Tool

FDP_ACF.1 Security attribute based access control

Itération 1: Administration central

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

FDP_ACF.1.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions d'administration centrale] to objects based on the following: [assignment:

Sujet:
- Monitoring application

Objets:
- Central administration functions

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:
- Request from the remote administration must be authenticated].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: Les requêtes d'administration distante sont authentifiées].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: Les requêtes d'administration distante ne sont pas authentifiées].

Refinement: This security functional requirement applies to the following TOE elements:
☐ Electronic Bracelet ☑ Monitoring unit ☐ Home Station
☐ Keyfob ☐ Installation Tool ☐ Diagnostic Tool

Itération 2: Supervision locale

Dependencies: FDP_ACC.2/Iteration_2

FDP_ACF.1.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions de supervision locale] to objects based on the following: [assignment:

Topic:

- Local supervisor

Objets:

- Access to the functions of the local supervisor

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:

- The requests of the local supervisor must be authenticated].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: Les requêtes de supervision locale sont authentifiées].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: Les requêtes de supervision locale ne sont pas authentifiées].

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

☑ Electronic Bracelet ☑ Monitoring unit ☐ Home Station
☐ Keyfob ☑ Installation Tool ☐ Diagnostic Tool

Itération 3: Administration locale

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

FDP_ACF.1.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions d'administration locale] to objects based on the following: [assignment:

Topic:

- Local administrator

Objets:

- Access to the functions of the local administrator

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:

- The requests of the local administrator must be authenticated].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: Les requêtes d'administration locale sont authentifiées].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: Les requêtes d'administration locale ne sont pas authentifiées].

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

☑ Electronic Bracelet ☑ Monitoring unit ☐ Home Station
☐ Keyfob ☐ Installation Tool ☑ Diagnostic Tool

Itération 4: Initialisation

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

FDP_ACF.1.1 The TSF shall enforce the [assignment: politique de contrôle d'accès aux fonctions d'administration locale] to objects based on the following: [assignment:

Sujet:

- Prison Officer

Objets:

- Access to initialisation functions

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:

- The requests of the prison officer must be authenticated].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: Les requêtes d’initialisation sont authentifiées].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: Les requêtes d’initialisation ne sont pas authentifiées].

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

☑ Electronic Bracelet ☐ Monitoring unit ☐ Home Station
☐ Keyfob ☐ Installation Tool ☐ Diagnostic Tool

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] shall be able to provide reliable time stamps for its own use.

Note: This security functional requirement enables the remote monitoring application to have a reliable time source available. In mode PSE the TOE synchronises its reference time with the remote monitoring centre time. In mode PSEM or DEPAR, the TOE synchronises its reference time via GPS satellites.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 <Only available in the full ST version>.

5.3 *Assurance requirements for the TOE*

The level aimed at is **EAL2 supplemented** by the ALC.FLR.3, ALC_DVS.1 and AVA_VAN.3 components.

Requirements		Descriptions
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_CENTRAL

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

The firmware found in the Monitoring Units, Keyfob, Electronic Bracelet and Home Station can be upgraded and deployed over the air via in-field upgrade. To achieve this, firmware for the Monitoring Units, Keyfob, Electronic Bracelet and Home Station is securely distributed to in-field Monitoring Units by the Monitoring Application.

F.ADMINISTRATION_LOCALE

This safety feature allows a prison officer with a diagnostic tool and a keyfob read access to certain parameters (status, battery level, serial number, ...) of elements the TOE, and write some settings for the TOE (telephone number of "data" and "voice" of the monitoring unit for GSM, ...).

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

F.SUPERVISION_LOCALE

This safety feature allows a prison officer with a diagnostic tool and a keyfob read access only to certain parameters (status, battery level, serial number, ...) of elements of the TOE.

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

F.INITIALISATION

This safety feature allows a prison officer with an installation tool and a keyfob to initialize the elements of the TOE, including changing the status of the electronic bracelet.

Access to the initialization function of the TOE requires identification and authentication of the agent of the prison administration. This identification and authentication is performed using the keyfob.

F.PROTECTION_COM_INTER_TOE

<Only available in the full ST version>

F.PROTECTION_COM_INTRA_TOE

<Only available in the full ST version>

F.ROLES

This security function enables management of the various roles within the TOE: remote monitoring centre application, subject, victim, local supervisor and 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 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 subject to.

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

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 bracelet 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/victim 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 document 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 evolutionary 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

The current security target does not claim conformity with a protection profile.

8 Reasons

8.1 Reasons for security objectives

8.1.1 Summary

Threats:

- M.ELT.PIEGEAGE_MATERIEL_FABRICATION
- M.ELT.PIEGEAGE_MATERIEL_LIVRAISON
- M.ELT.PIEGEAGE_LOGICIEL_FABRICATION
- M.ELT.PIEGEAGE_LOGICIEL_LIVRAISON

are not covered by security objectives for the TOE (Ot.), but by the assurance components of the TOE ALC_DVS ("Identification of security measures") and ALC_DEL ("Delivery Procedures") to ensure the protection of confidentiality and integrity of the TOE (sources and binaries TOE containing the symmetric key block) during its manufacture (ALC_DVS) and delivery (ALC_DEL).

		Hypothèses													Menaces																	Politiques de sécurité de l'organisation									
		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_DONNEES_DEVELOPPEUR	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	P.FIELD_UPGRADE
Objectifs de sécurité pour la TOE	OT.COM.INTRA_TOE.PROTECTION																							X	X	X	X											X			
	OT.FIELD UPGRADE																																								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.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		
Objectifs de sécurité pour l'environnem	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																										
	OE.AP.DOCUMENTATION_USER										X														X	X	X		X	X	X						X	X	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 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 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 to protect proprietary information. Complete coverage justification provided in [ST].

8.2 Reasons for security functional requirements

8.2.1 Summary

Exigences fonctionnelles de sécurité pour la TOE	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.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	OT.FIELD_UPGRADE
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														
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																					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																					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			X
FPT_ITI.1		X	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 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**

Exigences	Dépendances Critères Communs	Dépendances effectives	OK/NOK : argumentaires
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	Aucune	Aucune	OK
FMT_SMF.1/Iteration_2	Aucune	Aucune	OK
FMT_SMF.1/Iteration_3	Aucune	Aucune	OK
FMT_SMF.1/Iteration_4	Aucune	Aucune	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	Aucune	Aucune	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	Aucune	Aucune	OK
FIA_UID.2/Iteration_2	Aucune	Aucune	OK
FIA_UID.2/Iteration_3	Aucune	Aucune	OK
FIA_UID.2/Iteration_4	Aucune	Aucune	OK
Classe FPT : Protection of the TSF			
FPT_STM.1	Aucune	Aucune	OK
FPT_ITT.1	Aucune	Aucune	OK
FPT_ITT.3	FPT_ITT.1	FPT_ITT.1	OK
FPT_RPL.1	Aucune	Aucune	OK
FPT_PHP.2	FMT_MOF.1	Aucune	NOK. Voir argumentaire de non satisfaction ci-dessous.
FPT_PHP.3/Iteration_1	Aucune	Aucune	OK
FPT_PHP.3/Iteration_2	Aucune	Aucune	OK
FPT_ITC.1	Aucune	Aucune	OK
FPT_ITI.1	Aucune	Aucune	OK
FPT_EMSEC	Aucune	Aucune	OK
Classe FCS : Cryptographic support			
FCS_COP.1	FDP_ITC.1, ou FDP_ITC.2, ou FCS_CKM.1	Aucune	NOK. Voir argumentaire de non satisfaction ci-dessous.
	FCS_CKM.4	Aucune	NOK. Voir argumentaire de non satisfaction ci-dessous.
Classe FPR : Privacy			
FPR_ANO.1	Aucune	Aucune	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	Aucune	NOK. Voir argumentaire de non satisfaction ci-dessous.
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:

<Only available in the full ST version>

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

The cryptographic keys contained in the TOE 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.

8.3 Reasons for TOE security functions

	Fonctions de sécurité											
Exigences fonctionnelles de sécurité pour la 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 Supervisor and Local Administrator

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