



Plecs de prescripcions tècniques de licitació del contracte de serveis per a la contractació per procediment obert de:

“Gestió integral del Sistema de Seguretat únic T-mobilitat en explotació, rol ISO/IEC 24.014, i implementació de noves funcionalitats”

(EXP. C-42/2022)

Abril 2023



Índex	Pàgina
1. PRESCRIPCIÓNS GENERALS.....	4
2. DESCRIPCIÓ DELS TREBALLS	4
2.1. Antecedents	4
2.2. Context	5
2.3. El Projecte T-mobilitat	6
2.4. Justificació	8
2.5. Objecte del contracte o necessitats a cobrir	8
3. ACTIVITATS I FUNCIONS DE L'EMPRESA CONTRATISTA.....	11
3.1. Gestió dels SERVEIS DE SEGURETAT del SSu	11
3.1.1. Gestió integral en explotació dels SERVEIS DE SEGURETAT criptogràfics	11
3.1.2. Serveis de seguretat per dispositiu – Mòduls SAMs CBT.....	12
3.1.3. Serveis de seguretat per dispositiu – Centre HSM.....	15
3.1.4. Serveis de seguretat per dispositiu – SUS	17
3.1.5. Nous SERVEIS DE SEGURETAT a implementar.....	19
3.1.5.1. Identificació i securització dels entorns de treball	19
3.1.5.2. Activació de SUS personalitzat	20
3.1.5.3. Registre de Suport anònim.....	21
3.1.5.4. Gestió de versions d'ATlu	22
3.1.5.5. Securitació de dades personals en la personalització de SUS	22
3.2. Gestió en explotació de COMPONENTS físics del SSu.....	23
3.2.1. Gestió en explotació dels MÒDULS D'ACCÉS SEGURS, SAMs.....	23
3.2.2. Gestió en explotació dels CENTRES HSMs	26
3.2.3. Gestió en explotació dels DISPOSITIUS MÒBILS NFC	29
3.2.4. Serveis de Manteniment integral del SSu.....	31
3.3. Infraestructura de Gestió de CLAUS I EINES associades al SSu	35
3.4. Gestió i lideratge del PROGRAMA de C&A del SSu	37
3.4.1. Programa de C&A a Serveis de Seguretat.....	38
3.4.2. Programa de C&A als components SAMs CBT.....	40
3.4.3. Programa de C&A als components CHSM	41
3.4.4. Programa de C&A seguretat als dispositius mòbils NFC.....	43
3.4.5. Programa de C&A Infraestructura de gestió de claus.....	43
3.5. Gestió i lideratge d'ESPECIFICACIONS TÈCNIQUES del SSu	44
3.5.1. Sistema de Seguretat únic – visió general	44

3.5.2.	Serveis de Seguretat de les transaccions sense contacte T-mobilitat	45
3.5.3.	Components de seguretat local - SAM CBT	46
3.5.4.	Components de seguretat centralitzats – Centres HSM	47
3.5.5.	Components de seguretat per dispositius mòbils NFC	49
3.5.6.	Infraestructura de gestió de claus criptogràfiques	50
3.5.7.	Eines de gestió del Sistema de Seguretat únic	50
3.6.	TRACTAMENT DE RISCOS del SSu i nous desenvolupaments	51
3.7.	Gestió i LIDERATGE INTEGRAL del SSu com rol ISO/IEC 24.014 dins del MTC	52
3.8.	Mòdul de GESTIÓ DE FRAU	53
3.9.	Exportació de DADES DEL SIC	54
4.	FINALITATS I OBJECTIU A ASSOLIR	55
4.1.	Principis bàsics a complir	55
5.	SEGUIMENT I CONTROL DE LES CONDICIONS DEL CONTRACTE	56
5.1.	Descripció de la forma de prestació del servei	56
5.1.1.	Planificació del Projecte	56
5.1.1.1.	Fase de Planejament	56
5.1.1.2.	Fase d'Anàlisi i Enginyeria	56
5.1.1.3.	Fase de desenvolupament	56
5.1.1.4.	Fase de desplegament	57
5.1.1.5.	Fase d'explotació	57
5.2.	Mitjans Tècnics i Materials	57
5.2.1.	Infraestructura necessària per dur a terme el projecte	57
5.3.	Recursos humans	58
5.4.	Metodologia a aplicar	60
5.5.	Organització de l'execució del projecte	62
5.5.1.	Control i seguiment i seguiment del projecte	62
5.5.2.	Terminis d'execució	63
5.5.2.1.	Calendari	63
5.5.2.2.	Fites estratègiques	65
5.6.	Condicions generals d'execució	65
5.6.1.	Confidencialitat i publicitat del servei	65
5.6.2.	Propietat intel·lectual	66
5.6.3.	Tractament de dades de caràcter personal	66
5.6.4.	Criteris d'accessibilitat universal	66
5.6.5.	Criteris de sostenibilitat i protecció al medi ambient	66
5.7.	Proposta tècnica	67

1. PRESCRIPCIONS GENERALS

Aquest plec de prescripcions tècniques estableix les condicions de caràcter tècnic que han de regir el procés de contractació per a "*Gestió integral del Sistema de Seguretat únic T-mobilitat en explotació, rol ISO/IEC 24.014, i implementació de noves funcionalitats*" per a la protecció de totes i cadascuna de les Transaccions sense contacte T-mobilitat.

En el present document es descriuen els treballs a realitzar i el seu desenvolupament, es relacionen les matèries que han de ser objecte de desenvolupament, es defineixen les condicions i criteris que han de servir de base i es concreten els treballs que haurà de realitzar l'adjudicatari perquè, un cop garantida la seva qualitat, puguin ésser acceptats per l'Autoritat del Transport Metropolità de Barcelona

Amb la mera presentació de la seva oferta, l'empresa licitadora accepta les prescripcions tècniques establertes en aquest plec.

Qualsevol proposta que no s'ajusti als requeriments mínims establerts en aquest plec quedarà automàticament exclosa de la licitació.

2. DESCRIPCIÓ DELS TREBALLS

2.1. Antecedents

L'Autoritat del Transport Metropolità de l'àrea de Barcelona (d'ara endavant ATM) és un consorci interadministratiu de caràcter voluntari, creat en 1997, al que poden adherir-se totes les administracions titulars de serveis públics de transport col·lectiu, que pertanyin a l'àmbit format per les comarques de l'Alt Penedès, l'Anoia, el Bages, el Baix Llobregat, el Barcelonès, el Berguedà, el Garraf, el Maresme, el Moianès, Osona, el Vallès Occidental i el Vallès Oriental.

Actualment, les administracions consorciades són la Generalitat de Catalunya (51%) i administracions locals (49%), compostes per l'Ajuntament de Barcelona, l'Àrea Metropolitana de Barcelona (AMB) i l'Agrupació de Municipis titulars de serveis de Transport urbà de la regió metropolitana de Barcelona (AMTU). A més, l'Administració General de l'Estat està present en els òrgans de govern de l'ATM en qualitat d'observador.

D'acord amb els estatuts del consorci, l'ATM de Barcelona té com a finalitat articular la cooperació entre les administracions públiques titulars dels serveis i de les infraestructures del transport públic col·lectiu de l'àrea de Barcelona que formen part del consorci, i també la col·laboració amb aquelles que, com l'Administració General de l'Estat, estan compromeses financerament o són titulars de serveis propis.

Les principals funcions de l'ATM de Barcelona consisteixen a la planificació de les infraestructures i serveis de transport públic col·lectiu, la coordinació i el seguiment de les relacions amb els operadors de transport col·lectiu, l'elaboració de propostes i la concertació d'acords de finançament amb les administracions, l'ordenació de tarifes i la tramitació de plans de mobilitat.

En l'exercici de les seves funcions, l'ATM va iniciar en 2001 la implantació del sistema tarifari integrat, resultant ser una eina eficient per a la millora de les prestacions del sistema de transport públic. El sistema tarifari integrat permet la utilització de diferents

maneres de transport (metro, autobusos urbans, metropolitans i interurbans, tramvia, Ferrocarrils de la Generalitat de Catalunya i Renfe Rodalies) necessaris per realitzar un desplaçament amb un únic títol de transport, despenalitzant econòmicament els transbordaments. Actualment el sistema tarifari abasta 356 municipis i una població de 5,7 milions d'habitants.

Part del contingut d'aquestes prescripcions tècniques deriva del projecte “Serveis d'enginyeria per al disseny, desenvolupament, posada en servei i manteniment de la Plataforma de gestió integral del Sistema de Seguretat Criptogràfic” C-33/2020.

2.2. Context

Una de les principals activitats de gestió identificades en el **Model organitzatiu de referència basat en rols ISO/IEC 24014** associat a l'Autoritat de Confiança és la *Gestió del Sistema de Seguretat Criptogràfica* que en garanteixi el control, evolució així com el manteniment integral en tots els seus nivells de l'anomenat **Sistema de Seguretat únic**.

Totes les tecnologia està exposada a **problemes de seguretat**, encara que només sigui per l'augment exponencial de capacitat de procés que any darrere any proporciona la indústria de la tecnològica que en el nostre cas, és particularment perillós, perquè la base del Sistema Tarifari Integrat T-mobilitat és l'estandardització i l'ús de procediments normalitzats, és a dir, **coneguts i públics**.

En relació a la seguretat, en el cas del Sistema Tarifari sense contacte integrat i compartit amb múltiples actors associats en el projecte T-mobilitat, és particularment perillós perquè la base d'un *Sistema interoperable Global* és **l'estandardització i l'ús de procediments definits**, és a dir, coneguts i publicats.

Així, implantar un Sistema de Bitlletatge Electrònic sense contacte obert i interoperable basat en Normes Internacionals conegudes té grans avantatges, però només si va acompanyat d'un veritable Sistema d'Intercanvi d'Informació Integral compartit, transparent i interoperable, però que, sobretot i abans de res, disposi d'un **adequat SISTEMA DE SEGURETAT CRIPTOGRÀFICA**.

És, precisament el Sistema de Seguretat criptogràfica, la peça angular que ha de generar la confiança de tots els actors en el Sistema. És el **complement ocult** en les diferents operatives (casos d'ús) de qualsevol Aplicació del Sistema, també de *l'Aplicació de Transport Interoperable única (ATIU)*, implementant mecanismes, serveis i funcions de seguretat.

El Sistema de Seguretat criptogràfica és un instrument que ajuda a visualitzar i entendre el grau de confiança que s'ofereix respecte els diferents intercanvis de dades o transaccions, tot garantint **l'autenticitat, confidencialitat, integritat, no repudi**, etc., però també, des del coneixement de les amenaces i vulnerabilitats del sistema.

En aquest context el Sistema de Seguretat criptogràfic té una **FUNCIONALITAT TRANSVERSAL** que afecta a totes i cadascuna de les àrees del Sistema de Bitlletatge Electrònic sense contacte.

L'ATM, com a **Gestor del Sistema de Seguretat criptogràfica**, és la responsable de definir, desenvolupar, publicar, mantenir i evolucionar el **Sistema de Seguretat Únic Integrat**.

És en aquesta última àrea de competència on s'ubica **l'abast dels treballs tècnics** en

relació a la “*gestió integral del Sistema de Seguretat únic T-mobilitat en explotació, rol ISO/IEC 24.014, i implementació de noves funcionalitats*”, com element de protecció ocult de totes les transaccions sense contacte del Sistema Tarifari Integrat.

La missió del Sistema de Seguretat únic (SSu) és **garantir la seguretat de les Transaccions** sense contacte del Sistema Tarifari Integrat T-mobilitat a través d'establir i evolucionar els **Serveis de Seguretat que el sustenta**, així com dels elements segurs en què s'emmagatzemen aquests Serveis de seguretat.

El Sistema de Seguretat únic utilitza tant **criptografia simètrica** (en serveis on es necessita temps de respostes quasi real) com **criptografia asimètrica** (per la seguretat en l'intercanvi d'informació).

El principal objectiu del Sistema de Seguretat únic T-mobilitat és **articular un marc de treball comú, confidencial, compartit** amb els operadors i liderat per l'ATM per aconseguir la permanent protecció del Sistema Tarifari Integrat basat en tecnologia sense contacte de proximitat.

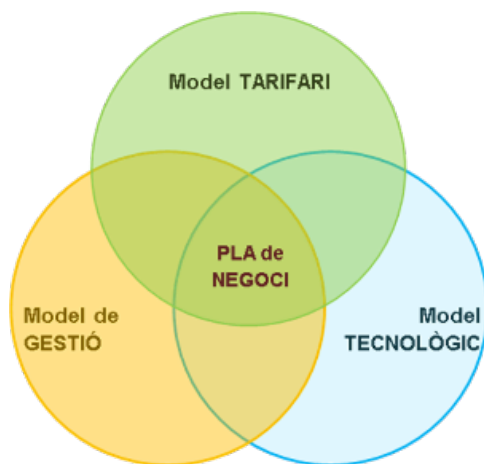
És en aquest context, i sota la responsabilitat que té l'ATM com a **Gestor del Sistema de Seguretat únic T-mobilitat**, en el qual s'emmarca la present licitació.

2.3. El Projecte T-mobilitat

El Projecte T-mobilitat és un projecte de l'ATM de Barcelona que va sorgir de la necessitat d'establir un nou sistema de Ticketing electrònic sense contacte donada la manifesta obsolescència tecnològica de banda magnètica.

En data 1 d'octubre de 2014 es va resoldre adjudicar el procediment de licitació del Projecte T-mobilitat per a la implantació d'un nou sistema tecnològic, tarifari i de gestió basat en tecnologia sense contacte de proximitat ISO/IEC 14.443, així com en el model de rols ISO/IEC 24.014 per garantir la interoperabilitat tècnica i funcional dels elements d'ús comú.

El Projecte T-mobilitat té com objectiu principal establir un nou **MODEL TECNOLÒGIC** que posat a disposició del **MODEL TARIFARI** permeti una millor i més eficient **GESTIÓ** del Sistema Tarifari Integrat que garanteixin els objectius globals per a una millor i més eficaç utilització del Transport Públic. Es tracta de donar respostes a una creixent necessitat de Mobilitat, en la qual el Transport públic té un paper tractor bàsic.



Imatge 1: Abast del Projecte T-mobilitat

Sota el desenvolupament del **Model Tecnològic T-mobilitat** s'estableix un **marc de treball comú, unificat, compartit i col·laboratiu** que integra tots els serveis de transport i de mobilitat basat en el *Model de rols ISO/IEC 24.014* que proporciona la base per al desenvolupament d'un **Sistema de gestió tarifaria interoperable, multi-operador, multi-proveïdor i multi-serveis**.

El **MODEL TECNOLÒGIC T-mobilitat** descriu les característiques estratègiques funcionals, organitzatives i tecnològiques dividit en dues grans àrees; **el MARC TECNOLÒGIC COMÚ**, que conté les especificacions i requeriments comuns a tots els operadors, i **el MARC TECNOLÒGIC ESPECÍFIC**, que conté les especificacions i requeriments propis de cada un dels operadors o grup d'operadors i dels quals en són responsables els propis operadors.

La missió del **Marc Tecnològic Comú** és garantir els principis estratègics que la T-mobilitat ha aplicat als elements d'ús transversal:

- la **Interoperabilitat tecnològica**, entesa com la capacitat del "HW" i del "SW" que corre als diferents equips de diferents proveïdors per intercanviar i utilitzar la informació,
- l'**Estandardització** com base per facilitar la implementació de la interoperabilitat tecnològica, i especificant allò que no estigui cobert per les normes actuals, garantint la no existència de "*Caixes negres*".
- la **Neutralitat tecnològica** que assegurï l'adaptabilitat dels elements d'ús transversal al progrés de la tecnologia, encoratjant la innovació, el "know-how" i la propietat intel·lectual,
- la **Independència tecnològica** respecte a qualsevol proveïdor tecnològic en el Sistema T-mobilitat, i
- l'**Escalabilitat** amb una organització modular portable com a garantia d'ampliació geogràfica i d'evolució en el temps.
- El **Sistema de Seguretat únic** és la peça angular del Sistema Tarifari Integrat per garantir una adequada protecció de totes i cadascuna de les Transaccions sense contacte realitzades.

Podem dir que és el complement ocult en les diferents operatives (validació, recàrrega, inspecció...) de l'*aplicació de Transport Interoperable única* (ATlu) que implementa mecanismes, serveis i funcions de seguretat basat en la utilització de criptografia forta.

És dins del Projecte T-mobilitat on se circumscriu el contingut i abast de la present prestació amb relació als Serveis Tecnològics necessaris per garantir una "*Gestió integral del Sistema de Seguretat únic T-mobilitat en explotació, rol ISO/IEC 24.014 i implementació de noves funcionalitats*", per a la protecció de totes i cadascuna de les Transaccions sense contacte T-mobilitat.

Es descriuen als paràgrafs següents, els treballs a realitzar i el seu desenvolupament, es relacionen les matèries que han de ser objecte de la prestació, es defineixen les condicions i criteris que han de servir de base per fer la proposta tècnica i es concreten

els treballs que haurà de realitzar l'Adjudicatari perquè, un cop garantida la seva qualitat dels treballs realitzats, puguin ésser acceptats per l'Autoritat del Transport Metropolità de Barcelona.

2.4. Justificació

El projecte T-mobilitat és un projecte de l'ATM de Barcelona que va sorgir de la necessitat d'establir un nou Sistema de Ticketing electrònic sense contacte donada la manifesta obsolescència tecnològica de la banda magnètica. En aquest sentit, i donat aquest nou sistema de Ticketing o sistema tecnològic, es va promoure la implantació d'un nou sistema tarifari i de gestió.

El Govern de la Generalitat de Catalunya, mitjançant acord de 8 d'octubre de 2013, va donar llum verda al projecte T-mobilitat com a mecanisme fonamental de la gestió de la mobilitat en un únic suport intel·ligent, i va establir un sistema d'informació pensant en el ciutadà, amb la creació de dos nous centres de treball: el Centre d'Atenció al Client i el Centre de Gestió de la informació del Transport, que d'una manera global, haurien d'informar en temps real del funcionament de l'oferta de transport públic integrat en tot el territori català.

La complexitat tècnica, jurídica i financera intrínseca derivada de la implementació del nou sistema tecnològic, tarifari i de gestió (projecte T-mobilitat) va justificar inicialment la necessitat de disposar d'un mecanisme flexible, especialment pel que fa a l'assignació de riscos, considerant per tant com a modalitat contractual òptima per licitar el projecte T-mobilitat el contracte de col·laboració entre el sector públic i el sector privat.

La licitació del contracte de col·laboració entre el sector públic i el sector privat del "Projecte T-mobilitat per a la implantació d'un nou sistema tecnològic, tarifari i de gestió" (expedient de contractació C-24/2012), es va iniciar en data 16 d'octubre de 2013, quan es va publicar l'anunci de la licitació en el Diari Oficial de la Unió Europea (DOUE) i en el Butlletí Oficial de l'Estat (BOE), i en data 17 d'octubre de 2013, en el Diari Oficial de la Generalitat de Catalunya.

En data 1 d'octubre de 2014 es va resoldre adjudicar el procediment de licitació del projecte T-mobilitat per a la implantació d'un nou sistema tecnològic, tarifari i de gestió.

En data 24 d'octubre de 2014 es va formalitzar el contracte del projecte T-mobilitat entre l'ATM i la SOCIETAT CATALANA PER A LA MOBILITAT, SA.

En relació amb l'objecte d'aquesta contractació, la clàusula 19.2.I del contracte CPP de 14 d'octubre de 2014 obliga a l'ATM de Barcelona a gestionar i proporcionar al *Sistema de Bitlletatge sense contacte T-mobilitat*, els Serveis Tecnològics necessaris derivats d'ús del Sistema de Seguretat únic a través de la utilització d'elements segurs (SAM per a la seguretat local i HSM per a la seguretat centralitzada) a fi de garantir la seguretat de totes i cadascuna de les transaccions sense contacte T-mobilitat.

2.5. Objecte del contracte o necessitats a cobrir

L'objectiu principal d'aquest contracte és el desenvolupament i posada en servei de nous Serveis de Seguretat criptogràfica a implementar a la T-mobilitat, així com disposar de serveis d'enginyeria i assistència tècnica per a la "*Gestió Integral del Sistema de Seguretat únic T-mobilitat en Explotació, rol ISO/IEC 24.14, i implementació de noves*

funcionalitats”, que va des del disseny dels nous processos, fins a la posada en servei, el manteniment i l'evolució de la *Plataforma de Seguretat criptogràfica*.

La gestió integral de l'SSu no s'entén si no és d'una manera holística, on el **sistema de seguretat, els seus components i les eines associades s'analitzen com un tot**, d'una manera global i integrada, ja que només des del punt de vista operatiu el seu funcionament només es pot comprendre d'aquesta manera i no com la simple suma de les parts.

Aquest plec de prescripcions tècniques té per objecte determinar el contingut i abast dels treballs que haurà de desenvolupar l'empresa adjudicatària de la present licitació.

Es descriuen els treballs a realitzar i el seu desenvolupament, la interrelació dels treballs a dur a terme, així com les condicions i els criteris pels quals, una vegada garantida la qualitat dels treballs realitzats, puguin ser acceptats per l'ATM de Barcelona.

L'abast del procés de contractació dels serveis d'enginyeria i assistència tècnica necessaris per disposar d'una *“Gestió Integral del Sistema de Seguretat únic T-mobilitat en Explotació i implementació de noves funcionalitats”* que contempla el següent.

L'abast dels treballs a desenvolupar dintre d'aquesta licitació **se circumscriu únicament a l'àmbit del Sistema de Seguretat únic**, que inclou la infraestructura de gestió de claus criptogràfiques, elements segurs d'ús local (SAM), elements d'ús centralitzat (Centres HSM), capa d'abstracció de la seguretat, gestió de la seguretat en dispositius mòbils NFC, entre altres.

L'abast de la present Licitació té per objecte **desenvolupar i posada en servei** dels nous serveis de seguretat identificats, així com el **manteniment integral, gestió d'incidències i problemes i petites evolucions** amb el sistema en explotació al llarg de tot el contracte.

Està dins de l'abast de la present licitació es troben tots els serveis d'enginyeria i assistència tècnica necessaris per portar a terme una *“Gestió integral del Sistema de Seguretat únic T-mobilitat en explotació, rol ISO/IE 24.014, i implementació de noves funcionalitats”*.

Així, l'abast de la present licitació és:

1. Gestió dels Serveis de Seguretat del SSu

Serveis d'enginyeria per a la gestió integral i manteniment en explotació de tots i cadascuns dels **Serveis de Seguretat criptogràfics** per a la protecció a les transaccions sense contacte implementats i distribuïts des del Sistemes Informàtics Centrals (SICs) als diferents elements segurs (SAMs i CHSM) continguts en els terminals sense contacte d'operador i en els SICs T-mobilitat a l'àrea integrada de Barcelona. El que coneixen com Sistema de Seguretat únic T-mobilitat – rol ISO/IEC 24.014.

2. Gestió en explotació dels components físics del SSu

Gestió i manteniment integral en explotació de tots i cadascuns dels **components del Sistema de Seguretat únic (SSu)** implementats i distribuïts al llarg de tota la infraestructura tecnològica T-mobilitat desplegada a l'àrea integrada de Barcelona.

Així com els serveis d'enginyeria per a la gestió integral del sistema d'**identificació i resolució d'incidències i problemes en explotació** amb relació al Sistema de Seguretat únic que pot afectar als Serveis de seguretat, als components del SSu i/o les eines tecnològiques associades a la T-mobilitat a l'àrea integrada de Barcelona.

Gestió del desenvolupaments, implementació, integració i posada en serveis de les petites **evolucions derivades de la resolució d'incidències i problemes** que segur apareixeran a l'explotació de la T-mobilitat a l'àrea integrada de Barcelona.

3. Infraestructura de Gestió de claus i eines associades al SSu

Gestió i manteniment integral de la infraestructura de gestió de claus criptogràfiques i de les **eines tecnològiques** (plataformes tecnològiques implementades) associades al Sistema de Seguretat únic T-mobilitat necessàries per operar a nivell de protecció de les transaccions sense contacte a l'àrea integrada de Barcelona.

4. Gestió del Programa de C&A del SSu

Gestió i manteniment integral del **Sistema de Conformitat i Acceptació** del Sistema de Seguretat únic per garantir en tot moment el compliment dels requeriments tècnics exigits als Serveis de Seguretat criptogràfica, als components segurs del SSu, així com a les eines necessàries associades, a la T-mobilitat en explotació a l'àrea integrada de Barcelona.

5. Gestió de les Especificacions tècniques del SSu

Gestió i manteniment integral dels **requeriments tècnics** d'obligat compliment i de les **especificacions tècniques** associades del Sistema de Seguretat únic que inclou els Serveis de Seguretat criptogràfics implementats, els components segurs i eines associades si s'escau, així com **manuals d'ús** en aquells casos que es consideri necessari.

6. Tractament de riscos dels SSu

Gestió del tractament de riscos del Sistema de Seguretat únic que inclou l'assistència tècnica a la identificació, **anàlisi i viabilitat de nous serveis de seguretat** necessaris a implementar, noves evolucions del Sistema de Seguretat únic en explotació, així com de les eines associats a la plataforma de seguretat, amb l'objectiu de mantenir el risc de seguretat residual en límits acceptables.

Gestió, desenvolupament, integració, proves de compliment i acceptació i posada en servei dels **nous serveis de seguretat** identificats com a necessaris a implementar al sistema de seguretat únic en T-mobilitat a l'àrea integrada de Barcelona, sempre sota els principis i directrius del Marc Tecnològic Comú.

7. Gestió integral, i lideratge, del SSu com rol ISO/IEC 24.014 dins del MTC

Gestió i lideratge de les **reunions tècniques** amb l'equip tècnic responsable del Marc Tecnològic Comú i altres actor de temes relacionats amb el Sistema de Seguretat criptogràfic T-mobilitat.

Està fora de l'abast de l'objecte d'aquest contracte qualsevol nou equipament necessari a futur, no inclòs a la llista de manteniment de la plataforma de seguretat del Sistema de seguretat únic T-mobilitat, derivats de nous desenvolupaments.

3. ACTIVITATS I FUNCIONS DE L'EMPRESA CONTRATISTA

L'oferta que presenti l'empresa licitadora ha d'abastar la totalitat de les activitats i funcions especificades en aquest plec i en el plec de clàusules administratives particulars, ja que són totes obligatòries per a l'admissió de les propostes.

Es descriuen en aquest apartat les principals activitats i funcions que l'empresa contractista ha d'assumir.

3.1. Gestió dels SERVEIS DE SEGURETAT del SSu

3.1.1. Gestió integral en explotació dels SERVEIS DE SEGURETAT criptogràfics

Els equips i elements segurs que componen Sistema de Seguretat únic implementen i integren un conjunt de **SERVEIS DE SEGURETAT que es consumeixen** dins del Sistema Tarifari Integrat T-mobilitat.

Dins de l'abast d'aquest contracte, l'adjudicatari haurà de gestionar de **manera integral tots els Serveis de Seguretat** ja implementats, així com els nous una vegada implementats, que l'SSu posa a disposició de la resta d'actors que operen en T-mobilitat.

Serà responsabilitat de l'adjudicatari garantir en tot moment la disponibilitat de tots i cadascun dels Serveis de Seguretat que l'SSu posa a disposició del Sistema Tarifari Integrat de l'àrea integrada de Barcelona, d'acord amb els nivells de qualitat acordats.

L'adjudicatari haurà de proposar el Pla de gestió integral dels Serveis de Seguretat T-mobilitat en explotació, que aprovat pel Model Tècnic Comú (ATM), garanteixi la disponibilitat de tots i cadascun dels Serveis de Seguretat de l'SSu a la T-mobilitat en explotació a l'àrea integrada de Barcelona.

Així, els **Serveis de Seguretat** es carreguen en elements segurs físics que estan distribuïts per tot el Sistema T-mobilitat, com són:

- **Els Mòduls d'Accés Segur – SAM**

És un element segur en format SIM amb un xip microprocessador amb característiques criptogràfiques sobre la qual es poden implementar Serveis de Seguretat, així com emmagatzemar les claus criptogràfiques.

- **Els Centres de Mòduls d'Hardware Segur – CHSM**

El Servidor Segur és un servidor criptogràfic que ofereix serveis de seguretat de tota mena que incorpora un element segur hardware amb fortes mesures de seguretat anomenat SHM.

- **Els Suports d'Usuari Sense Contacte – SUS**

Els SUS són elements segurs que estan més exposats a atacs, ja que estan en possessió de l'usuari i per tant fora del control del sistema.

El Sistema de Seguretat únic SSu és un ecosistema viu que no és un producte sinó que és un **procés de millora contínua** en relació amb la idoneïtat, l'eficàcia i l'adequació

permanent a les necessitats i a un entorn en canvi continu.

Així, amb relació als Serveis de Seguretat de l'SSu i des d'un punt de vista general, s'han de realitzar les tasques següents:

- A.** L'adjudicatari, en fase d'anàlisi i enginyeria, haurà de proposar el **Pla de gestió integral dels Serveis de Seguretat T-mobilitat en explotació**, que aprovat pel Model Tècnic Comú (ATM), garanteixi la disponibilitat de tots i cadascun dels Serveis de Seguretat de l'SSu a la T-mobilitat en explotació a l'àrea integrada de Barcelona.
- B.** L'adjudicatari, en fase d'anàlisi i enginyeria haurà d'identificar i especificar un **Pla de millora continua** basat en l'anàlisi intern (i accions associades) i extern (entorn canviant), la planificació sistemàtica en millora continua i el compromís de mantenir uns nivells de riscos assumibles que assegurin en tot moment la idoneïtat, l'eficàcia i l'adequació del Sistema de Seguretat únic, els seus components, la infraestructura tecnològica i les eines associades.

3.1.2. Serveis de seguretat per dispositiu – Mòduls SAMs CBT

Els mòduls d'ús local SAM (Secure Access Module) són elements segurs de nivell 1 que donen serveis de seguretat locals als TIUs que estan preparats per treballar "off-line" i són molt robustos davant de fallides de hardware, pel que la disponibilitat és molt alta i no cal redundar-los.

El Sistema Tarifari Integrat sense contacte T-mobilitat utilitza mòduls SAM per oferir en tems real els següents serveis de seguretat:

- **Magatzems segur d'informació**, que permet emmagatzemar informació i disposen de mecanismes de seguretat per l'accés segur al seu contingut.
- **Magatzems segur de claus**, que permet emmagatzemar claus del sistema de manera controlada, xifrada i auditada.
- **Control d'accés segur**, són els mecanismes que incorporen els equips per controlar l'accés als recursos que protegeixen: ús de PIN per a l'ajuda a la gestió, Autenticació per permetre l'accés a actors autoritzats, Canal segur per a l'intercanvi segur d'informació.
- **Gestió de jocs de claus de targeta**, segon els seu ús per fer desenvolupaments a l'entorn d'enginyeria, per a la integració a l'entorn de preproducció i reals a l'entorn de producció en explotació.
- **Mecanismes de diversificació de claus**, de càlcul unidireccional per mitigar el risc d'emmagatzemar claus mestres en elements distribuïts pel sistema.
- **Obtenir claus diversificades**, amb mecanismes d'accés suficients per permetre obtenir-les només als actors autoritzats.
- **Mecanisme d'autenticació**, que permet a un sistema corroborar que un actor diu qui és qui és.

- **Mecanismes d'autenticació mútua**, permet a dos actors autenticar (confirmar la identitat) entre tots dos mitjançant un mitjà de comunicació no segur.
- **Obtenir clau de sessió**, que es genera durant el procés d'autenticació, generada de forma aleatòria a cada autenticació, que permet que l'accés al *Suport d'Usuari Sense contacte* (SUS) T-mobilitat mitjançant ordres protegides mitjançant criptografia forta.
- **Comptadors de SAM**, que s'incrementen de manera automàtica en algunes accions generades en operar el sistema tarifari integrat.
- **Quotes de SAM**, que limita la quantitat d'operatives de recàrrega, venda, etc. que es poden fer amb un SAM sense connectar-se a un Centre HSM.
- **Canal segur**, que permet crear un canal de comunicació entre dos actors, de manera segura, a través d'un mitjà insegur.
- **Mecanismes de signatura**, que permet que uns actors puguin generar la signatura de certa informació coneguda i que altres puguin comprovar la signatura d'aquesta informació per comprovar-ne l'autenticitat.
- **Autenticació de SUS**, els SAMs fan una autenticació mútua abans de permetre al TIU corresponent tenir accés al contingut del SUS presentat en la seva àrea activa de radiofreqüència.

També disposen d'un parell de claus asimètriques que us permeten realitzar autenticacions PKI amb altres dispositius, com Centres HSMs.

- **Confidencialitat**, els mòduls SAM tenen la capacitat de xifrar i desxifrar les dades que envien quan s'ha de garantir la confidencialitat de les dades transmeses perquè contenen informació sensible que només ha de ser accessible per al destinatari de les dades tant amb criptografia simètrica com amb criptografia asimètrica.
- **Integritat**, de les dades es garanteix mitjançant la seva signatura de forma que:
 - Quan el SAM **rep un paquet de dades signades**, verifica la signatura, rebutjant les dades amb firmes no vàlides.
 - Quan el SAM **envia paquets de dades**, les signa de manera que se'n pugui verificar la integritat.

T-mobilitat signa totes i cadascuna de les transaccions sense contacte portades a terme.

La signatura amb claus asimètriques anomena també **certificat** i els SAMs preparats per generar certificats PKI.

Disponibilitat, els SAMs són dispositius que s'utilitzen als terminals TIU que tenen garantida l'alta disponibilitat pel fet que el canal de comunicació amb el SAM està integrat al mateix TIU i que el risc de fallida del maquinari del SAM és molt baix.

Això no obstant, si el SAM disposa de claus limitades per quota, quan aquesta s'esgota, el SAM deixa de donar el servei amb aquesta clau. Per garantir la disponibilitat de les claus limitades per quota, el TIU ha d'anar periòdicament actualitzant la quota del SAM mitjançant el Centre HSM d'operador.

- **No repudi**, els SAMs asseguruen el no repudi mitjançant la signatura de dades amb claus que són úniques a cada SAM que poden ser simètriques o asimètriques.
- **Anti-clonat dels SAMs**, mitjançant els mecanismes exigits a tot xip autoritzat a la T-mobilitat per protegir-se davant del clonatge de les dades que emmagatzemen, exigint demostrar alts nivells de protecció certificats per entitats acreditades con Common Criteria.

També la diversificació de claus de cada SAM ens protegeix davant del clonat dels missatges transmesos, ja que el clonat d'un missatge d'un SAM xifrat o signat amb una clau diversificada no serveix per suplantar el missatge d'un altre SAM diferent.

- **Auditabilitat**, implementat mecanismes d'identificació única i registre de tots els SAMs utilitzat a la T-mobilitat, que s'utilitza entre altres coses, per auditar totes i cadascuna de les transaccions efectuades amb cada SUS. Aquestes transaccions s'emmagatzemen els sistemes centrals i permet fer auditories en el moment que es vulgui.
- **Càlcul del número de factura**, per garantir la unicitat del número de factura al llarg del temps, fins i tot amb canvis d'ubicació del terminal ccTIU.
- **Abstracció de la seguretat del tipus de SUS, (SCAL)**, que es un servei de seguretat que implementa els SAMs CBT que permetre que l'ús de la seguretat del SSu sigui independent del SUS (targeta), es realitzin menys autenticacions rebaixant els temps de transacció, augmenta la seguretat ja que permetre controlar l'accés a camp amb granularitat de camp i es pot configurar des del els Sistemes Informàtic Centrals en temps quasi real.

Així, amb relació als **Serveis de Seguretat**, aquest últims ja implementats i els nous a anteriors, que dona els **components de seguretat local SAM CBT**, s'han de realitzar les tasques següents:

A. Gestionar tots i cadascun dels Serveis de Seguretat que proporcionen els SAMs i assegurar la permanent disponibilitat en explotació d'acord als SLAs establerts.

En fase d'anàlisi i enginyeria l'adjudicatari haurà d'identificar tots i cadascun dels servis de seguretat local, així com descriure el casos d'ús de les activitats relacionades amb l'ús de serveis de seguretat locals.

Es requereix una atenció especial al servei de seguretat de la capa d'abstracció de la Seguretat, ja que es un servei estratègic que requereix garantir la seva disponibilitat de manera permanent. També, amb relació a les eines de proves i plataformes de gestió.

B. Definir, desenvolupar i acordar els SLA (Acord de Nivell de Servei) de cadascun dels Serveis de Seguretat local donats pels SAMs CBT, necessaris per a la protecció de les transaccions sense contacte.

En fase d'anàlisi i enginyeria, es tracta d'acordar el nivell de servei que esperem de cadascun dels serveis de seguretat local que ens estableix el nivell de qualitat.

C. Definir, desenvolupar i implementar els KPIs (Indicadors Clau de Rendiment) dels Serveis de Seguretat local donats pels SAMs CBT, necessaris per a la protecció de les transaccions sense contacte.

En fase d'anàlisi i enginyeria, es tracta d'identificar KPIs que ens ajudin a promoure la millora contínua i l'eficàcia dels serveis de seguretat local a SAMs CBT.

El licitador farà una descripció amb detall que identifiqui la seva millor proposta tècnica amb relació als Serveis de Seguretat Locals, els SLAs i els KPIs, i que estan adscrites a l'execució d'aquest Projecte que servirà de valoració per a l'adjudicació.

3.1.3. Serveis de seguretat per dispositiu – Centre HSM

A més dels serveis de seguretat locals que ofereixen els SAMs, hi ha serveis de seguretat centralitzats que utilitzen equips i actors de forma remota dintre d'un entorn controlat com és el SIC que són els Centres HSM i que completen tot el ecosistema del Sistema de Seguretat únic.

Els Centres HSM són servidors segurs que disposen de dos parts ben diferenciades:

- **HSM** (*Hardware Security Module*), una part segura, formada per un conjunt d'elements segurs tamperitzats, on la lògica que executa i els recursos que protegeix disposen de mecanismes físics de protecció contra intrusions.
- **Servidor convencional**, formada per un hardware no segur, on la lògica que s'executa no es segura que està formada per elements de xarxa, ordinadors i sistemes d'emmagatzematge convencionals. L'HSM es troba instal·lat al seu interior, comunicant-se mitjançant un bus local a ell i la lògica del servidor convencional fa us de l'HSM

Cadascuns del Sistemes Informàtics Centrals **incorpora un Centre HSM** per oferir, a més dels serveis de seguretat locals que ofereixen els SAM, els següents serveis de seguretat centralitzats disponibles per instanciar als servidors segurs, segons el seu tipus:

- **Autoritat certificadora** (AC), per controlar els elements segurs (SAMs i HSMs) autoritzats al Sistema de Seguretat es realitza mitjançant una Autoritat Certificadora. Cada element segur autoritzat al sistema ha de tenir un certificat vàlid emès per l'AC.
- **Keystore**, on s'emmagatzemen les claus del servidor segur HSM per protegir-les davant de qualsevol atac, ja que només es té accés a les claus dins del propi element segur.
- **Generació de claus**, on la generació de qualsevol clau del Sistema de Seguretat únic, té lloc a l'element segur (HSM) dels servidors segurs i no poden sortir en clar

de l'element segur sota cap concepte.

- **Distribució de claus**, que permet exportar de forma controlada claus del sistema d'un element segur a un altre, es a dir, d'un keystore a un altre.
- **Gestió de llista d'accions del SAM**, que són el mecanisme que permet actualitzar el seu contingut des dels Sistemes Informàtics Centrals.
- **Gestió del firmware dels elements segurs**, que ha de ser actualitzable "en calent" de forma atòmica i segura, és a dir, un cop distribuïts i funcionant al sistema.
- **Control d'accés per quota als SAM**, com mecanisme de protecció contra robatoris per evitar que es pugui fer un us indegut d'aquests fora del sistema,
- **Assegurar els accessos als SUS**, amb la implementació de la *Capa d'abstracció de la Seguretat de SUS* (SCAL) que és un mecanisme que permet als terminals manejar l'estructura de camps de l'ATlu (lectura, escriptura, increment, creació, eliminació, etc.), així com la seguretat dels SUS independentment del tipus concret de targeta, dels ordres APDU i de la seva seguretat.
- **Intercanvi d'informació entre SIC i SAM**, de forma segura mitjançant els Centres HSM que signen i/o encripten la informació cap als SAM, i descripten i/o comproven la informació provinent del SAM.
- **Magatzems segur d'informació**, que permet emmagatzemar informació i disposen de mecanismes de seguretat per l'accés segur al seu contingut.
- **Magatzems segur de claus**, que permet emmagatzemar claus del sistema de manera controlada, xifrada i auditada.
- **Gestió de jocs de claus de targeta**, segon els seu ús per fer desenvolupaments a l'entorn d'enginyeria, per a la integració a l'entorn de preproducció i reals a l'entorn de producció en explotació.
- **Mecanismes de diversificació de claus**, de càlcul unidireccional per mitigar el risc d'emmagatzemar claus mestres en elements distribuïts pel sistema.
- **Obtenir claus mestres**, amb mecanismes d'accés forts per permetre obtenir-les només als actors autoritzats.
- **Obtenir claus diversificades**, amb mecanismes d'accés suficients per permetre obtenir-les només als actors autoritzats.
- **Mecanisme d'autenticació**, que permet a un sistema corroborar que un actor diu que és qui és.
- **Mecanismes d'autenticació mútua**, permet a dos actors autenticar (confirmar la identitat) entre tots dos mitjançant un mitjà de comunicació no segur.
- **Obtenir clau de sessió**, que es genera durant el procés d'autenticació, generada de forma aleatòria a cada autenticació, que permet que l'accés al Suport d'Usuari Sense contacte (SUS) T-mobilitat mitjançant ordres protegides

mitjançant criptografia forta.

- **Mecanismes de signatura**, que permet que uns actors puguin generar la signatura de certa informació coneguda i que altres puguin comprovar la signatura d'aquesta informació per comprovar-ne l'autenticitat.

Així, amb relació als **Serveis de Seguretat**, aquest últims ja implementats i els nous a anteriors, que dona els components de seguretat centralitzades Centres HSM, s'han de realitzar les tasques següents:

A. Gestionar tots i cadascun dels Serveis de Seguretat que proporcionen els Centres HSMs i assegurar la permanent disponibilitat en explotació d'acord als SLAs establerts.

En fase d'anàlisi i enginyeria l'adjudicatari haurà d'identificar tots i cadascun dels serveis de seguretat centralitzats, així com descriure el casos d'ús de les activitats relacionades amb l'ús de serveis de seguretat locals.

B. Definir, desenvolupar i acordar els SLA (Acord de Nivell de Servei) de cadascun dels Serveis de Seguretat centralitzats donats pels Centres HSMs, necessaris per a la protecció de les transaccions sense contacte.

En fase d'anàlisi i enginyeria, es tracta d'acordar el nivell de servei que esperem de cadascun dels serveis de seguretat centralitzats que ens estableix el nivell de qualitat.

C. Definir, desenvolupar i implementar els KPIs (Indicadors Clau de Rendiment) dels Serveis de Seguretat local donats pels Centres HSMs, necessaris per a la protecció de les transaccions sense contacte.

En fase d'anàlisi i enginyeria, es tracta d'identificar KPIs que ens ajudin a promoure la millora contínua i l'eficàcia dels serveis de seguretat centralitzats CHSM.

El licitador farà una descripció amb detall que identifiqui la seva millor proposta tècnica amb relació als Serveis de Seguretat Centralitzats, els SLAs i els KPIs, i que estan adscrites a l'execució d'aquest Projecte que servirà de valoració per a l'adjudicació.

3.1.4. Serveis de seguretat per dispositiu – SUS

Els SUS són dispositius del sistema que s'utilitzen per emmagatzemar les dades dels títols de transport necessaris per poder viatjar per la xarxa de transports. Aquests dispositius estan en possessió de l'usuari, cosa que els fa que siguin els dispositius del sistema més propensos a ser atacats.

Els SUS T-mobilitat ofereixen i/o utilitzen els següents serveis de seguretat:

- **Magatzems segur d'informació**, que permet emmagatzemar informació i disposen de mecanismes de seguretat per l'accés segur al seu contingut.
- **Magatzems segur de claus**, que permet emmagatzemar claus del sistema de manera controlada, xifrada i auditada.

- **Canal segur de comunicació**, que impedeix l'alteració de la seqüència de dades transmesos.
- **Mecanisme transaccional d'ordres**, que permeten l'execució de comandes de forma atòmica.
- **Mecanismes anti-caiguda**, que garanteixen que l'accés al sistema de fitxer no quedin en estats indeterminats.
- **Autenticació de SUS**, cada vegada que un SUS és utilitzat al Sistema Tarifari Integrat ha de demostrar la seva pertinença al sistema. Si l'autenticació no es fa amb èxit, el SUS és rebutjat.
- **Confidencialitat**, amb relació a dades sensibles emmagatzemen als SUS que han de ser tractades confidencialment, com ara dades personals de l'usuari, si s'escau.
- **Integritat**, mitjançant la signatura de les dades com mecanisme que assegura que un actor extern al sistema no pot modificar les dades intercanviades amb els SUS ja que, en cas de fer-ho, la signatura esdevindria invàlida. La clau amb què se signen les dades és una clau de sessió que s'obté durant el procés d'autenticació.
- **No repudi**, mitjançant la implementació d'una combinació de mecanismes que assegurin el no repudi, com la diversificació de claus, la signatura de dades transmeses i la utilització de canals segurs per transmetre les dades assegura que només els actors als extrems del canal segur poden enviar missatges vàlids, evitant que un actor aliè al canal segur pugui introduir missatges clonats en la comunicació.
- **Anti-clonat**, mitjançant els mecanismes exigits a tot xip autoritzat a la T-mobilitat per protegir-se davant del clonatge de les dades que emmagatzemen, exigint demostrar alts nivells de protecció certificats per entitats acreditades con Common Criteria.
- **Auditabilitat**, implementat mecanismes d'identificació única i registre de tots SUS utilitzat a la T-mobilitat, que s'utilitza entre altres coses, per auditar totes i cadascuna de les transaccions efectuades amb cada SUS. Aquestes transaccions s'emmagatzemen els sistemes centrals i permet fer auditories en el moment que es vulgui.
- **Securitació de dades personals en la personalització planificada de SUS**, implementant mecanismes criptogràfics de protecció de dades personals en SUS que incorporen dades personals impreses quan les dades passen al llarg dels diferents processos dins de l'ecosistema T-mobilitat, SICs (ATM i Operadors), mòdul de Producció i Personalització Planificada (P3S) i el propi personalitzador.

Així, amb relació als **Serveis de Seguretat**, aquest últims ja implementats i els nous a anteriors, que dona els SUS des del punt de vista de components de seguretat distribuït, s'han de realitzar les tasques següents:

A. Gestionar tots i cadascun dels Serveis de Seguretat que proporcionen els SUS físics i virtuals i assegurar la permanent disponibilitat en explotació d'acord als SLAs establerts.

En fase d'anàlisi i enginyeria l'adjudicatari haurà d'identificar tots i cadascun dels serveis de seguretat distribuïts en SUS, així com descriure el cas d'ús de les activitats relacionades amb l'ús de serveis de seguretat locals.

B. Definir, desenvolupar i acordar els SLA (Acord de Nivell de Servei) de cadascun dels Serveis de Seguretat donats pels Suports d'Usuaris Sense contacte, necessaris per a la protecció de les transaccions sense contacte.

En fase d'anàlisi i enginyeria, es tracta d'acordar el nivell de servei que esperem de cadascun dels serveis de seguretat que donen els SUS i que ens haurà de permetre saber el nivell de qualitat aconseguida.

C. Definir, desenvolupar i implementar els KPIs (Indicadors Clau de Rendiment) dels Serveis de Seguretat local donats pels SUS, necessaris per a la protecció de les transaccions sense contacte.

En fase d'anàlisi i enginyeria, es tracta d'identificar KPIs que ens ajudin a promoure la millora contínua i l'eficàcia dels serveis de seguretat implementats en els SUS/Xips autoritzat en T-mobilitat.

El licitador farà una descripció amb detall que identifiqui la seva millor proposta tècnica amb relació als Serveis de Seguretat en SUS, els SLAs i els KPIs, i que estan adscrites a l'execució d'aquest Projecte que servirà de valoració per a l'adjudicació.

3.1.5. Nous SERVEIS DE SEGURETAT a implementar

S'identifiquen a continuació una sèrie de nous serveis de seguretat a dissenyar, desenvolupar i implementar destinats a securitzar certs processos i funcionalitats, així com utilitzar el sistema de seguretat únic com a ajuda a la gestió operativa de la T-mobilitat.

3.1.5.1. Identificació i securització dels entorns de treball

T-mobilitat disposa de tres entorns de treball:

1. **Enginyeria:** és l'entorn de treball per al desenvolupament
2. **Preproducció:** és l'entorn on es fan tot tipus de proves sense posar en risc el sistema en operació.
3. **Producció:** és l'entorn d'operació real en explotació T-mobilitat.

Cadascun d'aquests entorns requereix implementar el grau de seguretat necessari, suficient i adequat a la feina a desenvolupar.

Per exemple, sent el format de les diferents claus criptogràfiques el mateix, l'entorn d'enginyeria necessita claus criptogràfiques conegudes, l'entorn de preproducció requereix generar claus criptogràfiques exactament igual que les de producció però han

de ser conegudes pel gestor de seguretat, l'entorn de producció requereix claus criptogràfiques no conegudes per cap actor de sistema i protegides per diversos custodis.

Així, en aquest context, s'han de realitzar les tasques següents:

- A. L'adjudicatari, en fase d'anàlisi i enginyeria, haurà **d'identificar i especificar el requeriments de seguretat** pel treball segur de cadascun d'aquets tres entorns amb relació als diferents elements d'ús comú que intervenen SAM/TIU, SUS, SIC-Operador/CHSM-Operador, SIC-ATM/CHSM-ATM, Claus criptogràfiques, identificació, etc.
- B. L'adjudicatari, en fase d'anàlisi i enginyeria, haurà **dissenyar, desenvolupar i implementar** els requeriments, mecanismes i condicions de configuració a carregar als SAMs segons tipus ja sigui d'enginyeria, de preproducció i de producció, inclòs els requisits de personalització lògica i física.
- C. L'adjudicatari, al llarg del contracte, haurà **personalitzar i distribuir els SAMs** que sota l'autorització de l'ATM sol·licitin els diferents actor del sistema segon la seva necessitat (enginyeria, proves o explotació), així com **gestionar i controlar** la seva distribució i ús en el Sistema.
- D. L'adjudicatari, en fase d'anàlisi i enginyeria, haurà **dissenyar, desenvolupar** (inclou el maquinari, si s'escau) i **implementar** els requeriments, mecanismes i condicions de configuració a carregar als CHSM segons el tipus d'entorn a donar servei, ja sigui d'enginyeria, de preproducció i de producció.

El licitador farà una descripció amb detall que identifiqui la seva millor proposta tècnica del Servei de Seguretat Local a donar pels SAMs CBT amb relació als requeriments de seguretat a cadascuns dels entorns de treballs T-mobilitat, i que estan adscrites a l'execució d'aquest Projecte que servirà de valoració per a l'adjudicació.

3.1.5.2. Activació de SUS personalitzat

T-mobilitat requereix implementar una nova funcionalitat per que permeti l'enviament dels SUS personalitzats per canals de distribució no segurs que no seran utilitzables en T-mobilitat fins que el client propietari no l'activi per un canal segur.

Així, en aquest context, s'han de realitzar les tasques següents:

- A. L'adjudicatari, en fase d'anàlisi i enginyeria, haurà **d'analitzar i proposar un mecanisme basat en la generació d'un PIN d'activació mitjançant un algoritme criptogràfic** per garantir l'ús segur dels SUS personalitzats en tot el seu cicle de vida, que haurà de ser aprovat per l'ATM, així com la bateria de proves necessàries que garanteixen el seu adequat funcionament.

S'haurà d'identificar i descriure tot **el cicle de vida i casos d'ús de l'activació del SUS personalitzat** que va des de la sol·licitud del SUS, procés de personalització, generació del PIN i consum del PIN per activar el SUS per part del usuari, inclòs les millores i/o alternatives segons el canal, per exemple, amb el mòbil NFC.

- B. L'adjudicatari, haurà **desenvolupar i implementar el mecanisme d'ús de PINes**

d'activació de SUS utilitzant un algoritme criptogràfic que garanteix la seva seguretat com un nou Servei de seguretat local dins dels SAMs i dins del CHSMs.

- C. L'adjudicatari, haurà de **garantir el bon funcionament del nou servei de seguretat per l'ús de PINes d'activació de SUS** implementat abans de posar-ho en producció mitjançant la validació funcional i compliment de la bateria de proves desenvolupades a cadascuns dels tres entorns (enginyeria, preproducció i producció).

El licitador farà una descripció amb detall que identifiqui la seva millor proposta tècnica del Servei de Seguretat Local a donar pels SAMs CBT amb relació a l'activació de SUS, i que estan adscrites a l'execució d'aquest Projecte que servirà de valoració per a l'adjudicació.

3.1.5.3. Registre de Suport anònim

T-mobilitat també considera implementar la funcionalitat de registrar un SUS anònim per recuperar i traspasar a un altre SUS els drets de viatge contingut en un SUS que l'usuari ha perdut o l'han robat, i que no estan donat d'alta en T-mobilitat.

Així, en aquest context, s'han de realitzar les tasques següents:

- A. L'adjudicatari, en fase d'anàlisi i enginyeria, haurà **d'analitzar i proposar un mecanisme basat en PIN** per garantir el registre de SUS anònims als usuaris que no vulguin donar-se d'alta com a client T-mobilitat, i la recuperació i traspàs dels drets de viatges (títols de transport), a tot el seu cicle de vida, que haurà de ser aprovat per l'ATM, així com la bateria de proves necessàries que garanteixen el seu adequat funcionament.

S'haurà d'identificar i descriure tot **el cicle de vida i casos d'ús del registre i traspàs de drets de viatges de SUS perduts o robats**, que va des de la seva generació al CHSM, temps de validesa configurable i consum del PIN per recuperar i traspasar els drets de viatges, inclòs les millores i/o alternatives segons el canal, per exemple, amb el mòbil NFC.

- B. L'adjudicatari, haurà **desenvolupar i implementar el mecanisme** d'ús de PINes d'activació de SUS utilitzant un algoritme criptogràfic que garanteix la seva seguretat com un nou Servei de seguretat local dins dels SAMs i dins dels CHSMs.

L'adjudicatari, haurà **desenvolupar i implementar el mecanisme**, amb l'algoritme de generació dels PINes de registre com un nou Servei de seguretat local dins dels SAMs per la recuperació i traspàs de drets de viatge a un nou SUS.

- C. L'adjudicatari, haurà de **garantir el bon funcionament del nou servei de seguretat per l'ús de PINes de registre de SUS** implementat abans de posar-ho en producció mitjançant la validació funcional i compliment de la bateria de proves desenvolupades a cadascuns dels tres entorns (enginyeria, preproducció i producció).

El licitador farà una descripció amb detall que identifiqui la seva millor proposta tècnica del Servei de Seguretat Local a donar pels SAMs CBT amb relació al registre de suport anònim, i que estan adscrites a l'execució d'aquest Projecte que servirà de valoració per a l'adjudicació.

3.1.5.4. Gestió de versions d'ATlu

El Sistema Tarifari Integrat en viu que requereix evolucions contínues que en major o menor mesura afecten tots els elements d'ús comú.

Un element de difícil evolució és l'Aplicació de Transport Interoperable única (ATlu) pel fet que emmagatzemen els drets de viatge adquirits pel client que instanciats als SUS que estan en possessió de l'usuari.

Tot i que la versió de versions d'ATlu en un procés transversal en què intervenen diferents elements el SAM haurà d'implementar un Servei de Seguretat per gestionar en explotació l'ús de versions d'ATlu.

Així, en aquest context, s'han de realitzar les tasques següents:

- A. L'adjudicatari, haurà **desenvolupar i implementar el mecanisme de seguretat a implementar per gestionar l'ús de versió de l'ATlu en explotació** que garanteix la seva seguretat com un nou Servei de seguretat local dins dels SAMs CBT.
- B. L'adjudicatari, haurà de **garantir el bon funcionament del nou servei de seguretat implementat per a la gestió de l'ús de versions d'ATlu en explotació** abans de posar-ho en producció mitjançant la validació funcional i compliment de la bateria de proves desenvolupades a cadascuns dels tres entorns (enginyeria, preproducció i producció), així com el desenvolupament i implementació de les eines necessàries.

El licitador farà una descripció amb detall que identifiqui la seva millor proposta tècnica de la gestió de versions de l'ATlu, i que estan adscrites a l'execució d'aquest Projecte que servirà de valoració per a l'adjudicació.

3.1.5.5. Securitització de dades personals en la personalització de SUS

Hi ha casos en el procés de personalització massiva de SUS que incorporen dades personals, com poden ser les corresponents a la T-Empleat o a la T-Rosa, s'han comunicar aquestes dades sensibles des de la font (entitat sol·licitant) i els diferents sistemes fins arribar al proveïdor de la personalització, passant, com a mínim, per altres sistemes com el SIC d'ATM i el P3S (mòdul de Producció i Personalització Planificada de SUS).

En aquest context, s'hauran d'implementar mecanismes per garantir la protecció i el control d'aquesta informació sensible.

Així, en aquest context, s'han de realitzar les tasques següents:

- A. L'adjudicatari, haurà **dissenyar, desenvolupar i implementar els mecanismes de seguretat criptogràfics** necessaris per la protecció de dades personals quan es fan comandes de personalització massiva de SUS i eines associades.
- B. L'adjudicatari, haurà de **garantir el bon funcionament del nou servei de seguretat implementat per a la securització de dades personals** mitjançant la validació funcional i compliment de la bateria de proves desenvolupades a cadascuns dels tres entorns (enginyeria, preproducció i producció), així com el

desenvolupament i implementació de les eines necessàries.

El licitador farà una descripció amb detall que identifiqui la seva millor proposta tècnica per a la seguretat en els processos de personalització massiva de SUS que incorporen dades personals, i que estan adscrites a l'execució d'aquest Projecte que servirà de valoració per a l'adjudicació

3.2. Gestió en explotació de COMPONENTS físics del SSu

Els serveis de seguretat del SSu es carreguen en diferents components físics amb l'objectiu de posar-los a disposició del sistema segons les necessitats.

Bàsicament, s'identifica dues tipus de components a gestionar:

- Els Mòduls d'Accés Segur (SAMs CBT) per donar aquests serveis quan cal fer transaccions ràpides que anomenem seguretat local,
- Els Centres d'Hardware D'Accés Segur (CHSMs) en altres situacions que anomenem seguretat centralitzada.

3.2.1. Gestió en explotació dels MÒDULS D'ACCÉS SEGURS, SAMs

El Mòdul d'Accés Segur o SAM és un element segur en format SIM amb un xip microprocessador amb característiques criptogràfiques sobre el qual s'implementen serveis de seguretat, així com emmagatzema les claus criptogràfiques.

Està dotat de fortes mesures de seguretat anti-tamperització que el protegeix d'atacs de diversos tipus (de canal lateral, d'enginyeria inversa, d'injecció de fallades...) que fan que sigui extremadament difícil, si no impossible l'extracció de les claus del seu interior.

Els SAMs no tenen bateria, de manera que per funcionar prenen l'alimentació del terminal sense contacte on estan instal·lats.

La missió dels Mòduls SAM és la de proporcionar Serveis de seguretat (autenticació, confidencialitat, integritat, no repudi ..., capa d'abstracció de la seguretat dels protocols i mecanismes de seguretat utilitzats en els suports SUS autoritzats en el sistema, etc.) en temps real allí on el Sistema Tarifari Integrat requereixi de protecció.

Un SAM s'utilitza de diferent manera depenent de l'estat en el seu cicle de vida.

Els estats es defineixen des de dos punts de vista del Sistema, segons la fase en què es troba:

- Fabricació, Pre-operacional, Operacional, Post-operacional i Destrucció.
- Diferents tipus de SAM (Enginyeria, Proves, Producció ...).

I en funció del propi cicle de vida funcional del SAM:

- Sense Sistema Operatiu, Sense kernel, Securitzat, Personalitzat, Actiu, Suspès, Desactivat, Compromès i Destrut.

La transició entre estats requereix registrar l'esdeveniment per auditar l'estat en què es

troba el SAM en tot moment.

El Gestor de Seguretat de SAM té la missió de gestionar tots i cada un dels estats del cicle de vida del SAM.

Entre altres funcionalitats de baix nivell, el Gestor de SAM s'encarrega de gestionar:

- Firmwares que necessita el SAM per funcionar com el firmware de base, reprogramacions, criptografia forta i aplicacions (serveis).
- Sistema d'arrencada,
- Versionat,
- Ordres de personalització,
- Altre

Així, amb relació a la gestió dels **Components SAMs CBT en explotació**, que donen els Serveis de seguretat local una vegada estan instal·lats als Terminals sense contacte T-mobilitat, s'han de realitzar les tasques següents:

A. Gestionar, controlar i mantenir actualitzats tots i cadascun dels estats del cicle de vida dels SAMs CBT fabricats i distribuïts per cadascun dels entorns de treball, enginyeria, proves i producció al llarg de tot el contracte.

En fase d'anàlisi i enginyeria l'adjudicatari haurà **d'identificar de manera explícita l'estat** tots i cadascun dels servis de seguretat distribuïts a cadascun dels entorns, així com **revisar i actualitzar tots els casos d'ús** de les activitats relacionades amb l'ús de serveis de seguretat locals.

B. Revisar, actualitzar, optimitzar, si s'escau, i mantenir els processos d'alta i personalització física i lògica de SAMs CBT ja en explotació, corresponent a la **fase pre-operacional** del SAM.

En fase d'anàlisi i enginyeria, s'analitzarà, es modificarà i es simplificarà, si es possible, els processos de:

- Personalització física garantint la identificació única i registre que dona el SIR,
- "Càrrega de firmware", mitjançant la plantilla de personalització,
- Alta de SAM en el Sistema de Seguretat únic,
- "Càrrega de Claus", mitjançant la plantilla d'exportació de Keysets,
- Personalització lògica en funció del rol en el sistema (Validació, recàrrega, consulta, etc.).

En fase d'anàlisi i enginyeria l'adjudicatari haurà d'identificar de manera explícita el pla de treball per a l'actualització dels processos de personalització segura de SAMs CBT, així com l'actualització de sistema de manteniment de SAM CBT en explotació.

C. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir la Plataforma de personalització de SAMs CBT al llarg del contracte i corresponent a la **fase pre-operacional**.

En fase d'anàlisi i enginyeria, es tracta d'analitzar explícitament el desenvolupament de la plataforma de personalització de SAM CBT per a la seva actualització i evolució tècnica, optimització i simplificació dels processos, si s'escau, etc..

D. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir el programa de C&A de personalització segura de SAMs CBT al llarg del contracte, corresponent a la fase pre-operacional.

En fase d'anàlisi i enginyeria, es tracta d'analitzar explícitament el programa de conformitat i Acceptació de la personalització segura de SAM CBT per a seva actualització, evolució i adaptació als processos de personalització segura de SAM CBT actualitzat.

E. Executar el Programa de C&A dels SAMs sol·licitats al llarg del contracte, corresponent a la fase pre-operacional per garantir la seva funcionalitat en explotació.

El licitador haurà de detallar àmpliament la seva proposta tècnica en relació a les tasques de millora i optimització dels processos i funcionalitats de la personalització segura de SAM CBT, corresponent a la **fase pre-operacional** del SAM CBT, així com de la plataforma i eines associades, que servirà de valoració per a l'adjudicació.

F. Revisar, actualitzar, optimitzar, si s'escau, i mantenir els processos corresponent a la fase operacional del SAM CBT.

En fase d'anàlisi i enginyeria, s'analitzarà, es modificarà i es simplificarà, si s'escau, els processos de distribució, instal·lació i monitorització dels SAMs CBT en explotació.

Especial atenció es tindrà amb la proposta tècnica per al control i seguiment de SAMs CBT en explotació mitjançant el disseny, desenvolupament i implementació d'eines d'ajuda a la monitorització en temps real del parc de SAMs CBT en explotació.

G. Revisar, actualitzar, optimitzar, si s'escau, mantenir i executar, tantes vegades com sigui necessari, els processos reprogramació segura en calent dels SAMs CBT en explotació corresponent a la fase operacional.

En fase d'anàlisi i enginyeria, s'analitzarà i es millorarà, si s'escau, els processos de reprogramació en calent segura dels SAMs CBT en explotació.

Especial atenció es tindrà amb la proposta tècnica per al control i seguiment dels processos d'actualització de SAMs en calent que inclou actualització ràpida, segura i atòmica, així com un potent programa de proves.

El licitador haurà de detallar àmpliament la seva proposta tècnica en relació a les tasques de control i seguiment a implementar per a la **fase operacional** del SAM CBT, que servirà de valoració per a l'adjudicació.

H. Revisar, actualitzar, optimitzar, si s'escau, i mantenir els processos corresponent a la fase post-operacional del SAM CBT.

En fase d'anàlisi i enginyeria, s'analitzarà, es modificarà i es millorarà, si s'escau, els processos de gestió i control de la vida útil dels SAMs CBT en explotació, es a dir, substitució per claus compromeses, per vida útil final i anàlisis derivats de les diferents casuístiques sorgides.

El licitador haurà de detallar àmpliament la seva proposta tècnica en relació a les tasques de control i seguiment a implementar per a la **fase post-operacional** del SAM CBT, que servirà de valoració per a l'adjudicació.

3.2.2. Gestió en explotació dels CENTRES HSMs

A més dels Serveis de seguretat locals que ofereixen els mòduls SAM, el Sistema Tarifari Integrat ha definit serveis de seguretat centralitzats que utilitzen equips i actors de forma remota dins d'un entorn controlat com és el SIC.

Aquests complementen l'ecosistema del sistema de seguretat únic i es generen per altres necessitats de protecció del sistema.

Un CHSM es un sistema que per si mateix, a nivell lògic, funciona com un sol element, però físicament té una arquitectura que està format pels següents elements:

- **Node HSM**

Un node és la unitat funcional mínima d'un CHSM. Un CHSM pot donar servei amb un sol node, però s'instal·len entre 3 i 4 per aconseguir alta disponibilitat i per aconseguir major potència de computació ja que aquesta és proporcional a la quantitat de nodes en servei.

Els nodes són autònoms i auto-continguts i, per tant, la caiguda d'un node no afecta a la resta.

Així, un node, a la seva vegada està compost per:

- o **Mòdul HSM (Hardware Secure Module)**

És un component segur, format per un conjunt d'elements segurs, on la lògica s'executa i els recursos que protegeix disposen de mecanismes físics de protecció contra intrusions.

Els mòduls HSM, físicament són plaques PCIe i abans de poder posar-se en explotació, han de donar-se alta en el SSu i ser inicialitzades pel gestor del SSu.

El seu contingut, a nivell lògic, està organitzat en particions i aquestes, a l'arrancar, estan desactivades, i per tant, l'accés al seu contingut està bloquejat. Per poder accedir al contingut de les particions, s'han d'activar.

- o **Ordinador host**

Està format per un hardware no segur, on la lògica que s'executa no és segura.

És un servidor estàndard per a treball en CPDs amb CPUs Xeon, interfícies de xarxa i sistemes d'emmagatzematge convencionals.

El HSM s'instal·larà en el seu interior i la lògica del ordinador fa ús del HSM.

- **Infraestructura de xarxa**

Són aquells elements necessaris per a que els servidors segurs es comuniquin de la forma adequada.

Els equips que els componen són dos firewalls/routers configurats en alta disponibilitat i el cablejat i adaptadors necessaris per a interconnectar els firewalls/routers amb els nodes.

Apart de los firewalls/routers, els CHSM disposen de balancejadors de càrrega que s'encarreguen de distribuir les peticions entre els diferents nodes del CHSM. Els balancejadors de càrrega dels CHSM no són elements en un CHSM hi ha tants balancejadors de càrrega com nodes. Els balancejadors de càrrega estan sincronitzats entre sí i configurats en alta disponibilitat, sent necessari tan sols un balancejador de càrrega actiu per a que el sistema funcioni correctament.

- **Activador remot de mòduls HSM**

Són els elements físics i lògics necessaris per activar els mòduls HSM remotament.

Aquests activadors són els responsables d'activar les particions dels HSM. El mecanisme d'activació, a part dels HSM objecte de l'activació, requereix d'un lector de targetes amb contactes estàndard PC/SC, targetes activadores i un software d'activació remota

Així, amb relació a la gestió dels **Components CHSMs en explotació**, que donen els Serveis de seguretat centralitzat una vegada estan instal·lats als Sistemes Informàtics Centrals T-mobilitat, s'han de realitzar les tasques següents:

A. Gestionar, controlar i actualitzar, si s'escau, l'Arquitectura física dels Centres HSM instal·lats i distribuïts per cadascuns dels entorns de treball, enginyeria, proves i producció al llarg de tot el contracte.

En fase d'anàlisi i enginyeria l'adjudicatari haurà **d'analitzar i revisar explícitament l'arquitectura dels Centres HSM, trobar punts de millores d'optimització i/o de seguretat.**

B. Revisar, actualitzar, optimitzar, si s'escau, els processos de gestió que formen part de la infraestructura de gestió segura de claus i informació que assegura el contingut del Centre HSM:

- o **Activació**, que permet l'activació remota d'un node HSM,
- o **Configuració**, que permet la configuració centralitzada dels CHSM des d'un servidor SFTP per part del gestor del Sistema de Seguretat únic.
- o **Registre**, que permet reportar registres de Seguridad que s'han generats

durant l'exploació del sistema T-mobilitat.

- o **Monitorització**, que permet auditar el estat del CHSM mitjançant diferents canals (SYSLOG i SNMP) i activar les alarmes corresponents.
- o **Relotge de temps real (RTC)**, que permet la sincronització horària amb la resta del sistema.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: **d'analitzar i revisar explícitament els processos de gestió dels Centres HSM.**

C. Revisar, actualitzar, optimitzar, si s'escau, els serveis operacionals que són útils per l'operació segura del CHSM mitjançant la publicació d'APIs o HTTP, entre els quals estan:

- o **Processament d'informació a ccTIU**, que permet processar la informació generada pels ccTIU amb la finalitat de verificar la veracitat dels registre transaccionals generats en els terminals gestionats per aquest SIC.
- o **Securització d'informació cap a ccTIU**, que permet xifrat complet de paquets, parcial, signar..., acoblats binaris d'ODs, llistes d'accions, configuracions del STI, etc.
- o **Firma de SIC**, que permet que el SIC pugui firmar informació per certificar la seva autoria. La seva utilitat és firmar una determinada informació que s'intercanvia amb altres SIC, o amb altre autoritats.
- o **Increment on-line de quota de SAM**, que permetre incrementar la quota que bloqueja els SAMs en explotació.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: **d'analitzar i revisar explícitament els serveis operacionals que donen els Centres HSM.**

D. Revisar, actualitzar, optimitzar, si s'escau, la infraestructura de comunicacions dels CHSM centralitzats amb relació a les altes exigències de disponibilitat i redundància dels sistemes: com són el disseny físic, el disseny lògic, adreçament IP, etc.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: **d'analitzar i revisar explícitament la infraestructura de comunicacions dels CHSM.**

E. Revisar, actualitzar, optimitzar, si s'escau, el sistema de monitorització dels CHSM, mitjançant l'anàlisi, control i seguiment de les mètriques de monitorització que es generen els diferents elements que formen part del CHSM (routers, balancejadors i nodes HSM), dels sistemes de monitorització utilitzats (activa (POLLS), passiva (TRAPS) o combinació d'ambdues).

En fase d'anàlisi i enginyeria l'adjudicatari haurà: **d'analitzar i revisar explícitament el sistema de monitorització dels CHSM.**

F. Revisar, actualitzar, optimitzar, si s'escau, el programa de proves específiques d'infraestructura i alta disponibilitat dels CHSM en les quatre línies d'actuació: Proves de serveis, proves d'activació, proves de monitorització i

proves de manteniment.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament el sistema de proves específiques d'infraestructura i alta disponibilitat dels CHSM, així com la seva execució.

G. Revisar, actualitzar, optimitzar, si s'escau, el casos d'ús, de les activitats relacionades amb l'ús de serveis de seguretat centralitzats, es a dir, les interaccions que es realitzen entre actors del Sistema de seguretat únic amb relació als CHSM.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament els casos d'ús relacionats amb els Centres HSMs.

El licitador haurà de detallar àmpliament la seva proposta tècnica en relació a les tasques per a la gestió tècnica dels Centres HSMs, que servirà de valoració per a l'adjudicació.

3.2.3. Gestió en explotació dels DISPOSITIUS MÒBILS NFC

La T-mobilitat integra la Tecnologia NFC al centre de l'escenari com a element impulsor de serveis en temps real utilitzant els dispositius mòbils intel·ligents NFC en els dos modes de treball que es poden utilitzar:

- Com un Terminal sense contacte d'ús personal en el moment i lloc que decidim: "*Com a Terminal d'Interacció amb l'Usuari (TIU personal)*".
- Com a nou Suport sense contacte per accedir directament al Transport "*Com a nou Suport d'Usuari Sense contacte (SUS NFC virtual)*".

La incorporació de:

- El Protocol de comunicacions "*Near Field Communication*" (NFC) als dispositius mòbils intel·ligents (smartphones), i d'altra banda,
- La Tecnologia "*Host Card Emulation*" (HCE) en el Sistema Operatiu Android.

Unit a la versatilitat de comunicació que tenen aquests dispositius mòbils intel·ligents, ofereix grans oportunitats de millorar l'experiència client i ajuda a realitzar un viatge intel·ligent.

Un viatge intel·ligent implica que el dispositiu mòbil NFC ha d'interactuar amb tota la infraestructura de transport i treballar junts per generar una experiència senzilla, en temps real i interactiva pel viatger, però sense oblidar implementar els mecanismes de seguretat que protegeixin les dades del viatger i el seu dret a viatjar de manera anònima.

Donat que la tecnologia HCE ofereix una seguretat limitada el sistema implementa serveis i mecanismes de seguretat específics per mitigar els riscos associats, com:

- **Servei de Tokenització.**

Que inclou la generació dels tokens mitjançant tècniques criptogràfiques

implementades de manera preceptiva dins d'un servidor segur, així com la modificació dels tokens mitjançant els serveis criptogràfics implementats, també dins d'elements segurs.

La gestió de tokens té en compte processos i funcionalitats com l'autorització de modificació de tokens, firma i xifrat de tokens, validesa i ampliació temporal dels tokens, mecanismes per a la transferència segura de tokens, etc.

- **Sistema de gestió de claus criptogràfiques:**

Que inclou la gestió de claus criptogràfiques específiques per a la protecció de dades utilitzades en entorns insegurs com som els dispositius mòbils NFC i la seva interacció amb el Sistema Tarifari Integrat sense contacte.

L'ecosistema mòbil inclou processos i funcionalitats com la:

- o Generació d'aquestes claus en funció del lloc on s'emmagatzemen, així com l'intercanvi segur amb els sistemes centrals i/o amb els elements segurs,
- o Utilització de claus criptogràfiques diversificades,
- o Autenticació mútua i ús de claus de sessió,
- o Limitació de l'ús temporal de claus criptogràfiques.

- **Mecanismes de gestió segura:**

Que inclou la gestió dels mecanismes i els serveis de seguretat per a la protecció de funcionalitats addicionals corresponen a l'ecosistema mòbil.

Conté processos i funcionalitats com:

- o Mecanismes segurs anti-caigudes per protegir la integritat de les dades.
- o Access segur al sistema d'arxius,
- o Signatura segura de transaccions sense contacte,
- o Mecanismes segurs de registre i autenticació d'usuaris,
- o Mecanismes criptogràfics que assegurin canals segurs per a l'intercanvi de dades.
- o Mecanismes criptogràfics per generar i modificar la validesa dels tokens,
- o Mecanismes per la detecció de mòbils "root"...

Així, amb relació a la **gestió segura de dispositius mòbils NFC en explotació**, per utilitzar aquests dispositius NFC a T-mobilitat tant com Suport sense contacte com a terminal sense contacte, s'han de realitzar les tasques següents:

A. Revisar, actualitzar, optimitzar, si s'escau, l'estructura de l'ATlu tokenitzada per el seu ús als dispositius mòbils NFC, gestió d'accés, autorització de modificació, targeta virtual, validesa temporal, verificacions de tokens, mecanismes criptogràfics emprats, transferència de tokens, gestió PKI, etc.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament l'estructura de l'ATlu tokenitzada per el seu ús als dispositius mòbils NFC, així com

els processos, mecanismes i algorismes necessaris per a la gestió segura de tokens.

- B. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir** el programa de proves específic per garantir la tokenització segura de l'ATIU en els dispositius mòbils NFC.

En fase d'anàlisi i enginyeria, es tracta d'analitzar explícitament el programa de proves específics per a la securització en l'ús de dispositius mòbils NFC a la T-mobilitat.

El licitador haurà de detallar àmpliament la seva proposta tècnica en relació a les tasques per a la gestió segura de dispositius mòbils NFC a la T-mobilitat, que servirà de valoració per a l'adjudicació.

3.2.4. Serveis de Manteniment integral del SSu

El Sistema de Seguretat únic és un element crític del Sistema Tarifari Integral T-mobilitat i com a tal cal mantenir-lo per tal que estigui disponible sempre.

Per garantir el funcionament general del Sistema de Seguretat únic, tots i cada un dels components i procediments que el formen requereixen un **Manteniment Integral específic d'Alta Disponibilitat en base a un monitoratge permanent**, un control local i remot, així com una permanent revisió en explotació que permeti:

- Preveure actuacions de forma anticipada,
- Actualització en la mesura que s'identifiquin millores o es requereixin noves funcionalitats, així com
- Planificació del cicle de vida tecnològic dels components que l'integren.

Les principals actuacions es concreten en els següents apartats:

1. Identificació d'equips i aplicacions

El servei de manteniment abasta tots i cada un dels components i programes (en endavant equips de forma genèrica). Concretament s'inclouen:

- o Arquitectura del Sistema de Seguretat criptogràfica,
- o Infraestructura de gestió de claus criptogràfiques (inclosos els processos i funcionalitats en explotació),
- o Plataforma de gestió de seguretat criptogràfica local (processos i funcionalitats de gestió del cicle de vida en explotació dels mòduls SAMs, inclosos),
- o Serveis de seguretat específics d'àrea local desplegats en els mòduls SAMs en explotació,
- o Els propis Mòduls SAMs desplegats al sistema, així com el control de monitorització en explotació.
- o Plataforma de gestió de seguretat criptogràfica centralitzada (processos i funcionalitats de gestió de tots els components de seguretat).

- o Serveis de seguretat específics d'àrea centralitzada (en el núvol) despleats en els Centres HSMs
- o Els Centres HSM instal·lats a cada un dels Operadors de Transport i l'ATM,
- o Centre HSM de respatller (backup),
- o Centre HSM d'enginyeria/preproducció,
- o Plataforma de gestió de seguretat criptogràfica per dispositius mòbils NFC (processos i funcionalitats en explotació inclosos),
- o Serveis de seguretat específics en dispositius mòbils NFC,
- o Gestió documental: manteniment i actualitzacions en explotació.

2. Actuacions preventives

Corresponen a les accions destinades a garantir la fiabilitat dels equips i components instal·lats abans que pugui produir-se un incident, problema o avaria per deteriorament, inclou el manteniment programat i manteniment predictiu.

Pel que fa als elements segurs físics com els mòduls SAMs i Centres HSMs implica actuacions periòdiques de les operacions, transaccions realitzades, paràmetres operatius, rendiment i possibles indicadors d'anticipació a fallades.

El licitador haurà d'especificar àmplia i detalladament la seva proposta tècnica en relació a les actuacions preventives necessàries en la Fase d'Explotació per dur a terme el manteniment preventiu dels diferents equips i components del Sistema de Seguretat criptogràfic.

3. Actuacions correctives

Corresponen a la correcció d'errors que es puguin produir en el funcionament de sistema que inclouen el manteniment:

o Manteniment correctiu de primer nivell.

És aquell que pot dur a terme personal no especialitzat, i inclou reparacions senzilles.

o Manteniment correctiu de segon nivell.

És aquell efectuat per personal qualificat (si és el cas, amb equip especial) a les mateixes instal·lacions. Inclourà la reparació de tot tipus d'avaries dels equips instal·lats a les seves dependències.

o Manteniment correctiu de tercer nivell.

Es refereix a la retirada de l'equip o del component de l'equip que tingui un mal funcionament i la seva reparació per part del subministrador en les seves pròpies instal·lacions.

El manteniment correctiu és el resultat d'una incidència a causa d'una situació en la que algun dels equips o programes en manteniment funciona de manera incorrecta o errònia.

Les accions correctives de qualsevol nivell, inclouen la identificació d'incidències funcionals i tècniques, detectades en el funcionament del sistema en explotació, i que requereixin la modificació i/o actualització d'alguns dels seus components.

Qualsevol actuació sobre el programari motivada per una fallada o error serà considerada sempre com a activitat pertanyent a l'assistència tècnica correctiva.

S'ha de disposar d'elements o components de substitució, especialment dels Centres HSMS, per a reposició temporal de l'equip o component malmès mentre es repara o s'adquireix l'original, el subministrament del qual no està inclòs en l'abast.

També s'inclouen els treballs d'anàlisi i resolució d'incidències que, sense suposar canvi o modificacions, puguin requerir actuacions tècniques, revisió i modificació de dades, revisió i modificació de configuracions, etc.

Amb relació a la disponibilitat del servei s'implementaran SLAs segons l'afectació al servei del portal web corresponen. A mode de referència s'exposa a continuació.

Incidència (categoria)	Temps de resposta	Temps resolució
Crítica	10 minuts en 24x7	2 horas en 24x7
Alta	20 minuts en 24x7	4 horas en 24x7
Mitjana	1 hora en 10x5	8 horas en 24x7
Baixa	Segons pràctica habitual de mercat	Segons pràctica habitual de mercat

S'entén per incidència:

- Crítica: pèrdua completa o falta de disponibilitat total del servei
- Alta: pèrdua o falta de disponibilitat parcial del servei.
- Mitjana: pèrdua menor del servei: errors puntuals o problemes de rendiment
- Baixa: incidència que no té impacte en el servei.

S'entén per:

- Temps de resposta: el temps en què l'adjudicatari registra la incidència en el sistema de gestió de tickets i aquesta es comunica als destinataris, mitjançant el workflow i canals establerts del codi, la definició i la tipificació de gravetat del mateix.
- Temps de resolució: temps que passa des de l'inici de la incidència (i no des del temps de resposta), fins al restabliment complet del servei, és a dir, fins que les alarmes i els sistemes de monitorització tornin notificar que el servei és correcte.

Així, amb relació a la **gestió dels serveis de manteniment integral del SSu en explotació**, de cada un dels seus components i els procediments que implementa, s'han de realitzar les tasques següents:

A. Revisar, actualitzar, i optimitzar, si s'escau, dels Serveis de Manteniment

integral del SSu en explotació que garanteix l'alta disponibilitat del SSu que requereix el Sistema Tarifari Integrat T-mobilitat.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament els Serveis de manteniment integral ja en explotació a fi de millorar, si s'escau, fer ajustos i modificacions a les eines i el programari de les plataformes.

- B. Revisar, actualitzar, optimitzar, si s'escau, i identificar els Equips i aplicacions dels SSu que són objecte de manteniment** identificant, al menys, la seva arquitectura, funcionalitat i nivell de criticitat en el sistema.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament els Equips i Aplicacions a mantenir en explotació, incloses les plataformes tecnològiques i eines associades al manteniment.

- C. Revisar, actualitzar, i optimitzar, si s'escau, els Sistemes de monitorització permanent** dels diferents equips i eines associades a la monitorització a fi de mantenir el nivell de qualitat esperat.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament els sistemes de monitorització ja en explotació, incloses les plataformes tecnològiques i eines associades al manteniment.

- D. Revisar, actualitzar, i optimitzar, si s'escau, els Sistemes de manteniment preventiu** dels diferents equips i eines associades per garantir la seva fiabilitat i preveure possibles incidències, problemes o averies per deteriorament.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament els sistemes de manteniment preventiu, incloses les plataformes tecnològiques i eines associades al manteniment, a fi de millorar la qualitat del sistema en qualsevol dels seus aspectes: reestructuració del codi, clarificació del codi, optimització del rendiment i eficiència, etc.

- E. Revisar, actualitzar, optimitzar, si s'escau, i disposar dels equips de recanvi** de cada element per a la substitució temporal en cas de dur a terme una acció correctiva de nivell 3, mentre l'equip malmès es repara o es decideix adquirir un altre original.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament els equips de recanvi i assegurar que continuen sent disponibles i funcionant correctament.

- F. Revisar, actualitzar, i optimitzar, si s'escau, els Sistemes de manteniment correctiu** resultat de la identificació d'una incidència en el SSu, degut a que alguns dels seus equips o component funciona de forma incorrecta o errònia.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament els nivells d'accions correctives (de primer, segon i tercer nivell), els nivells d'incidències, estat d'una incidència, temps i compromís de resposta i petites evolucions del SSu com a resposta a la resolució d'incidències i problemes, a fi de millorar la qualitat del sistema en qualsevol dels seus aspectes: reestructuració del codi, clarificació del codi, optimització del rendiment i

eficiència, etc..

El licitador haurà d'especificar de manera àmplia i detallada la seva proposta tècnica en relació a la revisió del Sistema de Manteniment Integral del SSu ja en explotació, que servirà de valoració per a l'adjudicació.

3.3. Infraestructura de Gestió de CLAUS I EINES associades al SSu

Quan es fa ús de xifrat criptogràfic és obligatori alinear els processos a les bones pràctiques recomanades pels organismes competents. En aquest context, amb la utilització d'algoritmes criptogràfics coneguts i contrastats per la comunitat de criptoanàlisi es transfereix el risc des de les dades a protegir, en el nostre cas les transaccions sense contacte, a una **gestió segura de les CLAUS criptogràfiques** utilitzades.

Les **CLAUS criptogràfiques formen el nucli** de tota informació informàtica basada en el xifrat criptogràfic. Igual que en el món real, de res serveix la fortalesa d'un algoritme si la clau cau en mans equivocades.

Generalment, a mesura que augmenten els actius per on passen les transaccions sense contacte protegides mitjançant xifrat criptogràfic, **s'incrementa també el nombre de claus a gestionar**.

La forma tradicional de gestionar claus de xifrat és un procés manual que requereix molts recursos i la participació de diverses persones i funcions que implica un **alt risc d'errors humans**.

La millor manera de protegir les claus criptogràfiques és a través de la implantació d'una **INFRAESTRUCTURA (Plataforma) d'alta seguretat** com a suport a l'ús de tècniques criptogràfiques extrem a extrem, que van des d'algoritmes criptogràfics contrastats, fins a la gestió segura de les claus criptogràfiques utilitzades, passant per la utilització de maquinari segur en la generació, l'intercanvi i l'emmagatzematge de serveis i claus criptogràfiques.

La Infraestructura d'alta seguretat està basada en la utilització de **servidors d'alta seguretat que tenen instanciats serveis en funció del tipus**, com: d'Autoritat Certificadora, KeyStore; Generació de claus; Gestió de llistes d'acció del SAM; Gestió de firmware dels elements segurs; Control de quotes; Autenticar accessos als diferents Suports d'Usuari sense Contacte (SUS); Intercanvi d'informació SIC i SAM; Intercanvi d'informació entre SICs...

Aquesta infraestructura és implementada sota els següents focus o enfocaments complementaris:

- Un **enfocament estratègic** basat en les bones pràctiques recomanades en els estàndards internacionals, a l'objecte de:
 - o Detectar i prevenir la manipulació de jocs de claus criptogràfiques, així com,
 - o Permetre certificar que una clau realment pertany a una entitat autoritzada en el sistema.
- Un **enfocament tàctic** basat en principis i la definició de requeriments simples i clars de compliment obligatori per a la protecció enfront:
 - o La manipulació, pèrdua o destrucció de claus al llarg de tot el cicle de vida de

l'ús de les claus,

- o La divulgació no autoritzada de claus criptogràfiques del sistema.
- Un **enfocament operacional** basat en normes i estàndards de seguretat acreditats, és a dir, procediments i mètodes que donin respostes segures a:
 - o La generació de claus pels diversos serveis de seguretat criptogràfics,
 - o L'obtenció de certificats de les claus generades,
 - o La distribució de claus criptogràfiques als usuaris,
 - o L'emmagatzematge segur de claus per al seu ús en el sistema,
 - o L'activació i/o canvi de claus criptogràfiques,
 - o La revocació de claus criptogràfiques.
 - o La recuperació de claus perdudes o corruptes,
 - o L'arxiu de claus, per històric d'informació,
 - o La destrucció de claus,
 - o El registre i auditories de les activitats relacionades amb la gestió de claus.

El resultat d'aplicar protecció contra la manipulació, pèrdua o destrucció de claus i/o divulgació no autoritzada comporta la utilització preceptiva dels anomenats **elements segurs** que són equips físicament protegits contra atacs a la infraestructura tecnològica del sistema.

Els elements segurs físics són els equips on s'emmagatzemen **claus criptogràfiques**, així com els **serveis i mecanismes de seguretat** que garanteixen una adequada protecció de les transaccions sense contacte i altra informació sensible en el sistema.

Els principals, però no únics, serveis i mecanismes de seguretat criptogràfics implementats en elements segurs van en la línia de garantir **l'autenticació, la confidencialitat, la integritat i el no repudi** de totes i cadascuna de les transaccions sense contacte dutes a terme en el Sistema.

Així, amb relació a la **Plataforma de seguretat criptogràfica** per a la gestió principalment de les claus criptogràfiques del SSu en explotació, s'han de realitzar les tasques següents:

- A. Revisar, actualitzar, i optimitzar, si s'escau,** la Plataforma de seguretat criptogràfica ja en explotació que implementa els processos funcionals principals que es poden automatitzar des del punt de vista de l'arquitectura de la plataforma, i que permetre:
 - Gestió de claus criptogràfiques,
 - Gestió de SAMs CBT
 - Gestió de Plantilles
 - Gestió de KeySet de claus
 - Gestió d'equips

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar

explícitament l'arquitectura de la plataforma de seguretat criptogràfica.

- B. Revisar, actualitzar, i optimitzar, si s'escau, els processos de gestió de claus criptogràfiques:** acreditació dels actors mitjançant infraestructura PKI i els seus components: autoritat certificadora, les estructures de dades jerarquitzades, petició de signatura de certificat, certificat o autorització per part de la CA, keystore, generació, identificació, diversificació i distribució de claus, gestor de funcionalitats, servidor de seguretat, cerimònia de claus, registre i auditories.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament els processos de gestió de claus criptogràfiques.

Especial atenció a l'eina visual que es connecta al servidor de seguretat i permet realitzar accions per gestionar la seguretat: consultar els elements segurs, registres d'auditoria dels HSM, realitzar cerimònia de claus, Crear CA, Crear PINes al Keystore, donar d'alta, personalitzar i inicialitzar SAM, crear particions HSM, etc.

- C. Revisar, actualitzar, i optimitzar, si s'escau, els processos de gestió de SAMs CBT i centres HSM** que permet donar d'alta, personalitzar-los lògicament mitjançant plantilles de personalització, consultar el seu estat, destrucció lògica del SAM, entre altres, per a cadascun dels tipus de SAMs (enginyeria, pre-producció i producció).

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament els processos de gestió de SAMS CBT.

- D. Revisar, actualitzar, optimitzar, si s'escau, el casos d'ús,** de les activitats relacionades amb infraestructura de gestió de claus criptogràfiques T-mobilitat, es a dir, les interaccions que es realitzen entre actors del Sistema de seguretat únic amb relació a l'ús segur de les claus criptogràfiques

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar i revisar explícitament els casos d'ús relacionats amb la gestió de claus criptogràfiques T-mobilitat.

El licitador haurà d'especificar de manera àmplia i detallada la seva proposta tècnica en relació a la revisió de la Plataforma de seguretat criptogràfica per a la gestió de les claus criptogràfiques T-mobilitat, així com la càrrega segura en els components de seguretat, que servirà de valoració per a l'adjudicació.

3.4. Gestió i lideratge del PROGRAMA de C&A del SSu

El Programa de Conformitat i Acceptació es el mecanisme que té el Model Tècnic Comú per garantir la interoperabilitat tècnica dels elements d'ús comú T-mobilitat mitjançant l'execució de test unitaris i d'integració per comprovar i validar el compliment de tots i cadascun dels requeriments tècnics MTC, sent un dels principals rols ISO/IEC 24.014 per tal de garantir la interoperabilitat tècnica i funcional.

Les proves del SSu del programa de C&A del MTC són funcionals. Així, i a causa de la gran complexitat tecnològica i confidencialitat que acompanya els complexos processos

criptogràfics implementats cal implementar proves específiques, complementàries al programa de C&A, definides, desenvolupades, integrades i executades des del SSu.

En aquest context i per a cadascuna de les àrees de treball, l'adjudicatari haurà de realitzar el corresponent programa de C&A i/o revisar i actualitzar, si s'escau.

3.4.1. Programa de C&A a Serveis de Seguretat

Així, amb relació a les proves d'acceptació específica complementaries a aplicar als serveis de seguretat, als components segurs i a les eines associades, per garantir en tot moment el compliment dels requeriments tècnics exigits, s'han de realitzar les tasques següents:

- A. Dissenyar, desenvolupar i implementar el casos de test unitaris, test d'integració, test de sistema i test d'interoperabilitat** per comprovar la funcionalitat prevista del nou servei de seguretat "**d'Activació de SUS personalitzats**".

L'adjudicatari haurà en incorporar aquest tes al Programa de Conformitat i Acceptació de Serveis de Seguretat segons el entorn al qui apliqui (enginyeria, preproducció o producció) i segons el component segurs a carregar aquest serveis (SAMs i CHSMs).

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scrips" que permetin executar les proves tantes vegades com calgui.

- B. Dissenyar, desenvolupar i implementar el casos de test unitaris, test d'integració, test de sistema i test d'interoperabilitat** per comprovar la funcionalitat prevista del nou servei de seguretat "**Registre de suport anònim**".

L'adjudicatari haurà en incorporar aquest tes al Programa de Conformitat i Acceptació de Serveis de Seguretat segons el entorn al qui apliqui (enginyeria, preproducció o producció) i segons el component segurs a carregar aquest serveis (SAMs i CHSMs).

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scrips" que permetin executar les proves tantes vegades com calgui.

- C. Dissenyar, desenvolupar i implementar el casos de test unitaris, test d'integració, test de sistema i test d'interoperabilitat** per comprovar la funcionalitat prevista del nou servei de seguretat per a la "**Gestió en explotació de l'ús de versió d'ATlu**".

L'adjudicatari haurà en incorporar aquest tes al Programa de Conformitat i Acceptació de Serveis de Seguretat segons el entorn al qui apliqui (enginyeria, preproducció o producció) i segons el component segurs a carregar aquest serveis (SAMs i CHSMs).

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scrips" que

permetin executar les proves tantes vegades com calgui.

- D. Revisar, actualitzar, optimitzar i desenvolupar de nous, si s'escau, els casos de test** unitaris, test d'integració, test de sistema i test d'interoperabilitat necessaris per comprovar el correcte funcionament dels serveis de seguretat ja implementats als **components de seguretat locals (SAM CBT)** i eines associades.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica als Serveis de Seguretat que proporcionen els SAMs CBT i a les eines associades. Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scrips" que permetin executar les proves tantes vegades com calgui.

- E. Revisar, actualitzar, optimitzar i desenvolupar de nous, si s'escau, els casos de test** unitaris, test d'integració, test de sistema i test d'interoperabilitat necessaris per comprovar el correcte funcionament dels serveis de seguretat ja implementats als **components de seguretat centralitzats (CHSM)** i eines associades.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica als Serveis de Seguretat que proporcionen els CHSM i a les eines associades. Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scrips" que permetin executar les proves tantes vegades com calgui.

- F. Revisar, actualitzar, optimitzar i desenvolupar de nous, si s'escau, els casos de test** unitaris, test d'integració, test de sistema i test d'interoperabilitat necessaris per comprovar el correcte funcionament dels **serveis de seguretat ja implementats als components de seguretat SUS** i eines associades. En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica als Serveis de Seguretat que proporcionen els SUS (mecanismes d'autenticació, mecanismes de canal segur, mecanismes d'anti-caiguda, etc.) i a les eines associades. Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scrips" que permetin executar les proves tantes vegades com calgui.

El licitador haurà d'especificar de manera àmplia i detallada la seva proposta tècnica en relació al Programa de Conformitat i acceptació a fi de garantir l'ús interoperable dels Serveis de Seguretat que haurà de proporcionar el Sistema de Seguretat únic.

3.4.2. Programa de C&A als components SAMs CBT

Així, amb relació a les proves d'acceptació específica complementaries a aplicar als components de seguretat local, SAMs CBT i a les eines associades, per garantir en tot moment el compliment dels requeriments i característiques tècniques exigides a tot mòdul SAM ABT abans de ser acceptat per al seu ús a la T-mobilitat, s'han de realitzar les tasques següents:

- A. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir** el programa de C&A d'acceptació (test unitaris, integració, sistema i interoperabilitat) de **subministrament de mòduls SAMs CBT** tant del maquinari com del programari al llarg del contracte.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica l'acceptació de subministrament de SAMs CBT tant al maquinari com al programari i a les eines associades. Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scrips" que permetin executar les proves tantes vegades com calgui.

- B. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir** el programa de C&A de **personalització segura de SAMs CBT** al llarg del contracte, corresponent a la fase pre-operacional.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica la personalització de SAMs CBT per a cadascun dels casos de test unitaris, integració, sistema i interoperabilitat i a les eines associades per a cada uns dels entorns de treball (enginyeria, preproducció i producció). Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scrips" que permetin executar les proves tantes vegades com calgui.

- C. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir** el

programa de C&A per l'acceptació d'actualització de la **capa d'abstracció de la seguretat (SCAL)** que inclou la configuració de l'SCAL des dels SIC, al llarg del contracte.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica la gestió de la capa d'abstracció de la seguretat (SCAL) i a les eines associades per a cada uns dels entorns de treball (enginyeria, preproducció i producció). Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scripts" que permetin executar les proves tantes vegades com calgui.

D. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir el programa de C&A de monitorització en remot dels SAMs ABT en explotació al llarg del contracte.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica la monitorització en remot de CHSM per a cadascun dels casos de tes unitaris, integració, sistema i interoperabilitat i a les eines associades per a cada uns dels entorns de treball (enginyeria, preproducció i producció). Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scripts" que permetin executar les proves tantes vegades com calgui.

El licitador haurà d'especificar de manera àmplia i detallada la seva proposta tècnica en relació al Programa de Conformitat i acceptació a fi de garantir l'ús interoperable dels Components de Seguretat local del Sistema de Seguretat únic.

3.4.3. Programa de C&A als components CHSM

Així, amb relació a les proves d'acceptació específica complementaries a aplicar als components de seguretat centralitzat CHSM i a les eines associades, per garantir en tot moment el compliment dels requeriments tècnics exigits a tot CHSM abans de ser acceptat per al seu ús a la T-mobilitat, s'han de realitzar les tasques següents:

A. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir el programa de C&A d'acceptació (test unitaris, integració, sistema i interoperabilitat) de subministrament de Centres HSM tant del maquinari com del programari al llarg del contracte.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar

explícitament tots i cadascuns dels casos de test específics que aplica l'acceptació de subministrament de CHSM tant al maquinari com al programari i a les eines associades. Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scripts" que permetin executar les proves tantes vegades com calgui.

B. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir el programa de C&A d'acceptació (test unitaris, integració, sistema i interoperabilitat) de la instal·lació de Centres HSM dins del SIC corresponent.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica l'acceptació de la instal·lació de Centres HSM dins del SIC corresponent i de les eines associades. Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scripts" que permetin executar les proves tantes vegades com calgui.

C. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir el programa de C&A de **personalització segura de CHSM al llarg del contracte, corresponent a la fase pre-operacional.**

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica la personalització de CHSM per a cadascun dels casos de test unitaris, integració, sistema i interoperabilitat i a les eines associades per a cada uns dels entorns de treball (enginyeria, producció i explotació). Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scripts" que permetin executar les proves tantes vegades com calgui.

D. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir el programa de C&A de **monitorització en remot del CHSM en explotació, al llarg del contracte.**

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica la

monitorització en remot de CHSM per a cadascun dels casos de tes unitaris, integració, sistema i interoperabilitat i a les eines associades per a cada uns dels entorns de treball (enginyeria, preproducció i producció). Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scrips" que permetin executar les proves tantes vegades com calgui.

El licitador haurà d'especificar de manera àmplia i detallada la seva proposta tècnica en relació al Programa de Conformitat i acceptació a fi de garantir l'ús interoperable dels Components de Seguretat centralitzat del Sistema de Seguretat únic.

3.4.4. Programa de C&A seguretat als dispositius mòbils NFC

Així, amb relació a les proves d'acceptació específica als mecanismes de seguretat complementaris implementats als dispositius mòbils NFC i a les eines associades, per garantir en tot moment el compliment dels requeriments seguretat exigits a aquests dispositius, s'han de realitzar les tasques següents:

- A. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir el programa de C&A per garantir la seguretat als dispositius mòbils NFC, així com de les eines associades, al llarg del contracte.**

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica a la seguretat que aplica als dispositius mòbils NFC i a les eines associades. Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scrips" que permetin executar les proves tantes vegades com calgui.

El licitador haurà d'especificar de manera àmplia i detallada la seva proposta tècnica en relació al Programa de Conformitat i acceptació a fi de garantir l'ús interoperable dels Components de Seguretat pels dispositius mòbils NFC.

3.4.5. Programa de C&A Infraestructura de gestió de claus

Així, amb relació a les proves d'acceptació específica complementaries a aplicar a la Infraestructura de gestió de claus i a les eines associades, per garantir en tot moment el compliment dels requeriments seguretat exigits a la gestió de les claus criptogràfica T-mobilitat, s'han de realitzar les tasques següents:

- A. Revisar, actualitzar, millorar, desenvolupar, si s'escau, i mantenir el programa de C&A per garantir els processos de gestió de claus**

criptogràfiques en relació al cicle de vida de les claus tecnològiques (generació, emmagatzemament, distribució, ús i revocació d'aquestes), així com de les eines associades al llarg del contracte.

En fase d'anàlisi i enginyeria l'adjudicatari haurà: d'analitzar, revisar i identificar explícitament tots i cadascuns dels casos de test específics que aplica a la gestió de claus criptogràfiques i a les eines associades. Cadascun d'aquest casos de test es revisaran i actualitzaran, si s'escau al llarg del contracte.

Especial atenció cal tenir en l'alineació dels diferents requeriments tècnics i especificacions amb els casos de test a aplicar a cada àmbit.

Aquestes casos de test s'automatitzaran en la mesura que es pugui, preferentment a les plataformes d'interoperabilitat basades en "scripts" que permetin executar les proves tantes vegades com calgui.

El licitador haurà d'especificar de manera àmplia i detallada la seva proposta tècnica en relació al Programa de Conformitat i acceptació a fi de garantir l'ús interoperable dels Components de Seguretat pels dispositius mòbils NFC.

3.5. Gestió i lideratge d'ESPECIFICACIONS TÈCNiques del SSu

La gestió de requeriments tècnics i especificacions tècniques d'obligat compliment, així com els requeriments funcionals i casos d'ús és una tasca essencial del Sistema de Seguretat únic que cal implementar amb molta cura i atenció, i destinar recurs necessaris degut a la complexitat i a que és informació estrictament confidencial.

Es requereix una gestió i manteniment integral dels requeriments tècnics i funcionals, així com de les especificacions tècniques i casos d'ús associades del Sistema de Seguretat únic que inclou els Serveis de Seguretat criptogràfics implementats, els components segurs i eines associades si s'escau, així com manuals d'ús en aquells casos que es consideri necessari.

La gestió de la documentació del Sistema de Seguretat únic requereix un tractament d'estricta i absoluta confidencialitat donada la informació que conté.

El licitador haurà d'especificar de manera àmplia i detallada la seva proposta tècnica en relació a la gestió i control documental del Sistema de Seguretat únic T-mobilitat, rol ISO/IEC 24.014, i segon el requerit al llarg de tot aquets capítol.

Així, amb relació a l'actualització i manteniment de les especificacions tècniques i funcionals del SSu que apliquen als Serveis de Seguretat, als Components segurs i a les eines associades, i sistema de gestió de claus criptogràfiques per garantir en tot moment el compliment dels requeriments tècnics exigits, s'han de realitzar les tasques següents:

3.5.1. Sistema de Seguretat únic – visió general

En aquest context, i amb relació a les especificacions tècniques i funcionals a aplicar al Sistema de Seguretat únic com rol ISO/IEC 24.014 des d'un punt de vista general, s'han de portar a terme:

A. Gestió segura de la documentació del Sistema de Seguretat únic necessària

per operar el sistema, definint les millors pràctiques de confidencialitat, els mètodes per garantir-la, con i qui pot accedir a la documentació, acords de confidencialitat, etc.

L'adjudicatari haurà de proposar un Pla de treball per a la gestió documental segura de la documentació del Sistema de Seguretat únic T-mobilitat que serà aprovat i mantingut per l'ATM de Barcelona.

- B. Definició i/o descripció del Sistema de Seguretat únic** que des d'un punt de vista global ens doni una **visió transversal** de la protecció del sistema de transaccions sense contacte T-mobilitat
- C. Definició i/o revisió**, si s'escau, **manteniment i evolucions** dels requeriments i especificacions tècnics que defineixen la **plataforma de gestió del Sistema de Seguretat únic** per a la protecció de les transaccions sense contacte T-mobilitat.

L'adjudicatari haurà de redactar un document amb la finalitat bàsica de donar una visió general del Model de Seguretat criptogràfic per a la protecció de les Transaccions sense contacte del Sistema Tarifari integrat, així com dels components en els quals descansa del Model de Seguretat Computacional.

- D. Definició i/o revisió**, si s'escau, **manteniment i evolucions de l'arquitectura de seguretat** on s'identifica tots els components (Mòduls d'Accés Segurs -SAM-, Centres de Mòduls d'Hardware Segurs -CHSM-, Suports SUS de diversa procedència, etc.), en relació a la seguretat utilitzats per a la protecció del Sistema Tarifari Integrat, així com l'intercanvi d'informació entre ells.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte l'arquitectura del Sistema de Seguretat únic per a la protecció de les Transaccions sense contacte del Sistema Tarifari integrat, així com dels components en els quals descansa del Model de Seguretat únic ISO/IEC 24.014.

- E. Definició i/o revisió**, si s'escau, **manteniment i evolucions dels casos d'ús del Sistema de Seguretat únic** on s'identifica les principals interaccions que porten a terme entre els diferents actor que ho utilitzen on s'identifica la seqüència d'activitats i el resultat esperat, però no com es porten a terme aquestes funcionalitats.

L'adjudicatari haurà d'especificar els principals casos d'ús del Sistema de Seguretat únic per a la protecció de les Transaccions sense contacte del Sistema Tarifari integrat, així com dels components en els quals descansa del Model de Seguretat únic ISO/IEC 24.014.

3.5.2. Serveis de Seguretat de les transaccions sense contacte T-mobilitat

Amb relació a les especificacions tècniques a aplicar als Serveis de seguretat de les transaccions sense contacte que es carreguen en elements segurs físics que estan distribuïts per tot el Sistema T-mobilitat, s'han de portar a terme:

- A. Definició i/o revisió**, si s'escau, **manteniment i evolucions** de les **especificacions tècniques** que defineixen els **Serveis i mecanismes de seguretat** des d'un punt de vista transversal i entorn de treball, en primer lloc, i

des d'una òptica de seguretat per dispositius que donen aquests serveis com són els Mòduls d'Accés Segurs (SAMs CBT), els Centres HSMS, els Suports d'Usuari Sense contacte (SUS), serveis de seguretat a dispositius mòbils NFC i de la infraestructura de claus criptogràfiques, en segons lloc.

L'adjudicatari haurà de redactar i/o actualitzar les especificacions tècniques dels Serveis de Seguretat de les transaccions que carregades als elements segurs proporcionen aquests serveis allà on es necessiten.

3.5.3. Components de seguretat local - SAM CBT

Amb relació a les especificacions tècniques per a la gestió dels Components Segurs SAMs CBT que contenen els Serveis de Seguretat local i que estan instal·lats a tots terminals sense contacte T-mobilitat, s'han de portar a terme:

- A. Definició i/o revisió**, si s'escau, **manteniment i evolucions** dels requeriments i característiques tècniques que han de complir els **Mòduls de Seguretat Local** SAMS CBT per ser utilitzats en el Sistema Tarifari Integrat T-mobilitat.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte els requeriments tècnics d'obligat compliment amb relació al Hardware del xip (requeriments de seguretat, de processament, de comunicacions, de memòria, de criptografia, etc.), a la seva identificació única, a les característiques físiques, al firmware (kernel) i als recursos de desenvolupament necessaris (emulador, entorn de desenvolupament, sistema de càrrega de kernel, llibreries d'accés a perifèrics, etc.).

Aquests requeriments i característiques tècniques son la base per la realització del programa de Conformitat i Acceptació dels Mòduls SAMs CBT.

- B. Definició i/o revisió**, si s'escau, **manteniment i evolucions** de les especificacions tècniques que han de complir els **Mòduls de Seguretat Local** SAMS CBT per ser utilitzats en el Sistema Tarifari Integrat T-mobilitat.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte les especificacions tècniques dels mòduls de seguretat local SAMs CBT, es a dir, informació estrictament confidencial d'informació sobre la implementació del SAM útil per entendre el seu funcionament con els firmwares que conté, el sistema d'arrencada, de reprogramació i/o formatat des firmwares, versionat, funcionalitats comuns, control d'accés, comunicacions, ordres APDUs, etc.

- C. Definició i/o revisió**, si s'escau, **manteniment i evolucions** de definir i especificar el procediment de comandes de **personalització de SAMs CBT**, que inclou tota la informació necessària per a la personalització, tant física como lògica, així particularitzar pels requeriments de seguretat a cadascuns dels entorns de treball (enginyeria, producció i seguiment).

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte el procediment de personalitzar SAMs que va des de la petició de la comanda i autorització de la comanda, obtenció dels SAMs físics a personalitzar, execució del procés de personalització (física i lògica), registres, proves d'acceptació i anàlisi de resultats, així com el lliurament dels SAMs i resolució i seguiments d'incidències,

si s'escau.

- D. Definició i/o revisió**, si s'escau, **manteniment i evolucions** de les especificacions tècniques que apliquen a la implementació i ús de la **Capa d'Abstracció de Seguretat de Targetes Sense contacte (SCAL)** T-mobilitat.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte les especificacions tècniques que apliquen a la Capa 'Abstracció de la Seguretat (SCAL), es a dir, informació estrictament confidencial d'informació sobre la implementació de la SCAL, així com la seva configuració, actualització, proves d'acceptació i elements i eines necessàries.

- E. Definició i/o revisió**, si s'escau, **manteniment i evolucions** del **Manual d'ús de Mòduls SAMs CBT per integradors** que recopila la informació necessària per que els integradors d'ODs T-mobilitat puguin fer ús dels SUS (lectura i modificació) mitjançant els servei proporcionats per els SAMs CBT i els Servidors segurs.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte del Manual d'ús de Mòduls SAMs CBT per integradors per fer el desenvolupament dels integradors mes fàcil i mantenir la confidencialitat de parts sensibles, la informació que es recopila en aquest document serà un subconjunt de la documentació complerta dels SAM i Servidors Segurs i orientada a la seva utilització, no a recollir la seva especificació confidencial de detall, tan sol per l'ús dels serveis de seguretat que contenen els SAMs CBT.

- F. Definició i/o revisió**, si s'escau, **manteniment i evolucions** dels procediments i plataforma de **gestió del cicle de vida dels SAMs CBT** en T-mobilitat.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte els procediments de gestió del cicle de vida dels SAMs CBT, es a dir, les fases, fluxos i estat per que passen els SAMs en el seu ús a la T-mobilitat (fase de fabricació, fase pre-operacional, fase operacional, fase post-operacional i fase de destrucció) que descriuen les etapes, accions, responsables, etc.

- G. Definició i/o revisió**, si s'escau, **manteniment i evolucions** dels procediments i plataforma de **gestió de la traçabilitat dels SAMs CBT** en T-mobilitat.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte els procediments i plataforma de gestió associada per la traçabilitat i control del SAMs CBT en totes les fases però especialment en les fases en les que encara no estan instal·lats ja que la seva pèrdua és més probable que quan estan instal·lats i monitoritzats en remot des dels SICs.

3.5.4. Components de seguretat centralitzats – Centres HSM

Amb relació a les especificacions tècniques per a la gestió dels Components Segurs CHSM que contenen els Serveis de Seguretat centralitzats i que estan instal·lats a tots els Sistemes Informàtics Centrals SICs T-mobilitat, s'han de portar a terme:

- A. Definició i/o revisió**, si s'escau, **manteniment i evolucions** dels requeriments i característiques tècniques que han de complir els **Mòduls de Seguretat**

Centralitzats CHSM per ser utilitzats en el Sistema Tarifari Integrat T-mobilitat.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte els requeriments tècnics d'obligat compliment amb relació a la plataforma Hardware, on s'executà la plataforma Software que proporciona el servei de seguretat centralitzats, es a dir, els requisits que apliquen al conjunt dels equips que componen els Centres HSM (Servidor host basat en CPU Xeon, equips de xarxa i plaques HSM de seguretat. Que haurà d'incloure l'adquisició (i proves d'acceptació d'acord al programa d'acceptació), instal·lació, posada en servei i monitorització.

Aquests requeriments i característiques tècniques son la base per la realització del programa de Conformitat i Acceptació dels Centres HSM.

- B. Definició i/o revisió**, si s'escau, **manteniment i evolucions** de les especificacions tècniques que han de complir els **Centres HSM** per ser utilitzats en el Sistema Tarifari Integrat T-mobilitat.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte les especificacions tècniques dels Centres HSM, es a dir, informació estrictament confidencial d'informació sobre l'arquitectura, els components hardware i software, fluxos, etc., per entendre el seu funcionament con els firmwares que conté, el sistema d'arrencada, de reprogramació i/o formatat des firmwares, versionat, funcionalitats comuns, control d'accés, comunicacions, ordres APDUs, etc.

- C. Definició i/o revisió**, si s'escau, **manteniment i evolucions** de definir i especificar els procediments d'**instal·lació i gestió dels Centres HSM en explotació**, així com la seva configuració per l'entorn de treball corresponen (enginyeria, producció i explotació).

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte els procediments d'instal·lació i gestió dels Centres HSM, que inclou tota la informació necessària per a la seva instal·lació i la seva gestió en remot dels Centres HSM, que inclou mecanismes segurs d'activació remota, la infraestructura de comunicacions (connexió amb el CPD d'operador, disseny físic i lògic, direccionalment IP, etc.), monitorització i administració en explotació.

- D. Definició i/o revisió**, si s'escau, **manteniment i evolucions** del **Manual d'ús del Centre HSM per integradors** que recopila la informació necessària per que els integradors d'ODs T-mobilitat puguin fer ús dels SUS (lectura i modificació) mitjançant els servei proporcionats per els Centres HSM. L'adjudicatari haurà d'especificar i mantenir al llarg del contracte del Manual d'ús de Centre HSM per integradors per fer el desenvolupament dels integradors mes fàcil i mantenir la confidencialitat de parts sensibles, la informació que es recopila en aquest document serà un subconjunt de la documentació complerta dels Centres HSM i orientada a la seva utilització, no a recollir la seva especificació confidencial de detall, tan sol per l'ús dels serveis de seguretat que contenen els CHSM.

- E. Definició i/o revisió**, si s'escau, **manteniment i evolucions** dels **procediments i plataforma de gestió de la monitorització en explotació dels Centre HSM** en T-mobilitat.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte els procediments i plataforma de gestió associada per la monitorització i gestió d'alarmes centralitzada de tots els Centres HSM en explotació i en tots els entorns de treball (enginyeria, preproducció i producció).

3.5.5. Components de seguretat per dispositius mòbils NFC

Amb relació a les especificacions tècniques per a la gestió dels Components de seguretat addicionals pels dispositius mòbils NFC amb relació als Serveis de Seguretat local i centralitzats necessaris per a la protecció de les transaccions fetes amb dispositius mòbils NFC, s'han de portar a terme:

- A. Definició i/o revisió**, si s'escau, **manteniment i evolucions** dels requeriments i característiques tècniques que han de complir els **mecanismes de tokenització, transferència i emmagatzemament de tokens**.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte els requeriments i característiques tècnics de caràcter estrictament confidencial i d'obligat compliment amb relació a l'estructura del Token, accessos, modificacions segures, signatura, validesa, etc.

Els requeriments i característiques tècniques hauran de ser identificats i definits per l'ús del dispositiu mòbil NFC:

- Com Suport d'Usuari Sense contacte (SUS), aplicació que anomenen NTIU.
- Com Terminal d'Interacció mb l'Usuari (TIU), aplicació que anomenen WUS.

- B. Definició i/o revisió**, si s'escau, **manteniment i evolucions de l'arquitectura de seguretat per l'ús de dispositius mòbils NFC**, i la seva utilització dels serveis de seguretat carregats als components segurs locals (SAMs CBT) i centralitzats (CHSM), per ser utilitzats en el Sistema Tarifari Integrat T-mobilitat.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte l'arquitectura de seguretat global de les Apps mòbils (NTIU i WUS) i fluxos amb els elements de seguretat, així com l'arquitectura general del Sistema Tarifari Integrat utilitzant els dispositius mòbils NFC i els fluxos amb els elements segurs SAMs CBT i CHSM, que haurà d'incloure la identificació única dels dispositius mòbils NFC, detecció de mòbils root, implementació de canals segurs per l'intercanvi d'informació, períodes de validesa dels tokens, entre altres.

- C. Definició i/o revisió**, si s'escau, **manteniment i evolucions del Manual d'ús de Suports virtuals per integradors** que recopila la informació necessària per que els integradors d'ODs T-mobilitat puguin fer ús dels SUS (lectura i modificació) mitjançant els servei proporcionats per els SAMs CBT i els Servidors segurs.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte del Manual d'ús de Suports virtuals per integradors per fer el desenvolupament dels integradors mes fàcil i mantenir la confidencialitat de parts sensibles, la informació que es

recopila en aquest document serà un subconjunt de la documentació completa dels SAM i Servidors Segurs i orientada a la seva utilització, no a recollir la seva especificació confidencial de detall, tan sol per l'ús dels serveis de seguretat que contenen els SAMs CBT i els CHSM.

3.5.6. Infraestructura de gestió de claus criptogràfiques

Amb relació a les especificacions tècniques per a la gestió de claus criptogràfiques centralitzada com a base del desenvolupament de Serveis de Seguretat computacional robustos que garanteixi la seguretat de les Transaccions del Sistema Tarifari Integrat, s'han de portar a terme:

- A. Definició i/o revisió**, si s'escau, **manteniment i evolucions** dels requeriments i característiques tècniques que han de complir el **Sistema de gestió de Claus criptogràfiques** per ser utilitzats en el Sistema Tarifari Integrat T-mobilitat i eines associades a la gestió de les claus criptogràfiques.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte els requeriments tècnics d'obligat compliment amb relació a la problemàtica de la gestió de les claus criptogràfiques, cicle de vida de les claus, actors i responsabilitats, algorismes criptogràfics a utilitzar, etc., així com de les eines associades a la generació, emmagatzemament i distribució de claus criptogràfiques.

S'haurà d'incloure la gestió de claus per a cadascun dels entorns de treball (enginyeria, preproducció i producció).

- B. Definició i/o revisió**, si s'escau, **manteniment i evolucions** dels processos d'inicialització del Sistema de Seguretat únic o cerimònia de claus criptogràfiques per la creació del parell de claus pública i privada de l'Autoritat Certificadora així com els parells de claus dels seus "Security Officers", i eines associades als processos.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte els processos de la cerimònia de generació segura de les claus criptogràfiques que haurà d'incloure les diferents etapes (crear les entitat PKI del sistema, Crear claus de gestió, crear els activadors UCC i securitzar amb els activadors les entitats PKI).

S'haurà d'incloure els casos d'ús estratègics com l'alta de SAMs i d'uCC, personalització de SAMs CBT, etc.

3.5.7. Eines de gestió del Sistema de Seguretat únic

Amb relació a les especificacions tècniques de les eines necessàries per a la gestió de dels Sistema de Seguretat únic T-mobilitat, s'han de portar a terme:

- A. Definició i/o revisió**, si s'escau, **manteniment i evolucions** de la Plataforma de gestió de la seguretat criptogràfica o **Gestor de Seguretat** que l'eina utilitzada per a la creació de les claus de l'Autoritat Certificadora T-mobilitat que executa una sèrie de scripts, aquest són els que contenen la lògica i la funcionalitat.

L'adjudicatari haurà d'especificar i mantenir al llarg del contracte el Gestor de Seguretat amb relació a les pantalles que hauran de detallar les funcionalitat i

finalitat de cadascuna d'elles, selecció, descripció i execució de scripts, versions, logs, etc.

S'haurà d'incloure la gestió de claus per a cadascun dels entorns de treball (enginyeria, preproducció i producció).

3.6. TRACTAMENT DE RISCOS del SSu i nous desenvolupaments

Conèixer els riscos a què estan sotmesos els elements o components d'ús comú que integren el sistema de Ticketing T-mobilitat. És el primer pas per poder gestionar-los i prendre les millors decisions amb relació a la seguretat del sistema.

Entenem com a Seguretat del Sistema de Ticketing a la **capacitat per resistir a incidents de seguretat** (esdeveniments que puguin provocar una interrupció o degradació dels serveis oferts pel sistema) amb un determinat nivell de confiança en relació amb:

1. **Accions il·lícites** o malintencionades,
2. **Accidents involuntaris**,
3. **Protecció de la privadesa** de les dades i el dret a viatjar de manera anònima.

En aquest context, la gestió de la seguretat està basada en un procés continu **d'anàlisi i la gestió corresponent dels riscos**:

- **L'Anàlisi de riscos del negoci** és part essencial del procés de seguretat sobre el qual es construeixen els plans d'accions per a la millora contínua de la protecció del sistema.
- Un cop obtinguda la foto exacta dels riscos, podem establir mesures de salvaguardes amb l'objectiu de reduir-los a un nivell que el Sistema considera acceptable. Aquest procés s'anomena **Gestió dels riscos**.

Tot i que la caracterització del Sistema de Gestió de la Seguretat de la informació (SGSI), identificació d'actius, anàlisi i gestió dels riscos no formen part d'aquesta licitació, si que ho està, el **tractament del risc residual** un cop implementades les salvaguardes de seguretat que són desenvolupades i implementades pel SSu a fi de tenir i mantenir en el temps els riscos dins d'un nivell acceptable.

La gestió del Tractament de riscos del Sistema de Seguretat únic inclou l'assistència tècnica a la identificació, anàlisi i viabilitat de nous serveis de seguretat necessaris a implementar, noves evolucions del Sistema de Seguretat únic en explotació, així com de les eines associats a la plataforma de seguretat, amb l'objectiu de mantenir els riscos de seguretat residual en límits acceptables.

Així, amb relació al tractament de riscos residuals del SSu per mantenir-los dins d'uns nivells rics acceptables, s'han de realitzar les tasques següents:

- A. Desenvolupament i posada en serveis de salvaguardes**, o paquets de salvaguardes, per contrarestar les noves amenaces que apareguin al llarg del contracte, i que apliquen sobre els actius d'ús comú (Interfície de RF, SUS, TIU, Claus del SSu i Registres transaccionals).

L'adjudicatari haurà de desenvolupar i/o millorar les accions recomanades reals per contrarestar amenaces de seguretat que puguin posar en perill la seguretat de les transaccions sense contacte T-mobilitat al llarg del contracte i que siguin necessàries per mantenir els riscos a nivells assumibles.

S'hauran d'implementar les salvaguardes necessàries que apliquen sobre els actius d'ús comú per a cadascun dels entorns de treball (enginyeria, preproducció i producció).

Atès que es desconeixen les salvaguardes a implementar, a causa de les noves amenaces que poguessin aparèixer al llarg del projecte, així com la possible necessitat d'implementar nous desenvolupaments (nous serveis de seguretat, noves funcionalitats, noves eines, etc.) se n'estableixen una borsa d'hores a consumir amb l'autorització prèvia de l'autoritat de confiança.

3.7. Gestió i LIDERATGE INTEGRAL del SSu com rol ISO/IEC 24.014 dins del MTC

Atesa l'especialització i complexitat del Sistema de Seguretat únic (SSu) basat en implementar les millors pràctiques de seguretat criptogràfica es requereix que l'adjudicatari gestioni i lideri el funcionament transversal en explotació del SSu.

En aquest sentit, haurà de conduir les reunions tècniques ja sigui amb l'equip tècnic del MTC i amb altres actors en temes de seguretat criptogràfica del SSu, guiar l'anàlisi de problemes i propostes de solució, proposar evolucions de millora del SSu, etc.

En qualsevol cas, correspon a l'ATM com a Autoritat de Confiança aprovar qualsevol canvi al SSu.

La gestió i lideratge integral del funcionament transversal de l'entorn de de seguretat compartit T-mobilitat inclou l'assistència tècnica a la identificació, anàlisi i viabilitat de nous serveis de seguretat necessaris a implementar, noves evolucions del Sistema de Seguretat únic en explotació, així com de les eines associats a la plataforma de seguretat. L'objectiu és proporcionar de manera permanent els Serveis de Seguretat necessaris per garantir la seguretat de les transaccions T-mobilitat.

Així, amb relació a la gestió i lideratge integral del funcionament transversal del Sistema de Seguretat únic, s'han de realitzar les tasques següents:

A. Assistència tècnica i lideratge en la gestió transversal Sistema de Seguretat únic com rol ISO/IEC 24.014, des d'un punt de vista transversal i integral per mantenir-lo en explotació en els nivells de seguretat mínims requerits, així com evolucionar-lo per tal de mantenir aquests nivells de seguretat.

L'adjudicatari haurà de liderar al llarg del contracte la gestió, control i evolució dels Serveis de Seguretat del SSu, de la gestió en explotació dels components físics segurs que proporcionen els Serveis de seguretat tant locals om centralitzats, de la infraestructura de claus criptogràfiques, de la gestió del Programa de Conformitat i acceptació del SSu, de les especificacions tècniques corresponen, d'implementar noves salvaguardes, si s'escau, de les eines associades, etc.

La gestió transversal inclou tots els entorns de treball (enginyeria, preproducció

i producció).

Tot i que l'adjudicatari haurà de liderar aquesta gestió transversal i integral del SSu l'aprovació de totes les accions proposades hauran de ser realitzades per ATM.

3.8. Mòdul de GESTIÓ DE FRAU

El Sistema de Seguretat únic permet protegir totes i cadascuna de les transaccions sense contacte T-mobilitat el resultat de les quals són els registres transaccionals comuns que s'envien al SIC-ATM.

En aquest context, cal implementar un mòdul per a la gestió del frau que haurà d'implementar funcions específiques per a la detecció, gestió i control de possibles frauds a diferents nivells (targetes no reconegudes pel sistema, SAM no autoritzats, descompensacions de Vendes (Recàrregues) i Validacions, etc.).

Aquesta gestió i anàlisi del frau haurà de permetre la definició d'alarmes de detecció de possibles frau (robatori d'equips de recàrrega, robatori de SAMs, ús de suports sense contacte no autoritzats, o robats, etc.).

Com a resposta als possibles casos de frau s'hauran d'implementar els mecanismes de protecció corresponents com el bloqueig o l'anul·lació de Targetes sense contacte, bloqueig o l'anul·lació de l'Aplicació de Transport Interoperable única, bloqueig o l'anul·lació de la identificació Usuari-Targeta, bloc o l'anul·lació de Perfils d'usuari i el bloqueig o l'anul·lació de la Càrrega associada a un títol.

Aquests mecanismes es podran dur a terme per operatives dinàmiques habilitades en el sistema o mitjançant llistes d'acció.

Aquest mòdul farà ús d'aquests mecanismes per defensar el sistema d'aquests atacs.

Així, amb relació al disseny, desenvolupament i implantació del mòdul de gestió del frau, s'han de realitzar les tasques següents:

A. Dissenyar, desenvolupar i implementar un mòdul per gestionar el frau mitjançant l'anàlisi i la cerca sistemàtica d'incoherències en l'ús del sistema tarifari integrat T-mobilitat.

L'adjudicatari haurà de dissenyar, desenvolupar, provar i posar en servei un mòdul per a la gestió possibles frauds possibles frauds i cerca d'incoherències en l'ús del Sistema Tarifari integrat que proporcioni informació sistemàtica per al control i la millora del sistema T-mobilitat.

Aquest mòdul haurà de córrer al Servidor host del Centre HSM, haurà de permetre la seva permanent actualització en calent, ser modular de manera que permeti incorporar fàcilment noves anàlisis sistemàtiques, la generació d'informes sistemàtics i visualització de resultat en temps quasi real.

En llista no exhaustiva, aquest mòdul ha d'incloure, entre altres, les següents funcionalitats:

- o Controlar i avisar de retards en el subministrament de dades de determinats equips.

- o Verificació de l'existència de càrrega associada a un títol concret anterior a l'execució de Validacions realitzades en el títol, així com comprovació de la coherència d'import carregat i les validacions realitzades.
- o Verificació de SAM de càrrega registrat i actiu amb què es va realitzar la càrrega associada al títol amb el SAM amb què es valida per a cada consum del títol. Si un SAM no està registrat i actiu s'inclourà en llista negra.
- o Control de temps màxims entre l'establiment de la comunicació i de retard en subministrament de dades dels equips de càrrega amb el sistema central per bloqueig de l'equip en cas que superi aquest temps.
- o Altres controls i accions parametrizables en funció de possibles frauds que puguin aparèixer.

El licitador haurà d'especificar de manera àmplia i detallada la seva proposta tècnica en relació a l'arquitectura, funcionalitats i eines associades per a la gestió del frau mitjançant l'anàlisi i la cerca sistemàtica d'incoherències en l'ús del sistema tarifari integrat T-mobilitat, que servirà de valoració per a l'adjudicació.

3.9. Exportació de DADES DEL SIC

La gestió de frau del Sistema Tarifari Integral requereix disposar de les dades de les transaccions realitzades en T-mobilitat en temps quasi real.

En aquest context, cal implementar un mòdul per a l'exportació de dades del SIC que ens permeti disposar dels registres transaccionals sense contacte consolidats.

En aquest cas, s'haurà de proposar possibles canals d'exportació de registres transaccionals via oracle a Kafka i/o via CHSM a Kafka, així com amb la recollida, emmagatzemant i publicació d'informació per al seu consum per altres actors, entre els quals hi ha el mòdul de gestió del frau.

Així, amb relació a l'exportació, emmagatzemament i publicació de dades de les transaccions sense contacte T-mobilitat, s'han de realitzar les tasques següents:

A. Dissenyar, desenvolupar i implementar un mòdul per gestionar l'exportació de dades del SIC que ens permeti disposar dels registres transaccionals sense contacte consolidats.

L'adjudicatari haurà de dissenyar, desenvolupar, provar i posar en servei un mòdul per a l'exportació de dades del SIC i posada a disposició d'aquestes dades als actors autoritzats, analitzant possibles alternatives i desenvolupant les eines necessàries per la publicació de registres del Sistema Tarifari Integrat via Kafka, per exemple, mecanismes de recollida, emmagatzemament i publicació també via Kafka, i desenvolupaments per l'anàlisi de dades per treure conclusions, estar millor equipades per prendre decisions estratègiques i donar serveis de mobilitat d'acord amb les necessitats dels clients del transport públic.

Aquest mòdul haurà de córrer al Servidor host del Centre HSM, haurà de permetre la seva permanent actualització en calent, ser modular de manera que permeti incorporar fàcilment noves anàlisis sistemàtiques, la generació d'informes sistemàtics i visualització de resultat en temps quasi real.

El licitador haurà d'especificar de manera àmplia i detallada la seva proposta tècnica en relació a l'arquitectura, funcionalitats i eines associades per a l'exportació de dades d'ús del Sistema Tarifari Integrat T-mobilitat, que servirà de valoració per a l'adjudicació.

4. FINALITATS I OBJECTIU A ASSOLIR

Les finalitats i objectius que s'han d'assolir mitjançant la realització d'aquest contracte són els següents:

4.1. Principis bàsics a complir

La present licitació es sustenta en uns principis bàsics que orienten el contingut següent:

- **Protecció de les transaccions sense contacte T-mobilitat**

El principal objectiu del Sistema de Seguretat únic és articular un marc de treball comú, confidencial, compartit amb els diferents operadors del sistema T-mobilitat i liderat per l'ATM per aconseguir la permanent protecció del sistema tarifari integrat basat en la tecnologia sense contacte de proximitat.

- **Gestió integral de la seguretat de les transaccions sense contacte**

El principal objetivo de la present licitació és mantenir i evolucionar el Sistema de Seguretat únic T-mobilitat, a través de gestionar en explotació els Serveis de Seguretat carregats en els components de seguretat locals (SAM CBT), els centralitzats (CHSM) i la infraestructura de claus criptogràfiques que el sustenta.

- **Integració Tecnològica Intersectorial**

La Solució tecnològica estarà dissenyada per confluïr de manera interoperable amb tecnologies de diversa procedència (del subministrament de xips segurs, de la telefonia mòbil i del transport) en un únic terminal de comunicació sense contacte de proximitat.

- **Solució Tecnològica innovadora**

La solució tecnològica a implementar serà proposada i adaptada per l'ATM i els Operadors específicament a les necessitats del Transport Públic amb relació a la utilització de xips de diferents fabricants de silici, amb relació a la utilització d'operatives dinàmiques modificable en calent i a la utilització de la capa d'abstracció de la seguretat (SCAL) que requereix nous mecanismes de seguretat.

- **Gestió i Control complet des de T-mobilitat**

El disseny tecnològic de la solució haurà de permetre la gestió i control complet del Serveis de Seguretat actualitzables en calent des dels Sistemes Informàtics Centrals.

- **Potent programa de Conformitat i Acceptació**

Amb els desenvolupament i evolució d'un potent programa de proves d'acceptació dels components i processos en línia amb la responsabilitat operativa del Sistema de Seguretat únic.

5. SEGUIMENT I CONTROL DE LES CONDICIONS DEL CONTRACTE

5.1. Descripció de la forma de prestació del servei

Es descriu en aquest apartat els requisits que s'han de complir en relació amb l'execució del Projecte per a la *“Gestió integral del Sistema de Seguretat únic T-mobilitat en explotació, rol ISO/IEC 24.014, i implementació de noves funcionalitats”*.

El licitador haurà de proposar, d'especificar i descriure amb detall la seva proposta d'implantació de totes les activitats i funcions a realitzar per l'adjudicatari identificades a l'apartat 3 d'aquests plecs on s'hauran de marcar les fites, tasques relacionades i lliurables.

Qualsevol altre projecte o activitat que impacte en el desenvolupament del projecte s'integrarà al pla proposat per l'Adjudicatari, d'acord amb ATM.

5.1.1. Planificació del Projecte

Pel que fa al desenvolupament del projecte, es descriuen a continuació a mode de referència les fases a desenvolupar per part de l'empresa que resulti adjudicatària d'aquesta licitació, així com altres aspectes essencials pel projecte.

5.1.1.1. Fase de Planejament

En aquesta fase l'Adjudicatari liderarà la confecció, redacció i validació del pla desenvolupaments, acceptació i posada en servei dels nous serveis de seguretat identificats a portar a terme dins d'aquest contracte, així com els serveis tecnològics a realitzar par a l'explotació del Sistema de Seguretat únic T-mobilitat.

5.1.1.2. Fase d'Anàlisi i Enginyeria

En aquesta fase s'analitza estat el contingut dels treballs a realitzar, adaptar i/o evolucionar els nous serveis de seguretat a implementar, mòduls i components als que afecten, el seu rendiment, validesa funcional davant de les necessitats actuals i futures, la mantenibilitat, així com especificacions tècniques, eines de treball associades, etc.

Aquesta fase ha de tenir una durada molt limitada en el temps.

L'objectiu genèric d'aquesta fase és l'anàlisi dels treballs contractats i concretar-les en els punts que calgui, ampliant i millorant els aspectes que siguin necessaris. És a dir, l'adjudicatari juntament amb l'ATM (MTC) concretarà el projecte presentat a l'oferta, ampliant i millorant el detall d'aquells punts que es considerin necessaris.

A la finalització d'aquesta fase, es disposarà de la definició concreta, detallada i acordada de tots i cadascun dels serveis i enginyeria i assistència tècnica amb relació al servei de gestió integral del Sistema de Seguretat únic en explotació, així com el pla de treball amb relació als nous serveis de seguretat a implementar.

5.1.1.3. Fase de desenvolupament

La finalitat d'aquesta fase és el desenvolupament i l'adaptació dels diferents sistemes, dels mòduls i components planificats dels nous serveis de seguretat a implementar

identificats una vegada actualitzat, acordat i aprovat a la fase anterior.

S'inicia amb l'acceptació de la documentació de la solució a implementar i finalitza amb l'acceptació explícita per part d'ATM dels treballs realitzats.

Aquesta fase finalitza amb la implantació i acceptació dels nous serveis de seguretat ja implementats a la T-mobilitat a nivell de preproducció.

5.1.1.4. Fase de desplegament

La finalitat d'aquesta fase és durà a terme el desplegament, posada en servei i integració dels nous serveis de seguretat desenvolupaments i acceptats a nivell de l'entorn de preproducció.

Aquesta fase s'inicia amb la validació dels desenvolupaments realitzats a nivell de preproducció i finalitza amb l'Acceptació Provisional dels serveis de seguretat implementats després d'un període de funcionament sense errors.

Durant la fase de desplegament, en cas de trobar-se errors s'executaran els procediments definits a la gestió de modificacions en fase de desplegament, podent arribar a aturar el procés d'instal·lació i/o acceptació.

5.1.1.5. Fase d'explotació

La finalitat d'aquesta fase és assegurar el bon funcionament de tots els Serveis de Seguretat criptogràfics dins del Sistema de Seguretat únic T-mobilitat per a la protecció de les transaccions sense contacte i altres serveis de seguretat implementats fent un seguiment i control del funcionament de tots i cadascun dels serveis, així com garantir-ne l'evolució i el manteniment al llarg de la resta del contracte.

Aquesta fase s'inicia un cop finalitza el desplegament amb relació als nous serveis de seguretats desenvolupats i a la firma del contracte amb relació a la gestió integral del Sistema de Seguretat únic a la resta de Serveis de Seguretat ja en explotació.

5.2. Mitjans Tècnics i Materials

Es descriu aquí els mitjans tècnics que l'Adjudicatari haurà de tenir adscrits a l'execució del contracte.

5.2.1. Infraestructura necessària per dur a terme el projecte

L'empresa adjudicatària disposarà d'instal·lacions pròpies adequades per donar cabuda a l'equip de projecte, així com infraestructures suficients per permetre i facilitar la seva feina.

En cas de ser necessari, l'ATM podrà requerir puntualment que l'equip de projecte de l'empresa adjudicatària treballi a les instal·lacions de la pròpia ATM o a qualsevol altra instal·lació que s'adeqüi per a aquest efecte.

El licitador farà una descripció que identifiqui la infraestructura necessària, contingut, laboratoris, ubicació, del suport tècnic, els elements informàtics i la base documental relacionada disponible i adscrits a l'execució del Projecte que servirà de valoració per a l'adjudicació.

5.3. Recursos humans

Atès que l'objecte del contracte tracta d'un projecte intersectorial amb una solució tecnològica innovadora, única i transversal a tot el sistema amb una forta dependència amb el model tarifari integrat actual T-mobilitat ja en explotació, es requereix:

a) Director/a executiu/iva del projecte

- o El Projecte haurà de ser dirigit i realitzat per un expert amb una experiència suficient demostrada en projecte similars que garanteix la col·laboració intersectorial necessària, la comunicació, el treball en equip, la resolució de problemes i conflictes, la gestió del temps i habilitats de lideratge.

El **“Project Manager”** o director/a executiu/iva del Projecte és la persona encarregada d'assolir els objectius del Projecte complint els objectius de temps, costos i funcionalitats. Haurà d'identificar i respondre als riscos que sorgeixin durant l'execució del mateix i serà el responsable de la comunicació amb tots els actors que intervenen al Projecte.

- o Per al rol de director/a executiu/iva del projecte es requereix, a més dels coneixements propis de direcció de projectes, de flexibilitat, bon judici, fort lideratge i habilitats per a la negociació.
- o El director/a executiu/iva proposat per a la direcció del projecte d'aquesta contractació haurà d'integrar-se de forma activa en els grups de treball que corresponguin amb relació a qualsevol aspecte identificat amb el projecte que la direcció de T-mobilitat estimi necessari.
- o En relació amb la seva experiència professional, haurà d'haver dirigit i realitzat almenys un projecte de continguts similars.

L'experiència professional i la dedicació mínima estimada que s'exigeix al director executiu del projecte és la següent:

Perfil	% Dedicació mínima	Experiència/Coneixements
Director/a del Projecte	5 %	Titulació universitària d'enginyer superior informàtic, de telecomunicacions o industrial i amb una experiència d'almenys 5 anys en direcció de projectes tècnics en projectes tecnològics similars.
		Haurà de disposar: • coneixements específics en desenvolupament de Sistemes de Seguretat criptogràfica aplicat a Sistemes de Ticketing sense contacte de proximitat i • experiència demostrada en el desenvolupament i la implementació de projectes de Sistema de Ticketing sense contacte de proximitat de característiques similars a aquest projecte amb relació a la Seguretat de les transaccions sense contacte utilitzant elements segurs SAMs i CHSMs.

Taula 1: Experiència/Coneixements del director/a executiu del projecte.

b) Director/a tècnic/a del projecte

- o A nivell tècnic, el projecte haurà de ser dirigit i executat per un expert en el desenvolupament de Terminals basat en tecnologia sense contacte de proximitat per inducció electromagnètica amb ampla i demostrada experiència en el desenvolupament i implementació de projectes de Sistema de Ticketing electrònic sense contacte que utilitzin elements segurs locals (SAMs) i elements segurs centralitzats (Centres HSMs) per garantir la seguretat dels sistemes de bitlletatge sense contacte.

El “**Technical Manager**” és la persona responsable d'execució del projecte, per tant és requisit necessari que sàpiga utilitzar les eines adequades, optimitzar la manera de fer servir els recursos i aportar les solucions tècniques més idònies.

- o Per al rol de director/a tècnic/a del projecte es requereix, a més dels coneixements amplis específics, capacitat de relació, capacitat per liderar i dirigir grups de treball tècnic.
- o El director/a tècnic/a proposat per a l'execució del projecte d'aquesta contractació haurà d'integrar-se de forma activa als grups de treball que corresponguin amb relació a qualsevol aspecte identificat amb el projecte que la direcció de T-mobilitat estimi necessari.
- o En relació amb la seva experiència professional, haurà d'haver dirigit i realitzat almenys un projecte de continguts similars

L'experiència professional i la dedicació mínima estimada que s'exigeix al director tècnic del projecte és la següent:

Perfil	% Dedicació mínima	Experiència/Coneixements
Director/a Tècnic/a del Projecte	10%	Titulació universitària d'enginyer superior informàtic, de telecomunicacions o industrial i amb una experiència d'almenys 5 anys en direcció de projectes tècnics que hagin implementat Sistemes de Seguretat criptogràfica aplicada al Sistemes de Ticketing sense contacte de proximitat utilitzant elements segurs locals SAMs i centralitzats com a centres HSMs.
		Haurà de disposar: • coneixements específics en desenvolupament de Terminals basat en tecnologia sense contacte de proximitat i • experiència demostrada en: - o Sistemes de radiofreqüència de proximitat (ISO/IEC 14.443 i NFC), - o Suports d'Usuari Sense contacte (SUS PVC, SUS Cartró i dispositius mòbils NFC com a SUS virtual), - o Terminals d'Interacció amb l'Usuari (TIUs dedicats i dispositius intel·ligents NFC com terminal), - o Sistemes de Ticketing sense contacte, en Seguretat física i lògica (en Ticketing de Transport contactless) utilitzant elements segurs (SAMs i HSMs).

Taula 2: Experiència/Coneixements del director/a tècnic/a del projecte.

L'Adjudicatari haurà de garantir la continuïtat dels tècnics proposat durant tot el termini d'execució dels treballs.

Qualsevol canvi haurà d'ésser autoritzat prèviament per l'ATM.

Els possibles canvis o modificacions en la composició de l'equip hauran de ser comunicats per escrit a l'ATM amb la deguda antelació i acceptats per aquesta.

En aquest supòsit, l'adjudicatari haurà de proposar una/es persona/es amb la formació i experiència requerida en la licitació, tenint en compte les característiques de la persona de l'equip valorada en la licitació, d'acord amb la seva oferta.

Adicionalment, en cas de substituir el Director/a executiu/va i/o el Director/a Tècnic/a del projecte proposat, s'exigirà el següent:

- Un període de formació, a càrrec de l'Adjudicatari, pel nou membre que s'incorpori a l'execució del contracte.
- Un període de coexistència, d'un mínim de 15 dies, entre la persona que causa baixa i la persona que s'incorpora.

A part d'aquests dos perfils, es requereix d'un equip més ampli que intervindrà en la realització dels treballs.

c) Equip de treball

Cal que el licitador inclogui en la seva oferta l'equip que s'adscriurà a l'execució del contracte tot indicant:

- l'historial professional detallat de cadascun dels seus membres,
- aportant els Currículum Vitae dels membres de l'equip de treball assignat,
- la dedicació mínima estimada per a cada perfil, així com
- la seva responsabilitat dins del projecte

IMPORTANT: NO es podran incloure en els sobres A i B ni els currículum, ni la titulació acadèmica, ni els certificats d'execució dels perfils oferts com a Director/a executiu/iva com del Director/a Tècnic/a del Projecte.

Tampoc es podrà presentar aquesta mateixa documentació en el sobre A pel que fa a l'equip de suport.

L'incompliment d'aquesta condició serà causa d'exclusió de la licitació.

5.4. Metodologia a aplicar

Per tal de garantir un adequat procés de gestió integral del Sistema de Seguretat únic T-mobilitat a l'àrea integrada de Barcelona i els desenvolupaments, acceptació i posada en serveis dels nous serveis de seguretat amb totes les garanties de funcionament durant la

fase de desenvolupament a l'entorn d'enginyeria, en la fase de proves i integració a l'entorn de preproducció i en l'operació real en l'entorn de producció, cal establir una metodologia de treball amb un enfocament disciplinat i sistemàtic per donar els serveis sol·licitats, així com els desenvolupaments identificats en aquest projecte.

S'entén per metodologia proposada com el conjunt de processos, tècniques, eines i suport documental que ajuda els desenvolupadors a fer i posar en servei el nou programari.

En aquest sentit d'actuació es valorarà:

- Amb relació als **serveis de gestió integral** del Sistema de Seguretat únic T-mobilitat:
 - o Existència de pautes de treballs sistemàtiques: nivell de servei, gestió de la capacitat, continuïtat dels serveis, gestió de canvis i/o ampliacions funcionals i tècniques, monitorització dels serveis i reporting.
 - o Cobertura completa del cicle de vida dels serveis de seguretat: passos a fer des de la detecció de qualsevol alteració del servei, la seva classificació i registre, assignar responsables fins als plantejament sistemàtics per la seva resolució.
 - o Gestió de l'equipament de seguretat: processos d'actuació sistemàtics amb relació al manteniment preventiu i correctiu, garantir disponibilitat, resolució eficient d'incidències i problemes.
- Amb relació al **desenvolupaments** dels nous serveis de seguretat a implementar:
 - o Existència de regles preestablertes: etapes, fases, tasques, entregues intermèdies, les tècniques i eines utilitzades.
 - o Cobertura completa del cicle de desenvolupament: passos a fer des del plantejament fins a l'acceptació del producte per part d'ATM.
 - o Verificacions intermèdies: sobre els lliurables de cada fase per comprovar-ne la correcció.
- Amb relació a la **integració** dels nous serveis de seguretat en T-mobilitat:
 - o Enllaç amb els processos de gestió: pautes o recomanacions per enllaçar les activitats de desenvolupament tècnic del Programari amb les activitats pròpies de la gestió global del projecte.
 - o Comunicació efectiva: directrius de comunicació efectiva entre els desenvolupadors per facilitar el treball en grup que faciliti la coordinació d'acords consensuats.

Totes les dades numèriques i gràfiques lliuraran en format MS-Excel, les presentacions a MS PowerPoint, els documents a MS Word i les planificacions a MS-Projectes.

En aquest context:

- El licitador haurà d'especificar la metodologia seguida en el desenvolupament del projecte.

Aquesta metodologia haurà d'assegurar la implicació i la participació activa amb

tots els organismes, institucions i unitats afectats pel projecte de definició i implementació del model d'operacions a tots els nivells, de manera que això faciliti que s'arribi a propostes consensuades.

- L'Adjudicatari haurà d'alinear la seva metodologia pròpia de desenvolupament de SW amb metodologia pròpia del Model Tecnològic Comú T-mobilitat ja en explotació, amb relació al:
 - o Desenvolupament del programari,
 - o La integració amb la T-mobilitat.

5.5. Organització de l'execució del projecte

Amb independència de l'estructura i organització interna del projecte de gestió integral del Sistema de Seguretat única, rol ISO/IEC 24.014, a l'àrea integrada de Barcelona, la coordinació i supervisió dels treballs tècnics relacionats amb la present licitació recaurà en el director/a tècnic/a proposat per l'empresa licitadora, prèvia supervisió del responsable d'aquest projecte nombrada per la Direcció de la T-mobilitat.

Són aquests dos perfils els únics interlocutors per al disseny, desenvolupament, execució, acceptació, desplegament, posada en servei i serveis tecnològics en explotació del projecte de comercialització dels canals externs T-mobilitat, evitant, d'aquesta manera, informacions creuades i gestions inconcluses per canvi d'assignació de les diferents qüestions que sorgeixin al llarg del desenvolupament d'aquest projecte.

En fase d'anàlisi i enginyeria el director/a del projecte i el responsable del contracte detallaran per escrit les regles de treball que garanteixi la coordinació de l'execució del projecte, les reunions periòdiques de seguiment, equips de seguiment, informes periòdics, etc.

També es regularà el seguiment i control de l'execució del projecte per part d'ATM i com es donaran les instruccions i directrius necessàries a l'adjudicatari.

5.5.1. Control i seguiment i seguiment del projecte

- L'adjudicatari serà el responsable de fer les tasques de direcció del projecte per a la gestió integral del Sistema de Seguretat únic sota les directrius del Marc Tecnològic Comú, rol ISO/IEC 24.014, per a l'àrea integrada de Barcelona.
- El director/a de projecte informará periòdicament de l'avenç i contratemps del projecte segons s'especifiqui al pla de projecte.
- L'adjudicatari lliurarà informes bimensuals en format digital on descriurà el grau d'avenç del projecte. En aquests informes s'inclouran, entre d'altres, els aspectes següents:
 - o Resum de les tasques realitzades durant el període
 - o Activitats previstes per a la següent
 - o Riscos i desviacions
 - o Estat actual de la planificació.
- ATM podrà, en qualsevol moment, fer controls i sol·licitar informes de seguiments

dels treballs realitzats.

5.5.2. Terminis d'execució

El termini d'execució del contracte de la present licitació serà de divuit mesos des de la data de formalització del contracte.

S'establirà un règim de lliuraments parcials segons les fases i les dates previstes d'aquests lliuraments.

Les franges de temps previstes a les taules que consten en aquest apartat són de compliment obligatori per raons de finançament.

L'adjudicatari està obligat durant el desenvolupament del projecte a implementar totes les mesures que siguin necessàries per recuperar els possibles retards que hi hagi.

L'adjudicatari està obligat a informar de forma permanent de qualsevol circumstància que pugui provocar un retard en el compliment del contracte, així com proposar les mesures mitigadores per corregir aquesta circumstància.

5.5.2.1. Calendari

Les fases i dates previstes són preceptives i les franges de temps previstos a la taula següent són de compliment obligatori.

CRONOGRAMA DEL PROJECTE		2023 - Trimestres				2024 - Trimestres			
Fases		1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T
PLANIFICACIÓ									
Planificació projecte									
ANÀLISI I ENGINYERIA									
Projecte constructiu									

Imatge 2: Planificació i Anàlisi i enginyeria

CRONOGRAMA DEL PROJECTE		2023 - Trimestres				2024 - Trimestres			
Fases		1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T
EXPLOTACIÓ									
Gestió de Serveis de Seguretat, ap. 3.1.1									
Gestió en explotació dels SERVEIS de SEGURETAT criptogràfics, ap. 3.1.1 del PPT									
Pla de gestió integral dels Serveis de Seguretat en explotació, apartat 3.1.1 A									
Pla de millora continua, apartat 3.1.1 B									
Serveis de seguretat per dispositiu – Mòduls SAMs CBT, apartat 3.1.2 del PPT									
Gestionar els Serveis de Seguretat que proporcionen els SAMs, apartat 3.1.2 A del PPT									
Definir, desenvolupar i acordar els SLA dels Serveis de Seguretat local, 3.1.2 B del PPT									
Definir, desenvolupar i acordar els KPIs dels Serveis de Seguretat local, 3.1.2 C del PPT									
Serveis de seguretat per dispositiu – Centre HSM, apartat 3.1.3 del PPT									
Gestionar els Serveis de Seguretat que proporcionen els CHSM, apartat 3.1.3 A del PPT									
Definir, desenvolupar i acordar els SLA Serveis de Seguretat centralitzat, 3.1.3 B del PPT									
Definir, desenvolupar i acordar els KPIs Serveis de Seguretat centralitzat, 3.1.3 C del PPT									
Serveis de seguretat per dispositiu – SUS, apartat 3.1.4 del PPT									
Gestionar els Serveis de Seguretat que proporcionen els SUS, apartat 3.1.4 A del PPT									
Definir, desenvolupar i acordar els SLA Serveis de Seguretat dels SUS, 3.1.4 B del PPT									
Definir, desenvolupar i acordar els KPIs Serveis de Seguretat dels SUS, 3.1.4 C del PPT									

Imatge 3: Explotació – Gestió de Serveis de Seguretat

CRONOGRAMA DEL PROJECTE		2023 - Trimestres				2024 - Trimestres			
Fases		1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T
EXPLOTACIÓ									
Gestió en explotació dels components físics del SSu, apartat 3.2 del PPT									
Gestió en explotació dels MÒDULS D'ACCÉS SEGURS, SAMs, apartat 3.2.1 del PPT									
Gestió dels Components SAMs en explotació, apartat 3.2.1 A, B, C, D, E, F, G i H del PPT									
Gestió en explotació dels CENTRES HSMs, apartat 3.2.2 del PPT									
Gestió dels Components CHSMs en explotació, apartat 3.2.2 A, B, C, D, E, F i G del PPT									
Gestió en explotació dels DISPOSITIUS MÒBILS NFC, apartat 3.2.3 del PPT									
Gestió segura de dispositius mòbils NFC en explotació, apartat 3.2.3 A i B del PPT									
Serveis de Manteniment integral del SSu, apartat 3.2.4 del PPT									
Gestió Serveis de manteniment integral SSu en explotació, 3.2.4 A, B, C, D, E i F del PPT									

Imatge 4: Explotació – Gestió de Components de Seguretat

CRONOGRAMA DEL PROJECTE		2023 - Trimestres				2024 - Trimestres			
Fases		1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T
EXPLOTACIÓ									
Infraestructura Gestió claus i eines associades al SSu, ap. 3.3 del PPT									
Plataforma de gestió de claus criptogràfiques del SSu, apartat 3.3.1 del PPT									
Plataforma de gestió de claus criptogràfiques del SSu, apartat 3.3.1 A, B, C i D del PPT									

Imatge 5: Explotació – Gestió de Claus criptogràfiques de de Seguretat

CRONOGRAMA DEL PROJECTE		2023 - Trimestres				2024 - Trimestres			
Fases		1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T
EXPLOTACIÓ									
Gestió del Programa de C&A del SSu, apartat 3.4 del PPT									
Programa de C&A a Serveis de Seguretat, apartat 3.4.1 del PPT									
Programa de C&A a Serveis de Seguretat, apartat 3.4.1 A, B, C, D, E i F del PPT									
Programa de C&A als components SAMs CBT, apartat 3.4.2 del PPT									
Programa de C&A als components SAMs CBT, apartat 3.4.2 A, B, C, D, E i F del PPT									
Programa de C&A als components CHSM, apartat 3.4.3 del PPT									
Programa de C&A als components CHSM, apartat 3.4.3 A, B, C i D del PPT									
Programa de C&A Infraestructura de gestió de claus, apartat 3.4.5 del PPT									
Programa de C&A Infraestructura de gestió de claus, apartat 3.4.5 A del PPT									

Imatge 6: Explotació – Gestió de la Conformitat i Acceptació dels components del SSu

CRONOGRAMA DEL PROJECTE		2023 - Trimestres				2024 - Trimestres			
Fases		1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T
EXPLOTACIÓ									
Gestió d'ESPECIFICACIONS TÈCNIQUES del SSu, apartat 3.5 PPT									
Sistema de Seguretat únic – visió general, apartat 3.5.1 del PPT									
Sistema de Seguretat únic – visió general, apartat 3.5.1 A, B, C, D i E del PPT									
Serveis de Seguretat de transaccions sense contacte T-mobilitat, apartat 3.5.2 del PPT									
Serveis de Seguretat de transaccions sense contacte T-mobilitat, apartat 3.5.2 A del PPT									
Components de seguretat local - SAM CBT, apartat 3.5.3 del PPT									
Components de seguretat local - SAM CBT, apartat 3.5.3 A, B, C, D, E, F i G del PPT									
Serveis de Seguretat de transaccions sense contacte T-mobilitat, apartat 3.5.2 del PPT									
Serveis de Seguretat de transaccions sense contacte T-mobilitat, apartat 3.5.2 A del PPT									
Components de seguretat centralitzats – Centres HSM, apartat 3.5.4 del PPT									
Components de seguretat centralitzats – Centres HSM, apartat 3.5.4 A, B, C, D i E del PPT									
Components de seguretat per dispositius mòbils NFC, apartat 3.5.5 del PPT									
Components de seguretat per dispositius mòbils NFC, apartat 3.5.5 A, B i C del PPT									
Infraestructura de gestió de claus criptogràfiques, apartat 3.5.6 del PPT									
Infraestructura de gestió de claus criptogràfiques, apartat 3.5.6 A i B del PPT									
Eines de gestió del Sistema de Seguretat únic, apartat 3.5.7 del PPT									
Eines de gestió del Sistema de Seguretat únic, apartat 3.5.7 A del PPT									

Imatge 7: Explotació – Gestió de requeriments i especificacions tècniques del SSu

CRONOGRAMA DEL PROJECTE		2023 - Trimestres				2024 - Trimestres			
Fases		1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T
DESENVOLUPAMENT I DESPLEGAMENT									
Gestió dels Serveis de Seguretat del SSu, apartat 3.1 del PPT									
Desenvolupament de nous SERVEIS DE SEGURETAT a implementar, ap.3.1.5 del PPT									
Identificació i securització dels entorns de treball, apartat 3.1.5.1 A, B, C i D del PPT									
Activació de SUS personalitzat, apartat 3.1.5.2 A, B i C del PPT									
Registre de Suport anònim, apartat 3.1.5.3 A, B i C del PPT									
Gestió de versions d'Atiu, apartat 3.1.5.4 A i B del PPT									
Securització de dades personals en la personalització de SUS, ap. 3.1.5.5 A i B del PPT									
Mòdul de Gestió de frau, apartat 3.8 del PPT									
Dissenyar, desenvolupar i implementar Mòdul per gestionar el frau, ap. 3.8 A del PPT									
Dissenyar, desenvolupar i implementar Mòdul per gestionar el frau, apartat 3.8 A del PPT									
Mòdul per a l'exportació de dades del SIC, apartat 3.9 del PPT									
Dissenyar, desenvolupar i implementar Mòdul d'exportació de dades SIC, ap. 3.9 PPT									
Dissenyar, desenvolupar i implementar Mòdul d'exportació dades SIC, apartat 3.9 A del PPT									

Imatge 8: Desenvolupament i desplegament de nous Serveis de seguretat i noves funcionalitats

CRONOGRAMA DEL PROJECTE		2023 - Trimestres				2024 - Trimestres			
Fases		1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T
DESENVOLUPAMENT I DESPLEGAMENT - BORSA HORES									
Tractament de riscos dels SSu, apartat 3.6, del PPT									
Desenvolupament i posada en serveis de salvaguardes, apartat 3.6 del PPT									
Desenvolupament i posada en serveis de salvaguardes, apartat 3.6 A del PPT									

Imatge 9: Desenvolupament i desplegament de Salvaguardes i nous desenvolupaments – BOSSA D'HORES

Tot i això, el calendari i la planificació d'aquests treballs aniran condicionats pel calendari del projecte T-mobilitat.

5.5.2.2. Fites estratègiques

S'identifiquen al gràfic següent les fites estratègiques del projecte que són de compliment obligat.

Gestió integral del Sistema de Seguretat únic T-mobilitat en explotació.		2023 - Trimestres				2024 - Trimestres			
FITES ESTRATÈGIQUES		1 T	2 T	3 T	4 T	1 T	2 T	3 T	4 T
1 Signatura contracte									
2 PLANIFICACIÓ Projecte									
3 ANÀLISI I ENGINYERIA - Projecte constructiu									
4 EXPLOTACIÓ - Gestió Integral de Serveis, Components, Claus, C&A i especificacions									
DESENVOLUPAMENT I DESPLEGAMENT									
5 Identificació i securització dels entorns de treball, apartat 3.1.5.1 A, B, C i D del PPT									
6 Activació de SUS personalitzat, apartat 3.1.5.2 A, B i C del PPT									
7 Registre de Suport anònim, apartat 3.1.5.3 A, B i C del PPT									
8 Gestió de versions d'ATlu, apartat 3.1.5.4 A i B del PPT									
9 Securitització de dades personals en la personalització de SUS, ap. 3.1.5.5 A i B del PPT									
10 Dissenyar, desenvolupar i implementar Mòdul per gestionar el frau, ap. 3.8 A del PPT									
11 Dissenyar, desenvolupar i implementar Mòdul d'exportació de dades SIC, ap. 3.9 PPT									
12 DESENVOLUPAMENT NOUS - BORSA HORES, apartat 3.6 del PPT									

Imatge 10: Fites estratègiques del projecte

La fita estratègica numero 3 correspon als serveis 24x7x365 per garantir que es donen els serveis de seguretat de manera permanent, així es un fita de permanent compliment.

La fita estratègica numero 11 correspon a la implementació de salvaguardes i altres funcionalitats necessàries, així que poden apareix en qualsevol moment al llarg del projecte.

5.6. Condicions generals d'execució

5.6.1. Confidencialitat i publicitat del servei

L'Adjudicatari està obligat a guardar secret respecte de les dades o informació que no sent públics o notoris estiguin relacionats amb l'objecte del contracte.

Qualsevol comunicat de premsa o inserció als mitjans de comunicació que el proveïdor faci referent al servei que presta a l'ATM haurà de ser aprovat prèviament.

Es garantirà el 100% de confidencialitat en totes les activitats dutes a terme en l'àmbit d'aquesta contractació.

Tota la informació corresponent als Sistemes Tecnològics de l'ATM que es tracti en aquesta contractació ha de ser tractada com estrictament confidencial.

Tots els documents generats en la present contractació serà propietat de l'ATM i no se'n podrà fer cap ús per part del contractista.

5.6.2. Propietat intel·lectual

Tota la documentació que es generi durant el servei és propietat exclusiva de l'ATM.

El licitador no la podrà utilitzar per a altres fins sense el consentiment exprés de l'ATM.

El licitador haurà d'indicar a l'oferta el tipus de llicència, si n'hi hagués, utilitzada en el desenvolupament de les aplicacions que es desenvolupin, sempre respectant els preceptes de propietat intel·lectual, ús i explotació de desenvolupaments específics per a ATM.

5.6.3. Tractament de dades de caràcter personal

L'adjudicatari tractarà les dades de caràcter personal a què accedeixi com a conseqüència de l'execució d'aquest contracte de conformitat amb allò establert a la normativa vigent en la matèria.

L'empresa adjudicatària es responsabilitzarà de l'ús adequat de la informació que es pugui obtenir per tal de protegir les dades personals, al llarg de tota la fase de realització de l'objecte del contracte i també una vegada finalitzada sobre la base de les normatives internacionals sobre això i de compliment obligat, entre ells i expressament, el Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016, sobre la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació de les dades esmentades, així com qualsevol altra normativa nacional i de la Unió Europea que sigui aplicable en matèria de protecció de dades i en relació amb les dades personals a què té accés durant la vigència d'aquest contracte per a la posada en servei i serveis tecnològics en explotació dels canals de comercialització externs T-mobilitat amb tecnologia sense contacte.

L'incompliment d'aquestes obligacions constitueix la infracció tipificada a la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia de drets digitals, sens perjudici de les responsabilitats exigides davant la jurisdicció ordinària

5.6.4. Criteris d'accessibilitat universal

L'empresa adjudicatària es responsabilitzarà de complir amb els criteris d'accessibilitat universal, tal com són definits aquests termes al text refós de la Llei General de drets de les persones amb discapacitat i d'inclusió social, aprovat mitjançant Reial Decret Legislatiu 1/2013, de 29 de novembre.

5.6.5. Criteris de sostenibilitat i protecció al medi ambient

L'empresa adjudicatària es responsabilitzarà de complir els criteris de sostenibilitat i protecció del medi ambient, d'acord amb les definicions i principis regulats als articles 3 i 4, respectivament, del *Reial Decret Legislatiu 1/2016, de 16 de desembre, pel qual s'aprova el text refós de la Llei de prevenció i control integrats de la contaminació*.

Sempre que sigui possible, l'empresa contractista haurà de fer una elecció intel·ligent de materials (ús de materials adequats per al medi ambient, evitant els que no ho siguin), equips d'eficiència energètica (reduir el cost energètic i la petjada de carboni col·lectiu), final de la vida útil i reutilització, etc.

5.7. Proposta tècnica

El licitador haurà de presentar una proposta tècnica que haurà d'una “*Memòria explicativa de la proposta presentada*”, la qual haurà d'incloure una explicació descriptiva dels continguts del projecte objecte de la contractació, la metodologia per al desenvolupament i l'organització del projecte, incloent-hi tant el calendari previst com a l'equip de treball necessari per a la realització del projecte (estructura de l'equip).

Sílvia Roig-Serra Bricall
Directora de l'Àrea de la T-mobilitat

Signat electrònicament