



Plec de Prescripcions Tècniques

Emisió i renovació certificats personals

Expedient: 16059587

Abril de 2024

Versió 1.0

**Solucions Corporatives
Àrea de Tecnologia**

Índex de continguts

1. Introducció.....	3
2. Objecte	3
3. Servei Gestió de certificats personals	3
3.1. Tasques de l'operador de registre	4
3.2. Tasques gestor de la plataforma centralitzada de certificats (GDG CRYPT)..	4
3.3. Procediment de generació de certificats.....	4
4. Requeriments organitzatius	5
4.1. Tasques genèriques	5
4.2. Aspectes funcionals.....	6
5. Confidencialitat	6
6. Seguiment del contracte.....	7

1. Introducció

L'Àrea de Tecnologia de TMB té la responsabilitat de definir, implantar i controlar la seguretat lògica en tots els entorns IT i la física de les dependències dels CPD on es troben els equips IT.

Dins d'aquesta responsabilitat s'inclou la de gestionar certificats digitals de empleats i sistemes que s'utilitzen per signatura electrònica i per assegurar les comunicacions entre sistemes.

Amb aquest objectiu, Ferrocarril Metropolità de Barcelona està constituïda como Autoritat de Registre (RA) de la Autoritat Certificadora (CA) Firma Profesional amb llicència per gestionar fins a 1200 certificats personals. S'encarrega tant de la custòdia com de la integració del certificats amb diferents entorns dins de TMB i per fer aquestes tasques es fa servir la plataforma GDG Crypt.

2. Objecte

L'objecte de la present licitació es la renovació de les llicències associades als certificats personals i la contractació com a servei de l'execució de les tasques de l'operador de registre de la Autoritat de Registre (RA) de la Autoritat de Certificadora (CA) Firma Professional:

LOT 1: Renovar el dret d'Autoritat de Registre de Ferrocarril Metropolità de Barcelona per 1200 certificats de Firma Profesional.

LOT 2: Contractació d'un servei per la Gestió de Certificats Personals que inclou les tasques d'Operador de la Autoritat de Registre de Ferrocarril Metropolità de Barcelona i les tasques de Gestor de la Plataforma centralitzada de certificats GDG Crypt.

3. Servei Gestió de certificats personals

El Servei serà **8x5** i contemplarà tot el cicle de vida dels certificats personals, inclou l'emissió, custòdia i renovació dels certificats així com suport als usuaris per la seva distribució, importació, verificació en la plataforma.

Això implica:

- La designació de l'Autoritat de Registre de la empresa ofertant com entitat associada a l'Autoritat de Registre de Ferrocarril Metropolità de Barcelona i certificar operadors per les tasques de operador de registre.
- Assignació d' Operadors Certificats per Firma Professional d'Autoritat de Registre amb perfil d'Emissor i Gestor d'entitats. Aquest perfil permetrà a l'operador realitzar les gestions característiques de l'entitat associada: sol·licitud, personació presència i remota per Vídeo, generació i emissió dels certificats d'Autoritat de Registre de TMB.
- Assignar operadors de la plataforma centralitzada de certificats GDG Crypt propietat de TMB.

3.1. Tasques de l'operador de registre

Les funcions principals que l'operador de la RA ha de realitzar són següents:

- L'operador generarà i administrarà les claus criptogràfiques necessàries per als certificats electrònics, assegurant la seva seguretat i confidencialitat utilitzant la plataforma Horus de Signatura Professional.
- Per la generació dels certificats la personació es farà de manera remota mitjançant vídeo trucada complint les normes aplicables a la personació online de firma Professional.
- Renovació i revocació de certificats: L'operador facilitarà la renovació de certificats electrònics que han expirat i revocarà aquells que han estat compromesos, ja no són vàlids o han estat revocats pel titular.
- Registre i manteniment de la base de dades: L'operador del RA mantindrà a través de la plataforma Horus de Firma Professional un registre centralitzat de tots els certificats emesos, incloent-hi informació com la identitat del titular, la clau pública, les dates d'emissió i venciment, entre altres dades.

3.2. Tasques gestor de la plataforma centralitzada de certificats (GDG CRYPT)

Les funcions principals en aquest àmbit són següents:

- Operar i gestionar la plataforma centralitzada GDG Crypt i assistència a l'usuari final al moment d'importar els certificats nous/renovats.
- Brindar assistència tècnica als empleats a la instal·lació i configuració de certificats digitals als seus dispositius.
- Resoldre problemes relacionats amb l'ús dels certificats digitals.
- Compliment Normatiu: assegurar que l'alta de certificats en la plataforma centralitzada compleixi amb les regulacions i polítiques de seguretat aplicables.
- Portar un registre detallat de totes les activitats relacionades amb l'ús de la plataforma GCG Crypt, incloent-hi l'emissió i la verificació de signatures electròniques. Aquests registres han de ser accessibles per a auditories de seguretat i compliment.
- Signar els logs d'importació de certificats electrònics per part de l'usuari amb la cadena de certificació reconeguda pel GDG Crypt.
- Monitoratge i Reports:
 - Supervisar l'estat de la plataforma i realitzar un seguiment de les mètriques de rendiment.
 - Generar informes periòdics sobre l'ús i estat dels certificats digitals

3.3. Procediment de generació de certificats

Pas 1. Recepció de Dades del Client.

CST es el helpdesk de l'àrea de tecnologia, gestionarà les sol·licituds de nous certificats a la plataforma de ticketing de TMB, se encarregarà de confirmar que el sol·licitant es empleat actiu

de TMB, és elegible per a disposar de certificat i recavarà les dades necessàries per la seva tramitació i assignarà el ticket al proveïdor per la seva tramitació.

Pas 2. Transcripció de Dades

Les dades de l'empleat es transcriuen acuradament en la plataforma de Certificats Electrònics de Firma Professional, assegurant la precisió i la integritat de la informació.

Pas 3. Generació del Contracte

Una vegada que les dades de l'empleat han estat ingressats en la plataforma, es genera automàticament un contracte d'emissió de certificat digital, el qual conté els detalls pertinents de l'empleat i les condicions d'ús del certificat.

Pas 4. Personació i signatura del contracte.

Es programa una videoconferència per a la personació i signatura del contracte, durant la qual l'empleat de TMB signa electrònicament el document. Si no es pot validar la identitat de l'usuari, llavors s'ha de realitzar un mètode alternatiu de validació o en defecte d'això sortir del procés de creació de certificats electrònics. Tot el procés ha de complir tota la normativa de seguretat del tractament de dades personals.

Pas 5. Aprovació de l'Emissió

L'operador de la plataforma revisa les dades i la signatura del contracte per a garantir la seva validesa i aprova l'emissió del certificat.

Pas 6. Enviament del Certificat

Una vegada aprovada l'emissió, la plataforma de certificats de Signatura Professional envia un enllaç a l'empleat perquè pugui descarregar el seu certificat digital.

Pas 7. Registre del Certificat

Finalment, l'empleat accedeix a la plataforma de gestió centralitzada (GDG Crypt) i registra el certificat digital per al seu ús dins de l'empresa, garantint així un seguiment i una administració adequada dels certificats emesos.

Pas 8. Instal·lació del certificat en l'equip del client

El proveïdor haurà de assegurar que el certificat s'instal·la correctament al equipo del usuari.

Aquest procés garanteix l'emissió segura i eficient de certificats digitals per als empleats de l'empresa, complint amb els protocols de seguretat i verificació necessaris en cada etapa del procés.

4. Requeriments organitzatius

4.1. Tasques genèriques

Els treballs s'executaran en els sistemes i programes propietat de TMB i responsabilitat de l'Àrea de Tecnologia.

4.2. Aspectes funcionals

La prestació del servei objecte d'aquesta contractació ha de complir amb els ítems següents:

La execució de les tasques es durà a terme principalment de forma remota. No obstant això, si TMB ho considera, per la naturalesa de la invenció o incidència, pot demanar realitzar les tasques de forma presencial. En aquest cas, de no indicar una altra cosa, es faran a l'oficina de TMB situada a la següent adreça:

Centre de Suport Tecnològic

C/Josep Estivill, 47

08027, Barcelona

La sol·licitud dels serveis es realitzarà, en els casos que no es tracti d'incidència, amb un període d'antelació, a convenir entre les parts, mai superior a una setmana natural.

El servei disposarà d'un referent que serà l'interlocutor amb el responsable del servei de TMB i es disposaran dels recursos necessaris per finalitzar les tasques en les dates acordades.

Es presentarà una planificació dels treballs a realitzar per acordar amb TMB la durada del treball en cas que es tracti de tasques que permetin aquesta planificació.

L'horari de les jornades serà de 8h a 14h els dies laborables.

5. Confidencialitat

L'empresa col·laboradora ha d'acceptar la Política de Seguretat Tecnològica i de la Informació de TMB. L'adjudicatari es compromet a no difondre i guardar el més absolut secret de tota la informació a la qual tingui accés en compliment del servei actual i a la qual només el personal autoritzat per TMB. L'adjudicatari serà responsable de les violacions del deure de secret que es puguin produir pel personal sota el seu càrrec.

Se l'obliga a aplicar les mesures necessàries per garantir l'eficàcia dels principis de mínim privilegi i necessitat de conèixer per part del personal que participi en el desenvolupament del servei.

Una vegada finalitzat el present servei es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per TMB, així com qualsevol altre producte obtingut com a resultat del present contracte.

L'empresa col·laboradora ha d'acceptar el compromís de confidencialitat respecte a les dades a les quals tindrà accés i que són propietat de TMB.

Els permisos d'accés als sistemes i aplicació, en cas de ser necessari, tindran el nivell necessari per al treball a realitzar i assignats a usuaris personals. En cas de precisar de l'accés amb un usuari amb privilegis elevats en el sistema es durà a terme a través de l'eina que disposa TMB per a aquest fi, de manera que quedin traçades les accions que es realitzin.

Compliment de la Llei Orgànica de Protecció de Dades de Caràcter Personal

L'adjudicatària es compromet a complir quantes obligacions li són exigibles en matèria de protecció de dades personals tant pel Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE ("RGPD") com per la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de dades de Caràcter Personal així com totes les altres normes legals o reglamentàries incideixin, desenvolupin o substitueixin les anteriors en aquest àmbit.

6. Seguiment del contracte

Per facilitar la bona marxa del contracte cal tenir en compte els següents punts:

Es realitzaran reunions periòdiques entre el responsable del servei de l'empresa adjudicatària i el responsable d'aquest a TMB.

La periodicitat es fixarà en funció de la marxa del servei, essent la proposta inicial d'una vegada cada tres mesos. En aquestes reunions es tractaran temes de la marxa del contracte, així com el consum i saldo de jornades.

Fdo:

Jesús Aguilar Morales

Responsable de Sistemes de Seguretat TIC