Ajuntament de Terrassa

DRET D'ÚS D'UNA PLATAFORMA DE GESTIÓ, EMMAGATZEMATGE I ÚS DE CERTIFICATS ELECTRÒNICS DURANT EL PERÍODE 2023-2025

Plec de Prescripcions Tècniques

Codi: 007-01-PPT-153

Terrassa, desembre 2022

El contingut d'aquest document és propietat de l'Ajuntament de Terrassa i no pot ser reproduït ni tramés total o parcialment a altres persones alienes de les incloses en la llista de distribució adjunta d'aquest document, sense autorització expressa de l'Ajuntament de Terrassa

Còpia Nº: 1

Ajuntament de Terrassa

Full de control de la documentació

Títol		
DRET D'ÚS D'UNA PLATAFORMA DE GESTIÓ, EMMAGATZEMATGE I ÚS DE CERTIFICATS ELECTRÒNICS DURANT EL PERÍODE 2023-2025 Plec de Prescripcions Tècniques		
Codi	**Revisió**	**Data**
007-01-PPT-0153	V1	23 de desembre de 2022

Classificació	**Tipus de document**	**Estat**
Públic	Document tècnic	Esborrany
Restringit intern **X**	Presentació	Informe Final **X**
Restringit client	Proposta/ Informe **X**	
	Altres:	
Nom d'arxiu	(D0133)007-01-PPT-0153_PPT_HSM_2023-2025.doc	
Ruta localització		
Paraules clau		

Resum del contingut

	Nom	**Firma**
Edició (TSI) (Responsable actualització doc.)	Manel Guerra	
Vist-i-plau (TSI)	Ignasi Hernández	

Full de registre de canvis

Versió	Data	Pàgines afectades	Notes i raons del canvi
1	23-des-2022	Totes	Elaboració del document

Ajuntament de Terrassa

Índex

1. ANTECEDENTS 4

2. OBJECTE 4

2.1. PRESTACIÓ DEL SERVEI I HORARI 5

3. REQUERIMENTS FUNCIONALS 5

3.1. CLIENT D'ESCRIPTORI 7
3.2. SIGNATURA REMOTA (VIA API) 7

4. REQUERIMENTS TÈCNICS 10

5. PROCÉS DE MIGRACIÓ DE SIGNATURES 11

6. DURADA DEL CONTRACTE 12

7. CONDICIONS DE PRESTACIÓ DEL SERVEI 12

7.1. ORGANITZACIÓ DEL SERVEI 12
7.2. LLOC DE PRESTACIÓ DEL SERVEI 13
7.3. MITJANS 13
7.4. ASSIGNACIÓ DE PERSONAL TÈCNIC DE L'ADJUDICATARI 13

8. OBLIGACIONS DE L'ADJUDICATARI 14

9. FALTES I PENALITATS 15

9.1. ACORD DE NIVELL DE SERVEIS (ANS) 15
9.2. FALTES LLEUS 15
9.3. FALTES GREUS 16
9.4. FALTES MOLT GREUS 16
9.5. PENALITATS APLICABLES 16

1. Antecedents

L'Ajuntament de Terrassa necessita cobrir les necessitats de gestió i emmagatzematge segura de certificats i les característiques avançades de signatura (diferents tipus) que necessita la organització.

L'actual sistema de gestió, emmagatzematge i ús de certificats i signatura és ViaFirma, que s'integra amb la CA de Firma Profesional, actual proveïdor dels certificats per Administració Pública de l'Ajuntament de Terrassa.

El sistema gestiona els certificats dels i les treballadores municipals proveïts per la pròpia organització, així com d'altres certificats d'altres CA també necessaris pel desenvolupament del treball, tant personals com no-personals (segells d'òrgan, etc.).

2. Objecte

L'objecte del present Plec de Prescripcions Tècniques (PPT) és la definició dels serveis a realitzar i condicions tècniques a complir per l'adjudicatari en la realització del "DRET D'ÚS D'UNA PLATAFORMA DE GESTIÓ, EMMAGATZEMATGE I ÚS DE CERTIFICATS ELECTRÒNICS DURANT EL PERÍODE 2023-2025", així com les relacions entre l'Ajuntament de Terrassa i l'adjudicatari en tot allò referent a aspectes tècnics del servei i seguiment del contracte. L'abast, no exhaustiu, dels serveis inclosos en aquesta contractació són:

a. Servei d'emmagatzematge i ús de certificats al núvol per a 1.200 usuaris personals
b. Servei de signatura en escriptori (signatures personals) per 1.200 usos anuals
c. Servei de signatura desatesa (signatures automatitzades via API) per 300.000 usos anuals
d. Servei de signatura desatesa (signatures personal via API) per 108.000 usos anuals

e. Treballs de migració o recreació dels certificats existents en el sistema actual.

2.1. Prestació del servei i horari

- La prestació del manteniment avançat es podrà dur a terme de manera remota o presencialment en les dependències de l'Ajuntament.
- Disponibilitat horària de 8:00h a 18:30h. de dilluns a dijous i de 8:30h a 15:00h els divendres.

3. Requeriments funcionals

A continuació es descriu amb detall les característiques de les tipologies de signatures, accessos i aplicacions que es volen tenir.

A nivell global, el servei ha d'estar disponible de manera remota, en servidors externs, de manera que sigui accessible des de qualsevol dispositiu autoritzat i sense passar per servidors municipals.

La signatura ha de permetre l'ús de qualsevol certificat aprovat per la organització, i la gestió fàcil dels mateixos.

Les signatures efectuades han de ser de diferents tipologies (CADES, XADES, PADES) i permetre diferents tipus de documents, així com diferents nivells de validació/conservació (B, EPES, LT...)

Els usos mínims necessaris, agrupats per tipología, son els següents:

- General
  - Disponibilitat local / internet, Windows, Linux, Android i IOS.
  - Integració de certificats via WS cridats des de l'emisor.
  - Permetre fer signatures de diferents tipus i amb segell de temps.

- Ús de certificats al navegador.
  - Plugins compatibles amb totes les versions de navegador.
- Integració amb Zabbix.
- Control d'activitat per usuari/certificat.
- Possibilitat de creació de WS.
- Possibitat de consultar estadístiques i quadres de comandament.

- Gestió de certificats i usuaris
  - Gestió d'altes, baixes i modificacions d'usuaris personals
  - Gestió d'altes, baixes i modificacions d'usuaris departamentals (o ficticis) per la gestió de certifictats generalistes (segells d'òrgan, per exemple)
  - Administració dels certificats a nivell d'usuari.
  - Permetre diferents certificats per cada usuari, sense límit.
  - Definició de polítiques d'ús i accés als certificat (llocs web o URL, horaris, per aplicació)
  - Avís de caducitat dels certificats amb antelació suficient.
- Aplicació client
  - Permetre als usuaris fer delegacions de l'ús de certificats a altres usuaris
  - Permetre escollir a l'usuari quin certificat pot fer servir per signar.
  - Compatible amb Citrix 7 (Servei d'aplicacions no d'escriptori).
  - Client instal·lat segons els requeriments de l'acord marc.
- Disposar d'una API per accedir a serveis de
  - signatura
  - cerca de certificats
  - recuperació de documents signats
- Seguretat
  - Compliment amb eIDAS-UE (seguretat, tipologia de signatures, revocabilitat, etc.)
  - Integració amb LDAP
  - Doble factor d'autenticació (amb diferents mètodes)

3.1. Client d'escriptori

- Permetre operacions d'autenticació mitjançant mecanismes de comprovació d'identitat.
- Permetre elecció del certificat que cal per signar (propis o delegats)

3.2. Signatura remota (via API)

- La solució ha de disposar d'una API que permeti la signatura electrònica al núvol.
- Es requereix disponibilitat 24x7 dels serveis de signatura proveïts per API.
- La solució ha d'estar adaptada 100% al marc normatiu eIDAS-UE pel que fa a seguretat i signatura digital avançada.
- La solució ha de permetre la integració d'aplicacions de tercers que necessitin integrar-se amb ella mitjançant l'API REST. Proveirà d'una consola web (al núvol) d'administració que permetrà configurar credencial, l'accés i l'ús de la plataforma.
- La solució ha d'assegurar l'autenticació dels usuaris amb certificats digitals allotjats a l'HSM, prèvia a l'accés als certificats propis o delegats (amb 1 o 2 factors d'autenticació) tant per signatura de documents com consulta del certificats.
- L'API de serveis ha de assegurar, l'autenticació de les aplicacions clients a les crides, mitjançant oauth2 .
- L'API de serveis ha de permetre abstraure a les aplicacions de les accions a baix nivell realitzades sobre els certificats digitals allotjats a l'HSM. Aquesta API ha d'oferir les següents funcionalitats:
  - Obtenir certificats de l'usuari
    - Obtenir el llistat de certificats actius per a un usuari amb certificats digitals allotjats a l'HSM
  - Obtenir un certificat de l'usuari
    - Obtenir un certificat en concret actiu per a un usuari amb certificats digitals allotjats a l'HSM.
  - Obtenir els certificats d'una aplicació client integrada
    - Obtenir el llistat de certificats actius per a una aplicació client.

- La solució oferirà una consola web (al núvol) d'administració per tal de gestionar la pujada i manteniment dels certificats (segells d'òrgan)

- Permetre la signatura sobre documents pels usuaris amb certificats digitals allotjats a l'HSM
  - El procés de signatura constarà dels processos de:
    - Autenticació del client
    - Sol·licitud de signatura
    - Autenticació i autorització de la sol·licitud de signatura
      - Es realitzarà des de la pròpia plataforma i en funció dels factors d'autenticació configurats a la consola web d'administració
    - Execució de la signatura
    - Recuperació del document/s signat/s
- Permetre la signatura la signatura desatesa (amb segell d'òrgan) per les aplicacions de tercers integrades amb el sistema:
  - Com s'indica a dalt, la solució oferirà una consola web (al núvol) d'administració per tal de gestionar la pujada i manteniment dels certificats (segells d'òrgan)
  - El procés de signatura desatesa, constarà dels processos de:
    - Autenticació del client
    - Sol·licitud de signatura (indicant el certificat amb el que es signarà)
    - Execució de la signatura
    - Recuperació del document/s signat/s
- L'API de serveis ha de permetre utilitzar/informar les següents característiques de signatura (per tots els casos) :
  - Tipus de signatura:
    - CADES-B
    - CADES-T
    - CADES-LT
    - CADES-LTA

- PADES-B
- PADES-T
- PADES-LT
- PADES-LTA
- XADES-B
- XADES-T
- XADES-LT
- XADES-LTA
- PKCS1

▪ Xifrat de la signatura:

- RSA-SHA1
- RSA-SHA224
- RSA-SHA256
- RSA-SHA384
- RSA-SHA512

▪ Embolcall de la signatura:

- ENVELOPED
- ENVELOPING
- DETACHED

○ Location de la signatura

○ Reason de la signatura

- L'API de serveis ha de permetre – a la signatura de documents PDF (PADES) - indicar les següents característiques de visualització de la signatura :
  - ○ Si es visible o no la signatura
  - ○ Pàgina de visualització
  - ○ Posició X,Y de la visualització de la signatura
  - ○ Text a afegir a la signatura
  - ○ Altura i ample de la signatura
  - ○ Rotació de la signatura

- Tipus de visualització de la signatura:
  - PDF
  - QR
  - CODI DE BARRES
  - IMATGE
  - TEXT

- L'API de serveis ha de permetre informar les següents característiques per signatures de tipus XADES:
  - Identificador del node a signar
  - Mètode de canonització del node
  - Rols del signant
- L'API de serveis ha de permetre informar les següents característiques per signatures que incloguin segell de temps:
  - URL de la TSA
  - Autenticació amb usuari/password
  - Autenticació amb certificat

4. Requeriments tècnics

- El servei ha de proporacionar la interfície API i funcionalitats del servei de ViaFirma, en ser aquesta la interfície d'integració que utiltizen TOTES les aplicacions de gestió de l'Ajuntament, sigui a nivell d'API o integrant-se via client (desenvolupaments interns o aplicacions de T-Systems, entre d'altres)
- El servei/software s'ha d'integrar amb l'Autoritat de Certificació de Firma Profesional i la seva RA per tal de generar automàticament els certificats a l'HSM.
- El software que s'hagi de desplegar localment en equips municipals ha de complir amb el que s'esmenta al Document Marc d'Infrastructures de l'Ajuntament de Terrassa (Annex I).

5. Procés de migració de signatures

Dins del procés d'establiment del servei s'han de migrar els certificats de la plataforma HSM actual (ViaFirma) al nou servei d'emmagatzematge i gestió de signatures.

En cas de no poder-se migrar els certificats actualment en ús (tant les d'administració pública de Firma Profesional com d'altres entitats emissores), serà necessari la replicació i inserció dels ja existents en aquesta nova plataforma, a càrrec de l'adjudicatari.

El volum d'usuaris del que parlem és d'uns 1200 usuaris amb ús de certificat, i uns 1400 certificats amb diferents polítiques d'ús i delegació.

Els passos a seguir serien els següents:

- Reproducció dels certificats de Firma Profesional:
  - exportar les dades dels usuaris actuals
  - càrrega del conjunt d'usuaris a la CA de Firma Profesional.
  - generació dels certificats dins el nou HSM, establiment de polítiques d'ús i accés i gestió de la documentació associada
- Desplegament de certificats d'altres CA:
  - desplegament del diferents conjunt de certificats associats a usuaris, establiment de les polítiques de delegació, ús i accés segons les actualment desplegades.
  - Validació i proves del correcte funcionament.

Per a la correcta execució d'aquestes tasques, l'Ajuntament de Terrassa donarà els permisos i rols necessaris dins dels seus sistemes d'informació als operaris/es de l'adjudicatari.

6. Durada del contracte

El manteniment del servei a contractar tindrà vigència per un període màxim de TRES (3) anys, amb data de finalització de 23 de febrer de 2026.

7. Condicions de prestació del servei

7.1. Organització del servei

L'adjudicatari designarà un Coordinador ó Responsable de Servei que serà l'interlocutor amb l'Ajuntament per a tot el relacionat amb l'objecte d'aquesta contractació. Entre altres, formen part de les seves obligacions les següents:

a. Actuar com interlocutor de l'empresa contractista enfront la l'Ajuntament, canalitzant la comunicació entre l'adjudicatari i el personal integrant de l'equip de treball adscrit al contracte i també en tot el relatiu a les qüestions derivades de l'execució del contracte.

b. Distribuir el treball entre el personal encarregat de l'execució del contracte, i impartir a aquells les ordres i instruccions de feina que siguin necessàries en relació a la prestació del servei contractada.
c. Supervisar el correcte acompliment per part del personal integrant de l'equip de treball pel que fa a les funcions encomanades, així com controlar l'assistència d'aquest personal al lloc de treball.
d. Organitzar el calendari de vacances del personal adscrit a l'execució del contracte a l'objecte de no alterar la prestació del servei.
e. Informar a l'Ajuntament sobre les variacions, ocasionals o permanents, en la composició de l'equip de treball adscrit a l'execució del contracte.

Per part de l'Ajuntament, s'assignarà un responsable del contracte que vetllarà pel compliment del contracte i realitzarà amb l'adjudicatari el seguiment de la correcta prestació del servei.

7.2. Lloc de prestació del servei

L'adjudicatari prioritzarà la realització del manteniment des de les seves dependències, sempre que això no suposi demora en el pla previst ó impacti en la qualitat del servei realitzat. L'Ajuntament facilitarà els codis d'accés per a realitzar connexions segures des dels equips informàtics de l'adjudicatari als sistemes servidors existents en la l'Ajuntament. Per raons de seguretat no es podran realitzar connexions a nivell de xarxa informàtica del proveïdor contra els equips de la l'Ajuntament.

D'altra banda i en els cassos en que sigui precís, l'adjudicatari haurà de realitzar determinades accions en les pròpies dependències de la L'Ajuntament. A tal efecte, l'adjudicatari facilitarà la relació detallada de personal pel que es sol·licita l'accés a la l'Ajuntament. El personal de seguretat de la l'Ajuntament autoritzarà l'accés prèvia identificació en els seus registres. El personal tècnic desplaçat a dependències de la l'Ajuntament està obligat a portar l'acreditació en un lloc visible durant la seva estada en el centre.

7.3. Mitjans

L'adjudicatari haurà de disposar dels terminals, llicències, etc. per tal de realitzar els serveis de manteniment i actualització que es sol·liciten en aquesta contractació. El llicenciament del programari d'explotació dels sistemes servidors de la l'Ajuntament correrà per compte d'aquesta.

7.4. Assignació de personal tècnic de l'adjudicatari

A l'objecte de donar compliment als terminis de temps fixats, no es podran considerar causes de demora, entre d'altres, les següents:

a. La variació del personal de l'adjudicatari assignat al servei per criteris d'assignació a altres projectes o per baixa en l'empresa.
b. La no disponibilitat del personal de l'adjudicatari per raons subjectes a incapacitats laborals temporals.

L'adjudicatari procurarà la substitució, si fos el cas, del personal tècnic assignat al servei de manteniment sense que això suposi demora en el pla de treball establert.

8. Obligacions de l'adjudicatari

L'empresa adjudicatària es compromet a:

- Complir totes les prescripcions contingudes en aquest plec de prescripcions tècniques.

- Mantenir la confidencialitat durant i després de l'execució del contracte, de la informació a la qual pugui tenir accés durant el desenvolupament de la prestació del servei, quedant prohibida la publicació, exposició i comercialització de qualsevol informació que disposi durant l'execució del servei objecte de l'expedient. Les persones que pertanyin a l'equip de treball, independentment de la seva funció, quedaran subjectes al compromís de confidencialitat que s'estableix per l'adjudicatari.

- Informar als seus empleats, de forma explícita, de les condicions de confidencialitats exigides. Ni l'adjudicatari ni cap de les persones empleades pel mateix podran publicar, transferir, comercialitzar o distribuir la informació obtinguda en el curs de la prestació contractada, a menys que l'Ajuntament ho autoritzi expressament.

9. Faltes i penalitats

L'aplicació de faltes es podrà produir per raons subjectes a la forma en que es proporciona el servei de manteniment donant lloc a faltes de tipus lleu, greu o molt greu, que es traduiran en penalitats de tipus econòmic.

9.1. Acord de Nivell de Serveis (ANS)

Dins d'aquest apartat, definim *temps de resolució d'incidències* com el temps transcorregut des que una incidència és notificada fins a la resolució completa.

Davant l'aparició d'incidències que afectin al servei de signatura remota, segons la seva afectació, s'hauran de resoldre dintre del següent marge temporal:

- Afectació lleu
  - Únicament afecta a un mateix usuari, certificat o document i el document a signar no està dintre d'una tramitació considerada crítica.
  - S'estableix un temps màxim de resolució de 8 hores laborables.
  - El no compliment dels ANS comptabilitzarà com a falta lleu.
- Afectació greu
  - Afecta a totes o un gran número les peticions realitzades durant un període temps de 30 minuts o el document a signar està dintre d'una tramitació considerada crítica.
  - S'estableix un temps màxim de resolució de 1 hora.
  - El no compliment dels ANS comptabilitzarà com a falta greu.

9.2. Faltes lleus

Es consideraran faltes de tipus lleu:

a. No acreditar-se oportunament al personal de seguretat de l'Ajuntament.
b. Substituir el personal tècnic sense coneixement per part de l'Ajuntament.
c. Malmetre, voluntària o involuntàriament, béns de les dependències de la L'Ajuntament.

d. Tracte inadequat i/o irrespectuós amb el personal de l'Ajuntament o tercers.

9.3. Faltes greus

Es consideraran faltes de tipus greu:

a. Incompliment d'alguna de les clàusules d'aquest PPT.
b. Baixa qualitat del servei ofert segons requeriments d'aquest PPT.
c. Documentació incompleta, errònia ó fora de termini.
d. L'acumulació de TRES (3) faltes lleus en el període d'un mes.

9.4. Faltes molt greus

Es consideraran faltes de tipus molt greu:

f. Baixa qualitat contrastada i reiterada en la prestació del servei.
g. Mal funcionament dels sistemes implantats per causes no imputables a l'Ajuntament.
h. Pèrdua parcial i/o total d'informació dels sistemes d'informació per raons imputables a l'adjudicatari.
i. Rebre atacs informàtics a través de les plataformes de maquinari/programari utilitzades per l'adjudicatari.
j. Incórrer en TRES (3) faltes greus en el període d'un mes.

9.5. Penalitats aplicables

L'Ajuntament podrà establir penalitats econòmiques d'acord amb l'esquema de faltes que s'ha detallat anteriorment. No es podran aplicar més de DEU (10) faltes en el mateix període.

Faltes i penalitats aplicables		
Id.	Falta	Penalitat
2	Lleu	Escrit d'advertència
1	Greu	Descompte 2% import mensual
0	Molt greu	**Descompte 5% import mensual**

Figura 1 Quadre de faltes i penalitats

Aquesta pàgina es deixa intencionadament en blanc