

PROVISIÓ D'UNA SOLUCIÓ PER SIGNAR UTILITZANT DISPOSITIUS MÒBILS

Data: juliol 2024

Plec de Prescripcions Tècniques



1. OBJECTE DEL CONTRACTE.....	2
2. REQUERIMENTS TÈCNICS.....	2
2.1 Llicències.....	2
2.2 Dispositius mòbils.....	6
3. LLOC DE LLIURAMENT.....	7

1. OBJECTE DEL CONTRACTE

L'objecte és el subministrament de maquinari i llicències de programari necessàries per tal que la plataforma d'administració electrònica pugui continuar prestant els serveis de signatura en dispositius mòbils, integrant els serveis de l'empresa Peakway S.L. que permetin assolir els següents objectius:

1. Els signants han de poder utilitzar els serveis de signatura des d'un dispositiu mòbil evitant l'ús de targetes criptogràfiques tipus *smartcard*.
2. Els signants, si s'escau segons el context de producció del document, han de poder utilitzar com a dades de creació de signatura, la digitalització de la seva signatura biomètrica de traç.
3. Els signants, si s'escau segons el context de producció del document, han de poder utilitzar com a dades de creació de signatura, la clau privada vinculada a un certificat electrònic qualificat de signatura avançada custodiat per un HSM del proveïdor de solució.
4. Les signatures produïdes han de tenir la consideració jurídica d'avançades segons els requeriments de l'article 26 del RE 910/2014 eIDAS.

2. REQUERIMENTS TÈCNICS

2.1 Llicències

El contracte inclou l'adquisició de les llicències de programari, o dret d'ús de programari, que permetin la generació de signatures mitjançant dispositius mòbils satisfent, en general, els següents requeriments:

1. Disposar d'un entorn d'ús de pre-producció, sense cost afegit, per fer proves i formació.
2. Disposar d'una API de serveis web documentada i d'accés sense cost afegit.
3. El programari i els serveis que l'acompanyen han de funcionar les 24 hores del dia i els 365 dies de l'any en mode SaaS.



4. Les signatures electròniques generades han de tenir la consideració jurídica d'avançades segons l'article 26 del RE 910/2014 eIDAS. En qualsevol cas, s'ha de mantenir la identitat electrònica del signant i la correspondència a les dades signades. Atès que es tracta d'actes de signatura atribuïbles a persones físiques, no s'accepta en cap cas l'ús de segells.
5. El signant ha de veure el document objecte de signatura al dispositiu mòbil abans de realitzar la signatura seguint la premissa *What You See Is What You Sign*.
6. S'ha de poder personalitzar la imatge corporativa de tots els correus electrònics, webs, ... per afegir els logotips de Diputació de Tarragona.
7. La solució ha d'estar integrada amb els serveis actuals del mòdul de gestió de signatures electròniques del Sistema de Gestió Documenta de Diputació de Tarragona. Per optimitzar les comunicacions entre ambdós sistemes, l'API d'integració ha de suportar un intercanvi de missatges tipus *push*, on com a mínim haurà de tenir les següents funcionalitats o operacions:
 - a. Iniciar una ordre de signatura enviant el fitxer vinculat al document electrònic a signar. S'han de poder enviar fitxers de fins a 10 Mb de mida.
 - b. Cancel·lació d'una ordre de signatura iniciada prèviament.
 - c. Rebre l'esdeveniment en mode *push* quan el procés de signatura hagi acabat, tenint en compte si s'ha generat o no la signatura:
 - i. Si s'ha generat, s'ha de poder descarregar la signatura *attached* o *detached* que correspon al document per poder ingressar-la al Sistema de Gestió Documental.
 - ii. Si no s'ha generat, s'ha de poder obtenir el motiu pel qual el signant ha cancel·lat o rebutjat la signatura.
 - d. Descàrrega d'altres evidències o proves electròniques relacionades amb els processos de signatura finalitzats, ja siguin de forma correcta o incorrecta.
8. Per assegurar la interoperabilitat, les signatures electròniques generades han de tenir un format segons els estàndards inclosos a l'eIDAS que consten a la següent URL:

<https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Standards+and+specifications>

A part dels requeriments generals, pel cas concret de generació de signatures biomètriques de traç s'han de satisfer els següents requeriments:

1. Disposar d'un entorn de gestió i administració de cadascun dels dispositius donats d'alta per realitzar la signatura biomètrica de traç.
2. Disposar d'una llista de dispositius tàctils de captura de signatura biomètrica de traç compatibles.



- a. L'adjudicatari haurà de presentar una llista de dispositius certificats vàlids per utilitzar la seva solució.
 - b. L'adjudicatari haurà de comunicar, per mitjans electrònics, com a mínim un cop l'any, la llista de dispositius certificats actualitzada.
3. El programari de captura de la signatura biomètrica de traç s'ha de poder instal·lar a cadascun dels dispositius tàctils compatibles identificats al punt anterior.
4. El programari de digitalització de la signatura biomètrica de traç ha de garantir la integritat de la signatura, la identitat electrònica del signant i la confidencialitat de les dades biomètriques. També ha d'assegurar les comunicacions amb els dispositius tàctils xifrant-les mitjançant TLS (*Transport Layer Security*) o similar.
5. El signant ha de poder acceptar les condicions de digitalització de la seva signatura biomètrica de traç mitjançant una pantalla prèvia al procés de signatura. Aquesta acceptació haurà d'incloure la generació d'un certificat d'un sol ús tipus OTC (*One-Time Certificate*).
6. Un cop acceptades les condicions, el signant haurà de realitzar la signatura sobre el dispositiu tàctil de la mateixa forma que la realitzaria amb un paper. El programari de digitalització haurà de recollir les dades biomètriques del traç, el nom i l'identificador (DNI, NIE o PASSAPORT) i enviar-les al sistema del proveïdor per fer-ne la digitalització garantint la seguretat i integritat de les comunicacions tal i com s'ha especificat al punt 3 anterior.
7. L'aplicació instal·lada als dispositius tàctils per capturar les dades biomètriques ha de funcionar en sistemes operatius iOS i Android. En cap cas ha de tenir dependència a un ordinador local.
8. El dispositius tàctils actuaran com a dispositiu de captura de les dades biomètriques de signatura simulant el que seria la signatura tradicional en paper. El programari de digitalització de la signatura biomètrica ha de tenir la capacitat tecnològica necessària per capturar les dades biomètriques de la signatura produïda als dispositius tàctils, i convertir-la en una signatura electrònica avançada vàlida segons l'article 26 del RE 910/2014 eIDAS utilitzant el certificat tipus OTC creat específicament per cada operació de digitalització. Un cop utilitzat el certificat el proveïdor s'haurà de desfer de la clau privada per evitar fer servir aquest certificat en un altre procés de signatura.
9. La identitat digital vinculada a la signatura electrònica de la digitalització de la signatura biomètrica ha de ser d'un sol ús tipus OTC (*One-Time Certificate*), vinculada a la persona física que cedeix les seves dades biomètriques, i generada per un prestador extern que estigui inclòs en la llista de proveïdors de confiança eIDAS. No es requereix que aquest certificat tipus OTC sigui qualificat.
10. Les dades biomètriques digitalitzades incloses a la signatura electrònica s'hauran de xifrar amb criptografia asimètrica per evitar l'accés a persones i sistemes d'informació no autoritzats. La custòdia de la clau pública utilitzada per xifrar les dades biomètriques anirà a càrrec d'un tercer de confiança del proveïdor.



11. El licitador haurà d'acreditar que la solució compleix els estàndards ISO relatius a recollida i codificació de dades biomètriques següents: ISO/IEC 19794-7 i ISO/IEC 29109-7. D'aquesta manera es garanteix la seva pericial futura independentment de l'evolució tecnològica.

A part dels requeriments generals, pel cas concret de la generació de signatures avançades al núvol, utilitzant un certificat custodiat en un HSM per l'adjudicatari del contracte, s'han de satisfer els següents requeriments:

1. L'adjudicatari del contracte haurà de tenir un HSM per l'emmagatzematge segur dels certificats pujats pels usuaris.
2. Disposar d'un entorn d'administració i gestió d'usuaris amb capacitat per generar signatures electròniques avançades en mobilitat.
3. Cadascun dels usuaris amb capacitat de generar signatures electròniques avançades al núvol ha de disposar d'un entorn per fer la gestió dels seus certificats qualificats de signatura. Les funcionalitats bàsiques han de ser:
 - a. Pujar al HSM els certificats qualificats de signatura en format PKCS#12.
 - b. Eliminar certificats.
 - c. Visualitzar els certificats pujats. Les metadades mínimes a mostrar han de ser la seva descripció o àlies i la data de caducitat del certificat de clau pública.
4. Cadascun dels usuaris ha de poder pujar més d'un certificat qualificat de signatura.
5. El sistema del licitador ha de garantir que només l'usuari propietari del certificat l'ha de poder utilitzar en processos de signatura.
6. El sistema del licitador ha de proporcionar als usuaris que hagin pujat com a mínim un certificat qualificat de signatura, un entorn a mode de portasignatures que compleixi els següents requeriments:
 - a. Ha de ser accessible des de dispositius mòbils iOS i Android, i també des de ordinadors d'escriptori.
 - b. Els usuaris han de poder utilitzar com a mecanisme d'autenticació:
 - i. Usuari i contrasenya.
 - ii. Un *Identity Wallet*.
 - c. Un cop identificats, els usuaris han de poder:
 - i. Visualitzar una llista de documents pendents de signar.
 - ii. Rebutjar o cancel·lar documents pendents de signar.
 - iii. Signar individualment o en bloc, utilitzant els certificats qualificats pujats segons el punt tercer d'aquest mateix apartat.



2.2 Dispositius mòbils

El contracte també inclou el subministrament de maquinari necessari per habilitar i mantenir funcionant cada punt de digitalització de signatura biomètrica.

Cada punt o unitat de digitalització de signatura biomètrica estarà format per:

1. Dispositiu tàctil de com a mínim 10 polzades amb sistema Android o Apple iOS amb connexió WiFi i 4G.
2. El dispositiu tàctil ha de poder recollir les dades biomètriques de traç per permetre al programari de digitalització complir els estàndards ISO relatius a recollida i codificació de dades biomètriques següents: ISO/IEC 19794-7 i ISO/IEC 29109-7
3. *Pen, Stylus* o similar per realitzar la signatura biomètrica. Per facilitar el dia a dia, cal que funcioni sense pila i que incorpori un mecanisme que impedeixi que es perdi amb facilitat, com ara un cordó o similar.
4. Suport pel dispositiu tàctil, amb base per a taula de treball, que faciliti l'ús per part del ciutadà alhora de visualitzar el document i realitzar la signatura biomètrica. Que combini robustesa i ergonomia per garantir la durada del dispositiu.
5. Extensió de garantia de 3 anys que cobreixi tots els components que formen un punt de digitalització de signatura biomètrica. La garantia comptarà a partir de la data lliurament.

3. LLOC DE LLIURAMENT

Tots els ítems objecte del contracte s'hauran de lliurar a l'adreça de la Diputació de Tarragona, Passeig Sant Antoni 100, de Tarragona.