PLEC DE PRESCRIPCIONS TÈCNIQUES PEL SUBMINISTRAMENT DE TARGETES CRIPTOGRÀFIQUES - AOC-2023-40

▪ *ÍNDEX DE CLÀUSULES I ANNEXOS*

1. Prescripcions tècniques particulars

1.1 Objecte

Subministrament de targetes criptogràfiques amb el xip qualificat “CHIPDOC V2 ON JCOP 3 P60 in SSCD configuration, version V7b4_2” (JCOP3 P60, en endavant), el programari de gestió associat (“middleware”), amb la personalització exterior aplicada per adequar-les a les actuals T-CAT i els serveis de manteniment i suport tècnic del programari.

1.2 Descripció del subministrament i servei a proveir

D’acord amb el Reglament (UE) núm. 910/2014 (ReIDAS), l’emissió dels certificats qualificats ha de realitzar-se en dispositius (targetes i xips criptogràfics), productes, tecnologia i proveïdors que també han de ser qualificats. Aquestes qualificacions l’atorguen laboratoris especialitzats i també estableixen una data de caducitat de la mateixa (amb una vigència determinada o indeterminada fins a la revocació de la validesa).

Al Servei de Certificació Digital s’estava utilitzant el xip criptogràfic Sm@rtCafe 7.0 (amb nom tècnic “SmartCard Sm@rtCafe Expert 7.0 (chip: SLE78CLFX4000P (M7892), Infineon Technologies; OS: Sm@rtCafe Expert 7.0 C1 Giesecke&Devrient)”) per a l’emissió dels certificats electrònics qualificats T-CAT en targeta. Si bé inicialment la qualificació d’aquest xip criptogràfic tenia una vigència indeterminada, des del passat mes de juliol de 2022, consta l’1 d’octubre de 2023 com a data de pèrdua de la condició de qualificat a la llista de dispositius qualificats segons el ReIDAS[1]. Tot i tractar-se d’una situació sobrevinguda i aliena al Consorci AOC (perquè depèn dels processos d’avaluació dels laboratoris especialitzats i dels reguladors), aquesta circumstància comporta que l’actual T-CAT en targeta també deixi de tenir la consideració de certificat qualificat per l’ús de certificats digitals que conté, segons el ReIDAS, a partir de l’octubre del 2023.

Per seguir oferint el servei T-CAT en targeta dins del Servei de Certificació Digital més enllà d’octubre de 2023, és necessari adquirir les targetes i programaris indicats a l’objecte per tal de garantir la continuïtat de la prestació del servei T-CAT en targeta i durant els 4 anys de vigència pels que s’emeten els certificats dins de la targeta.

L’aplicació d’aquest requisit, també implica substituir totes les aproximadament 80.000 targetes T-CAT existents per aquest nou model abans de la data de fi de qualificació. El Servei de Certificació Digital es presta mitjançant els serveis contractats en l’expedient AOC 2020 3, Serveis de Certificació Digital (SCD) lot 3: Serveis de Certificació Digital a l’empresa FIRMAPROFESIONAL S.A., actualment prorrogat. Per la continuïtat també d’aquest contracte, s’ha escollit aquesta targeta que té un preu similar al previst en el contracte per les targetes criptogràfiques i és compatible amb el sistema d’emissió i ús actual i en servei.

Per aquesta exposició de motius, cal adquirir un volum addicional de targetes per cobrir aquesta situació.

[1] “Qualified Signature/Seal Creation Devices and Secure Signature Creation Devices” : https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD

1.3 Requisits del xip criptogràfic i del sistema operatiu del mateix

1.3.1 Requisits de certificació

La targeta ha de ser certificada, idealment d'acord amb la norma ISO 15408 – Common Criteria EAL4+ o superior indicant el compliment del perfil de protecció descrit a l'especificació tècnica CEN CWA 14169, d'acord amb allò previst per l'article 28 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

La targeta haurà de complir amb els requisits i condicions de seguretat del cicle de vida de claus criptogràfiques descrit a les especificacions tècniques CEN CWA 14169 i ETSI TS 101 456. En concret, les claus seran generades sempre en la targeta o en un mòdul criptogràfic amb la certificació CEN CWA 14167 o equivalent i mai podran ser exportades de la targeta.

1.3.2 Requisits de funcionalitats i característiques de la targeta

La targeta ha d'incloure les següents funcionalitats de criptografia i signatura digital, amb funcionalitat per a les següents operacions criptogràfiques, com a mínim:

- Generació a la targeta de claus asimètriques RSA amb longitud de clau de 2048 bits, tant a la zona de seguretat alta (certificada), com a la zona de seguretat mitjana (zona no certificada).
- Sol·licitud i descàrrega, i gestió posterior, de certificat digital de clau pública ITU-T Rec. X.509v3, d'acord amb els perfils estàndards de Consorci AOC.
- Xifratge simètric amb els algorismes 3DES i AES.
- Xifratge asimètric amb l'algorisme RSA amb longitud de clau de fins a 4096 bits.
- Resum criptogràfic amb els algorismes SHA-256, SHA-384, SHA-512.
- La targeta ha de tenir un mínim de memòria de 144 KBytes i permetre un mínim d'un certificat digital a la zona de seguretat alta (certificada) i 3 certificats a la zona de seguretat mitjana (zona no certificada), amb les seves claus públiques i privades associades de fins a 4096 bits.

La targeta i la seva arquitectura ha de ser compatible amb la norma ISO/IEC 7816, parts 1 a 5 i amb l'especificació tècnica d'interoperabilitat entre targetes i lectors PC/SC versió 2.0.

L'estructura de fitxers corresponent a l'aplicació de signatura electrònica de la targeta haurà de ser compatible amb la norma ISO/IEC 7816, part 15 o en el seu defecte la PKCS#15.

Tot i que la targeta pugui treballar amb un perfil de seguretat certificat (seguretat alta), aquesta s'ha de poder utilitzar en mode de seguretat mitjana, això significa poder gravar tots els certificats (signatura i identificació) dins de la zona no certificada (on no hi haurà trusted channel ni obligació de posar el PIN cada vegada que s'hagi de realitzar una signatura).

En qualsevol cas, l'usuari ha de poder ser autenticat per a accions concretes, amb exigència de la corresponent autenticació per a cadascuna, o per a una sessió de treball dins d'una aplicació concreta – mentre la targeta es trobi inserida en el lector i dins d'un període de temps concret, que ha de poder ser configurat emprant l'aplicació d'administració de la targeta – sense que, en aquest darrer cas, sigui exigible una nova

autenticació per a cada acció, fins que la sessió expiri. És a dir, que disposi d'un sistema que permeti fer servir un PIN de sessió, almenys pel cas que els certificats que no estiguin a la zona certificada.

La targeta implantarà mesures de seguretat contra atacs laterals: d'anàlisi de potència (SPA i DPA) i de diferencial d'errors (DFA).

És necessària la implantació d'un mecanisme de canal fiable (trusted channel) per a la comunicació entre les aplicacions de sistemes externs, i en especial sistemes operatius PC, i l'aplicació criptogràfica de la targeta, mitjançant autenticació mútua de la targeta i el sistema extern, i el posterior establiment de sessió basada en missatgeria segura ISO/IEC 7816, o mecanisme amb garantia equivalent.

1.4 Requisits del programari "middleware" de la targeta

El programari middleware que s'instal·larà a les màquines dels usuaris i la targeta, han de ser compatibles amb les infraestructures actualment desplegades, això inclou compatibilitat amb els lectors més habituals, i compatibilitat amb els models i middelware de targeta actuals del Consorci AOC (Sm@rtCafe 7.0).

1.4.1 Requisits del "middleware" de la targeta

El licitador aportarà totes les llicències necessàries (com a mínim 1 per targeta) d'una aplicació d'administració/gestió de la targeta, que permeti que l'usuari final configuri els diversos elements del comportament de la targeta que, com a mínim, seran:

- Mostrar els certificats i PKCS#12 registrats al sistema operatiu.
- Importar certificats i PKCS#12
- Estat de registre al sistema operatiu i preferències de l'ús del certificat
- Esborrar el token
- Canviar el PIN i el PUK
- Desblocar el PIN

Aquest middleware serà compatible amb aplicacions i sistemes operatius estàndard a l'hora de realitzar signatures i xifrat de dades, com a mínim amb Windows, Mac OS X i Linux.

El PIN i PUK de la zona certificada de la targeta com de la zona no certificada ha de ser el mateix sempre i el middleware ha de vetllar per aquest fet en la interacció amb l'usuari.

Aquesta aplicació haurà de complir amb les normes d'accessibilitat i usabilitat que s'estableixen per a les administracions públiques.

Aquesta aplicació haurà d'estar traduïda a català i castellà normalitzats, i podrà ser revisada per Consorci AOC per tal d'adequar la nomenclatura de forma exacta.

Cal incloure un manual d'ús en català i castellà normalitzats i en format electrònic editable. El consorci AOC el podrà incorporar al seu portal de suport a l'usuari.

El programari del middleware s'haurà de poder configurar per a que instal·li automàticament els certificats arrel de la jerarquia d'entitats de certificació de Consorci AOC, així com tota la documentació d'ajuda, enllaços a diferents adreces webs amb informació sobre el Consorci AOC. També ha d'incloure la instal·lació directa del mòdul PKCS#11 dins del navegador Firefox, en cas que el programa instal·lador en detecti que hi ha una instància d'aquest navegador instal·lada.

El proveïdor ha de facilitar un acord de nivell de servei per a la resolució de problemes tècnics o de compatibilitat entre el middleware i els diferents sistemes operatius i aplicacions finals. En cas de trobar-se alguna incompatibilitat greu amb algun dels programaris anteriors, el licitador es comprometrà a solucionar el problema abans de 2 mesos.

S'hauran d'aportar versions silencioses de middleware que permetin la instal·lació desatesa, entre la que caldrà també la instal·lació del mòdul PKCS11 dins del navegador Firefox per al seu ús amb les targetes criptogràfiques.

1.4.2 Requisits de llibreries de serveis criptogràfics

Cal aportar llibreries de serveis criptogràfics des de sistema operatiu, compatibles amb les especificacions d'interfície de programació criptogràfica més habituals: RSA Labs PKCS#11/Cryptoki, Microsoft CryptoSPI/CryptoAPI.

Caldrà aportar versions de CSP Microsoft per a totes les versions de Microsoft Windows a partir de Windows 10.

1.5 Requisits de documentació

Es requereix el subministrament:

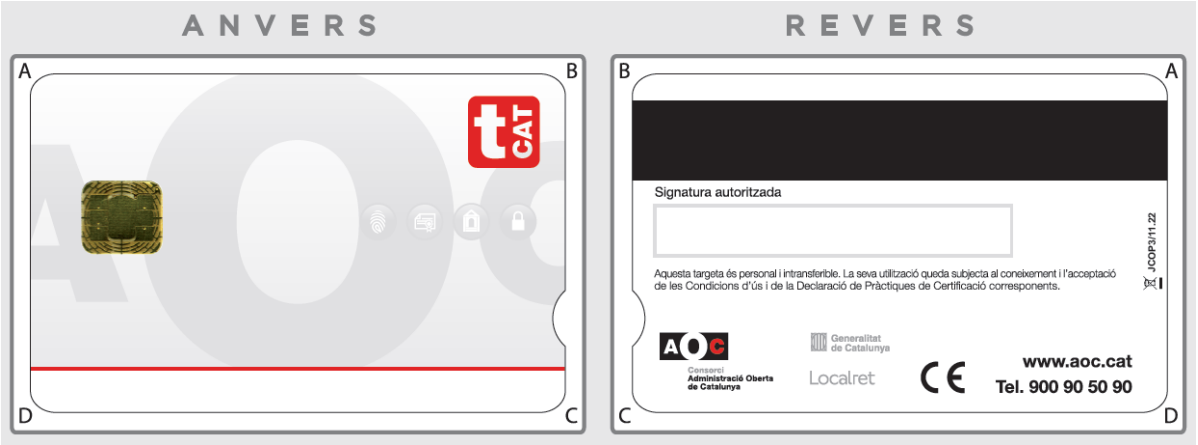
- D'una còpia de tots els informes referits a certificacions o avaluacions rebudes pel xip, sistema operatiu i aplicació criptogràfica, per part d'organismes externs d'avaluació.
- El manual del middleware en català, castellà, sempre en format electrònic editable per Consorci AOC per tal d'adaptar-lo.

1.6 Requisits de les característiques físiques

La targeta de Consorci AOC pren com a referència les normes ISO 7810, 7811/2,4 i 5, 7813 i 7816 (Identification Cards), les quals es consideren supletòries del que no hagi estat previst en les presents prescripcions.

1.6.1 Requisits del suport plàstic

Les dimensions físiques de la targeta de Consorci AOC són de 85,5 x 54 mm. El disseny actual, encara que no es descarta l'ús d'altres dissenys és :



El gruix de la targeta és de 0,80 mil·límetres (en endavant mm) o 0,0316 polzades (en endavant in).

Les cantonades estan arrodonides sobre un radi de 3,18 mm, és a dir, 0,125 in evitant qualsevol desalineació sobre els cantons rectilinis.

El material de la targeta serà de PVCA (copolímer de clorur de vinil i acetat de vinil) o de PVC (policlorur de vinil) o materials com polietilens o polièsters, sòlida o laminada, amb inserció de xip criptogràfic i amb inserció, o sense, d'altres materials, i amb característiques delimitades en les normes ISO 7810, referents a capacitat de deformació, inflamabilitat, resistència a agents químics, estabilitat a la temperatura i humitat. El material amb què es fabriqui la targeta no ha d'oferir perill tòxic i ha d'ésser un material que permeti el seu ús continuat i freqüent sense deterioraments durant el seu període de vigència estimat, és a dir, 4 anys.

S'anomenarà revers a la cara de la targeta que contingui un suport magnètic, i anvers al seu oposat.

El Consorci AOC podrà demanar, sense cost extra, suports plàstic amb identificador tàctil d'osca per a invidents basats en la norma UNE-EN 1332-2:1999 "Sistemes de targetes d'identificació. Interfície home-màquina. Part 2: Dimensions i posició del l'identificador tàctil para targetes ID-1".

1.6.2 Requisits de la banda magnètica

El revers de la targeta, porta a la part superior una banda magnètica de lectura escriptura (ISO 7811/2-1985) a una distància de la vora superior de la targeta de 5.54 mm (0,218 in) el seu límit superior i de 15,82 mm (0,623 in) el seu límit inferior.

La banda magnètica haurà d'estar integrada en la targeta i podrà ser, a elecció del Consorci AOC, d'alta o baixa coercitivitat i de 3 pistes.

1.6.3 Requisits de posició del xip

El xip que s'implantarà en aquestes targetes serà dissenyat per ser inserit en targetes amb xip d'acord a la norma ISO 7816.

1.6.4 Requisits del fons de la targeta

La targeta incorporarà imprès a l'anvers el logotip i la denominació de l'entitat emissora (Consorci AOC) i, a mida més reduïda, el logotips i denominacions de la Generalitat de Catalunya, de Localret i del Consorci AOC.

Al revers de la targeta, a la part inferior de la banda magnètica, es reservarà un espai per a la signatura del titular (en un panell de signatura incorporat al plàstic) i s'imprimiran el textos, logotips i denominacions.

Per a la impressió dels logotips i textos se seguiran els dissenys corresponents i les normes sobre identificació visual. A tal fi, es proporcionarà a l'adjudicatari un original del disseny de l'anvers i del revers de la targeta.

1.7 Requisits de subministrament

El licitador haurà de proveir d'un telèfon de suport tècnic del middleware i de la targeta així com per a la gestió dels subministraments.

El licitador inclourà a la seva oferta l'acord de nivell de servei ofert per a la resolució de les possibles incidències tècniques, de subministrament, i de tots els altres aspectes exposats en aquest plec, tot indicant els temps de resposta i resolució segons la gravetat de les mateixes.

Exemples de possibles incidències:

- incidència amb una versió concreta de sistema operatiu
- que es detecti alguna incompatibilitat en la interacció del procés de gravació de certificats deguda al middleware.
- incompatibilitat del middleware amb una aplicació de signatura de gran abast, com per exemple l'Office.
- retard en l'enviament de targetes

Barcelona,

El Cap de Projectes,

Francesc Ferrer i Grevolosa