

PLECS DE PRESCRIPCIONS TÈCNIQUES RELATIU AL SUBMINISTRAMENT, IMPRESSIÓ I PERSONALITZACIÓ DE TARGETES CORPORATIVES I SERVEI D'ASSESSORAMENT DE CLAUS MESTRES, SUBMINISTRAMENT DE TARGETES SAM I LECTORS/PROGRAMADORS I DESENVOLUPAMENT D'UN PROGRAMARI PER CREAR TARGETES CORPORATIVES, DIVIDIT EN 2 LOTS

Expedient núm.: 2020/0004486

ÍNDEX

INTRODUCCIÓ.....	1
DEFINICIONS.....	1
LOT 1 – SUBMINISTRAMENT, IMPRESSIÓ I PERSONALITZACIÓ DE LES TARGETES CROPORATIVES	2
1. SUBMINISTRAMENT.....	2
2. DISSENY I IMPRESSIÓ DE LA TARGETA	2
3. PERSONALITZACIÓ.....	4
3.1. IMPRESSIÓ	4
3.2. PROGRAMACIÓ DE LA TARGETA	4
3.3. TARGETA SAM	4
4. TRANSFERÈNCIA D'INFORMACIÓ	5
5. COORDINACIÓ AMB LOT 2	6
6. CONTROL DE QUALITAT	6
7. TERMINIS.....	6
LOT 2 – SERVEI D'ASSESSORAMENT DE CLAUS MESTRES, SUBMINISTRAMENT DE TARGETES SAM, LECTORS/PROGRAMADORS I DESENVOLUPAMENT DE PROGRAMARI PER CREAR TARGETES CORPORATIVES.	7
1. INTRODUCCIÓ	7
2. ASSESSORAMENT PER LA GENERACIÓ DE CLAUS MESTRES	7
3. DESENVOLUPAMENT DEL PROGRAMARI	7
3.1. ESTRUCTURA D'APLICACIONS I FITXERS.....	8
3.2. FUNCIONALITATS DEL PROGRAMARI	9
3.2.1. CREAR L'ESTRUCTURA D'APLICACIONS I FITXERS CORPORATIVA	9
3.2.2. AFEGIR APLICACIONS DE TERCERS	9
3.2.3. LLEGIR INFORMACIÓ	9
3.2.4. ESCRIURE INFORMACIÓ	10
3.2.5. LECTURA MASSIVA DE TARGETES	10
3.2.6. PROGRAMACIÓ MASSIVA DE TARGETES.....	10
3.2.7. CREAR APLICACIONS DE FORMA MASSIVA	10
3.2.8. CONFIGURACIÓ DE L'APLICACIÓ.....	10
3.2.9. LLISTA D'ESDEVENIMENTS	11
3.2.10. ROLS D'USUARI.....	11
3.3. INTERFÍCIE GRÀFICA	11
3.4. CONFIGURACIÓ DEL PROGRAMARI	11
4. SUBMINISTRAMENT LECTORS/PROGRAMADORS	12
5. ENTREGA PER FASES DEL PROGRAMARI	12



6.	RESOLUCIÓ D'ERRADES DEL PROGRAMARI	12
7.	FORMACIÓ I MANUAL D'ÚS	12
8.	COORDINACIÓ AMB EMPRESA CONTRACTISTA LOT 1.....	13
ANNEX 1 – CARACTERÍSTIQUES TÈCNIQUES.....		14
1.	TARGETA CORPORATIVA	14
2.	TARGETA SAM	14
ANNEX 2 – ESTRUCTURA I DADES ENREGISTRADES		15
1.	ESTRUCTURA	15
2.	ESTRUCTURA FITXERS TARGETA.....	16
ANNEX 3 – INTERFÍCIE GRÀFICA PROGRAMARI.....		19

INTRODUCCIÓ

Els funcionaris de la Diputació de Barcelona disposen d'una targeta d'identificació amb el número d'empleat, el DNI, la data d'incorporació, el nom i cognoms i la fotografia impresos en ella. Hi ha també una targeta equivalent pels càrrecs electes i targetes sense logotip pel personal extern.

La tecnologia utilitzada és la de HID ISOProx II de 125Khz Clock&Data i s'utilitza per:

- Control horari
- Accedir al servei d'impressió
- Control d'accés de persones i vehicles

S'han detectat diverses problemàtiques:

- La tecnologia de la targeta no és segura, ja que el número de sèrie intern es pot llegir fàcilment i qualsevol pot fer les còpies que desitgi, aquestes còpies són indistingibles de les originals.
- La tecnologia de la targeta no permet emmagatzemar dades, això provoca que no es puguin implantar noves funcionalitats com instal·lar panys electrònics per gestió de despatxos, armariets, sales, etc.
- La tecnologia d'impressió no disposa de mesures de seguretat.

La finalitat de la contractació és substituir la targeta d'identificació actual de la Diputació de Barcelona per una amb mesures de seguretat impreses i amb tecnologia segura i moderna.

DEFINICIONS

Disseny base: és aquell disseny imprès a la targeta corporativa sense cap personalització. Poden haver-hi diferents dissenys base, segons el tipus de targeta.

Personalització: és el procés d'imprimir i programar una targeta per assignar-la a una única persona. S'imprimeix la fotografia i algunes dades personals. Es programen diferents dades al xip de la targeta.

Programació: és el procés d'accedir al xip de la targeta subministrada de fàbrica per tal d'inserir les claus criptogràfiques corporatives, crear les diferents aplicacions, fitxers i finalment afegir les dades xifrades de la persona a la que se li assignarà la targeta.

Targeta SAM: SAM és acrònim de Secure Acces Module. És una targeta amb un xip criptogràfic on es poden emmagatzemar de forma segura claus criptogràfiques.

AMK: Acrònim d'Application Master Key. És una clau criptogràfica que dona accés a la configuració d'una aplicació de la targeta Mifare DESFire. Aquesta clau permet crear i esborrar fitxers de la mateixa aplicació.

CMK: Acrònim de Card Master Key. És una clau criptogràfica que dona accés total al xip de la targeta. Permet tenir el control de creació i esborrat d'aplicacions així com altres operacions.

Key Settings: Paràmetre de configuració de les claus criptogràfiques programades al xip.

UUID: Acrònim de Universal Unique IDentifier. És el número de sèrie únic del xip de cada targeta.

Fitxer CSV: Els fitxers CSV (de l'anglès comma-separated values) són un tipus de document en format obert simple per a representar dades en forma de taula, en què les columnes se separen per comes.

Fitxer log: Fitxer d'enregistrament seqüencial dels esdeveniments o accions succeïdes on s'indica la marca temporal, l'acció o esdeveniment fet, l'usuari que ho ha realitzat i altra informació.

LOT 1 – SUBMINISTRAMENT, IMPRESSIÓ I PERSONALITZACIÓ DE LES TARGETES CORPORATIVES

En aquest lot s'indicaran les prescripcions tècniques del subministrament de la targeta corporativa, de la impressió i la seva personalització.

1. Subministrament

L'empresa contractista haurà de subministrar 10.000 targetes amb les característiques tècniques indicades al primer punt de l'Annex 1. Del total de les targetes subministrades, es preveu que 8.000 estaran personalitzades i la resta tindran només la impressió del disseny base.

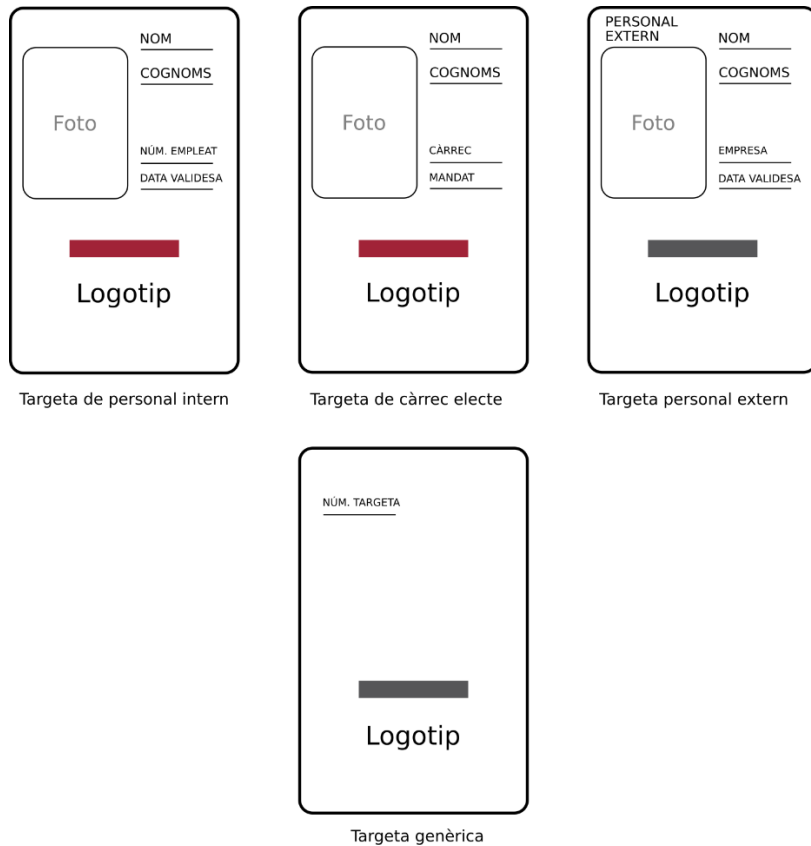
L'entrega de les targetes sense personalitzar s'haurà de realitzar d'acord amb les previsions del punt 2 i les targetes personalitzades segons les previsions del punt 3.

2. Disseny i impressió de la targeta

L'empresa contractista haurà d'imprimir 10.000 targetes amb diferents dissenys base. S'hauran de realitzar un mínim de 4 dissenys base d'acord amb els models que consten en aquest apartat i la Diputació podrà afegir 2 dissenys addicionals, un cop iniciada la vigència del contracte

El disseny serà en vertical i hi hauran els elements següents:

- Espai per fotografia a l'esquerra
- Espai per les dades personalitzades a la dreta
- Resta d'espai per logotips o altres patrons.
- Revers sense espai a personalitzar



El disseny de la figura anterior mostra les línies generals del disseny, no és representatiu del disseny final que dependrà del triat per la subdirecció d'Imatge Corporativa i Promoció Institucional.

L'empresa contractista haurà de facilitar a la Diputació de Barcelona les plantilles i la informació per tal que la subdirecció d'Imatge Corporativa i Promoció Institucional pugui fer el disseny desitjat. Així mateix, haurà de participar a les reunions que s'indiquin per acordar el disseny.

El disseny serà completament fet per la Diputació de Barcelona amb l'assessorament de l'empresa contractista. A continuació es defineixen les característiques que haurà de disposar la impressió de les targetes:

- Impressió d'offset en quadricromia (CMYK + UV) a 600dpi amb capa ultravioleta pels detalls de seguretat.
- Acabat en mate però amb parts brillants definides pel disseny acordat.

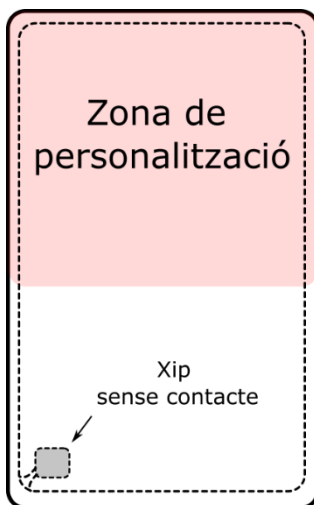
Una vegada definit els dissenys finals l'empresa contractista haurà d'imprimir targetes de prova perquè aquestes quedin validades per la Diputació de Barcelona. Com a mínim s'haurà d'imprimir 4 targetes per cada disseny base amb dades fictícies. Dues de les targetes de cada disseny base hauran d'estar personalitzades amb fotografia i dades que no corresponguin a cap de les persones afectades.

En el termini màxim dues setmanes des de la validació dels dissenys, la Diputació comunicarà a l'empresa el nombre de targetes que ha d'imprimir de cada un dels dissenys i els haurà de lliurar en el termini màxim previst en el punt 7.

3. Personalització

L'empresa contractista haurà de personalitzar aproximadament 8.000 de les targetes totals. El nombre definitiu de les targetes a personalitzar s'indicarà en el termini màxim de 2 mesos des de la signatura del contracte.

3.1. Impressió



S'hauran d'imprimir les dades següents per cada targeta personalitzada:

- Fotografia de la persona
- Dades com: nom, cognom, núm. empleat, caducitat i altres que es decideixin per disseny.

La impressió per a la personalització s'ha de realitzar en 600dpi i en una tècnica que respecti el disseny brillant i mate de la targeta.

L'empresa contractista haurà de crear una plantilla de personalització on s'encaixi les dades amb el disseny base. La tipografia del text serà l'acordada amb la Diputació de Barcelona.

La zona de personalització només estarà a la part superior de l'anvers de la targeta. El xip sense contacte haurà de quedar a la part inferior esquerra

3.2. Programació de la targeta

Una vegada impresa la targeta s'haurà de realitzar les següents operacions:

- Canvi de la clau CMK i KeySettings de la targeta.
- Creació d'aplicacions.
- Canvi de claus criptogràfiques de les aplicacions.
- Creació del fitxer/s corporatius.
- Escripció de la informació als fitxers segons taula d'Excel.

En l'Annex 2 es pot observar el detall de les aplicacions corporatives i externes on s'indica tota la informació necessària per crear-les. Durant l'execució podrà variar algun aspecte menor, com afegir una aplicació, fitxer o número de claus criptogràfiques a afegir.

3.3. Targeta SAM

La Diputació de Barcelona subministrarà a l'empresa contractista una targeta SAM amb les claus criptogràfiques programades. L'empresa contractista haurà de:

- Custodiar-la durant el procés de creació de targetes de forma segura.
- Retornar-la una vegada finalitzada la personalització de les targetes.

En cas de pèrdua de targeta, l'empresa contractista haurà de re-programar les targetes corporatives amb una nova targeta SAM i fer-se càrrec de les despeses de generar noves claus mestres.

4. Transferència d'informació

La Diputació de Barcelona lliurarà a l'empresa contractista les dades de les targetes mitjançant un fitxer Excel que hi estigui xifrat. Les dades estaran separades per columna. Cada columna representarà un camp que s'imprimirà o enregistrarà a un fitxer de la targeta. Hi haurà un identificador únic decimal per cada targeta. Per les dades que es vulguin imprimir la columna tindrà el nombre màxim de caràcters que càpiguen per la plantilla d'impressió.

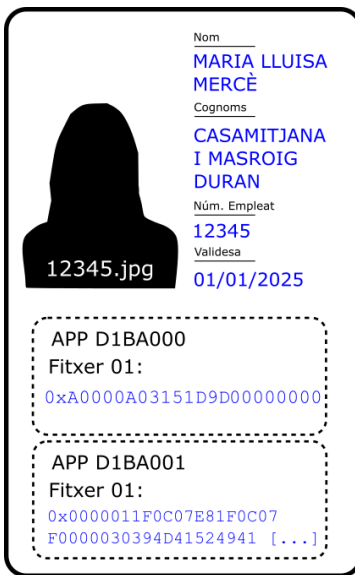


Diagrama d'una targeta corporativa amb els següents camps:

- Nom:** MARIA LLUISA
- Cognoms:** CASAMITJANA I MASROIG DURAN
- Núm. Empleat:** 12345
- Validesa:** 01/01/2025
- Foto:** 12345.jpg
- APP D1BA000**
- Fitxer 01:** 0xA0000A03151D9D00000000
- APP D1BA001**
- Fitxer 01:** 0x0000011F0C07E81F0C07F00000F0000030394D41524941 [...]

La Diputació de Barcelona serà l'encarregada de validar les dades entregades i l'ordre de l'Excel serà el mateix que l'empresa contractista haurà d'entregar a l'hora de subministrar les targeta.

Les fotografies s'entregaran en format JPEG amb la relació d'aspecte i resolució acordades en el disseny. S'entregaran les fotografies amb el mateix nom de fitxer que l'identificador únic (en l'exemple és el número de funcionari). Les fotografies s'entregaran a part del fitxer Excel de forma xifrada.

Tots els arxius que continguin dades personals (incloent-hi imatges) s'entregaran de forma xifrada que asseguri garantir la protecció de dades.

A continuació es mostra un exemple de com seria una fila del fitxer d'Excel amb aquesta proposta de disseny. Es pot observar a la taula com estaran separades les dades:

Núm. empleat 	Nom F1	Nom F2	Cognom F1	Cognom F2	Cognom F3
12345	MARIA LLUISA	MERCÈ	CASAMITJANA	I MASROIG	DURAN

Validesa	Fitxer 01 – APP 0xD1BA00	Fitxer 01 – APP 0xD1BA01	Foto	UUID
01/01/2025	0xA00A03151D9D	0x0000011F0C07E81F0C07F00000F00000 [...]	12345.jpg	[Retorn de l'empresa]

La columna "Fitxer 01 – APP D1BA00" i "Fitxer 01 – APP D1BA01" estarà el valor en hexadecimal que s'haurà d'escriure als respectius fitxers de la targeta.

Es possible que durant l'execució del contracte s'hagin d'afegir més dades, però es facilitaran amb el mateix format que el comentat en aquest apartat.

L'empresa contractista haurà de retornar a la Diputació de Barcelona l'Excel relacionant el número d'empleat amb la UUID de la targeta que se li ha assignat.

5. Coordinació amb lot 2

L'empresa contractista del lot 1 haurà de coordinar-se amb l'empresa contractista del lot 2, en el cas que sigui diferent. Ho haurà de fer en els aspectes següents:

- Seguir les indicacions pel procés de programació de targeta.
- Utilitzar la targeta SAM facilitada per utilitzar les claus AES generades així com fer la diversificació de claus.
- Participar a les reunions de coordinació indicades pel Gabinet de Prevenció i Seguretat
- Entregar targetes de mostra perquè l'empresa contractista del lot 2 validi la programació correcta de la targeta.
- La coordinació amb la contractista del LOT 2 en cap cas implica la cessió de dades personals.

6. Control de qualitat

L'empresa contractista haurà de realitzar un control de qualitat de les targetes abans de ser entregades tant les personalitzades com les no personalitzades. Per les targetes personalitzades haurà de validar que està programada correctament.

L'empresa contractista del lot 1 haurà d'entregar a l'empresa contractista del lot 2 mostres de dues targetes personalitzades amb dades diferents que no siguin reals/que no pertanyin a les persones afectades al lot 1, per tal de validar que la programació és correcta abans de realitzar la producció.

L'empresa contractista haurà d'assumir el cost de tornar a imprimir les targetes que presentin defectes d'impressió.

7. Terminis

L'empresa contractista haurà d'entregar les targetes sense personalitzar en el termini màxim 30 dies hàbils des de la comunicació del disseny base definitiu i les targetes personalitzades en un termini màxim de 30 dies hàbils a comptar a partir de l'entrega per part de la Diputació de totes les dades de les targetes.

LOT 2 – SERVEI D'ASSESSORAMENT DE CLAUS MESTRES, SUBMINISTRAMENT DE TARGETES SAM, LECTORS/PROGRAMADORS I DESENVOLUPAMENT DE PROGRAMARI PER CREAR TARGETES CORPORATIVES.**1. Introducció**

L'empresa contractista del lot 2 haurà de:

- Desenvolupar un programari per llegir i escriure a les targetes corporatives.
- Assessorar al Gabinet de Prevenció i Seguretat de com generar i guardar de forma segura les claus mestres per la targeta corporativa així com les diferents aplicacions que s'instal·laran indicades a l'Annex 2.
- Subministrar targetes 25 SAM per enregistrar les claus mestres generades amb les característiques tècniques indicades al punt 2 de l'Annex 1,
- Subministrar 3 lectors/programadors.

El programari, maquinari i targetes ha de permetre poder generar, gestionar, copiar i accedir a la claus criptogràfiques

2. Assessorament per la generació de claus mestres

L'empresa contractista haurà d'assessorar a la Diputació de Barcelona de com generar claus criptogràfiques de forma segura per ser utilitzades a la generació de targetes. Assessorarà també quin serà l'esquema de seguretat per guardar-les.

L'assessorament haurà de cobrir els següents aspectes.

- Formació en el programari entregat/desenvolupat per generar claus i gestionar les SAM.
- Emmagatzematge segur de les claus.
- Altres aspectes relacionats amb les claus.

3. Desenvolupament del programari

L'empresa contractista haurà de desenvolupar un programari informàtic amb les característiques següents:

El programari haurà de ser compatible amb Windows 10, podrà ser desenvolupat en qualsevol llenguatge de programació i el codi font haurà de ser propietat de la Diputació de Barcelona. La seva execució no haurà de requerir permisos d'administració.

L'objectiu del programari és poder gestionar les targetes corporatives. Haurà d'afegir les dades personals, llegir targetes d'altres organismes associats i afegir aplicacions de tercers (SALTO, DORLET, etc.).

El programari haurà de:

- Crear l'estructura d'aplicacions i fitxers corporativa.
- Afegir aplicacions de tercers.
- Llegir les dades corporatives.
- Escriure les dades corporatives.

- Permetre la lectura massiva de targetes i guarda-ho en un fitxer CSV.
- Permetre l'escriptura massiva de targetes amb la informació d'un fitxer CSV.
- Accedir a les diferents claus de forma segura mitjançant una targeta SAM.
- Crear aplicacions de forma massiva.
- Definició dels organismes, suborganismes, tipus de targeta, habilitacions i aplicacions.

3.1. Estructura d'aplicacions i fitxers

La targeta tindrà una aplicació amb la ID 0xD1BA00 on s'emmagatzemarà les dades personals del treballador: nom, cognoms, número d'empleat, organisme, sub-organisme, data creació de la targeta, data caducitat, número de treballador, càrrec o empresa. Aquesta aplicació podrà ser llegida per totes les entitats que disposin de la clau de lectura.

D'altra banda, cada ens dependent de la corporació (entitat) podrà disposar d'una altra aplicació pròpia on enregistrar el seu número únic de targeta perquè sigui utilitzat pels seus sistemes. La Diputació tindrà l'aplicació amb ID 0xD1BA01 on s'emmagatzemarà el número de targeta.

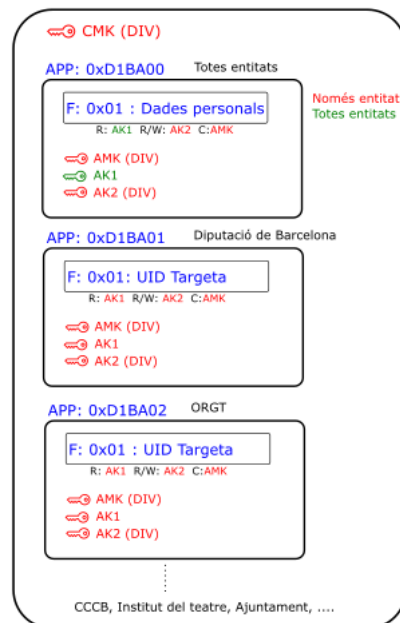


Figura 1 – Estructura d'aplicacions i claus de la targeta corporativa

Aquesta diferenciació d'aplicacions permetrà que un treballador tingui un número de targeta diferent per cada entitat. Per exemple, un treballador amb targeta de Diputació de Barcelona podrà accedir a un edifici de l'organisme de gestió tributària. En la figura 1 es mostra la representació d'una targeta amb l'aplicació 0xD1BA00 amb la informació comuna, l'aplicació 0xD1BA01 amb el número de funcionari de la Diputació i l'aplicació 0xD1BA02 amb el número d'identificació de l'Organisme de Gestió Tributària. En l'Annex 2 es pot observar com es codificarà la informació de les dades personals i el número de targeta.

3.2. Funcionalitats del programari

3.2.1. Crear l'estructura d'aplicacions i fitxers corporativa

Si l'usuari estàndard apropa al lector una targeta de fàbrica i prem “Nova targeta” el programari haurà de fer les operacions següents:

- Canviar l'CMK i key settings de la targeta nova.
- Crear les aplicacions corporatives (0xD1BA00 i 0xD1BA01) i les aplicacions externes amb les AMK i Key Settings indicades.
- Escriure les dades personals i dades de la targeta

La primera vegada que s'escriu a la targeta s'haurà de guardar la data de creació i aquesta no podrà canviar-se a posteriori si no s'esborra la informació de la targeta.

3.2.2. Afegir aplicacions de tercers

A la configuració del programari l'usuari estàndard afegirà una llista d'aplicacions de tercers amb la ID corresponent així com les key settings. L'aplicació permetrà afegir o eliminar les aplicacions externes definides a la configuració. Si es llegeix una aplicació que no es troba a la llista s'haurà d'indicar en parèntesis. No s'haurà de crear ni escriure cap fitxer d'aplicacions externes.

3.2.3. Llegir informació

L'aplicació distingirà si la targeta és pròpia de l'organisme o d'un organisme extern. Si és pròpia de l'organisme (s'ha pogut autenticar amb l'AK2) mostrarà l'etiqueta “Targeta de l'organisme”. Si llegeix el valor hexadecimal propi de l'organisme, però no s'ha pogut identificar amb l'AK2 correctament haurà de mostrar un missatge d'error, ja que indica que aquella targeta no forma part de l'organisme. Si el programari no s'ha pogut identificar amb l'AK2, però sí amb l'AK1 vol dir que la targeta és d'un organisme extern i haurà de mostrar el missatge “targeta organisme extern”. Si no es pot identificar amb cap, s'haurà d'indicar que la targeta no és reconeguda.



El programari haurà de llegir tota la informació del fitxer 0x01 de l'aplicació 0xD1BA00 i mostrar-lo en pantalla. Si la targeta és d'un organisme extern no podrà llegir el número de targeta, tipus, ni les habilitacions, ja que és informació que no està compartida. S'haurà de mostrar enfosquit a la interfície gràfica indicant a l'usuari que no es pot llegir.

Si la informació d'algun camp no està definida en la configuració es mostrarà com “Camp no reconegut” i es mostrarà el valor en hexadecimal entre parèntesis.

3.2.4. Escriure informació

Si l'aplicació es pot autenticar amb l'AK2 de l'aplicació 0xD1BA00 i la 0xD1BA01 l'aplicació permetrà escriure o canviar la informació següent:

- les dades personals: núm. , empleat, nom, cognoms, càrrec o empresa.
- número de targeta
- tipus de targeta
- les habilitacions

Si l'aplicació es pot autenticar amb la CMK permetrà afegir o eliminar aplicacions o esborrar la targeta deixant-la de fàbrica.

3.2.5. Lectura massiva de targetes

L'aplicació haurà de permetre llegir tots els paràmetres de forma massiva i guardar els registres en un fitxer .csv. Cada vegada que l'usuari estàndard passi la targeta pel lector, l'aplicació guardarà els valors en una línia del fitxer. El lector o programari hauria d'emetre un so cada vegada que es faci una lectura correcta per indicar a l'usuari estàndard que apropi una altre targeta. S'hauria de mostrar en l'aplicació el valor llegit cada vegada.

3.2.6. Programació massiva de targetes

L'aplicació permetrà crear/escriure de forma consecutiva diverses targetes. L'aplicació ha de llegir el fitxer .CSV indicat per l'usuari i mostrar el número de registres. De manera automàtica crearà l'estructura d'aplicacions i afegirà la informació de cada línia. Les dades de la targeta que s'enregistraran es mostraran a l'aplicació. Les lectures correctes/incorrectes s'hauran d'indicar mitjançant sons del lector perquè l'usuari pugui retirar i posar una nova targeta.

3.2.7. Crear aplicacions de forma massiva

El programari tindrà una opció per escriure les aplicacions indicades de forma automàtica. Una vegada seleccionada les aplicacions i prement el botó iniciar, el programari instal·larà les aplicacions a cada targeta que s'apropi al lector. El programari indicarà de forma sonora si s'ha instal·lat correctament o si hi ha algun error.

3.2.8. Configuració de l'aplicació

L'aplicació disposarà d'un apartat de configuració on es vincularà el nom de: tipus de targeta, organisme, sub-organisme amb un valor hexadecimal. En l'apartat d'habilitacions es guardarà el nom de cada bit. El bit MSB és l'activació de la targeta i queda definit per defecte, la resta de bits es podran anomenar.

En l'apartat de configuració també s'indicaran les IDs de les aplicacions corporatives on s'emmagatzemen les dades generals i el número de targeta. També on es relacionarà l'AMK, AK1 i AK2 de les aplicacions corporatives amb el número de clau de la SAM.

En el mateix apartat o en un altre s'haurà d'indicar quin és el lector de targetes, quin és el lector de SAM, la clau per accedir a la targeta SAM i el nomenament de cada clau de la targeta SAM.

Hi haurà un apartat per definir les claus AES d'una nova targeta SAM o per generar-les de forma aleatòria. Aquest apartat no cal desenvolupar-lo si l'empresa contractista subministra un altre programari per fer la tasca de definir les claus AES d'una nova targeta SAM.

3.2.9. Llista d'esdeveniments

De les diferents operacions que es facin, llegir, escriure, etc. L'aplicació mostrarà si s'ha realitzat correctament, hi ha hagut algun error o cal avisar d'algun aspecte. Es mostrarà com una llista que es podrà navegar (scroll). S'haurà d'emmagatzemar un fitxer de tipus log de tots els esdeveniments fets amb un nombre màxim de registres guardat i amb la marca temporal. En el fitxer no es poden enregistrar dades personals. Per cada acció feta s'haurà d'indicar el nom d'usuari.

3.2.10. Rols d'usuari

El programari tindrà dos rols que es defineixen a continuació:

1. **Usuari estàndard:** podrà fer les operacions d'escriure, llegir, crear nova targeta i instal·lar aplicacions.
2. **Usuari administrador:** podrà definir les APPs, les claus criptogràfiques, donar d'alta usuaris estàndard i la resta de configuració.

El primer cop d'obertura el programari haurà de demanar que el primer usuari defineixi una contrasenya d'administrador. L'administrador haurà de donar d'alta els usuaris estàndards, s'utilitzarà el mateix nom d'usuari que el del domini de Windows. Si el programari s'executa dins d'una sessió amb un usuari autoritzat s'obrirà amb el perfil sense demanar res més, si no demanarà la contrasenya d'administrador.

La interfície gràfica per aquesta funcionalitat no està definida i la proposarà l'empresa contractista.

3.3. Interfície gràfica

L'empresa contractista haurà de desenvolupar el programari amb la interfície gràfica descrita a l'Annex 3. L'empresa contractista podrà proposar canvis en la interfície gràfica o altres optimitzacions. A continuació s'indiquen algunes funcionalitats generals de la interfície:

- L'usuari administrador podrà copiar el text de tots els camps de text siguin o no editables. Per exemple: UUID, Núm. de Targeta, data, missatges d'error, etc. La forma de copiar-ho podrà ser amb doble clic, seleccionar-ho i amb tecles control + c, o qualsevol altre mètode estàndard.
- Els textos hauran d'estar en català.
- La finestra podrà ser maximitzada i tots els elements s'hauran d'adaptar a la mida de la finestra.

3.4. Configuració del programari

El programari haurà de guardar la configuració del programari en un fitxer que pugui ser llegit i editat amb editor de text i no guardarà res en el registre de Windows. De manera que aquesta configuració es pugui exportar fàcilment a un altre ordinador.

La configuració haurà de ser comuna per tots els usuaris de l'ordinador.

4. Subministrament lectors/programadors

L'empresa contractista haurà de subministrar tres lectors/programadors amb capacitat d'emmagatzemar una targeta SAM. Aquests lectors/programadors seran els utilitzats per generar les noves targetes corporatives i han de ser compatibles amb Windows 10. La connexió dels lectors han de ser via USB i alimentats per aquest. El programari desenvolupat haurà de ser compatible amb els lectors/programadors entregats.

Els lectors/programadors s'hauran de subministrar al moment de la segona entrega del programari.

5. Entrega per fases del programari

L'empresa contractista haurà de fer les entregues del programari al GPS d'acord amb el següent detall:

- Primera entrega: document amb el contingut següent: llenguatge de programació i tecnologia que s'utilitzarà pel desenvolupament del programari, funcionalitats detallades, captures de pantalles de la interfície gràfica segons l'esquema de l'Annex 3 en el termini màxim d'un mes a l'entrada en vigor del contracte.
- Segona entrega: prototip funcional del programari amb les funcionalitats desenvolupades següents: crear l'estructura d'aplicacions i fitxers corporativa, llegir la informació, escriure informació, afegir aplicacions de tercers. S'haurà d'entregar el codi font i el programa funcional en el termini màxim de tres mesos a l'entrada en vigor del contracte.
- Tercera entrega: programari amb totes les funcionalitats desenvolupades. S'haurà d'entregar el codi font i el programari funcional en el termini màxim de cinc mesos a l'entrada en vigor del contracte.
- Entrega final: Instal·lador del programari amb la versió final i errades corregides. Controladors (drivers) dels lectors entregats i codi font del programari. L'empresa contractista haurà d'entregar la documentació per registre electrònic en el termini màxim de 8 mesos des de l'entrada en vigor del contracte.

6. Resolució d'errades del programari

L'empresa contractista haurà d'aplicar mètodes de control de qualitat per validar el programari entregat amb els tests unitaris fets a cada funció. El GPS farà diferents proves per validar el programari entregat i indicarà a l'empresa contractista les errades trobades. L'empresa contractista haurà de corregir totes les errades indicades abans de fer la següent entrega.

7. Formació i manual d'ús

L'empresa contractista haurà de:

1. Realitzar, com a mínim, una sessió formativa de 2h als usuaris de l'aplicació desenvolupada. Aquesta formació podrà ser presencial o remota i s'acordarà de mutu acord entre l'empresa i el Gabinet de Prevenció i Seguretat. Els licitadors poden oferir com a millora 2 sessions de 2 hores cada sessió d'acord amb el criteri d'adjudicació 2 (clàusula 1.11 PCAP)

2. Fer un manual d'usuari del programari desenvolupat on s'expliquin les diferents funcionalitats.

8. Coordinació amb empresa contractista lot 1

L'empresa contractista del lot 2 s'haurà de coordinar amb la del lot 1 per:

- Assessorar-la de com haurà de realitzar la programació de les targetes.
- Facilitar les comandes de creació d'aplicació i creació de fitxers.
- Entregar una targeta SAM amb les claus mestres generades.
- Analitzar la programació de les targetes de mostra i validar-la.

ANNEX 1 – CARACTERÍSTIQUES TÈCNIQUES

1. Targeta corporativa

Les característiques tècniques de la targeta han de ser les següents:

- Complir amb l'estàndard ISO/IEC 7810 per les targetes ID-1
 - o Ample x Alt: 85,60 mm x 53,98 mm
 - o Gruix: 0.70mm a 0,90mm
 - o Cantonades arrodonides entre 2,88 i 3,48mm
- El material de la targeta haurà de ser de PVC.
- Les làmines exteriors del disseny base hauran de ser de PVC transparent
- Acabat mate amb detalls brillants definits per disseny
- XIP de NXP MIFARE DESFire EV1 4KB o equivalent:
 - o Interfície ISO/IEC 14443 Type A
 - o 4KB de memòria no volàtil
 - o Retenció de dades fins a 10 anys
 - o Duració de 500.000 cicles d'escriptura/lectura
 - o 28 aplicacions al PICC
 - o 32 fitxers per aplicació
 - o Certificació EAL4+
 - o Una clau mestra per targeta
 - o 14 claus criptogràfiques per aplicació
 - o Maquinari específic per processar claus AES de 128 bits.

2. Targeta SAM

Les característiques tècniques que ha de tenir la targeta SAM:

- MIFARE SAM AV3
- Criptografia MIFARE Crypto1, DES, TDEA (112 and 168 bits), AES (128, 192 and 256 bits), RSA (up to 2048 bits) i ECC (up to 256 bits).
- Certificat EAL6+
- FIPS 140-2
- 32KB de codi i data per personalitzar EEPROM
- 1KB de RAM

ANNEX 2 – ESTRUCTURA I DADES ENREGISTRADES

1. Estructura

Targeta

- **Card Master Key:** AES 128 bits diversificada amb l'UUID de la targeta seguint l'algoritme definit a (NXP Semiconductors, 2019).
- **PICC Master Key Settings:** 0x0A.

Aplicació

- **AID:** 0xD1BA00
 - **Key Settings 1:** 0x09
 - **Key Settings 2:** 0x83
 - **AMK:** AES 128 bits diversificada amb UID||00
 - **AK1:** AES 128 bits
 - **AK2:** AES 128 bits diversificada amb UID||02
- **AID:** 0xD1BA01
 - **Key Settings 1:** 0x09
 - **Key Settings 2:** 0x83
 - **AMK:** AES 128 bits diversificada amb UID||00
 - **AK1:** AES 128 bits
 - **AK2:** AES 128 bits diversificada amb UID||02
- **AID:** [SALTO]
 - **Key Settings 1:** 0x09
 - **Key Settings 2:** 0x83
 - **AMK:** AES 128
- **AID:** 0x7D0399 [DORLET]
 - **Key Settings 1:** 0xEB
 - **Key Settings 2:** 0x8D

Fitxers APP D1BA00

- **FID:** 0x01
 - **Access rights:** 0x1220



- **Communication settings:** 0x03
- **File size:** 0xC80000 (200 bytes)

Fitxers APP D1BA01

- **FID:** 0x01
 - **Access rights:** 0x1220
 - **Communication settings:** 0x03
 - **File size:** 0x0A0000 (10 bytes)

2. Estructura fitxers targeta

Codificació

D: Decimal

A: ASCII Estès (ISO/IEC 8859-1)

B: Binari

APP: 0xD1BA00

FID: 0x00 [10 bytes]

Dada a enregistrar	Mida	Byte inici	Byte final	Exemple Hexadecimal	Codificació	Exemple
Habilitacions	2	0	1	A0 00	B	1010000000000000
Tipus targeta	1	2	2	0A	D	10
Núm. targeta	4	3	6	03 15 1D 9D	D	51715485
Reserva	3	7	9	00 00 00 00	-	-

Cadena completa a programar en hexadecimal, cada camp està en un color alternatiu i la mida total és de 10 bytes:

A0	00	0A	03	15	1D	9D	00	00	00	00
----	----	----	----	----	----	----	----	----	----	----

APP: 0xD1BA01

FID: 0x00 [200 bytes]

Dada a enregistrar	Mida	Byte inici	Byte final	Exemple Hexadecimal	Cod.	Exemple DECIMAL
Organisme	2	0	1	00 00	D	0
Sub-organisme	2	2	3	01	D	1
Dia creació targeta	1	4	4	1F	D	31
Mes creació targeta	1	5	5	0C	D	12
Any creació targeta	2	6	7	07 E8	D	2024
Dia caducitat targeta	1	8	8	1F	D	31
Mes caducitat targeta	1	9	9	0C	D	12
Any caducitat targeta	2	10	11	07 F0	D	2032
Núm. Funcionari / Extern	4	12	15	00 00 30 39	D	12345
Nom	30	16	45	4D 41 52 49 41 20 4C 4C 55 49 53 41 20 4D 45 52 43 C8 00 00 00 00 00 00 00 00 00 00 00 00	A	MARIA LLUISA MERCÈ
Cognom 1	30	46	75	43 41 53 41 4D 49 54 4A 41 4E 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	A	CASAMITJANA

Cognom 2	30	76	105	49 20 4D 41 53 52 4F 49 47 20 44 55 52 41 4E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	A	I MASROIG DURAN
Carrec / Empresa	30	106	135	44 49 50 55 54 41 44 41 00	A	DIPUTADA
Reserva	64	136	199	00 00	-	-

Cadena completa a programar en hexadecimal, cada camp està en un color alternatiu i la mida total és de 200 bytes:

00 00 01 1F 0C 07 E8 1F 0C 07 F0 00 00 30 39 4D 41 52 49 41 20 4C 4C 55 49 53 41 20 4D 45 52 43 C8 00 00 00 00 00 00 00 00 00 00 00 00 43 41 53 41 4D 49 54 4A 41 4E 41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 49 20 4D 41 53 52 4F 49 47 20 44 55 52 41 4E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 49 50 55 54 41 44 41 00

ANNEX 3 – INTERFÍCIE GRÀFICA PROGRAMARI

Programador de targetes

Fitxer

Dades
Aplicacions
Configuració
Lector i SAM

Targeta:

UUID: 042D155A472180

Habilitacions:

☐ Fitxar
☒ Control d'accés

Núm.: 51715485

Tipus: Càrrec electe [0x0A]

Caducitat: 01/01/2024

Creació: 01/01/2023

Estat: ☒ Activa

APP Externes

ORGT

SALTO

DORLET

[0xF56173]

Esborrar

Afegir

Organisme:

Organisme: Diputació de Barcelona [0x0000]

Sub-organisme: Organisme de Gestió Tributària [0x000A]

Targeta de l'organisme

Dades personals:

Núm. empleat: 12345

Nom: MARIA LLUÏSA MERCÈ

1r Cognom: CASAMITJANA

2n Cognom: I MASROIG DURAN

Càrrec \ Empresa: DIPUTADA

Nova Targeta

☒ Càrrega massiva

☐ Lectura
☒ Escriptura

Fitxer: empleats.csv

Registres: 30

Posició: 5

Esborrar targeta

Llegir Targeta

Escriure targeta

Esdeveniments:

Estatus	Operació	Options
Avis	Llegir targeta	No es pot llegir núm. targeta, no pertany a l'organització.
Error	Llegir targeta	No s'ha trobat APP DIBA
Correcte	Escriure targeta	S'ha escrit correctament targeta UUID: 042D155A472180

En la figura anterior es mostra la interfície gràfica de la finestra principal del programari. A continuació es descriuen els elements bàsics que haurà de tenir:

- **Informació sobre la targeta:** s'hauran de mostrar els elements que s'indiquen a la figura en cas que la targeta sigui corporativa i es pugui llegir. Si els elements no es poden llegir hauran d'aparèixer desactivats. S'haurà de mostrar entre parèntesis el valor en hexadecimal de les habilitacions.
- **APP Externes:** Quan es produeixi una lectura de la targeta haurà d'aparèixer la llista d'aplicacions d'aquesta. Si l'aplicació està definida a la configuració haurà d'aparèixer el seu nom establert. Si no es coneguda, haurà d'aparèixer la seva ID en hexadecimal entre claudàtors.

- **Organisme:** L'usuari no podrà seleccionar l'organisme o sub-organisme de la targeta. Aquests paràmetres seran els que estiguin establerts a la configuració de l'aplicació com a "Organisme" o "Sub-organisme" actual. Si al produir-se una lectura no es coneix l'organisme codificat haurà d'aparèixer el missatge "Organisme no conegut" en un altre color i el valor en hexadecimal entre parèntesis.
- **Dades personals:** quan es faci una lectura de les dades de la targeta hauran d'aparèixer totes les dades personals. Si en la codificació no es troba un camp determinat apareixerà en blanc. El camp màxim de text és el que estigui limitat en la codificació, tant el camp numèric com el de text. S'ha de tenir en compte que els camps de text l'últim caràcter codificat ha de ser un valor NULL per indicar la fi de la cadena de text. La codificació serà en ASCII Ampliat i no es permeten caràcters fora d'aquesta codificació. Es permetrà escriure camps que no estiguin omplerts, però si el camp: nom, cognoms o número d'empleat estan buits, el programari haurà d'informar a l'usuari que estan buits i si desitja continuar.
- **Càrrega massiva:** si es selecciona aquesta opció l'usuari haurà d'indicar un fitxer .CSV. Haurà d'aparèixer una icona de carpeta al costat del nom del fitxer, quan es premi aquest haurà d'aparèixer una finestra de navegació per elegir el fitxer a llegir/escriure. Si és de lectura, el propi programari crearà les columnes (nom, cognoms, número de targeta, etc.), els botons de navegació quedaran inhabilitats. Si és d'escriptura el fitxer haurà de tenir les columnes adequades i com a mínim un registre, en cas contrari haurà d'aparèixer un error. Hi hauran 4 botons de navegació. Dos serviran per anar a les posicions d'inici o de final i els altres dos serviran per moure una posició davant o una posició darrera. Si no hi ha registres a cada extrem, els botons quedaran inhabilitats respectivament. Hi haurà una etiqueta que mostrarà la posició actual i una altre amb els registres totals. Cada vegada que es mou el cursor la interfície gràfica haurà de mostrar les dades llegides a la línia el fitxer .CSV. Cada registre es llegirà/escriurà quan el programari detecti que s'ha posat una nova targeta al lector.
- **Botons:** Els botons quedarà activats/desactivats segons els rols de l'usuari. "Nova targeta", "Escriure" o "Esborrar targeta" només estaran activats pels usuaris amb permís d'escriptura.

Programador de targetes

Fitxer

Dades Aplicacions Configuració Lector i SAM

Instal·lació aplicacions externes:

Lista APP

ORGT
SALTO
DORLET

Esborrar **Afegir**

Dades última targeta:

UUID: **042D155A472180**
Nom: MARIA LLUÏSA MERCÈ

Recompte i estat:

Programades: **10**
Errors: **0** **Reiniciar**

Iniciar
Instal·lar APPs

Configuració aplicacions externes:

APP

ORGT
SALTO
DORLET

Esborrar **Afegir**

Nom: ID:

Key Settings 1: Key Settings 2:

AMK: **Desar**

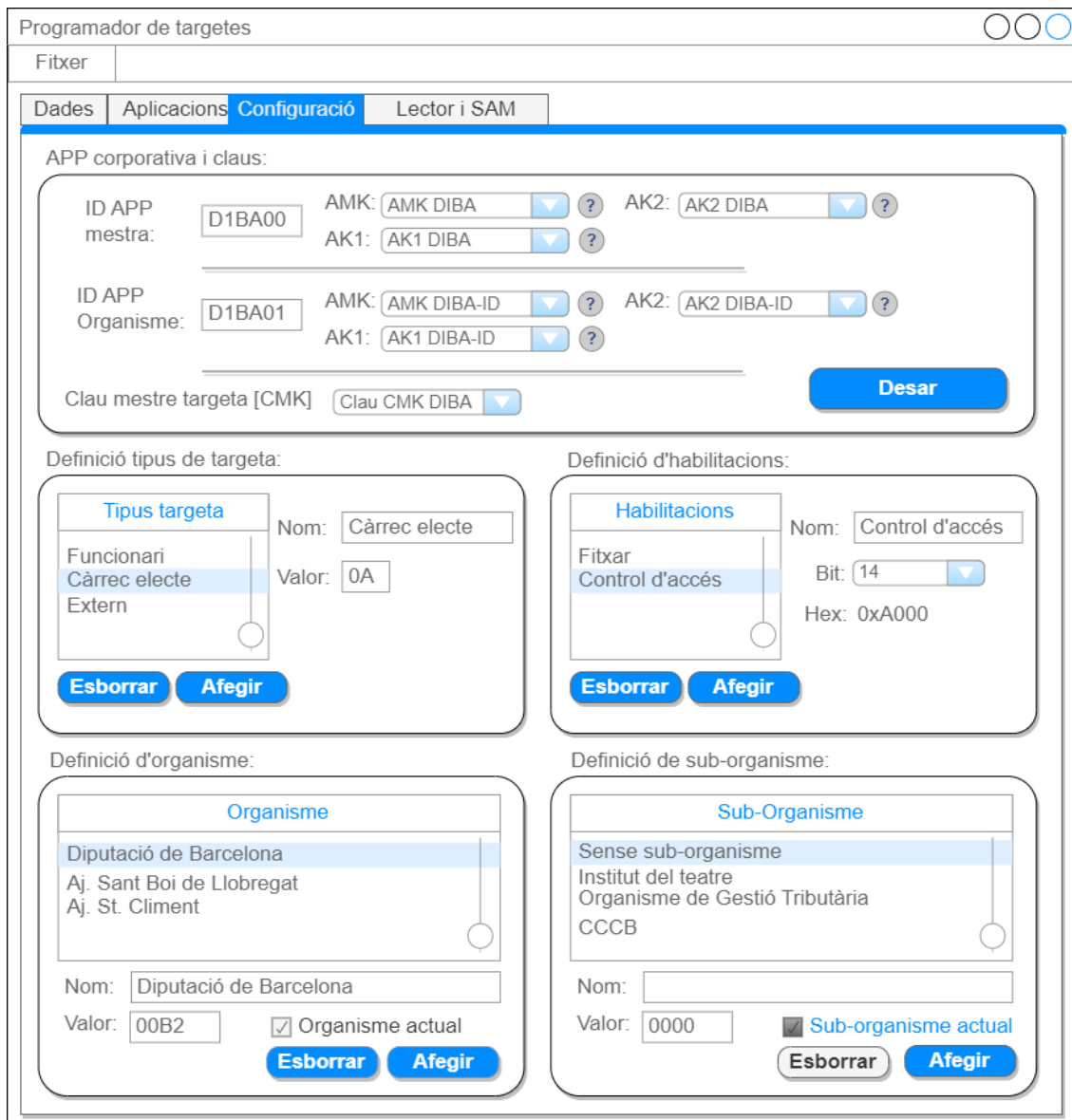
☒ Afegir APP a les targetes noves

Esdeveniments:

Estatus	Operació	Options
Avís	Instal·lar APP	Aplicació DORLET ja instal·lada
Error	Instal·lar APP	La clau CMK proporcionada és incorrecte
Correcte	Instal·lar APPs	S'ha instal·lat correctament l'aplicació [SALTO, ORGT, DORLET]

En la figura anterior es mostra l'apartat on es defineixen les aplicacions i on es poden instal·lar les aplicacions de forma massiva. A continuació es descriuen els elements bàsics que haurà de tenir:

- **Instal·lació d'aplicacions externes:** A la llista d'APP apareixeran per defecte les aplicacions que estiguin configurades com a "Afegir APP a les targetes noves" tot i que l'usuari ho podrà modificar, afegint o traient-les. Quan l'usuari prem "Iniciar" el programari haurà de reconèixer la targeta corporativa posada en el lector i afegir les aplicacions que estiguin a la llista. El programari indicarà amb sons acústics quan s'ha finalitzat la instal·lació perquè l'usuari posi la següent targeta. Hi haurà un comptador de les targetes programades i els errors que s'han produït. Apareixerà el UUID de la targeta i el nom i cognoms de la última targeta programada correctament. El botó "Iniciar" serveix per la programació seqüencial de targetes i el "Instal·lar APPs" per programar-ne només una.
- **Configuració aplicacions externes:** Aquesta opció només apareixerà si l'usuari és administrador. Es podran donar d'alta les aplicacions externes conegudes. Les Key Settings i AMK només seran configurades per les aplicacions que es vulguin afegir a les targetes.



En la figura anterior es mostra la pàgina de configuració de l'aplicació a continuació es descriuen els diferents elements de la interfície:

- **APP corporativa i claus:** en aquest apartat l'usuari indicarà la ID de les dues aplicacions corporatives que hi haurà a la targeta. La primera és l'aplicació mestra on s'emmagatzemen les dades personals i la segona on s'emmagatzema el número de targeta. A cada una d'elles s'indiquen les tres claus, la mestra (AMK), la de lectura (AK1) i la d'escriptura (AK2). També s'haurà d'indicar la clau mestre CMK de la targeta.
- **Definició tipus de targeta:** la interfície gràfica ha de tenir una llista on apareguin els diferents tipus de targeta. L'usuari administrador podrà afegir i treure els tipus de targetes. Com a màxim poden haver-hi 255 tipus de targeta ja que està definit per un byte. L'usuari haurà de poder moure's mitjançant les tecles de pujar i baixar i automàticament haurà d'apareixer el valor hexadecimal de cada tipus. El programari haurà d'avisar si el valor ja està repetit i no permetrà posar altres valors que no siguin d'un byte definit en hexadecimal. Si només s'indica un caràcter s'assumirà que els primers 4 bits són 0 i el programari l'haurà d'afegir automàticament.

- **Definició d'habilitacions:** la interfície gràfica ha de tenir una llista on apareguin les diferents habilitacions. L'usuari administrador podrà anomenar fins 14 habilitacions. Hi haurà un menú desplegable on apareixeran el número de bit que s'assignarà a l'habilitació. El bit 0 està reservat per l'activació de la targeta, aquesta opció a la pestanya de dades. Al moure's per la llista d'habilitacions haurà d'aparèixer el valor el número de bit. L'etiqueta Hex mostrarà el valor en hexadecimal de totes les habilitacions.
- **Definició d'organisme i sub-organisme:** la interfície gràfica ha de tenir una llista on l'usuari administrador pugui afegir els diferents organismes amb el seu nom i el seu valor en hexadecimal. Cada organisme tindrà els diferents sub-organismes. Si es selecciona un organisme, hauran d'aparèixer els seus sub-organismes a la llista del costat. L'usuari administrador seleccionarà només un organisme i sub-organisme com "actual" que serà el que s'enregistrarà a les targetes i el que es validarà com a propi. El valor 0x0000 del sub-organisme indica que no n'hi ha. Hi haurà una opció que sigui "sense sub-organisme" que no es podrà esborrar.

Programador de targetes

Fitxer

Dades Aplicacions Configuració **Lector i SAM**

Lectors:

Lector targeta: NXP-PEGODA

Lector SAM: SMART-CARD Reader

☒ Activar so llegir/escriure

Accés a SAM:

Clau: *****

Nomenament de claus:

Clau

CMK

AMK DIBA

AK1 DIBA

AK2 DIBA

Nom: CMK

Núm. Clau: 1

☒ Diversificada amb UUID

Generació claus:

A definir

Esdeveniments:

Estatus	Operació	Options
Avís	Accés SAM	No s'ha trobat targeta SAM
Error	Accés SAM	Clau d'accés incorrecte
Correcte	Generació Claus	S'ha creat la clau 01 a la targeta

En la figura anterior es mostra la pàgina de configuració de l'aplicació a continuació es descriuen els diferents elements de la interfície:

- **Lectors:** en aquest apartat apareixeran els lectors/programadors de targeta i SAM detectats. L'usuari administrador podrà seleccionar si hi ha més d'un. Es podrà seleccionar l'opció de que el lector faci els sons en la lectura/escriptura o deixar-lo silenciàt.
- **Accés SAM:** en aquest apartat l'usuari administrador haurà de posar les credencials per desbloquejar la targeta SAM. La caixa de text amb les credencials permetrà enganxar el valor de la clau per facilitar els gestors de contrasenyes. El botó autenticar permetrà verificar que la claus és correcte i es pot accedir a la SAM.
- **Nomenament de claus:** l'usuari administrador podrà anomenar les claus que la SAM tingui donades d'alta. Les claus sempre seran AES de 128 bits. L'usuari podrà indicar si aquesta clau

està diversificada amb la UUID. Si l'usuari esborra una clau que està utilitzada en l'apartat de configuració el programari haurà d'informar.

- **Generació de claus:** L'empresa contractista haurà de proposar la interfície gràfica de com generar o programar les claus a la targeta SAM. Aquest apartat es pot no incloure si s'entrega un programari extern que faci la mateixa funció.

Metadades del document

Núm. expedient	2020/0004486
Tipus documental	Plec de clàusules o condicions
Títol	PPT relatiu al subministrament, impressió i personalització de targetes corporatives i servei d'assessorament de claus mestres, subministrament de targetes SAM i lectors/programadors i desenvolupament d'un programari per crear targetes corporatives, dividit en 2 lots

Signatures

Signatari	Acte	Data acte
Juan Miguel Capell Manzanares (SIG)	Cap de Gabinet de Prevenció i Seguretat Signa	16/01/2024 16:51

Validació Electrònica del document

Codi (CSV)	Adreça de validació	QR
0e3dae581dfcfd9536aa	https://seuelectronica.diba.cat	

