



Conveni de col·laboració entre el Ministeri d'Administracions Públiques i el Consorci Administració Oberta Electrònica de Catalunya per a la prestació mútua de serveis d'administració electrònica

ANNEX II

SERVEIS OFERTS PEL MAP PER A LA VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA

- I. Condicions generals**
- II. Condicions tècniques i funcionals**



ANNEX II

SERVEIS OFERTS PEL MAP PER A LA VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA D'UN CIUTADÀ

I. CONDICIONS GENERALS

1. OBJECTE

L'objecte d'aquest annex és regular els drets i les obligacions que s'estableixen per a la prestació al Consorci AOC, per part del MAP, dels serveis de verificació de dades d'identitat i de verificació de dades de residència.

En l'àmbit de l'Administració general de l'Estat, el passat 28 d'abril de 2006 es van aprovar dos reials decrets en relació amb els procediments administratius de l'Administració general de l'Estat i dels organismes públics vinculats o dependents:

- El Reial decret 522/2006, pel qual se suprimeix l'aportació de fotocòpies de documents d'identitat.
- El Reial decret 523/2006, pel qual se suprimeix l'exigència d'aportar el certificat d'empadronament com a document per provar el domicili i la residència.

En aquests reials decrets s'estableix que els documents esmentats es poden substituir per una consulta al Sistema de Verificació de Dades d'Identitat (SVDI) i al Sistema de Verificació de Dades de Residència (SVDR), les regulacions dels quals estan establertes, respectivament, en l'Ordre PRE/3949/2006, de 26 de desembre, i en l'Ordre PRE/4008/2006, de 27 de desembre.

A causa de l'interès per part de la resta d'administracions públiques per desenvolupar els elements normatius i tècnics equivalents per eliminar l'obligació d'aportar els documents esmentats, s'estableix l'oportunitat d'utilitzar els serveis desenvolupats pel MAP per a la verificació de dades d'identitat i la verificació de dades de residència.

2. ABAST

L'aplicació d'aquest annex habilita qualsevol aplicació informàtica dels òrgans o de les entitats de les administracions catalanes a utilitzar l'SVDI i l'SVDR per verificar les dades d'identitat i de residència dels ciutadans en els termes que es desenvolupen més endavant.



3. OBLIGACIONS DEL PRESTADOR DEL SERVEI

El MAP, com a prestador de l'SVDI i de l'SVDR, assumeix les obligacions següents:

- (i) Posar a disposició de les administracions catalanes, a través del Consorci AOC, els serveis de verificació i consulta de dades d'identitat i de residència d'un ciutadà.
- (ii) Disposar d'entorns de prova de la integració dels serveis a fi de garantir-ne la correcta operació amb caràcter previ a la posada a disposició dels usuaris finals.
- (iii) Habilitar els mecanismes per oferir el suport necessari als equips d'integració i desenvolupament del Consorci AOC per a la integració de les seves aplicacions amb els serveis.
- (iv) Disposar dels recursos necessaris per atendre i resoldre les consultes i les incidències derivades de l'ús dels serveis.
- (v) Proporcionar els elements d'auditabilitat de les operacions realitzades que permetin certificar el no-repudi de les transaccions.
- (vi) Adoptar totes les mesures de seguretat necessàries per protegir degudament la informació i els serveis de verificació de dades d'identitat i de residència oferts.
- (vii) Garantir l'escalabilitat, la robustesa, la disponibilitat, la integritat i la confidencialitat de totes les dades relacionades amb la prestació dels serveis de verificació de dades.

4. OBLIGACIONS DEL BENEFICIARI DELS SERVEIS

El Consorci AOC, en nom de les administracions catalanes beneficiàries de l'SVDI i de l'SVDR, assumeix els compromisos següents:

- (i) Dur a terme les tasques de connectivitat i desplegament pertinents per poder accedir des de les seves pròpies dependències o instal·lacions a l'SVDI i a l'SVDR a través del Sistema d'Aplicacions i Xarxes per a les Administracions (SARA), desenvolupat pel MAP.
- (ii) Complir les mesures de seguretat i els requisits d'autenticitat, confidencialitat i integritat establerts en l'apartat II d'aquest annex.
- (iii) Concertar amb el MAP la realització de proves de rendiment o monitoratge dels serveis, a fi de no comprometre la disponibilitat d'altres serveis oferts a la resta d'usuaris d'aquests sistemes de verificació de dades.
- (iv) Designar un responsable, que serà l'encarregat d'autoritzar els accessos en l'àmbit de les administracions públiques catalanes a través del Consorci AOC, i comunicar el seu nomenament i cessament al Ministeri d'Administracions Públiques.



- (v) Coordinar amb el MAP els processos d'administració d'aplicacions i sistemes usuaris de l'SVDI i l'SVDR, subministrant al MAP la informació requerida per donar d'alta tant empleats públics com aplicacions informàtiques usuàries dels serveis.

5. ACORD DE QUALITAT DELS SERVEIS

Els serveis objecte d'aquest annex estan subjectes a les condicions tècniques i funcionals que recull l'apartat II.

6. REFERÈNCIES

El MAP pot fer pública la relació d'organismes usuaris dels serveis en qualsevol llista de referència de beneficiaris o en qualsevol butlletí de premsa publicat, i sense autorització prèvia.

El Consorci AOC pot informar de la utilització dels serveis esmentats sense autorització prèvia per part del MAP.

7. CONTACTES DE REFERÈNCIA

La resolució de consultes tècniques relacionades amb la utilització dels serveis i de consultes de caràcter administratiu relatives a l'abast d'aquest annex s'ofereix a través dels contactes de referència següents:

SERVEI	SVDI i SVDR
Oferent del servei	Ministeri d'Administracions Públiques
Responsable tècnic del servei	Director de la Divisió de Projectes Tecnològics per a l'AGE Telèfon: 91 273 24 61 Adreça electrònica: sgprotec@map.es Adreça postal: María de Molina, 50, 9a planta 28071 Madrid
Responsable Administratiu de l'annex	<u>José Luis Redondo Pérez</u> Vocal assessor de la Direcció General de Modernització Administrativa Telèfon: 91 273 24 63 Adreça electrònica: joseluis.redondo@map.es Adreça postal: María de Molina, 50, 9a planta 28071 Madrid

II. CONDICIONS TÈCNIQUES I FUNCIONALS DEL SISTEMA DE VERIFICACIÓ DE DADES D'IDENTITAT I RESIDÈNCIA



Índex

1. DESCRIPCIÓ DELS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA.....	6
2. ADOPCIÓ DE MESURES DE SEGURETAT, ORGANITZATIVES O TÈCNIQUES, PER A L'ACCÉS ALS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA.....	6
3. ACCÉS ALS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA.....	7
4. REQUISITS D'AUTENTICITAT PER ACCEDIR ALS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA	7
5. REQUISITS DE CONFIDENCIALITAT DELS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA	7
6. REQUISITS D'INTEGRITAT DE LA INFORMACIÓ PROPORCIONADA PELS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA	8
7. REQUISITS DE DISPONIBILITAT DE LA INFORMACIÓ PROPORCIONADA PELS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA	9
8. GARANTIES JURÍDIQUES DELS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA DAVANT POSSIBLES RECURSOS	9
9. CONDICIONS DE LA PRESTACIÓ DEL SERVEI.....	10



1. DESCRIPCIÓ DELS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA

El Sistema de Verificació de Dades d'Identitat posat a disposició de les administracions públiques per part del Ministeri d'Administracions Públiques s'estableix com a servei horitzontal per a la consulta i la comprovació de les dades del document d'identificació del ciutadà custodiades per la Direcció General de la Policia i de la Guàrdia Civil a partir del que disposa la Llei orgànica 2/1986, de 13 de març, de cossos i forces de seguretat, que atribueix al Cos Nacional de Policia la funció d'expedició del document nacional d'identitat i el control d'entrada i sortida del territori nacional d'espanyols i estrangers. Aquesta informació es troba registrada i custodiada als fitxers de la Direcció General de la Policia i de la Guàrdia Civil, que són les que assumeixen la gestió del document nacional d'identitat i de la targeta d'identificació d'estrangers (les seves denominacions, segons les ordres INT/1751/2002, de 20 de juny i INT/2190/2006, de 19 de juny, són ADDNIFIL i ADEXTTRA, respectivament).

El Sistema de Verificació de Dades de Residència posat a disposició de les administracions públiques per part del Ministeri d'Administracions Públiques s'estableix com a servei horitzontal per a la consulta i la comprovació de les dades sobre residència dels ciutadans mitjançant l'accés als padrons municipals coordinats per l'Institut Nacional d'Estadística, a partir del que disposa la Llei 7/1985, de 2 d'abril, reguladora de les bases de règim local, en relació amb el padró municipal, en la qual s'atribueix a l'Institut Nacional d'Estadística, entre d'altres, la funció de coordinació dels diferents padrons municipals. Aquesta informació està registrada i custodiada en els fitxers de l'Institut Nacional d'Estadística, registrats en l'Agència de Protecció de Dades amb la denominació «PADRONS MUNICIPALS», segons l'Ordre ECO/143/2002, de 10 de gener, publicada en el BOE 26, de 30 de gener de 2002.

2. ADOPCIÓ DE MESURES DE SEGURETAT, ORGANITZATIVES O TÈCNIQUES, PER A L'ACCÉS ALS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA

- 2.1. Amb caràcter general, els organismes que accedeixin als sistemes de verificació de dades d'identitat i de residència han de complir les mesures de seguretat, conservació i normalització que es detallen en els criteris de seguretat, normalització i conservació de les aplicacions utilitzades per a l'exercici de potestats, aprovats pel Consell Superior d'Administració Electrònica mitjançant Resolució de 26 de maig de 2003 i les revisions posteriors.
- 2.2. L'abast i la intensitat d'aplicació de les mesures de seguretat, conservació i normalització dependran del resultat de l'anàlisi i la gestió de riscos que es faci. A aquest efecte, es recomana utilitzar la metodologia d'anàlisi i gestió de riscos dels sistemes d'informació (MAGERIT) del Consell Superior d'Administració Electrònica.
- 2.3. El que disposa aquest document s'ha d'aplicar d'acord amb el que preveu la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal i la resta de normativa aplicable en aquesta matèria, com el Reglament de mesures



de seguretat dels fitxers automatitzats de dades de caràcter personal, aprovat pel Reial decret 994/1999, d'11 de juny.

3. ACCÉS ALS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA

- 3.1. L'accés als sistemes de verificació de dades d'identitat i de residència es fa a través del Sistema d'Aplicacions i Xarxes per a les Administracions Públiques (SARA), seguint l'esquema de connexió que té establert per a qualsevol departament o organisme públic.
- 3.2. Els sistemes de verificació de dades d'identitat i de residència presenten dues formes d'accés per fer les consultes corresponents sobre la identitat i el lloc de domicili i residència d'un ciutadà:
 - Una interfície accessible a través d'un navegador d'Internet, d'acord amb l'RFC 2616: protocol de transferència d'hipertext (HTTP/1.1 o superior) de l'IETF, en què un empleat públic, degudament acreditat i identificat, pot realitzar consultes disposant només d'un navegador amb accés a SARA i signatura electrònica.
 - Una interfície automatitzada de servei web, d'acord amb l'estàndard WSDL 1.1 o superior del W3C, la definició inicial i les actualitzacions successives de la qual es posen a disposició dels departaments i organismes a través del Consell Superior d'Administració Electrònica i la Comissió Permanent.

4. REQUISITS D'AUTENTICITAT PER ACCEDIR ALS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA

- 4.1. Els accessos als sistemes de verificació de dades d'identitat i de residència s'efectuen utilitzant certificats electrònics reconeguts que compleixin la recomanació UIT X.509, versió 3 o superiors (ISO/IEC 95948 de 1997).
- 4.3. No es poden utilitzar certificats electrònics caducats o revocats per accedir als sistemes de verificació de dades d'identitat i de residència.

5. REQUISITS DE CONFIDENCIALITAT DELS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA

- 5.1. El Sistema de Verificació de Dades d'Identitat ofereix consultes en les quals, a partir del número del document d'identificació del ciutadà o estranger, es retorna el total, o un subconjunt, de les dades incorporades en el document esmentat:
 - nom i cognoms del titular del document,
 - lloc i data de naixement,
 - nom dels pares,
 - sexe i
 - estat de vigència del document.



En tractar-se de dades de caràcter personal, el responsable de cada òrgan administratiu ha de signar una autorització, degudament justificada, per a cada usuari i aplicació que accedeixi al sistema.

5.2. El Sistema de Verificació de Dades de Residència, a partir del número del document d'identificació del ciutadà o d'un conjunt de dades personals suficients per identificar-lo unívocament, retorna el total, o un subconjunt, de les dades referents al domicili i la residència associades a un ciutadà:

- província,
- municipi,
- entitat col·lectiva,
- entitat singular,
- nucli i
- adreça (via, km, número, número superior, bloc, portal, escala, planta i porta).

En cas que les dades introduïdes no siguin suficients per identificar de manera unívoca un ciutadà, el sistema no proporcionarà informació sobre cap ciutadà en la resposta.

En tractar-se de dades de caràcter personal, el responsable de cada òrgan administratiu ha de signar una autorització, degudament justificada, per a cada usuari i aplicació que accedeixi al sistema.

5.3. En el Consorci AOC hi ha un responsable o administrador delegat dels sistemes esmentats que determina els usuaris de la seva administració que hi tenen accés i les dades que poden obtenir.

5.4. Per consultar els sistemes de verificació de dades d'identitat i de residència, és necessari el consentiment de l'interessat les dades del qual s'hagin de consultar, tret que una norma de rang de llei autoritzi la consulta. Aquest consentiment haurà de constar en la sol·licitud d'iniciació del procediment, o en qualsevol altra comunicació posterior, sempre que la comunicació sigui prèvia a la consulta en el sistema, i no es podrà fer cap consulta en cas de no comptar amb el consentiment de manera fefaent. Els impresos o formularis electrònics de sol·licituds d'iniciació de procediments administratius s'han d'adequar per recollir el consentiment esmentat.

5.5. La consulta i l'accés a la informació proporcionada pels sistemes de verificació de dades d'identitat i de residència s'ha de fer amb una finalitat concreta, que ha de quedar recollida en el moment de la consulta. La informació obtinguda només es podrà utilitzar per a aquesta finalitat.

6. REQUISITS D'INTEGRITAT DE LA INFORMACIÓ PROPORCIONADA PELS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA



Totes les consultes que es facin als sistemes de verificació de dades d'identitat i de residència, com també les respostes que retornin, han d'haver estat signades electrònicament. Aquesta signatura electrònica té per objectiu garantir tant la integritat de les dades bescanviades com la identitat de les parts que hi intervenen i el no-repudi de la consulta.

De la mateixa manera, totes les consultes que els sistemes de verificació de dades d'identitat i de residència hagin de fer a la Direcció General de la Policia, a l'Institut Nacional d'Estadística o a altres organismes amb capacitat d'informar sobre la identitat o la residència dels ciutadans, com també les corresponents respostes obtingudes, han de ser degudament signades electrònicament per garantir tant la integritat de la informació com la identitat d'ambdós organismes.

7. REQUISITS DE DISPONIBILITAT DE LA INFORMACIÓ PROPORCIONADA PELS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA

Els sistemes de verificació de dades d'identitat i de residència estan disponibles els 7 dies de la setmana i les 24 hores del dia.

8. GARANTIES JURÍDIQUES DELS SISTEMES DE VERIFICACIÓ DE DADES D'IDENTITAT I DE RESIDÈNCIA DAVANT POSSIBLES RECURSOS

- 8.1. Els serveis web proporcionats per aquests sistemes segueixen l'estàndard d'intercanvi de dades definit per la iniciativa de substitució de certificats de suport paper del Consell Superior d'Administració Electrònica, que reuneix, a partir de la normativa vigent, les garanties jurídiques aplicables a l'intercanvi de dades entre administracions públiques.
- 8.2. Els sistemes de verificació de dades d'identitat i de residència disposen d'un mòdul d'auditoria, en el qual es registren totes les consultes de dades de residència realitzades, la informació de context associada, la identitat del sol·licitant, la data i la finalitat de la consulta, i aquells esdeveniments rellevants desencadenats a partir de la mateixa consulta. Es garanteix la integritat i el no-repudi de la informació registrada mitjançant tècniques de signatura electrònica i segellament de temps, i s'estableixen, així mateix, mesures tècniques per garantir la disponibilitat i la recuperació de la informació que no es mantingui en línia per motius d'eficiència tècnica o seguretat.
- 8.3. Per certificar la data i el temps de les activitats i els successos registrats en els sistemes de verificació de dades d'identitat i de residència, es fa ús del servei de segellament de temps de la plataforma de validació de signatura electrònica del Ministeri d'Administracions Públiques, sincronitzada amb el Reial Institut i Observatori de l'Armada, d'acord amb el que preveu sobre l'hora legal el Reial decret 1308/1992, de 23 d'octubre, pel qual es declara el laboratori de l'Armada com a laboratori dipositari del patró nacional de temps i laboratori associat al Centre Espanyol de Metrologia, i segons les condicions tècniques i els protocols que estableixi l'organisme esmentat.



8.4. Solament el personal de l'Administració pública degudament autoritzat i acreditat pot accedir a les funcions d'auditoria dels sistemes de verificació de dades d'identitat i de residència.

9. CONDICIONS DE LA PRESTACIÓ DEL SERVEI

9.1. La gestió dels sistemes de verificació de dades d'identitat i de residència correspon al Ministeri d'Administracions Públiques.

9.2. Els òrgans i els organismes públics de les administracions catalanes que facin ús, a través del Consorci AOC, d'aquests serveis estan subjectes a les mesures de seguretat, els requisits d'autenticitat, integritat, confidencialitat, disponibilitat i criteris tècnics establerts en aquest document.