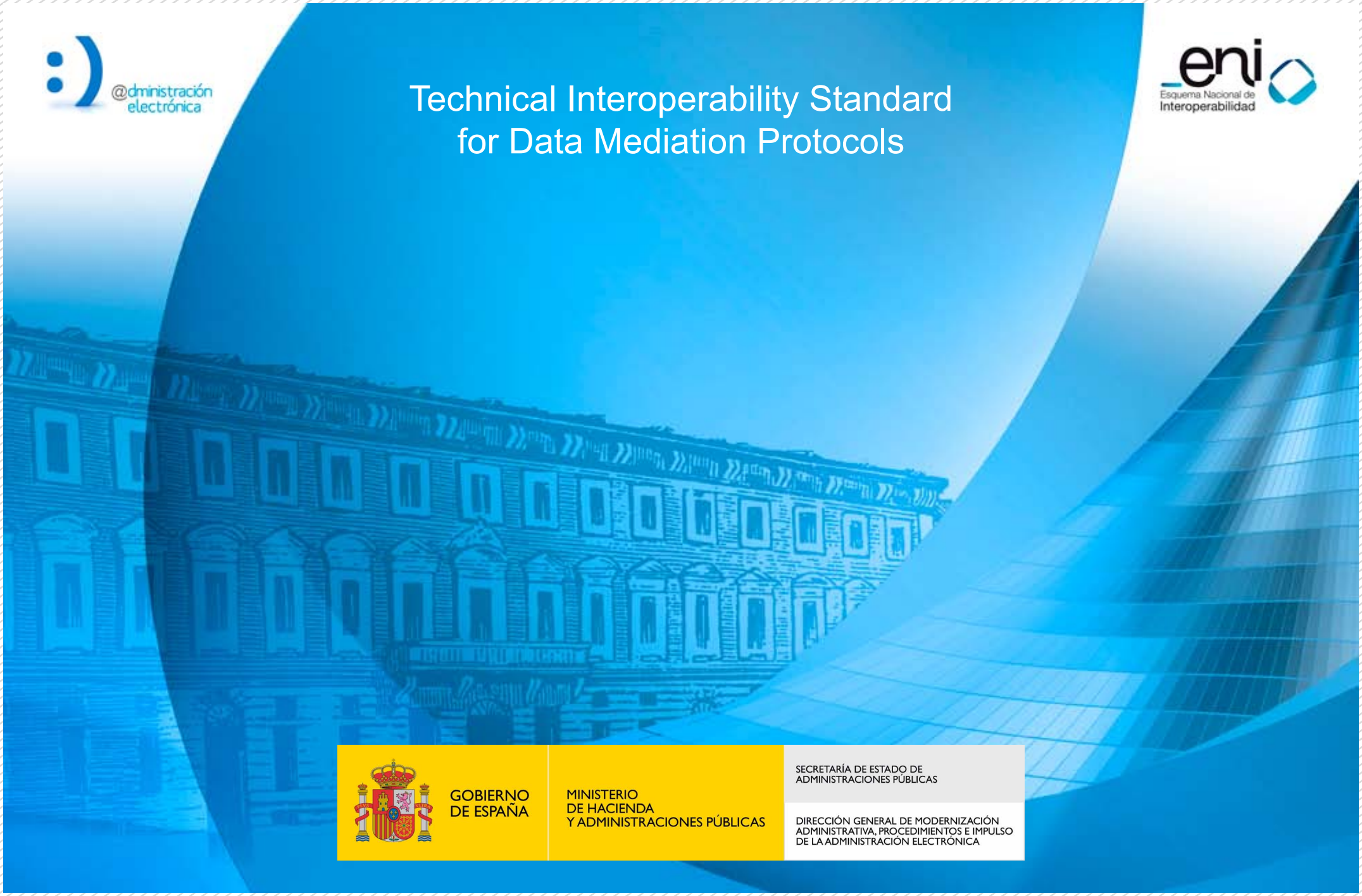
@dministración electrónica

eni Esquema Nacional de Interoperabilidad

Technical Interoperability Standard for Data Mediation Protocols



GOBIERNO DE ESPAÑA

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRÓNICA

TITLE: Technical Interoperability Standard for Data Mediation Protocols / **TÍTULO**: Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos

Translation into English checked by : General Directorate for Administrative Modernization, Procedures and Promotion of Electronic Administration / Traducción al inglés revisada por: Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica

This document is a translation of: Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos, published in the Spanish Official State Gazette (BOE). It is not an official translation and therefore has no legal validity. The original version can be found at:
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2012-10049

Digital edition with Adobe Acrobat 5.0

Available this publication at / Disponible esta publicación en el Portal de Administración Electrónica (PAe):
http://administracionelectronica.gob.es/

Published:
© Ministry of Finance and Public Administration
Technical Secretariat,
Information, Documentation and Publications Unit
Publication Center

Edita:
© Ministerio de Hacienda y Administraciones Públicas
Secretaría General Técnica
Subdirección General de Información,
Documentación y Publicaciones
Centro de Publicaciones

NIPO: 630-12-209-7

III. OTHER PROVISIONS

MINISTRY OF FINANCE AND PUBLIC ADMINISTRATION

10049 Resolution of the Secretary of State for Public Administration of 28 June 2012, giving approval to the Technical Interoperability Standard for Data Mediation Protocols.

The National Interoperability Framework, established in Article 42, Section 1, of Law 11/2007, of 22 June, on Citizens' E-Access to Public Services, is aimed at creating the conditions necessary to guarantee an appropriate level of technical, semantic and organisational interoperability of the systems and applications used in the Public Administration, allowing the exercise of rights and the fulfilment of obligations through e-access to public services, while acting in the interest of effectiveness and efficiency.

Royal Decree 4/2010, of 8 January, regulating the National Interoperability Framework for E-Government, establishes in Additional Provision 1 the development of a series of Technical Interoperability Standards, which must be complied with in the Public Administration.

The Technical Interoperability Standards describe specific aspects of a wide range of topics such as e-documents, digitisation, e-files, authentic copy and conversion, signature policy, standards, data mediation, data models, e-document management, connection to the communication network of the Spanish Public Administration, and data models for the exchange of registry entries and declaration of conformity, all of which are necessary to guarantee the more practical and operational aspects of interoperability between Public Administration agencies and citizens. These Technical Operability Standards shall be further developed and improved over time, parallel to the progress of e-government services, their supporting infrastructure, and the evolution of technology, in order to meet the provisions in Article 42.3 of Law 11/2007, of 22 June.

Within the Technical Interoperability Standards, the one related to data mediation is in accordance with Article 9 of Law 11/2007, of 22 June, and the provisions in Article 8 of the aforementioned Royal Decree 4/2010, of 8 January, on the access to and use of data and document exchange services between Public Administration agencies, defining a mediated data exchange model. Mediated exchanges are internationally recommended by such organisations as EU, OECD or UN, given their effectiveness as interoperability tools that allow for standardisation and reuse of exchange services.

The Technical Interoperability Standard for Data Mediation Protocols generally defines the roles of the actors involved in mediated data exchanges and sets forth the conditions for mediated data exchange processes with the mediation platform of the Ministry of Finance and Public Administration (MINHAP), which can apply to the mediation platform of other Public Administration agencies.

Said roles and conditions are defined in terms of technology interoperability and shall be applied together with the provisions applicable to the information being exchanged or the data being transferred, in compliance with the regulations in force.

Drafted in collaboration with all the Public Administration agencies to which it applies, the present Technical Standard has received a favourable report from the Standing Committee of the High Council for E-Government, at the proposal of the E-Government Sector Committee.

In accordance with the provisions in Section 2 of Additional Provision 1 of Royal Decree 4/2010, of 8 January, the Secretary of State decides:

One

To approve the Technical Interoperability Standard for Data Mediation Protocols.

Two

That the Technical Interoperability Standard for Data Mediation Protocols that is being approved by virtue of this document shall come into force on the day following its publication in the Official State Gazette, irrespective of the clauses in Transitory Provision 1 of Royal Decree 4/2010, of 8 January, regulating the National Interoperability Framework for E-Government.

Madrid, 28 June, 2012. Secretary of State for Public Administration Antonio Germán Beteta Barreda.

Technical Interoperability Standard for Data Mediation Protocols

CONTENTS

I. General provisions

I.1 Purpose

The Technical Interoperability Standard for Data Mediation Protocols establishes the characteristics of mediated data exchange between Public Administration agencies and related or reporting public bodies (hereinafter referred to as “organisations”).

cve: BOE-A-2012-10049

I.2 Scope of application

1. The contents of this Standard shall apply to the mediated data exchanges using the mediation platform of the Ministry of Finance and Public Administration within the scope established in Article 3 of Royal Decree 4/2010, of 8 January, regulating the National Interoperability Framework for E-Government.

2. The requirements on the actors involved in mediated data exchanges set forth in this Standard shall also apply to other mediation platforms within the scope established in Article 3 of Royal Decree 4/2010, of 8 January, regulating the National Interoperability Framework for E-Government.

3. The requirements on the MINHAP mediation platform shall also apply to mediated data exchanges using other mediation platforms within the scope in clause 2 above.

4. The conditions established in this Standard shall also apply to non-mediated data exchanges and other interoperability nodes.

II. Actors involved in mediated data exchanges

II.1 Transferor and issuer

1. A transferor is any organisation owning information about citizens that might be necessary for another organisation to exercise their competencies. The transferor shall be responsible for said information, as established by Organic Law 15/1999, of 13 December, on Personal Data Protection, and shall offer it to transferees via an issuer.

2. An issuer is the actor making the data transfer possible in terms of technology.

3. Transferors who enable the transfer of the data they own shall be considered as both transferors and issuers for the purpose of this Standard.

4. Any interoperability node involved in data issue or transfer procedures shall also be considered as issuer for the purpose of this Standard, also performing e-signature tasks for the communications it issues.

5. Functions of transferors:

a) Transferors shall provide the information for the cataloguing or registration of its data exchange services available to other organisations for consultation.

b) Regarding authorisation to access services, transferors:

b.1) Shall develop the protocols and access requirements for the data exchange services it they offer, the consultation methods allowed and the information to be provided by requesters.

b.2) Shall account for access denials.

b.3) Shall design an audit policy and conduct audits on a regular basis of consultation system use.

c) Transferors can delegate some of these functions on issuers or interoperability nodes.

6. Functions of issuers:

a) Issuers shall set forth the technical requirements for the data exchanges they offer, the consultation methods allowed and the technical audits and controls. These functions can also be performed at an interoperability node.

b) They shall determine data access criteria and controls in order to ensure the confidentiality of information (access management and control policies and procedures for users and bodies).

c) They shall provide the data relevant to each enquiry, ensuring their integrity and confidentiality.

d) They shall inform of the availability of the exchange services they offer, and the associated support and problem solving mechanisms, including contact details for these services.

e) They shall produce service-level agreements (SLAs) regulating the provision of services and the incident response mechanisms according to service criticality.

f) They shall keep the trace of all requests and answers.

II.2 Transferee and requester

1. A transferee is any organisation authorised to search for citizens' data in information owned by a transferor.

2. A requester is the actor making said search possible in terms of technology.

3. Transferees who make their own searches shall be considered as both transferees and requesters for the purpose of this Standard.

4. Any interoperability node involved in data search procedures shall also be considered as requesters for the purpose of this Standard, also performing e-signature tasks for the communications issued.

5. Functions of transferees:

a) Transferees shall request information that must be relevant to the procedures authorised by transferors and framed within administrative procedures.

b) They shall meet the access requirements set forth by transferors.

c) They shall seek consent from interested parties unless exempt by law and store the answer from the system with the corresponding file.

d) They shall use the information found in each search for the purposes stated, making as many searches as necessary in the context of an administrative procedure and taking responsibility for failures to comply with this clause.

e) They shall be involved in auditing tasks when required to do so, providing transferors with all the relevant information or documents for search control purposes.

6. Functions of requesters:

a) Requesters shall meet the information access requirements set forth by issuers.

b) They shall make sure their requests contain identification data, requested information and procedure it will be used for, as well as information on the transferee when necessary.

c) They shall keep the trace of all requests and answers.

d) They shall be involved in auditing tasks when required to do so.

e) They shall perform monitoring and control tasks to make sure their search service works properly.

f) They shall ensure the security and confidentiality of all searches, protecting the privacy of the data found during both the exchange itself and the handling of the information afterwards. For this purpose, they shall establish authorisation, access and use controls for their various applications, keep the information up to date of the users or applications accessing the system and cancel their registration in due time.

g) They shall not store more personal information about citizens than required for the administrative procedure in question and by the organisation it was collected for, and they shall keep said information no longer than necessary.

III. Mediation Platform of the Ministry of Finance and Public Administration

III.1 Functions

1. The Ministry of Finance and Public Administration shall act as an interoperability node through a mediation platform which, in accordance with the definition of interoperability node in Royal Decree 4/2010, of 8 January, shall perform common functions for the exchange of information between issuers and requesters.

2. The MINHAP mediation platform shall perform the following functions:

a) Managing the actions of transferees and requesters in compliance with the requirements set forth by transferors.

b) Deleting the personal information about citizens obtained in data exchanges once they have finished.

c) Ensuring the confidentiality and integrity of the data exchanged using its mechanisms.

d) Hosting an information website containing all the relevant documents about the platform as well as:

d.1) A catalogue of all the data exchange services available from different organisations, including their access protocols, consultation methods allowed, relevant technical data, and the required information about requesters.

d.2) The service access request forms.

d.3) The agreements for the provision of the services available and the MINHAP mediation platform.

d.4) News of platform services.

e) Keeping the system running 24/7.

f) Giving support to organisations and managing communications and incidents, in collaboration with issuers and requesters.

g) Setting up user service centres to manage system errors and platform use incidents. taking the searches made from or to each organisation into account.

h) Writing platform activity and use reports taking the searches made from or to each organisation into account.

i) Developing and maintaining systems ensuring data security and privacy in compliance with the regulations in force.

j) Being involved in auditing tasks when required by issuers or transferors, preserving traceability information and statistical data as stipulated, giving access to them when necessary and authorising the reproduction of system operation sequences when relevant.

III.2 System governance

1. Any organisation can access the information about data exchange services available using the MINHAP mediation platform or through an interoperability node.

2. The inclusion of new services in the mediation platform shall be coordinated by the Ministry of Finance and Public Administration and the transferring organisation involved.

The inclusion of the common services offered by Autonomous Communities shall be approved by the E-Government Sector Committee.

3. In order to access data exchange services:

a) Requesters shall send issuers a service access form (cf. Annex I) using the MINHAP mediation platform. This operation shall be performed individually for every transferee.

b) Issuers shall send requesters the authorisation from the transferor in answer to their request. Said authorisation shall include account for the requester's legitimacy and competency and be recorded in the mediation platform.

4. The functions of every actor involved in the authorisation procedure can be performed by the MINHAP mediation platform itself, or by an interoperability node after signing the corresponding agreement with the Ministry of Finance and Public Administration.

III.3 Technical requirements of exchanges

1. The MINHAP mediation platform shall guarantee the interoperability, availability, reliability and security of the information transferred through it between organisations.

2. To access the MINHAP mediation platform, actors shall use the communication network of the Spanish Public Administration, in compliance with the Technical Interoperability Standard for Spanish Public Administration Communication Network Connection Requirements.

III.4 General security issues

Data exchanges between the MINHAP mediation platform and organisations shall meet a series of requirements in order to ensure their authenticity, confidentiality, integrity, availability and traceability:

a) Authenticity: All the actors involved in a data exchange shall be adequately identified in every exchange. The security measures in Royal Decree 3/2010, of 8 January, grouped under "operating frameworks" in "Access control [op.acc]" and "protective measures" in "Protection of information [mp.info]" shall be complied with.

b) Confidentiality and integrity of exchanged data: They shall be protected by the security measures grouped under "protective measures" in chapters "Protection of communications [mp.com]" and "Protection of information [mp.info]" in Royal Decree 3/2010, of 8 January, and by the security measures in Organic Law 15/1999, of 13 December, and the associated enforcement regulations, ensuring that no personal information about citizens is stored.

c) Platform availability: Guaranteed by the measures grouped under "protective measures" in chapter "Protection of services [mp.s]" in Royal Decree 3/2010, of 8 January.

d) Traceability: In compliance section III.3 of this Standard.

III.5 Technologies and standards

1. The technologies used in data exchanges shall be implemented on the basis of open, interoperable standards, in compliance with the Technical Interoperability Standard for Standard Catalogues.

2. Data exchanges can be implemented via web services which, as sets of open standards and protocols to develop specific data structures for each type of exchange, shall include the security mechanisms required for communication.

3. Said web services shall be designed on the basis of:

a) Services defined in WSDL (Web Services Description Language).

b) Messages in XML (eXtensible Mark-up Language) format whose structures are based on published XML schemas to facilitate their interpretation.

c) Point-to-point communication security standards using the TLS (Transport Layer Security) protocol with client authentication at transport or application levels using protocols ensuring point-to-point security in web services.

4. Data exchanges shall use protocol SCSP (Sustitución de Certificados en Soporte Papel, Replacement of Paper Certifications), version 3.0, whose specification is available at the PAE/CTT E-Government website at http://administracionelectronica.gob.es/es/ctt/scsp.

Version 2.0 can be used for existing services that do not require additional security mechanisms, even when updated versions of said services do exist.

III.6 Traceability and audit of exchanges

1. Issuers and requesters shall keep the traces of the data exchanges they facilitate. For this purpose, they can rely on the functions of the MINHAP mediation platform and the provisions in Royal Decree 3/2010, of 8 January.

2. The traces kept in the MINHAP mediation platform, in compliance with the security measures in Royal Decree 3/2010, of 8 January – op.exp.10, “Protection of activity records”; op.exp.8, “Recording of user activity”; mp.info.5, “Timestamps” – shall contribute to the audit of exchanges. The information in the platform shall be complemented by that used to retrieve the data exchanged, stored by issuers and requesters.

3. The MINHAP mediation platform shall not store information on the contents of data exchanges or perform traceability or auditing functions other than those established in section III.6, adequately documenting the definition of functions and mechanisms to make such information available to interested parties. Transferors may audit data transfers to check compliance with requirements.

4. In order to ensure the traceability of data exchanges, every request or search will have a single locator to enable the reproduction of the sequence of operations performed.

5. The information stored for exchange or search traceability must contain at least the elements below:

a) Operation locator.

b) Data transferor, requester and end user (civil servant or application, if available).

cve: BOE-A-2012-10049

c) Type of information requested.

d) Date and time of search.

III.7 Catalogue of data exchange services

1. The catalogue or register of the data exchange services offered by each transferor shall be part of the MINHAP mediation platform catalogue and may be used as reference by potential requesters.

2. The catalogue of data exchange services shall be available for consultation through one of the following channels:

a) Transferor's information point or issuer's information point when this function is delegated on the latter (may be e-offices).

b) The MINHAP mediation platform.

c) The interoperability tools in Royal Decree 4/2010, of 8 January, namely:

i. Inventory of administrative procedures and services provided.

ii. Public Administration Semantic Interoperability Centre.

3. The catalogue or register shall include for every service available or general exchange situation at least the general information in Annex II.

4. New services shall be published in the MINHAP mediation platform using UDDI (Universal Description, Discovery and Integration) or directory services to facilitate the dynamic search of new services, although their use shall always depend on the completion of all the required authorisations.

ANNEX I

Service access request form

Type of request		
☐ **Registration**	☐ **Change**	☐ **Cancellation**

Environment	
☐ **Production**	☐ **Pre-production**

1) Data transferee*	**Locator**	
Name:	TIN	
Unit in charge:		
Address:		Postcode:
Town:	Province:	
Service:		
Purpose:		
Competencies (specify regulations and article/s):		

*Include the full branch of organisation chart the body is part of. If the body is identified with a code (e.g. TIN), included it in code description. Intermediary requesters shall include this competency: "Requester on behalf of the administrative bodies described as transferees in the procedure chart".

Identification certificate:*	
Subject (distinguished name):	TIN:
Application name (common name[1]):	
Application code or series number:	
Certification authority:	
The certificate's public data shall be sent in encrypted form (extension .cer) to this e-mail address: soporte.supresionfotocopias@seap.minhap.es	

* One or several.
Attach this form to the public side of the certificate, which shall be used for identification and data verification purposes.
1 "Common name" is the server name + domain name the certificate is associated with.

cve: BOE-A-2012-10049

2) Contact persons for management and authorisation purposes	
Name and surname:	ID number:
Position:	Phone number:
E-mail address:	Employee number:

* The name and surname must be written exactly as they appear in the person's ID card (DNI/NIE/TIE).

3) Contact persons for auditing purposes*	
Name and surname:	ID number:
Position:	Phone number:
E-mail address:	Employee number:

* The name and surname must be written exactly as they appear in the person's ID card (DNI/NIE/TIE).

4) Contact persons for computer/technology purposes*	
Name and surname:	ID number:
Position:	Phone number:
E-mail address:	Employee number:

* The name and surname must be written exactly as they appear in the person's ID card (DNI/NIE/TIE).

5) Requested permissions*
[Code of requested service. Name of certificate to be authorised.]

* One or several.

6) Requester's signature	
Name and surname:	ID number:
Position:	

The user states that all the data included in this form are true and agrees to their verification by adequate digital means.

In ....., on..... ..... ,.....

cve: BOE-A-2012-10049

Administrative procedures*

Procedure name	Description	Consent	Laws/ Regulations	Articles	Transferee	URL

* Procedures the system shall be used for:

For every procedure, indicate name and whether the search is being performed with the interested party's consent or in compliance with relevant laws/regulations. In either case, indicate the article of applicable law/regulation. Also describe the administrative procedure the requested data are needed for.

E.g.

Emergency/catastrophe subsidies. Aid to victims of natural disasters and emergencies situations requiring registration certificate. / Written consent. / RD 307/2005, of 18 March, enforced by means of order int./277/2008, of 31 January.

Usability information*

* Estimation of system searches to be performed (on a monthly basis):

These data are only indicative and will be used to gather information on the system for future improvements of existing applications and optimisation of end user performance.

6) Additional provisions

- By signing this form document, the transferee undertakes to seek the consent of the interested parties about whom they request information or find a regulation/law exempting them from this.
- This request form can be cancelled at any time without prior notice if the issuer of the data considers it necessary to do so due to misuse or inadequate use of the requested information. It can also be cancelled without prior notice if the data entered in this request form are found to be incorrect. This faculty is regulated by the service-level agreement (SLA) governing the provision of the service.
- The head of the body signing this form states that they shall be responsible for the use of the information requested only for the purpose described in section 1 of this form and in the context of the specific administrative procedure described here, the confidentiality of the information requested, its use in accordance with the purpose of the file containing it and compliance with obligations, guarantees and regulations on the provision and communication of information.
- The body requesting the information undertakes to comply with Organic Law 15/1999, of 13 December, and the associated enforcement regulations. The obligations in said Law shall be transferred to the transferee as actor handling the information in case of misuse or failure to protect the data in question.
- Both the issuer and the requester shall take the necessary security measures, in compliance with Organic Law 15/1999, of 13 December, and the associated enforcement regulations, given the personal nature of the information exchanged. Likewise, they shall have a security document that can be required for data transfer authorisation. Said measures include access and authorisations controls, and system use and activity records.
- The requester shall have the responsibilities described in the Technical Interoperability Standards that make the National Interoperability Framework.
- The Ministry of Finance and Public Administration guarantees the security and confidentiality of all the personal data users have access to in the provision of this service.
- In compliance with Organic Law 15/1999, of 13 December, and the associated enforcement regulations, users are hereby informed that the data entered in this form and those generated by its processing can be included in a file and handled for data communication authorisation request purposes.
- Users have a right to change their personal data in case of errors by filling the forms available in the CTT website at http://administracionelectronica.gob.es/es/ctt/svd. They must be registered users of said website to operate.

del CTT http://administracionelectronica.gob.es/es/ctt/svd siendo

- The user, requester or person in charge states that all the data included in this form are true and agrees to their verification by adequate digital means.

ANNEX II

Data exchange service description information

DATA EXCHANGE SERVICE DESCRIPTION	
Service code	Code identifying the general exchange situation required to make the corresponding data requests
Data being exchanged	Description of the information available for exchange or transfer
Authorisation required?	Field to indicate whether the data transfer or exchange is authorised by law and, therefore, exempt from special authorisation by interested parties.
Required data	Data to enter in the transfer or exchange request in order to identify the information being exchanged
LOPD level	Protection level of the information being exchanged, in compliance with Organic Law 15/1999, of 13 December, and the associated enforcement regulations.
Issuer	Identification of the actor providing the service or managing the general exchange situation.
Transferor	Identification of the actor owning the information being exchanged.
Special requirements	Special requirements set forth by the issuer.
Service/situation approval date	Date when the general exchange situation is approved and the service becomes available.
End of service	Estimated time or period when the exchange service becomes unavailable.
Authorisation expiration	Expiration conditions or periods for the authorisation granted to issuer in case of: i. Failure to use service after getting authorisation (new authorisation may be required). ii. Failure to use service for a period of time.
Additional information	Other technical data that may be useful for exchange management or contribute to interoperability (e.g. request and answer field design, web exchange service, etc.).

cve: BOE-A-2012-10049