Trustful e-Services in the Government-to-Government Context

Lluís-Esteve Casellas
City Council of Girona (Catalonia)

Trusting Records in the Cloud
Associazione Nazionale Archivistica Italiana (ANAI)
Biblioteca Nazionale Centrale
Rome, December 10, 2018

(Vancouver, 2019)

Aim and purpose

- How do e-Services affect RM and the preservation of authenticity.
- To get a strategy to manage services provided in the Cloud.
- To influence policies of Public Administrations as e-Services providers.

Some context

General Administrative Procedures Act (October 2015)

- **2016 October** - Fully digital case files.
- **2018 October** - Digital Archive Service (postponed to 2020...).
  If not, Digital Archive Service (Cloud) provided by Spanish Government (mandatory).

Towards e-Government…

- **Increase of e-Services between Public Administrations**.
- Exchange data between Public Administrations: less complexity for citizens.
- Main objective: economic saving (CORA Report) not necessarily trust.
- Technological component > organizational.

Records Management System?

- Not mandatory by law in the Spanish Government nor Regional Government.
- Mandatory in Catalan Public Administrations by A&RM Act (2001).

e-Services: what, who and how

E-Service:

- Technological resources (infrastructures or applications) that facilitate the access to management platforms, information exchange, data interoperability, data validation or the management or provision of services to citizens.

Public Administrations as providers:

- Spanish Government.
- Regional Government (e.g. Catalonia Government).
- Provincial Government.
- *Open Administration of Catalonia (AOC, 2001, intermediation function)*

Consortium of Catalan Public Administration: digital transformation

Can Public Administrations trust each others?

And the citizens, should they trust Public Administration?

Trustworthiness by default?

Requirements for Cloud Services Providers

Baseline **requirements** for e-Service providers:

- **Contract management**: legal regulation, terms of use, subcontracting...
- **Information security**: infrastructure, portability, data location, security measures, audits...
- **Confidentiality and data privacy**: data ownership, access and PI rights, responsibilities...
- **Control of records / data**: records management, characteristics of records, disposal...

How would it be materialized?

Private providers

- Bid specifications
- Check-list for private providers
- Statements of responsibility

Public Administrations

- Policies and procedures to agreement *
- Verifying test.

Public Administration as Provider

Policies and procedures to agreement

	General Policy	Platform Policy	e-Service Policy
SPANISH GOVERNMENT	-	*(e-Gov. Portal)*	-
CATALAN GOVERNMENT	-	*(e-Gov. Portal)*	-
OPEN ADMINISTRATION OF CATALONIA (AOC)*	"YES"	"YES"	"YES"
PROVINCIAL GOVERNMENT	-	*(e-Gov. Portal)*	-

* "*General Terms and Conditions of Use"* are > Technical Specifications" level.

→ *Appendix C. Digital Records Maintenance and Preservation Strategies (IP-2, Preserver Guidelines)*

- National Standard of Security and National Standard Interoperability are mandatory.
- No specific policies about how they are providing e-Services nor terms included in other Policies.

Tools to control these e-Services by the Public Administration as user

- **Catalogue of e-Services** (Public Administration as provider)
- ***Catalogue of Applications*** *(mainly for private cloud services providers)*
- ***Internal Register of Authorized Users*** *of cloud services of others Public Administrations*

How does it affect records management

Spanish Government' e-services:

- *E-government and services to citizens*
- *Internal management*
- *Infrastructures*

AOC' e-services (Open Administration of Catalonia):

- *Relations with citizens*
- *Internal management*
- *Relations between Public Administrations*
- *Identity and electronic signature*

E-services Classification RM viewpoint

Actions upon records or in relation to them

1. **Creation of records**, usually by means of a structured form.
2. **Transmission of data and records.**
3. **Publication** of data and records on platforms, official registers or official journals.
4. **Verification** and consultation of data and records, which substitutes documentation provided by citizens.
5. ***Software applications*:** business management, temporary storage, preservation.
6. ***Identity and digital signature*** *as a means of access to e-Services and records validation.*

Preservation of the authenticity

- Services are clearly **oriented towards digital signature** and even to the re-signature of records.
- Can they guarantee the authenticity of the records and the traceability of the actions without the digital signature?

Review under the perspective of InterPARES 2 criteria:

Preserver Guidelines. Preserving digital records: Guidelines for organizations.

"Appendix 2: Requirements for Assessing and Maintaining the Authenticity of Electronic Records."

Creation of records or evidences

- *Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records. (**Requirements Set A**)*

Obtaining authentic copies from systems

- *Baseline Requirements Supporting the Production of Authentic Copies of Electronic Records. (**Requirements Set B**)*

REQUIREMENTS	E-SERVICES							
	CREATION		TRANSMISSION	PUBLICATION			VERIFICATION	
	SiNI@ (- DMS -)	SPECIFIC APPLICATIONS	GENERIC APPLICATIONS	PUBLIC REG. OF GRANTS	OFF. BULL. OF CATALONIA	PROVINCIAL OFF. BULLETIN	DISABILITY DEGREE	PERSONAL INCOME TAX
FORMAL AGREEMENT (terms of use)	NO	YES	YES	NO	NO	NO	- YES -	- YES -
USERS CONTROL	Provider	Provider	Provider	???	Provider	User	Provider	Provider
PRESUMPTION AUTHENTICITY								
A.1.a Name of persons	NO	YES	YES	YES	YES	YES	YES	YES
A.1.a.ii Name of action or matter	NO	NO	NO	YES	YES	YES	YES	YES
A.1.a.iii Data(s)	NO	YES	YES	YES	YES	YES	YES	YES
A.1.a.iv Archival bond	NO	- *YES* -	- *YES* -	NO	NO	NO	NO (YES)	NO (YES)
A.1.a.v Indication of attachments	NO	YES	YES	/	/	/	/	/
A.1.b Integrity	NO	/	/	/	/	/	/	/
A.2 Access Privileges	YES	YES	YES	YES	YES	YES	YES	YES
A.3 Protection: loss and corruption	NO	YES	YES	NO	YES	???	??? (YES)	??? (YES)
A.4 Protection: media and technology	NO	YES	YES	NO	YES	???	??? (YES)	??? (YES)
A.5 Documentary forms	NO	YES	YES	YES	YES	YES	NO (YES)	NO (YES)
A.6 Authentication of records	NO	YES	YES	???	YES	YES	YES (YES)	YES (YES)
A.7 Id. of authoritative record	NO	- *YES* -	- *YES* -	NO	NO	NO	NO	NO
A.8 Removal and transfer	NO	YES	YES	NO	YES	???	YES	YES
	Catalan Gov.	AOC	AOC	Spanish Gov.	Catalan Gov.	Provincial Gov.	Catalan Gov.	Spanish Gov.

REQUIREMENTS	E-SERVICES							
	CREATION		TRANSMISSION	PUBLICATION			VERIFICATION	
	SiNI@ (-DMS-)	SPECIFIC APPLICATIONS	GENERIC APPLICATIONS	PUBLIC REG. OF GRANTS	OFF. BULL. OF CATALONIA	PROVINCIAL OFF. BULLETIN	DISABILITY DEGREE	PERSONAL INCOME TAX
FORMAL AGREEMENT (terms of use)	NO	YES	YES	NO	NO	NO	- YES -	- YES -
USERS CONTROL	Provider	Provider	Provider	???	Provider	User	Provider	Provider
PRESUMPTION AUTHENTICITY								
A.1.a Name of persons	NO	YES	YES	YES	YES	YES	YES	YES
A.1.a.ii Name of action or matter	NO	NO	NO	YES	YES	YES	YES	YES
A.1.a.iii Data(s)	NO	YES	YES	YES	YES	YES	YES	YES
A.1.a.iv Archival bond	NO	- *YES* -	- *YES* -	NO	NO	NO	NO (YES)	NO (YES)
A.1.a.v Indication of attachments	NO	YES	YES	/	/	/	/	/
A.1.b Integrity	NO	/	/	/	/	/	/	/
A.2 Access Privileges	YES	YES	YES	YES	YES	YES	YES	YES
A.3 Protection: loss and corruption	NO	YES	YES	NO	YES	???	??? (YES)	??? (YES)
A.4 Protection: media and technology	NO	YES	YES	NO	YES	???	??? (YES)	??? (YES)
A.5 Documentary forms	NO	YES	YES	YES	YES	YES	NO (YES)	NO (YES)
A.6 Authentication of records	NO	YES	YES	???	YES	YES	YES (YES)	YES (YES)
A.7 Id. of authoritative record	NO	- *YES* -	- *YES* -	NO	NO	NO	NO	NO
A.8 Removal and transfer	NO	YES	YES	NO	YES	???	YES	YES
	Catalan Gov.	AOC	AOC	Spanish Gov.	Catalan Gov.	Provincial Gov.	Catalan Gov.	Spanish Gov.

Where is the record, where is the evidence?

	e-SERVICE	CITY COUNCIL	INTERMEDIARY PROVIDER	ADDRESSEE / PROVIDER	ACTION'S EVIDENCE
CREATION	*SÍNI@ (- DMS -)*	(0)	-	X	NO
	SPECIFIC APPLICATIONS	(x')	X	X'	YES
TRANSMISSION	*GENERIC APPLICATIONS*	X	X'	X'	YES
	CITY PLANNING PROJECTS	X	-	X'	NO
PUBLICATION	*E-NOTICEBOARD*	X	X'	X'	YES
	GRANTS' PUBLIC REGISTER	X'	-	X	(NO)
	OFF. BULL. of CATALONIA	X'	-	X	(NO)
VERIFICATION	*DISABILITY DEGREE*	z'	-	Z	YES
	PERSONAL INCOME TAX	z'	-	Z	YES
	VEHICLE OFF. REPORTS	(0)	-	Z	NO

Some recommendations

REGULATION

1. **Planning the design** of e-Services: who will use them, with who or whom will be connected.
2. **General policies** that guarantee the basic principles of **security**, **confidentiality**, **data protection**, and **preservation of the authenticity** of the information. These are key elements in generating **trust**.
3. The **granularity of policies** is important. They should cover the **institution** but also they have to be developed at **platform** and **service level**.
4. **Statements of responsibility,** if the security policies can not be disclosed as a measure of protection of the institution.
5. **Regulated procedure** for the **adhering to a platform or service**. This would facilitate to maintain a Catalogue of e-Services used in each organization, now very difficult.
6. **Terms of use** for every e-Service.
7. Regulated procedures for the **management of users**, since users' control reinforces the presumption of the integrity and the authenticity. This also facilitates the maintenance of a Register of Authorized Users in each organization.

Some recommendations

PROVISION OF SERVICES

1. E-Services should always be based on **intermediation services**, for the following reasons:
   - **Normalizing** effect.
   - **Multiplier effect** as a mediator between administrations.
   - **Efficiency** of adaptation and integration *1:n,* no *n:m*.
   - Possibility of **automated integration** with the systems of each organization (not *craft* solutions).
2. **Exchange of records** should be a tendency instead of “sending” files, especially in bulky files.
3. **Users' control** should always be provided to the user institution for supervision, even limited, to avoid the lack of knowledge in the own organization of who does what.
4. **Control of access** must always respond to **individuals**, no a groups of them.
5. E-Services must provide **different levels of access** also within the framework of a same institution.

Some recommendations

AUTHENTICITY PRESUMPTION

Apart from the issues related to security, access management and confidentiality that reinforce the presumption of authenticity, it is necessary to take into account:

1. **Creation of records** has always meet the **requirements of authenticity** (IP-2, Req. A), especially in the design of e-Services based on business management applications.
2. The service public providers have to allow **access and control of records** to the organizations that have produced them.
3. The **consultation or verification of data** in information systems should always to obtain **evidence** or copy of the record or data with guarantees of presumption of authenticity (IP-2, Req. B)
4. All electronic services have to implement **traceability requirements** for actions carried out by users. (**Who, What, When, How**).
5. Data of **traceability have to be available** for user Administrations.
6. The use of e-Services should tend to **complete integration** to reinforce **automatic traceability** and to avoid manual incorporation of records into the systems.

Some recommendations

However, if all of these points fail, everything will depend on the willingness of the **people** who create, transmit, verify or publish records in the Cloud; thus, the **training and awareness** becomes essential in any case.

In conclusion, all of this is to avoid that the *big fish eats the small fish*.

(But don't forget that **citizens** are always the smallest...)

Thanks for your attention!!

Trustful e-Services
in the Government-to-Government Context

Lluís-Esteve Casellas
City Council of Girona (Catalonia)
lecasellas@ajgirona.cat
@lecasellas