Personal data protection, certificate service providing and e-Government: a feasible equation?

Julián Valero*

Departamento de Derecho Administrativo, Universidad de Murcia, Spain
E-mail: julivale@um.es
*Corresponding author

Daniel Sánchez Martínez

Departamento de Ingeniería de la Información y las Comunicaciones, Universidad de Murcia, Spain
E-mail: dsm@dif.um.es

Abstract: This paper analyses the risks of e-Government scenarios for personal data protection, from a legal point of view, especially those related to Certificate Service Providers (CSPs) and the verification of certificates’ status. CSPs can be considered Trusted Third Parties (TTP) that receive certain personal information about the users of e-Government services, being necessary to establish the legal and technical mechanisms to control the processing of these data. This work analyses the implications of this mechanism for the right to personal data protection in the field of e-Government services, according to Directive 95/46/EC and the Spanish regulation in this field.

Keywords: e-Government; personal data protection; certificates service providers; certificate validation; electronic identification card.


Biographical notes: Julián Valero is Administrative Law Lecturer at the University of Murcia. He is the Author of numerous works on data protection in the field of e-Government and the relationships between technology and Administrative Law. Currently, he teaches Informatics Law at the Faculty of Law, directs an online course on the legal implications of data protection.

Daniel Sánchez Martínez is Associate Professor of the Information and Communications Engineering Department of the University of Murcia. Currently, he is working in projects related to security services based on smart cards and web services, such as electronic signature and authentication systems for e-Government.
1 Technological modernisation of public administrations and citizen’s identification issues

Although technology allows a higher level of efficiency it is clear that the risks for user’s rights are also more worrying. Specifically, a citizen’s fundamental right to personal data protection is subjected to new and intense dangers when referring to e-Government services, since collecting and processing systems have considerably advanced. Personal data protection, owned by public administrations, has raised numerous and significant questions up to now since they probably have the most complete data bases about citizens, but e-Government demands a new effort in order to notice that not all the actions that technology make possible are acceptable from a legal point of view.

One of the main requirements in order to implement online services is the use of security tools by citizens so as to be identified and guarantee the authorships of documents. The compulsory use of unique or sector-based identifiers in order to have access to certain online administrative services and, specifically, the use of electronic identification cards provided by public authorities, brings about a new problem in the field of data protection.\textsuperscript{1} We are indeed faced with quite a useful tool in order to make possible citizens’ identification when using online services, but interconnection of different and heterogeneous data bases from the perspective of their finality and content may reveal a serious danger for the analysed, since it permits to make personalised profiles of the users in a very simple way, at least for those who can gain access to these multiple sources of information.

This problem is particularly relevant in the field of public administrations since the exercise of their competences frequently demands the use of personal information and, consequently, personal data management and access to data bases owned by third parties, sometimes under the protection of a legal obligation. Moreover, if we bear in mind the number and diversity of administrative tasks in modern states, it may happen that information provided by citizens in order to obtain a favourable administrative decision – for instance, obtaining a subsidy or an authorisation to carry out an economical activity - could be used for a different public purpose but with a negative or restrictive dimension for citizens’ rights.

It is necessary to notice that technological modernisation of public administrations’ activity offers a new dimension of data protection issues since, on one hand, the interconnection of data bases becomes easier and, on the other hand, online relationships between citizens and public bodies requires the use of a new and singular tool that raises relevant privacy issues: certification services with associated digital signatures. So, it is hardly surprising that Article 29 Data Protection Working Party has paid a special attention to the national systems of the individual’s identification in the Working Document on e-Government, where the legal situation in the member States is examined and the different models of identification exposed.\textsuperscript{2} Recently, Spain has passed Royal Decree 1553/2005 on Electronic Identification Card (DNI-e), a regulation that does not provide for the compulsory use of digital signature services associated with this document, but extends the service – potentially at least - to all Spanish citizens who wants to have it for free with no extra cost. We will analyse in this paper the particular situation of this initiative from the point of view of the risks ans problems that come up for the citizens’ right to data protection guaranteed by the Directive 95/46/EC, of the European Parliament and of the Council of 24 October, 1995, and the Spanish Constitution and 1999 Personal Data Protection Act.
Although some other questions related to data protection could be analysed in-depth, certification services provided by public authorities is one of the main challenges of e-Government from a legal perspective, especially if they are associated with unique or sector-based compulsory identifiers. On one hand, digital certificates must be considered as an essential tool when using those electronic public services that requires a secure identification of citizens, due to the relevant juridical consequences of this kind of relationship; for instance, access to administrative documents or submission of an application form. On the other hand, a digital signature assures the documents’ authenticity and checks if they have been produced by the owner of the certificate and/or the have been modified. In both cases, the appropriate working of certification services requires the intervention of TTP – CSP, id est, Certification Service Providers – who are in charge of providing certificates to users and answering for their secure generation and their validity. These legal obligations demand giving clear and updated information about the revocation of certificates since, otherwise, it would be impossible to know whether they are still valid and reliable.

2 The origin of the problem: technical implications of certificate validation

In next sections we are going to describe, in a basic way, the main mechanisms of certificate validation, looking into the flows of information established by the different actors of these kinds of services in each validation request. After that, we will illustrate these mechanisms inside an e-Government scenario, showing the data interchanged between the different elements of the system will be analysed, and studying with special emphasis some considerations about personal data protection. Finally, some technical conclusions about the analysis performed, that could establish some design and implementation steps in these kinds of contexts, will be presented.

2.1 Different certificate validation mechanisms: advantages and inconveniences

2.1.1 Offline validation: Certificate Revocation List (CRL)

Distribution of certificate revocation lists (CRL)³ is the most traditional method to validate certificates. CSP creates, signs and publishes these lists periodically, making their downloading easy for potential clients. A CRL contains a list of the digital certificate serial numbers revoked by the own CSP, besides the revocation reason, date and time of each operation. In addition, the CRLs are ordered and valid until a certain date that is also indicated in the CRL. When the validity of the CRL expires, the client must download the new version of the CRL.

During the life cycle of CSPs, the CRLs increase their size progressively, showing two possibilities of design. In the first option each new version of a CRL replaces the previous one entirely. In the second one the new CRL complements the preceding one, adding the new revoked certificates since the last version of the CRL (delta-CRL). Moreover, the CRLs can be split by other factors (usage, localisation …). The validation mechanism is very simple: the client downloads the CRL on a local machine, and then performs all the status checking operations of different certificates against that list. So this kind of validation is called ‘offline’ validation. This can be seen in Figure 1.
This easy mechanism shows some clear problems. The first one is the task of downloading and updating the CRLs, which is a responsibility of the client in this kind of validation. If the client does not update the CRL, the results of checking operations will not be reliable. The second one is the increasing of complexity in the processing of clients, who have to download, install and understand the lists, performing all the status checking operations by themselves. The third, and the most important one, is about the frequency of new lists. It is possible that a certificate is revoked between the generation of a revocation list and the next one, but the certificate validation may still be positive. So, this mechanism is not very trustworthy for application contexts in which certificate validation is a critical factor.

2.1.2 Online validation: Online Certificate Status Protocol (OCSP)

Nowadays, Online Certificate Status Protocol (OCSP) is the most extended online validation mechanism, and becomes an alternative to the distribution of lists (CRL). The main difference with the CRL mechanism is about which entity has the responsibility of checking the certificate state. In this protocol this task is performed by an OCSP Responder service inside the CSP infrastructure.

A client makes state checking requests according to the protocol, sending the certificate identification code (serial number) to the OCSP Responder service. The service processes each request and sends back a signed response which contains the state of the certificate and the time in which the checking has been performed (Figure 2). The ‘online’ feature of this validation mechanism gets to know the exact state of certificates at a particular moment, improving the lack of reliability in CRLs.
2.1.3 Certificate validation and e-Government services: a potential risk for personal data protection

We are going to analyse now the process of certificate validation in electronic Government services, depending on the validation mechanism used, taking special care over data protection issues derived from these practices. e-Government processes usually require three main players: a user who has an electronic credential, the own telematic service established by Government, and a TTP that offers some validation information about the user’s credentials to the Government service.

In Spain, a common scenario shows a user, without any technical knowledge, in possession of an electronic Identity National Document (DNI) generated by the Spanish Department of the Interior. Electronic DNI has two qualified certificates: an authentication certificate that allows user’s authenticating against a service, and a non-repudiation certificate, which allows the user to perform electronic signature processes over electronic documents.

Normally, the final user does not know what information contains the electronic DNI and does not understand the flows of data that are generated over its insertion in a smart card reader of a computer for accessing a governmental web portal. The user does not know anything about the existence of a TTP and its interaction with e-Government services trying to validate the presented credentials either. Finally, the user ignores the fact that the TTP often stores some information about the usage of its services, for statistical reasons, security policies and control against hacking activities.

2.2 e-Government services and CRLs

In Figure 3, the main flow of information between the different roles described above can be seen in a typical scenario in which the certificate validation is performed through the usage of CRLs. First of all, the service administrator must download and install the CRL generated by the CSP. This task can be programmed and performed periodically, according to the generation frequency of new CRLs by the CSP. Each time the service downloads a new version of the CRL, the CSP is able to add a new entry into a database record (CRLs downloads log file), getting exact knowledge about the electronic Government services that are using this offline validation mechanism (Table 1).

When the CRL is correctly installed and configured in the local machine, the service is available for all the users of the system. After this moment a user can introduce his electronic identification card inside a smart card of a personal computer and access any e-Government service. So, in this technical process, the authentication certificate inside the DNI is sent to the service during the authentication handshaking. When the service receives a user credential it performs a checking of its certificate validity, looking into the certificates revocation list (locally stored) and searching for the user’s certificate. If it is not included in the revocation list (CRL), the service can trust the validity of the credential, allowing the final user access to all the functionality. The following requests will be resolved in the same way, coming back to check the certificate status of the user against the local CRL. The policy service of processing allows the definition of the CRLs download frequency, which is a critical element to make sure of the reliability of the validation process.
Figure 3  e-Government scenario I. CRLs

![Diagram of e-Government scenario I. CRLs]

Table 1  CRL downloads log file

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>CRL downloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/12/2006</td>
<td>09:11</td>
<td>e-Government service 1</td>
</tr>
<tr>
<td>02/12/2006</td>
<td>10:07</td>
<td>e-Government service 5</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>02/13/2006</td>
<td>09:12</td>
<td>e-Government service 1</td>
</tr>
</tbody>
</table>

2.3  e-Government services and OCSP

In this second scenario, shown in Figure 4, we can observe an information flow slightly different from the previous one because of the online feature of this kind of certificate state checking. Initially, this process starts in a similar way to the preceding scenario, with the e-Government service receiving the authentication certificate of the identity card (DNI). Next, the service performs a new task, trying to get the serial number of the user certificate, and sends this information to the CSP through an OCSP request of certificate state. The CSP returns an OCSP response to the e-Government service, verifying whether or not the validity of the certificate is associated with the serial number checked.

At the same time, the CSP can store some particular information about the received request: for example the requester service identifier, the serial number of the certificate checked, and the exact time of the checking operation. The following validation requests will also be able to generate the proper entries into the OCSP request log file (Table 2). So the CSP, through this validation mechanism, can keep a clear record of all the serial numbers of certificates that the e-Government service has checked during its life cycle, even being able to know the total quantity of checking operations over each certificate and the precise moment of each operation.
Figure 4  e-Government scenario II. OCSP

Table 2  OCSP request log file

<table>
<thead>
<tr>
<th>Date</th>
<th>Date and time</th>
<th>Service</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/12/2006</td>
<td>09:11</td>
<td>e-Government service 1</td>
<td>00001</td>
</tr>
<tr>
<td>02/12/2006</td>
<td>10:07</td>
<td>e-Government service 5</td>
<td>03670</td>
</tr>
<tr>
<td>02/13/2006</td>
<td>09:12</td>
<td>e-Government service 1</td>
<td>00434</td>
</tr>
</tbody>
</table>

Usually, a CSP has a lot of different elements and services that cover the life cycle of any digital certificate (registry authority, certificate request service, validation service, revocation service ...). So, the CSP can know at any moment, on the one hand, all the information about its certificates (stored in the directory service) and, on the other hand, all the entries about the requests of certificate status checking, generated by the certificate validation service and stored in the request log file.

From a technical point of view, the connection between both repositories of information makes it possible to generate reports about the users, and their usage of the electronic Government services. For example, a CSP could obtain reports, indexed by user, with the dates and times in which each service has been used (Figure 5), even reports indexed by service, with the dates and times in which each user has accessed this service.
3 Legal focusing: personal data protection in the field of certificate service providing. Special reference to the Spanish electronic identification card

From a legal perspective, the main problem raised by identification systems is based on the use of digital certificates and is closely related to the aspect of personal data protection regulation. According to Article 15 of 1999 Digital Signature Act, on the one hand, these certificates can be used as tools to identify their owners when using electronic services; on the other hand, they guarantee, as well, the authentication of digital documents. In both cases, the correct working of certification services demands the intervention of a TTP – CSP-, who must provide access to the certificates’ status so that Public Administrations can know if the certificate is still valid. Therefore, access to certification revocation information is a key issue for e-Government services that demands citizens’ identification. As a consequence, although Article 8.2 of Directive 99/93/EC, of the European Parliament and of the Council of 13 December 1999, on a Community framework for electronic signatures, contains a general ban for CSP to collect personal data from data subjects in order to use them for purposes other than issuing and maintaining certificates, it is necessary to extend that authorisation to the diffusion of information related to those certificates that have been revoked. Despite the fact that a strict interpretation of the expression ‘maintaining’ would not include this kind of data processing, adequate providing of certification services requires that publicity since the last analysis, and CSP’s liability could be engaged according to Article 6.2 Directive 99/93/CE. Regarding the administrative online services, when public administration needs to validate the certificates used by citizens, it will be necessary to contact the CSP since, otherwise, it will have to accept the consequences that may result from their previous revocation. Spanish regulation is clearer...
on this point since Article 10 1999 Digital Signature Act has forced CSP to offer a
validation service with all the information related to the status of certificates.

Access to Certificate Revocation Lists (CRL) can be considered as the most authentic
system with data protection requirements since public administration verifying the
validity of certificates already have –and need– the information about citizens’ activity
associated with the enquiry: the main problem in this case is later use of these data for
different finalities, since the information collected can not be processed in a way
incompatible with the initial purposes. Whereas, Online Certificates Status Protocol
(OCSP) demands a direct consultation to a third party’s information systems and, as a
consequence, this service provider may know which websites are visited by the
certificate’s owner and how often he comes back again and makes online operations that
requires his digital identification. So, it is necessary to assure the opacity of this data
processing in order to avoid unfair profiles of certificates’ users.

Therefore, potential risks to personal data protection are really obvious, since an
inappropriate implementation of the revocation verification systems may involve an
unfair and excessive processing that infringe Article 6 Directive 95/46/EC and paper 4 of
1999 Spanish Act. Sure enough, if the CSP decides to connect both data bases – the one
containing data related to certificates and their owners and the files with the information
about the validity of certificates and the enquiries made by public administrations
providing e-government services– it will be possible to know the activities made by
citizens using their certificates. So since the information is absolutely unnecessary for
certificate service providing, it would not be justified that CSP could know and use it
and, as a consequence, will be legally obliged to separate both information systems.
Further, it will not be authorised to collect those data on the consultations made by public
administrations –or private subjects– about the validity of certificates.

In the Spanish case, although the use of the certificate associated with the electronic
Identification Card is completely voluntary, we must take into account the fact that all
citizens are obliged to have this document and, therefore, the potential number of users is
really high. Moreover, as certification services will be provided by the Police Force
according to Articles 3 and 12 of the Royal Decree 1553/2005, there is an additional risk
since the collected data of the users of certificates could be unfairly used for police
purposes and, therefore, public confidence in e-Government services may be seriously
affected. However, as shown in the information offered through the official website,6
it must be emphasised that validation services will not be provided directly by the CSP
since they are delegated to other public authorities such as the Ministry for Public
Administration and the Fábrica Nacional de la Moneda y Timbre.

Unluckily an essential question is still without a clear answer. On the one hand,
according to Article 20 of 1999 Act on Data Protection, public authorities responsible for
files containing personal data must approve a regulation for creating them and it has not
been officially published for the electronic Identification Card yet. On the other hand, a
relevant content of this regulation is the reference to the security measurements that will
be put in force depending on the kind of data collected. As has been just said, we have no
official information about this issue up to now and, therefore, it is impossible to know
whether the Ministry for the Interior –and specifically the Police Force– will be able to
gain access to data concerning the internet activities of citizens in any situation and/or
under any circumstances.
4 Conclusions

It very useful that validation services store the information about the requests of status checking, received from e-Government services, in records or log files. These kinds of records are justified by technical reasons (tracing hacking activities and unauthorised access) and evaluation system reasons (obtaining conclusions about the usage of the validation services). However, these previous reasons do not make it essential to collect the identification of each certificate checked (serial number field). The security system does not suffer any kind of menace from ignoring the serial numbers checked; and there are no limitations in knowing the usage of the validation mechanism either. So it is indispensable that validation services define their internal process of performance through some policies, suggesting always the compromise of not storing any data about the serial number of the certificates checked. The fulfilment of this compromise makes the crossover of information impossible later, and the generation of reports which publish privacy information about a concrete user.

In short, CSP must dissociate data regarding revoked certificates and the identity of their owners, both for internal management and the provision of information about certificate revocation. This personal data processing only could be done by the public administration which is in charge of the electronic services that require the use of digital certificates. If we bear in mind that unique or sector-based digital identifiers usually assume that all citizens own a certificate provided by the same CSP, the risks from this model of digital identifications are obvious, especially when it is a free service for users. The respect of the data protection law requires a strict dissociation between the information about certificates and the verification requests made by public administrations and, additionally, that they are not collected by CSP: an eventual security problem would allow making out a complete profile of the activities made by citizens when using their digital certificates. Therefore, although in the case of public digital identifiers associated with compulsory identifiers – Identity Cards such as Spanish Documento Nacional de Identidad– these problems become singularly relevant because of the high number of citizens involved; our conclusions may be extended to the activity of any public or private CSP.

We have used the Spanish case as an example and the European regulation on Data Protection and Digital Signatures has been exposed as a reference, but concrete and definitive conclusions in this field can only be reached for each national case with a previous and detailed analysis of its legal framework.

Notes

1 Potential risks of these identification systems were noticed by Directive 95/46/EC of the European Parliament and of the Council of 24 October, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which Article 8.7 rules that Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

2<http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/e-government_en.pdf>, pp.8 and 9. All the websites quoted in this paper have been visited on the 10th March.


Websites


Bibliography


