14-9-2015

Breaking the Web Barriers of the e-Administration Using an Accessible Digital Certificate Based on a Cryptographic Token

Rafael Conde Melguizo

Boni García

Ana García

Yolanda Hernández

Miguel Ángel Valero

Hindawi Publishing Corporation
Advances in Software Engineering
Volume 2015, Article ID 568087, 11 pages
http://dx.doi.org/10.1155/2015/568087

Research Article

Breaking the Web Barriers of the e-Administration Using an Accessible Digital Certificate Based on a Cryptographic Token

Boni García,[1] Ana Gómez,[1] Rafael Conde,[1] Yolanda Hernández,[2] and Miguel Ángel Valero[1]

[1] *Departamento de Ingeniería Telemática y Electrónica, Universidad Politécnica de Madrid, Carretera de Valencia km 7, 28031 Madrid, Spain*
[2] *ASPAYM Madrid, Camino de Valderribas 115, 28038 Madrid, Spain*

Correspondence should be addressed to Boni García; boni@diatel.upm.es

Received 19 May 2015; Accepted 27 July 2015

Academic Editor: Phillip A. Laplante

The purpose of developing e-Government is to make public administrations more efficient and transparent and to allow citizens to more comfortably and effectively access information. Such benefits are even more important to people with a physical disability, allowing them to reduce waiting times in procedures and travel. However, it is not in widespread use among this group, as they not only harbor the same fears as other citizens, but also must cope with the barriers inherent to their disability. This research proposes a solution to help persons with disabilities access e-Government services. This work, in cooperation with the Spanish Federation of Spinal-Cord Injury Victims and the Severely Disabled, includes the development of a portal specially oriented towards people with disabilities to help them locate and access services offered by Spanish administrations. Use of the portal relies on digital authentication of users based on X.509, which are found in identity cards of Spanish citizens. However, an analysis of their use reveals that this feature constitutes a significant barrier to accessibility. This paper proposes a more accessible solution using a USB cryptographic token that can conceal from users all complexity entailed in access to certificate-based applications, while assuring the required security.

1. Introduction

In 2006, the European Union launched its i2010 e-Government Action Plan [1], which was subsequently revised in The European e-Government Action Plan 2011–2015 [2], aimed at modernizing the public services of EU member states and making them more effective to reduce the burden of bureaucracy and ineffectiveness citizens must deal with. Accordingly, all EU states which are engaged in the generation of e-Government applications focused, first, on meeting the needs of and enhancing their own internal management processes and, second, on meeting the needs of society with regard to transparency, information, and provision of services.

The development of new e-Government services entails a series of further measures, both nationally and internationally. Owing to their direct impact on citizens, such services must have a digital identification that enables unequivocal authentication in online procedures. The confidentiality, integrity, and authenticity of data handled in such transactions must also be assured [3].

To meet this demand, many European countries are promoting the use among their citizenry of X.509 certificates [4] for their dealings with the administration, both in software and through secure portable devices. In Spain, as in other European countries, an additional functionality has been added to the existing ID card that is mandatory for all citizens, namely, a chip. This chip contains X.509 certificates and the necessary password in order to execute secure transactions with the administration.

Spanish public administrations allow for bidirectional interaction and full processing of public services with high levels that are greater than the average of the EU27 [5]. However, although some 80% of the Spanish population above the age of 14 has a digital identity card, only a small number of citizens use the services provided by the public administration. The reasons lie, first, in citizens' reluctance to use the new tool and, perhaps, more importantly, in the difficulty of using it.

In this situation, persons with disabilities, who account for approximately 8.5% of Spain's population [6], face a twofold challenge in accessing e-Government services: they have to cope with barriers to physically enter buildings or premises, in addition to an even greater obstacle in acceding telematically. A solution will require actions that minimize the digital gap and maximize these peoples' accessibility to telematic services, which have a great potential to improve their quality of life.

This piece of research has actively participated in developing and verifying a solution that helps persons with disabilities access e-Government services. It involves the use of simple device like a USB cryptographic token that can conceal from users all the complexity of accessing certificate-based applications [7]. The authors' work is part of a broader project undertaken in cooperation with the Spanish Federation of Spinal Cord Injury Victims and the Severely Disabled (ASPAYM) which also includes the development of a portal specially oriented towards persons with disabilities that helps them locate and access Spanish e-Government services.

The reminder of this paper is structured as follows: Section 2 presents the issue of accessibility in relation to e-Government and the use of digital certificates; Section 3 offers a qualitative analysis aimed at identifying the principal difficulties faced by persons with disabilities in using e-Government services. Based on this analysis, Section 4 discusses the different options that have been proposed to solve the problems identified, and Section 5 presents the solution ultimately implemented. Section 6 describes the technical assessment performed to verify the proposal. Section 7 describes how the system has been adopted by final users. Lastly, Section 8 presents our conclusions and future work deriving from our research.

2. Background

This section provides an analysis of the situation of digital certificates as the framework for this research. It also discusses related studies available in the literature.

2.1. Digital Certificates. A public key certificate, generally known simply as a certificate, is a digitally signed declaration that links a public key value to the identity of a person, device, or service that possesses the corresponding private key [8].

An electronic identity card (e-ID) is a document issued by an official authority that can identify users both online and offline. The following countries currently issue e-IDs: Belgium, Germany, Italy, the Netherlands, Pakistan, Rumania, Estonia, and Spain. In Spain, the e-ID is known as DNIe (or the *Documento Nacional de Identificación Electrónico* in Spanish). The Spanish government offers the DNIe in order to provide authentication and the capacity for electronic signatures. The DNIe follows the standard ISO 7816, which, in turn, is an evolution of the PKCS#15 standard [9].

At January 2015, Spain had issued more than 38 million DNIe (http://www.dnielectronico.es/). The DNIe contains two citizen X.509 certificates, one of authentication and the other for signature, in addition to private keys associated with each. According to a survey on equipment and use of information and communication technologies of the National Institute of Statistics of Spain, only 4.7% make use of the DNIe in their dealings with electronic public administrations [10]. The following factors should be noted with regard to these low levels of use:

(i) Not all people holding a DNIe with a generated certificate have stored the PIN needed to use it.

(ii) Not all citizens have a properly configured computer (drivers and card reader) for using the DNIe.

(iii) DNIe certificates expire every 30 months and require in-person renewal at the police station.

In view of the drawbacks of using the DNIe in dealings with e-Government, other types of digital certificates can be used. Of the twenty electronic certificates currently valid in Spain, the most popular is the Ceres certificate issued by the national Mint which is class 2CA [11, 12].

Use of an electronic certificate allows for carrying out a multitude of procedures and steps online, thus saving time in travel and telephone calls. This is of unquestionable value to people of reduced mobility and their family members and care providers. Further, procedures can be executed any day of the week at any time of day, with no need to travel or involve another person, with the attendant time savings (bearing in mind that the time required by a person of reduced mobility is greater than that needed by other citizens).

Although many services can be processed telematically, these are not yet in major use among persons with disabilities. The reasons lie in the difficulty of using them for a person not familiar with handling electronic certificates, which are the basis for all the services offered by administrations. It must be noted that this difficulty does not affect only persons with disabilities, but rather the majority of citizens. However, it is more significant in a group that could hugely benefit from their use.

2.2. Related Publications. In our study of the literature prior to undertaking this research, we found no papers reporting work that was similar to this paper. This alone constitutes a good reason to carry out the project. What follows is a brief overview of some of the related references we have found.

Heichlinger and Gallego describe the introduction of the electronic identity card (DNIe) in Spain [13]. In its conclusions, the article states that the DNIe in Spain was a case of good design and implementation, but with slow acceptance and low level use of the electronic identification function for online authentication. In their discussion of the DNIe, Ruiz-Agundez and Bringas propose an authentication service with electronic identity cards for VoIP. The authors set forth as future lines of work the use of other e-IDs apart from the DNIe [14].

The article by Olsen et al. [15] examines the advantages and drawbacks of e-Administration compared to traditional administration. Their results suggest that, after an initial investment and learning curve, e-Administration provides significant savings in time and effort. The main drawbacks are the initial cost of the software and the technical support necessary to successfully set up and operate the systems.

In their book *Constructing Accessible Web Sites*, the authors explain different techniques for constructing accessible web applications in terms of contents, browsing, data entry, tests, tools, and so forth [16]. But they do not study security from the point of view of accessibility, revealing a knowledge vacuum in this interdisciplinary mix (i.e., accessibility plus security).

Consequently, a solution must be sought that combines the advantages of the digital certificate and accessibility. The next section describes the methodology used to carry out a preliminary study to detect elements that negatively influence access to public administration in the use of secure web applications.

3. Methodology

The first step towards fostering the use of e-Administration among persons with disabilities consists in ascertaining the specific difficulties they face when they wish to carry out a procedure with the administration. A quantitative analysis was designed, requiring (i) a selection of a significant sample of public services offered by the administration, (ii) preparation of a user sample that is representative of the population group targeted by the technology solution, and (iii) the design of field work to allow users to try the telematic services. We shall now describe how the survey was performed and what results it produced.

3.1. Selection of Services. To select the services, work of documentation and deliberative analysis was conducted with persons with disabilities. First, the principal official literature on the international evaluation of e-Administration was consulted. At a global level, use was made of the United Global Nations Global E-Government Survey [17] for Europe; we used the *e-Government Indicator* of the Statistical Office of the European Union, Eurostat [18], and for Spain the Law of Public Electronic Access to Public Services [19], which defines the rights that e-Government services should allow.

The above information was used to create a questionnaire covering the main services identified in order to distinguish between them according to their greater or lesser use. Lastly, both the conclusions in the literature and the results of the questionnaire were debated in three discussion groups comprised of people with each of the disabilities included in the research project: cerebral damage, spinal cord injury, and cerebral palsy. The final result was a selection for study of ten basic services that are considered highly useful to persons with disabilities, at all levels of the state administration.

3.2. User Profiles. The three profiles included for the tests were cerebral palsy (CP), cerebral damage (CD), and spinal cord injury (SCI). The common denominator of these three profiles is a mobility difficulty associated with the disability. This is why telematic services provide a solution to a real problem encountered by persons with disabilities, as they shorten waiting times in procedures, reduce travel, and facilitate communication with the administration.

Separately, each of these groups has its own characteristics that hinder the performance of such procedures either in person or through telematic means:

(i) Cerebral palsy: this group has not historically been responsible for tasks related to procedures with the administrations. This work has always been carried out, like any other tasks related to care for these people, by parents, family members, or the legal guardian of the person. In many cases, particularly the most severe ones, this has led to legal incapacity for some individuals. Hence, the greatest problem is to train and provide information on such tasks to both the user and the family and on the importance of empowering persons with disabilities in any type of activity. Also, coupled with difficulties of mobility (remedied with supporting products) are cases of intellectual disability, resulting in difficulties in the processing of information.

(ii) Cerebral damage: as the vast majority of such people were "socially active" prior to the injury, they seek to achieve the greatest possible autonomy. Although they have shown great interest in this type of activity, the main problem lies in the cognitive problems: inability to understand certain texts and to process information and/or images and, in the website itself, problems of attention, of memorizing codes or passwords, and so forth.

(iii) Spinal cord injury: in the case of spinal cord injuries, the problems we found were similar to those of the general population, as this group is a faithful reflection of the real situation of society as a whole. The main problems were lack of knowledge of telematic services, fear of carrying out procedures online, the difficulty of accessing such services, frustration at several failed attempts, and so forth and problems that are often more pronounced owing to their difficulty in accessing computers (problems in typing or using a mouse).

3.3. User Sample. A representative sample of users was created to test the selected services. As the intention was not to obtain data that would be applicable to the rest of the population, it was not a random sample but rather a structural sample, understood as a sample with a bias toward structural saturation and not a statistical representation. The objective of the sample was to compile all the profiles considered significant in identifying barriers to access to e-Administration services:

(i) The first structural variable was the level of dependency. Due to the homogeneity of disabilities among the groups participating in the study, we decided to use the scale in the Spanish Dependency Law [20].

This law identifies three levels of dependency according to an individual's capacity to be autonomous in the activities of everyday life: moderate dependency, severe dependency, and major dependency. As the typology was elaborated with the aim of evaluating all types of disabilities, the tool can be used to structure the sample with a variable objective that is transversal to different disabilities.

(ii) Second, three levels of experience were defined in the use of technology prior to participation in the research project, and individuals with no previous experience were excluded. The remainder was classified in three levels: low for those who use technology sporadically, medium for those who habitually use technologies as a user, and high for those who habitually use technology and possess advanced knowledge such as how to install a program or solve a problem with the operating system.

(iii) Lastly, we sought parity between women and men.

With these three structural criteria, a minimum of two individuals per profile were established. With two individuals per profile, we obtained a structural sample of 36 people, structured as follows:

(i) 12 people are for each level of dependency.

(ii) 12 people are for each level of previous experience in the use of new technologies.

(iii) 24 people are of each gender.

(iv) Each individual performed two tests, so a total of 72 tests were conducted. Hence, each service was tested at least 7 times.

(v) Half the tests were conducted with a digital identity and the other half without such an identity.

This composition of the structural sample allows considering that the criteria of qualitative saturation have been met for the validity of the research.

3.4. Field Work. This research was carried out in collaboration with the Spanish Federation of Spinal Cord Injury Victims and the Severely Disabled (ASPAYM). Pilot tests were carried out in the Spanish offices of the federation of Madrid, Toledo, Cuenca, Albacete, and Murcia, and in the households of some users. In each pilot test, users were asked to carry out a procedure in two websites and evaluate them. The observer did not intervene if the user did not need assistance. The pilot test information was gathered in three ways:

(i) Direct observation of people responsible for the pilot tests.

(ii) A questionnaire on the accessibility experience at the end of each pilot test. The questionnaire was named ACDM-16 and it was prepared on the basis of the WCAG 2.0 accessibility standards.

(iii) A nonstructured interview after the questionnaire on matters observed during the test.

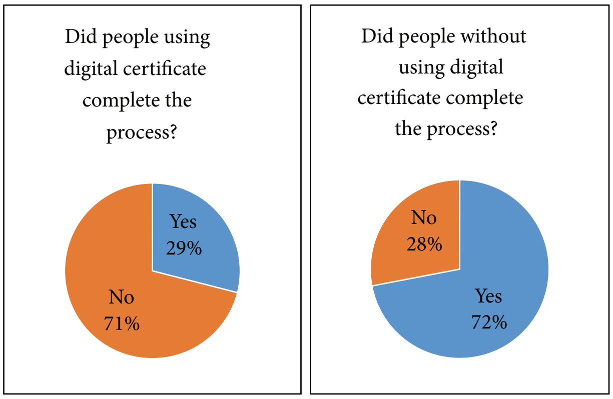


Figure 1: Results related to certificate use.

3.5. Analysis of Results and Conclusions. After the field work, the information gathered was analyzed. First, a descriptive analysis of the results of the ACDM-16 questionnaire was carried out through bivariable crossings between usability experience and the structural variables of the sample: level of dependency, experience in use of new technologies, and gender. The results of the descriptive analysis were analyzed on the basis of information garnered in the observation and informal interviews.

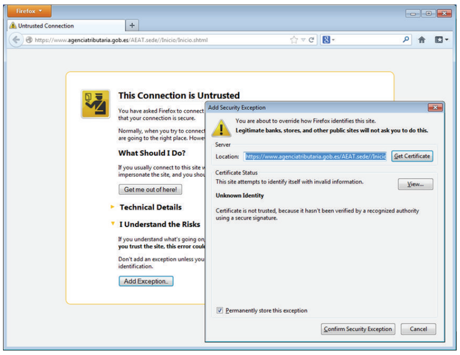
The variable with the most influence in the accessibility experience of telematic services of the administration was the type of disability, mainly through characteristics of cognitive development associated to each of the disabilities. These results lead to the conclusion that the technology solution must include elements related to cognitive accessibility, such as ease of reading, minimizing link routes, and use of pictograms, coupled with technical accessibility elements related to management of the digital certificate or the browsing experience.

Another of the significant results of this study was the finding that use of certificates possesses major difficulties for persons with disabilities, whether such certificates are installed in the browser or whether they are available through the citizen's identity card (see Figure 1).

First, difficulties are found for the initial use of the identity card which, although not specific to this group, often leads people who try to use e-Administration services to give up. This is because, before implementation, one must have a card reader, for which a special driver must often be installed and a cryptographic module downloaded from the official website of the authority issuing the identity card.

The first difficulty in use is due to the repeated requests to users to enter their PIN when carrying out a procedure with the administrations (as many times as the application requires access to the card). This PIN, which is composed of a series of random alphanumeric characters, is unmanageable (it contains between 8 and 16 characters, including uppercase and lowercase letters and other characters).

However, the main obstacle for a user no familiar with the handling of certificates relates to the security alerts of the browser, in the form of intimidating pop-up windows (see Figure 2), that warn of the browser's lack of trust in the web



This Connection is Untrusted

You have asked Firefox to connect
that your connection is secure.

Normally, when you try to connect
are going to the right place. Howe

What Should I Do?

If you usually connect to this site w
impersonate the site, and you shou

If you understand what's going on
you trust the site, this error coul

Don't add an exception unless you
identification.

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://www.agenciatributaria.gob.es/AEAT.sede//Inicio

Certificate Status

This site attempts to identify itself with invalid information.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

☑ Permanently store this exception

Figure 2: Example of unverified connection in Firefox.

server being accessed. To avoid such alerts, once must install the root certificates of the Certification Authorities [21] that have issued certificates involved in the transaction (our own and that of the server) [22]. Electronic portals usually have help pages for users to deal with these messages, but their explanations must be adapted to the operating system, browser, and the version of these being used. In view of the difficulties users encounter, they will often give up the idea of using a digital certificate after a fruitless attempt to carry out a transaction.

Owing to such difficulties, we decided to work in two complementary fields. First, we focused on designing a website that would be totally accessible and specifically oriented to persons with disabilities in order to enable them to comfortably access the services in the highest demand among them.

Second, we sought to design a solution to facilitate interaction with the administration through the use of a device that would be an alternative to the digital identity card. This device would not need a card reader and would be easy to use, freeing users from the cumbersome procedures of keying in a long PIN and not showing alert messages that frighten them. In addition the device would automatically update the browser and its certificates, would enable Java through the browser, and would install and update an antivirus, all of them without any user action. The latter solution is presented in the rest of this paper.

4. Design

The solution proposed in this piece of research to provide secure and comfortable access to electronic services of public e-Administration has been named the *CDA* (http://bonigarcia.github.io/cda/) (Accessible Digital Certificate, *Certificado Digital Accesible* in Spanish). The requirements set out for the design of this system are as follows:

(1) A cryptographic token would be used to store the user's digital certificate. This solution would allow people with disabilities to undertake any administrative procedures at home with their own computer. It had the additional advantage of being a portable device that would enable users to move to ASPAYM and make their administrative procedures with the help of a support person, like they had traditionally done.

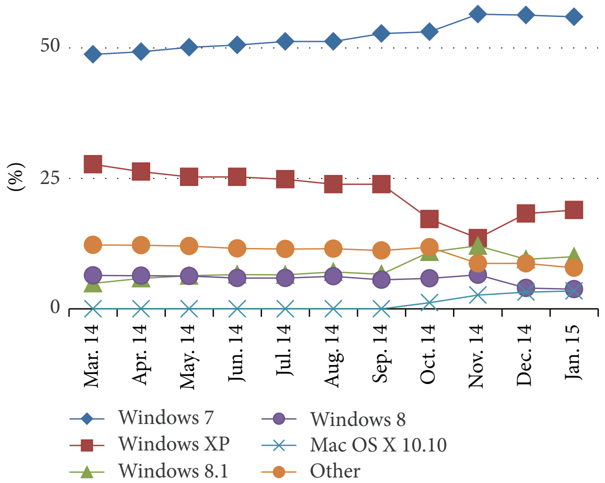


Figure 3: Use of desktop operating systems.

(2) The token would also have a fully configured web browser ready for use in secure web applications.

(3) When the token is connected via USB to the user's computer, the portable browser should automatically launch.

(4) When the user closes the browser, the USB device would be securely and automatically ejected.

(5) The browser certificate store would be updated automatically, as well as Java and the antivirus regardless of the user.

The following sections herein describe the design decisions made with regard to the operating system, browser, and the cryptographic token selected for the system. Lastly, a scenario of use with the components designed for the CDA is shown.

4.1. Operating System. The CDA runs on computers with a desktop operating system. According to the statistics of the company Net Applications (http://marketshare.hitslink.com/operating-system-market-share.aspx) (see Figure 3), Microsoft Windows is the dominant operating system in this market. Thus, the CDA had to be implemented for Windows 7, 8, 8.1, XP, and Vista.

4.2. Browser. To ensure ease of use in browsing secure web applications, the certificates handled by the browser must be kept in mind. A browser can use two types of certificates:

(1) A user digital certificate: it is an electronically signed document that confirms the user's identity. As discussed in Section 2, the most popular electronic certificates currently being issued in Spain by public authorities are the DNIe and the Ceres certificate.

(2) Digital certificates of severs or trusted authorities: these are issued by intermediate certification entities and certification entities and required to properly verify a certificate. Server certificates must be updated periodically to include new certificates and eliminate those that have expired or have been revoked.

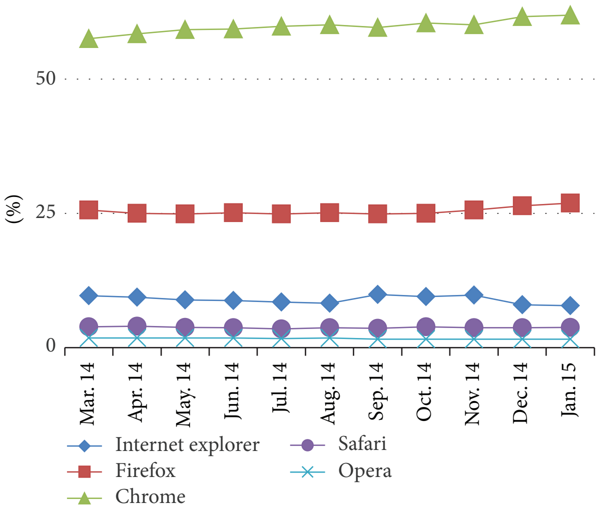


Figure 4: Use of web browsers.

The most commonly used browsers, according to figures from the W3Schools (http://www.w3schools.com/browsers/browsers_stats.asp), are Internet Explorer, Firefox, Chrome, Safari, and Opera (see Figure 4). Of these browsers, the Windows versions of Internet Explorer, Chrome, and Safari use the native key storage of Windows. For this reason, these browsers cannot form part of the CDA, as the key storage must be portable along with the token's browser. The possible alternatives are Firefox and Opera, both of which use their own key storage, making them portable.

Firefox uses the NSS (http://www.mozilla.org/projects/security/pki/nss/) (Network Security Services) key storage. NSS is a set of libraries designed to allow multiplatform development of distributed and secure applications. The great advantage of NSS is that it offers a wide variety of development tools that are highly useful in facilitating implementation. Hence, NSS was seen as the best option against Opera's own key storage, and thus the browser chosen for the CDA system was *Firefox*.

Entering into greater detail on NSS, Firefox certificates are stored in a Berkeley DB database located in the file *cert8.db* [23]. To ensure the ease of use of the CDA Firefox browser, this database will be updated automatically. For this reason, a web server was added to the CDA system for hosting an up-to-date *cert8.db* database. The token securely connects to the server to update the database in a manner that is transparent to the user. Hence, this avoids situations in which the browser cannot confirm that the connection with certain applications is secured (see Figure 2). Security exceptions are stored by Firefox in a text file called *cert_override.txt*. Therefore, this file must also be stored on the server along with *cert8.db* [24].

4.3. Cryptographic Token. A cryptographic token is an electronic device that provides authentication and authorization services. The token to be used in implementing the CDA must be capable of storing the user digital certificate securely. It must also have storage capacity for the USB-accessible portable web browser.

A multitude of cryptographic tokens are available on the market. A detailed comparison of such tokens is beyond the scope of this paper. Based on the requirements defined for CDA, the device chosen was the *iAM* cryptographic token developed by the company Bit4id (http://www.bit4id.com/en/). It is a USB device based on a cryptographic microprocessor incorporating a micro-SD memory with applications for electronic signatures and encryption and verification of electronically signed documents. The device includes a SIM card that can store personal user certificates. Access to the certificate is protected with PIN/PUK codes. It also incorporates a Mifare 1K S50 proximity contactless chip to control access/presence. This token has the certification guarantees of Common Criteria EAL4+ and FIPS 140-2 level 3.

According to Spanish legislation, users who want to electronically interact with Spanish administrations need a recognized certificate, that is, a digital certificate issued by a recognized Service Provider Certification. These certificates offer a guarantee that the identity linked to the action taken with the digital certificate is real. Therefore, before issuing the cryptographic token to users, their identities have to be checked by a qualified entity (Registration Authority). In order to facilitate to persons with disabilities the process of checking their identities, ASPAYM was authorized by a Service Provider to act as Registration Authority so persons with disabilities can get their cryptographic token with their certificate in a familiar and not stressful environment while they can make appropriate questions to clarify any aspect of its operation.

4.4. Use Scenario. To implement requirements 2 and 3 set out at the start of this section, the simplest solution was to create an application that runs when the USB token is connected to the user's machine. Given that the solution was being developed for Windows systems, the Autorun (http://msdn.microsoft.com/en-us/library/cc144206(VS.85).aspx) component could have been used. Since Windows 95, Autorun allows running certain processes when a removable medium is inserted. Actions run with this method are listed in a file called autorun.inf in the connected medium. Closely related to Autorun, Windows 98 introduced Autoplay (http://msdn.microsoft.com/en-us/library/cc144210(VS.85).aspx). This Windows feature examines the content of a removable device connected to the system and offers a series of options.

Microsoft's Autorun [25] has often been used to transmit malware [26]. For this reason, Autorun has been disabled for USB devices since Windows 7. A 2011 study by Microsoft found that 26% of infections of Windows systems came from the installation of malware via USB devices [27]. For this reason, in February 2011, security update KB971029 (http://support.microsoft.com/kb/971029) was released for Windows XP systems and later, under which Autorun for USB was disabled.

Therefore, and based on the requirements set forth, the design of a CDA system using the following components was undertaken:

(i) CDA-Listener: software component that is installed in the user's machine. It has a listener even programmed to detect the USB connection of the token

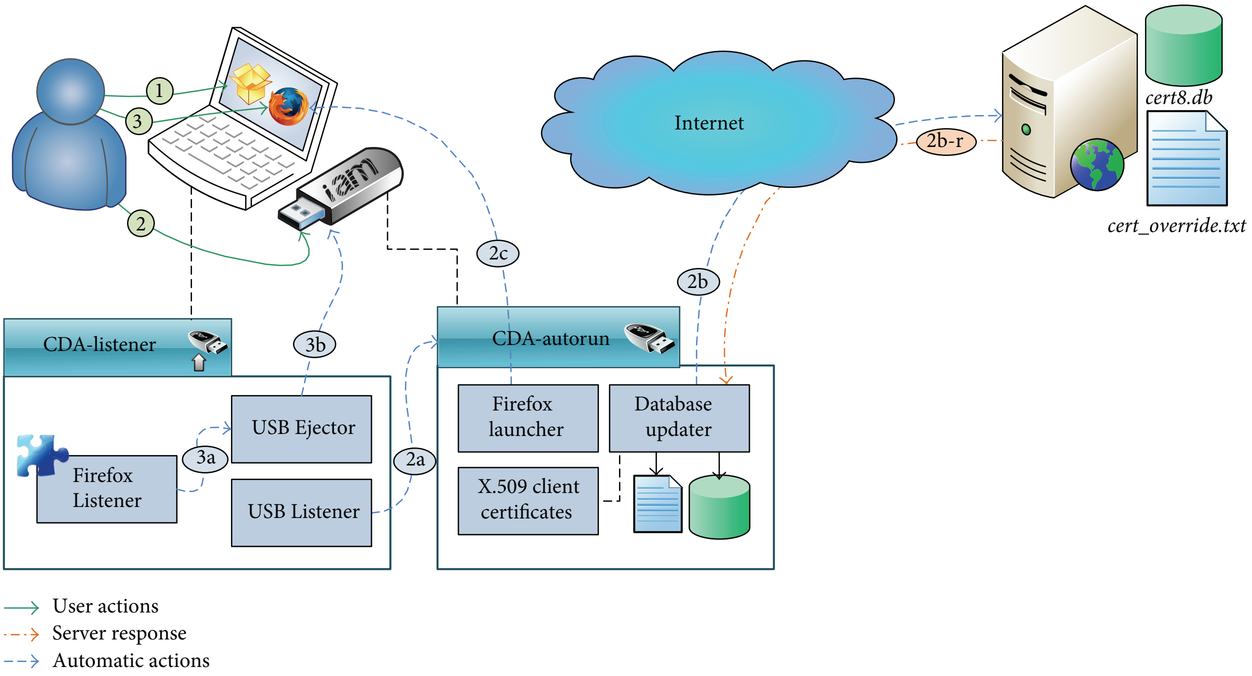


Figure 5: Use scenario.

in the system. When it detects the connection, it launches CDA-Autorun stored in the token. It also contains a component that detects the shutdown of the token's portable browser, and it securely ejects the USB token.

(ii) CDA-Autorun: software component that is stored in the token. It updates the certificate database of the token's portable Firefox. It securely connects to a web server that contains an updated certificate database. After the update, it launches Firefox so that the user can run the browser with his digital certificate.

The procedure for the CDA token is illustrated in Figure 5. Given that the main objective of this project is accessibility, the centerpiece of this scenario is the user. The user must take the following steps to use the token:

(1) Install the CDA-Listener component in the user's operating system (step labeled as 1 in the diagram). The installer of the component is implemented with a simple wizard that requires the user's attention only to accept the installation through a number of successive screens. This step is carried out by the user only once, as the CDA-Listener will be installed in the system thus creating an entry in the Windows registry so that the program will launch at the start of a session.

(2) Connection of token via USB: at that moment, with the CDA-Listener installed in the system, the component detects that the token has been connected, and it launches the CDA-Autorun in the token (step 2a). CDA-Autorun connects to a webs server to update the certificate database (step 2b). To make the connection secure, it uses a series of X.509 client certificates. The response will be the updated Firefox certificate database, that is, the files *cert8.db* and *cert_override.txt* (step 2b-r). Then, the portable Firefox browser is launched (step 2c).

(3) The user uses the browser securely and with their user certificate. When the user decides to end browsing, the user closes the Firefox browser. Then, the Firefox Listener component of CDA-Listener will call USB Ejector to securely eject the USB device (step 3a). Finally, the user is informed that the token may be removed (step 3b).

5. Implementation

To implement CDA-Listener and CDA-Autorun, C# programming language was chosen. The decision was determined by the platform on which the CDA system is to be run, namely, Windows. C#, as a development language made by and for Microsoft, offers advanced access to all the functions of Windows. This will prove particularly useful in developing the USB device listener.

5.1. CDA-Listener. This component was developed as an application that is visible as an icon on the Windows taskbar. It is implemented as a single-instance application, which means that it should be present only once in the system.

5.1.1. USB Listener. Detection of a connection of USB devices (USB Listener in Figure 5) was implemented through programming of a WQL event (WMI Query Language). WMI (Windows Management Instrumentation) is the Microsoft implementation of the CIM (Common Information Model)

```
stringusbScope = @"root\CIMV2";
stringusbQueryString = "SELECT * FROM _InstanceOperationEvent
WITHIN 3 WHERE TargetInstance ISA 'Win32_DiskDrive'";
usb_listener = new ManagementEventWatcher(usbScope,
usbQueryString);
usb_listener.EventArrived += new
EventArrivedEventHandler(usb_connected);
usb_listener.Start();
```

Listing 1: USB Listener.

```
exports.onUnload = function(reason) {
  // Components.classes and Components.interfaces
  var {Cc,Ci} = require("chrome");

  // Reading user environment variable %ProgramFiles%
  varuserEnvironment=Cc["@mozilla.org/process/environment;1"].
    getService(Ci.nsIEnvironment);
  varprogramFiles = userEnvironment.get("ProgramFiles");

  // Call USB Ejector (inside CDA-Listener)
  var file = Cc["@mozilla.org/file/local;1"].
    createInstance(Ci.nsILocalFile);
  file.initWithPath(programFiles + "\\Certificado Digital
    Accesible\\CDA-Listener.exe");
  var process = Cc["@mozilla.org/process/util;1"].
    createInstance(Ci.nsIProcess);
  varargs = ["eject"];
  process.init(file);
  process.run(false, args, args.length);
};
```

Listing 2: Firefox add-on CDA-Ejector (main.js).

standard of DMTF (Distributed Management Task Force) [28]. The CIM standard, and consequently WMI, defines a series of classes that provide system information that allow for local and remote management of said system [29].

The WQL query listens for any event of the kind it handles of all the events in a machine whose origin is a disk drive. The query is run every three seconds. Therefore, the code in C# of listening for USB devices can be seen in Listing 1.

5.1.2. Firefox Listener. In the first implementation of CDA-Listener, this part was developed by programming a MQL query that listened for the end of the process of the token's portable Firefox. Although this solution functions correctly, it may pose certain problems for the user, as from the moment the user shuts down the browser until the moment the system terminates the process, there is a period of time in which the user does not know that the device is being ejected.

To improve this function, this part has been implemented as an add-on of the token's portable Firefox. Thus, the browser itself gives an alert that the user has shut it down. Then, a call is made to the USB Ejector of CDA-Listener to initiate a secure disconnection of the USB device. Meanwhile, a splash screen informs the user of the process underway of secure ejection of the token.

To implement this part, we used an online tool for the development of Mozilla add-ons, the Add-on Builder (https://builder.addons.mozilla.org/). The creation of the add-on requires only a fragment of JavaScript code (*main.js*) from Listing 2.

5.1.3. USB Ejector. For secure ejection of the USB device, the open source tool USB Disk Ejector (http://quickandeasysoftware.net/software/usb-disk-ejector) has been incorporated to CDA-Listener. This tool is portable and flexible and it can be called with different arguments from the command line. But the main reason for choosing this tool is the fact that, before securely ejecting the USB device, it detects what applications have been launched from the device and forces them to shut down.

This is quite useful in a system like CDA, as processes launched by the portable Firefox directly from the USB sometimes remain in a waiting state that prevents the secure

```
curl--remote-time --remote-name --ciphers RSA --cert cda-
client.crt --key cda-client.key --cacertcda-ca.crt
https://innova.diatel.upm.es/db.ssl/cert8.db
```

Listing 3: cURL command.

ejection of the device. This may create a problem of accessibility for CDA users. The problem is solved by including USB Disk Ejector as a tool for secure ejection of the USB.

5.2. CDA-Autorun. The iAM token includes CDA-Autorun, which updates the certificate database and launches the portable Firefox.

5.2.1. X.509 Client Certificates for Secure Connection to the Server Certificates. This section explains how X.509 client and server certificates are generated to securely download the files *cert8.db* and *cert_override.txt*, which are stored on the web server of the system. The purpose of using these certificates in the communication of the CDA token with the web server is to run mutual authentication between client and server and to ensure secure communication between the two entities. To generate X.509 certificates, the open source tool OpenSSL (http://www.openssl.org/) is used.

5.2.2. Database Updater. The CDA system requires up-to-date maintenance of a master certificate database in a web server (*cert8.db* and *cert_override.txt*). To download these files, the open source tool *cURL* (http://curl.haxx.se/) is used, specifically the version with SSL support. The syntax of the command to download the SSL database from the web server with a copy of the master database *cert8.db* is described in Listing 3.

The downloaded database must be merged with the local database of the token, thus installing locally any new certificates and updating existing ones. The merger of contents for the text file *cert_override.txt* is done through a line-by-line comparison of the file downloaded from the server with the local file of the token. For *cert8.db*, the tool *certutil* (http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html) of the certificate database tool package of NSS was used.

5.3. Token Configuration. The iAM token includes the parts explained in the foregoing sections: CDA-Listener installer, CDA-Autorun, client certificates, and CA (*cda-client.crt*, *cda-client.crt,* and *cda-ca.crt*) and the tools *cURL* and *certutil*. Further, the plug-in CDA-Ejector must be installed in the portable Firefox.

Lastly, to ensure that use of the browser is independent of the final user's system, Flash, Adobe Reader, and portable Java plug-ins are to be installed in the portable Firefox.

6. Verification

Following development of all the components proposed herein, with the token properly configured and the server ready, a series of laboratory experiments were conducted to verify the viability of the proposal. Different virtual machines were used of different Windows operating systems as set out in the requirements (XP, Vista, 7, 8, and 8.1). These virtual machines were installed in a VMWare Workstation 8.0. The VMWare snapshots system was used to store different test states used to evaluate the virtual machines.

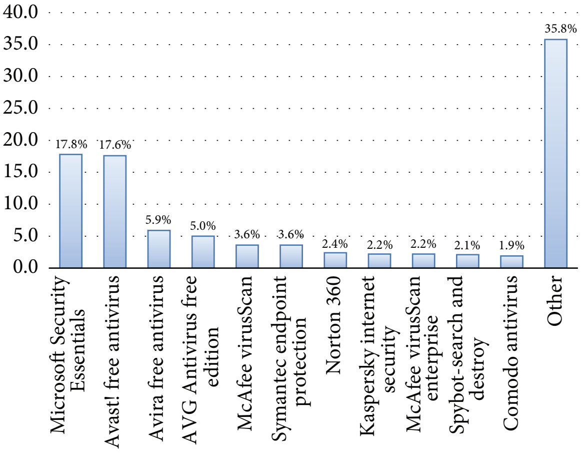


Figure 6: Use of antivirus programs.

For each of these five Windows virtual machines, tests with different antivirus programs were performed. According to the statistics company Internet Opswat (https://www.opswat.com/resources/reports/antivirus-and-compromised-device-january-2015), the most commonly used antivirus programs in January 2015 were Microsoft Security Essentials and Avast Free Antivirus (see Figure 6).

Hence, tests were conducted for Windows with each of these antivirus programs and in another scenario of a Windows system without an antivirus program. 13 snapshots were available for the tests. This figure is the result of the multiplication of the antivirus configurations by the number of operating systems and subtracting two scenarios, due to the fact that Windows 8 and 8.1 cannot be tested without an antivirus, as they include the new version of Security Essentials, called Windows Defender. For each of these 13 snapshots, the test procedure was as follows:

(1) Install CDA-Listener.

(2) Connect iAM token.

(3) Check that CDA-Autorun runs automatically and that the certificates of the portable Firefox browser are being updated.

Table 1: Summary of test results.

<table>
<tr><th></th><th>No antivirus</th><th>Security Essentials</th><th>Avast</th></tr>
<tr><td>Windows XP</td><td>√</td><td>√</td><td>√</td></tr>
<tr><td>Windows Vista</td><td>√</td><td>√</td><td>✗</td></tr>
<tr><td>Windows 7</td><td>√</td><td>√</td><td>✗</td></tr>
<tr><td>Windows 8</td><td colspan="2">√</td><td>✗</td></tr>
<tr><td>Windows 8.1</td><td colspan="2">√</td><td>✗</td></tr>
</table>

(4) Check that portable Firefox does not conflict with a previously installed version of Firefox in the system.

(5) Browse with the portable Firefox using the user digital certificate of the token.

(6) Close the portable Firefox.

(7) Check that it is automatically ejected.

Table 1 contains the test results. The symbol "√" means that all the tests showed satisfactory results. The symbol "✗" means that problematic situations arose in the tests. These problems were detected when the antivirus program Avast was installed in the user system (Windows Vista, 7, 8, and 8.1).

The reason for such problems is that, by default, Avast does not trust the components making up the system, such as CDA-Listener and CDA-Autorun. The user must expressly tell the program that these components are secure; the components continue to run and they completed their tasks correctly. The solution to this program involves excluding CDA components from the Avast Sandbox analysis.

7. User Acceptance Testing

Both tests of web site and CDA solution were conducted during the last week of January 2014 at the headquarters of ASPAYM in Madrid. A total of 30 CDAs were distributed among volunteers with physical disabilities, members of ASPAYM, who regularly used the computer, and therapists so they will learn how the new system works and spread its use between affiliates.

The tests were undertaken by a sociologist and a person with disabilities (wheelchair) that helped eliminate existing reluctance among participants. In a similar manner, as was previously done, participants were asked to carry out two different administrative procedures that require digital authentication and to evaluate the usability of the CDA after the trial through a questionnaire. The two people responsible for performing the tests did not intervene if the user did not need assistance and observe the reactions of the participants. At the end of each test they made an unstructured interview with them about issues observed during testing.

The results showed that less than 60% of participants managed to finish their procedures, but analysis confirm that it was not due to problems arising from the use of the CDA but the inherent difficulty of the procedure. Some other problems were found when accessing some e-Government services because no provision was made for the use of certificates as the ones included in the CDA.

Use of CDA was considered especially useful among those that were "socially active" prior to the injury because they can now perform their administrative procedures by themselves, enjoying the autonomy they want.

However, the vast majority of participants attached great importance to the point that this solution had helped them to raise awareness of the possibilities of e-Government hitherto unknown to most. It is therefore expected that from now on these people will make full use of services provided by e-Government.

8. Conclusions and Future Work

ICT are a great opportunity for providing skills for universal access to information and they may become an important ally for dependent people and their families, who can benefit with equal opportunities from many of the services of present-day society. ICT can help improve the quality of life of many people who face discrimination owing to their functional diversity and provide them with new personal and professional opportunities.

However, barriers to access to telematic services that affect the general population can often become insurmountable for persons with disabilities. To avoid this, new actions must be undertaken to minimize the digital gap and maximize these people's accessibility to telematic services, which can potentially make significant improvements in their quality of life.

This is the framework for which the solution proposed in this paper has a special meaning. The development of a CDA cryptographic token that allows the general population a secure and comfortable access to electronic services of public administrations is especially useful for persons with disabilities. This token hides from citizens all the complexity involved in the use of certificates, thus providing an accessible solution to enable persons with disabilities to benefit from the services offered by e-Administration.

The launch of a new accessible web portal for services offered by public administrations, combined with the use of the cryptographic token, has greatly contributed to increasing general awareness of e-Government services. More specifically, the solution provided has facilitated people with disabilities to make administrative procedures more easily and thus it eliminates new barriers that open in front of them.

It is to be hoped that the administrations will gradually achieve higher levels of accessibility and usability in its services, and that the problems discussed herein are resolved shortly. In the meanwhile, the solution in this paper will allow citizens with a disability to benefit, starting now, from the substantial advantages of e-Administration.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This paper has been developed within the framework of the ASTIC project (Accessibility in Intelligent Telematic

Services for Citizens, *Accesibilidad en los Servicios Telemáticos Inteligentes para el Ciudadano*), with funding from the Spanish Ministry of Industry, Tourism and Commerce through assistance provided under the Plan Avanza 2011.

References

[1] European Commission, *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All*, European Commission, 2006.

[2] European Commission, *The European eGovernment Action Plan 2011–2015. Harnessing ICT to Promote Smart, Sustainable and Innovative Government*, European Commission, 2010.

[3] C. Rughiniş and R. Rughiniş, "Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union," *Computers & Security*, vol. 43, pp. 111–125, 2014.

[4] D. W. Chadwick, A. Otenko, and E. Ball, "Role-based access control with X.509 attribute certificates," *IEEE Internet Computing*, vol. 7, no. 2, pp. 62–69, 2003.

[5] European Commission, *Eurostat e-Government Statistics: Online Interactions of European Businesses and Citizens with Public Administrations*, European Commission, 2009.

[6] Spanish Statistical Office—INE, *Survey on Disability, Independence, and Dependency Situations*, Spanish Statistical Office—INE, 2008.

[7] C. Cachin and N. Chandran, "A secure cryptographic token interface," in *Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF '09)*, pp. 141–153, IEEE, July 2009.

[8] Y. Kortesniemi and M. Särelä, "Survey of certificate usage in distributed access control," *Computers & Security*, vol. 44, pp. 16–32, 2014.

[9] M. Nystr and M. Nyström, "PKCS #15—a cryptographic token information format standard," in *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology (WOST '99)*, p. 5, USENIX Association, Berkeley, Calif, USA, 1999.

[10] Spanish Statistical Office—INE, *Survey on the Equipment and Use of Information and Communication Technologies (ICT-H) in Households*, Spanish Statistical Office—INE, 2013.

[11] P. Wohlmacher, "Digital certificates: a survey of revocation methods," in *Proceedings of the Workshops on Multimedia*, pp. 111–114, ACM, Los Angeles, Calif, USA, October 2000.

[12] N. Leavitt, "Internet security under attack: the undermining of digital certificates," *Computer*, vol. 44, no. 12, Article ID 6096548, pp. 17–20, 2011.

[13] A. Heichlinger and P. Gallego, "A new e-ID card and online authentication in Spain," *Identity in the Information Society*, vol. 3, no. 1, pp. 43–64, 2010.

[14] I. Ruiz-Agundez and P. G. Bringas, "Service authentication via electronic identification cards: voip service authentication through the DNIe," in *Proceedings of the Annual SRII Global Conference (SRII '12)*, pp. 602–607, IEEE Computer Society, San Jose, Calif, USA, 2012.

[15] D. R. Olsen, S. A. Wygant, and B. L. Brown, "Electronic survey administration: assessment in the twenty-first century," *Assessment Update*, vol. 16, no. 3, pp. 1–15, 2004.

[16] P. Kotzé, K. Renaud, and J. V. Biljon, "*Don't* do this—pitfalls in using anti-patterns in teaching human-computer interaction principles," *Computers & Education*, vol. 50, no. 3, pp. 979–1008, 2008.

[17] United Nations Public Administration Network (UNPAN), *United Global Nation's Global e-Government Survey*, United Nations Public Administration Network (UNPAN), 2012.

[18] European Commission, *Eurostat Statistic Theme 10: Good Governance*, European Commission, 2011.

[19] Spanish Official State Gazette—BOE, *Law 11/2007 of Public Electronic Access to Public Services*, Spanish Official State Gazette—BOE, 2007.

[20] Spanish Official State Gazette—BOE, *Law 39/2006 of Promoting Personal Autonomy and Care for People in Situations of Dependency*, Spanish Official State Gazette—BOE, 2006.

[21] J. Feghhi, J. Feghhi, and P. Williams, *Digital Certificates*, Addison-Wesley, 1999.

[22] A. Rwabutaza, M. Yang, and N. Bourbakis, "A comparative survey on cryptology-based methodologies," *International Journal of Information Security and Privacy*, vol. 6, no. 3, pp. 1–37, 2012.

[23] J. Marchesini, S. W. Smith, and M. Zhao, "The surprising insecurity of client-side SSL," *Computers & Security*, vol. 24, no. 2, pp. 109–123, 2005.

[24] R. Gallo, H. Kawakami, and R. Dahab, "Case study: on the security of key storage on PCs," in *Proceedings of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom '13)*, pp. 1645–1651, IEEE, July 2013.

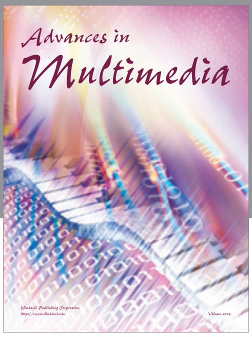
[25] InfoSecurity, "Windows Autorun trojan tops November malware chart," 2009.

[26] J. Clark, S. Leblanc, and S. Knight, "Compromise through usb-based hardware trojan horse device," *Future Generation Computer Systems*, vol. 27, no. 5, pp. 555–563, 2011.

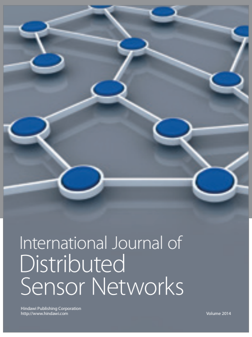
[27] Microsoft, "Microsoft security intelligence report volume 11," Tech. Rep., Microsoft, 2011.

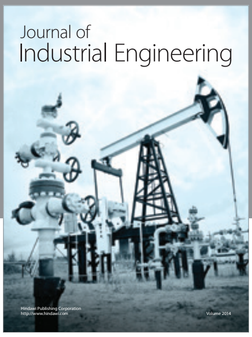
[28] R. Siddaway, *PowerShell and WMI*, Manning Publications Co. Series, O'Reilly Media, 2012.

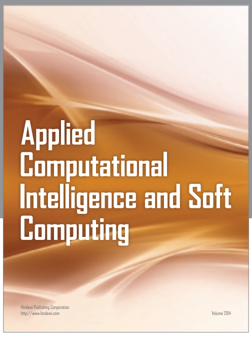
[29] K. Chan and I. Poernomo, "QoS-aware model driven architecture through the UML and CIM," *Information Systems Frontiers*, vol. 9, no. 2-3, pp. 209–224, 2007.

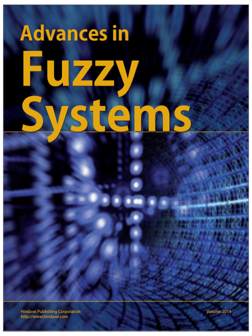

Advances in
Multimedia

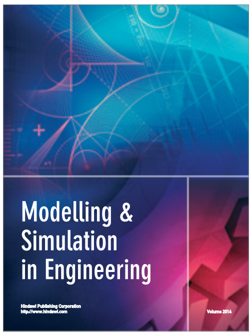
The Scientific
World Journal

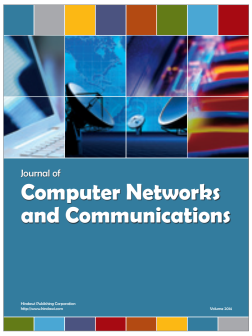

International Journal of
Distributed
Sensor Networks

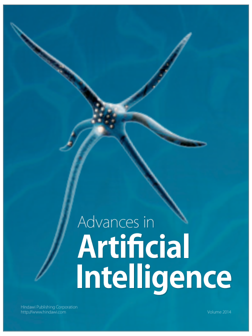

Journal of
Industrial Engineering

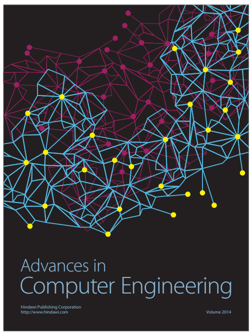

Applied
Computational
Intelligence and Soft
Computing


Advances in
Fuzzy
Systems

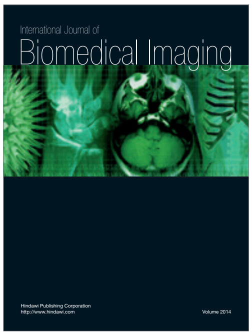

Modelling &
Simulation
in Engineering

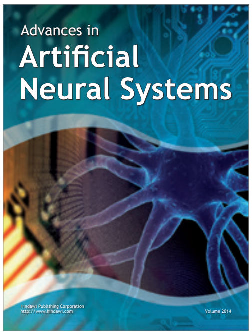

Journal of
Computer Networks
and Communications

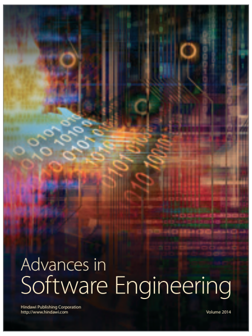

Advances in
Artificial
Intelligence


Advances in
Computer Engineering

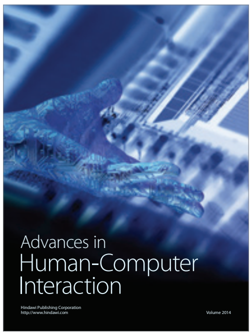
International Journal of
Computer Games
Technology

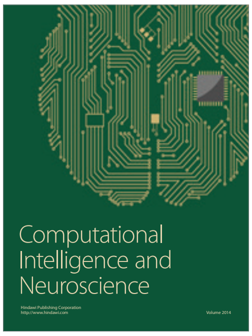

International Journal of
Biomedical Imaging


Advances in
Artificial
Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer
Interaction


Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering