Service Authentication via electronic identification cards

VoIP service authentication through the DNIe

Igor Ruiz-Agundez and Pablo G. Bringas
DeustoTech Computing
Deusto Institute of Technology, University of Deusto
Bilbao, Basque Country
{igor.ira,pablo.garcia.bringas}@deusto.es

Abstract— **User authentication is one of the most popular techniques used in access control systems. It provides with trustful confirmation about the identity of a person when she attempts to use a service. It ensures that a user is who she claims to be verifying by that she is allowed to use a certain service. Different governments and agencies have attempted to create a universal authentication device to allow easy access to e-government services and potentially to any corporative service. Authentication contributes to the unequivocal identification of the user. In this research, we focus on the Spanish electronic identification card (also known as DNIe). In our research we focus on authentication through the DNIe because it provides with two levels of security. Authenticating with the DNIe implies having the electronic identification card (eID card) and knowing the card holder's verification password. We implement a methodology that integrates DNIe authentication in any application through a service library component seamlessly. This authentication methodology takes advantage of all the DNIe capabilities and includes the following steps: connection to the eID card, load of user certificates, generation of a verification challenge, signing and verification of this challenge by using cryptographic techniques, and finally, accepting or rejecting user identification. In order to validate this methodology, we integrate our seamless authentication library in a Voice over IP application. Currently, this methodology is being used in call-centres that need to unequivocally validate the identity of the operators in each call and operation they perform.**

Keywords- DNIe; electronic identification card; service authentication; VoIP

I. Introduction

Identity is personal and cannot be transferred. Its verification gives us access to the doors we are authorise to cross and constrains us from entering into places we are not supposed to traverse.

Translating the users' identity to the services world is not a new task. User authentication is one of the most popular techniques used in access control systems. It provides with trustful confirmation about the identity of a person when she attempts to use a service. It ensures that a user is who she claims to be.

It is worth mentioning the difference between authentication and authorisation. The authentication provides with the verification of the identity of a person or element (who are you?). On the other hand, authorisation validates if an identity can access a given resource or service (are you allowed to access?). Hence, performing an authorisation requires an authentication first.

In recent history, the most popular authentication method has been fingerprint analysis. Further, its reliability has been proved to be weak [10]. Other methods, such as passwords, challenge responses, tokens, and so on have their own advantages and disadvantages. Furthermore, the number of authentication mechanisms is increasing and their standardisation seems to be complex.

Still, different governments and agencies have attempted to create a universal authentication device to allow easy access to e-government services and potentially to any corporate service.

In this research, we focus on the Spanish electronic identification card (henceforth the DNIe). The Spanish government supplies this DNIe in order to provide authentication and electronic signature capabilities. Authentication contributes to the unequivocal identification of the user and the digital signature authenticates the sender of a message by providing with message integrity and non-reputation.

The deployment of the DNIe is complete and more than 47 million citizens can use its potential. Furthermore, the ecosystem of services and applications that use the DNIe is growing.

Many countries of the European Union, and all over the world, have started to distribute these electronic identification cards (eID cards) among their citizens [15]. Up to the writing of this paper, ten European countries have successfully deployed their eID cards and others are considering doing it.

Regarding traditional telephony, the identity of the participants is done by recognising the other person's voice or by means of a prearranged password. Thought, this method only works if the participants know each other or are able to exchange the password through a secure channel. This informal security approach is not enough in corporate and administrative scenarios in which the identity of the user must be univocally guaranteed.

Against this background, we advance the state of the art of service authentication via eID cards in two main ways. First, we introduce a new method of authentication that extends the application of an existing eID card. Second, we evaluate the method through its application in a Voice over Internet Protocol (VoIP) service.

The remainder of this paper is organised as follows. Section II introduces the related work in service authentication, eID cards (focusing on the DNIe), and their use in VoIP authentication. Section III details the proposed eID card authentication method. Section IV presents the results of applying this method to a VoIP service. Finally, Section V concludes and outlines the avenues of future work.

II. Related Work

User authentication can be classified in three basic methods. First, knowledge factors are based on something the user knows (e.g. passwords, pass phrase, challenge response or personal identification number). Second, ownership factors: using something the user has (e.g. identification card, cell-phone, or electronic token). Finally, inherent factors: evaluating something the user is or does (e.g. voice, face, fingerprint, or retinal pattern).

It is worth mentioning that there could be other less well known factors than those based on vouching factors, which rest on somebody you know [1].

Depending on the number of methods used for authentication, this can be unimodal or multimodal. Unimodal authentication uses just one of the three basic methods. On the other hand, multimodal authentication uses any combination of them.

Besides the authentication method, we can classify the authentication mechanisms used by the system:

- Biometric authentication: recognition is based on intrinsic physical or behavioural traits.
- Authentication based on tokens: uses physical devices that generate an authorisation password.
- Single Sign-On authentication (SSO): user logs in once and gains access to all the services in the system. Besides simple passwords, there are other SSO authentication mechanism:
  - One-time passwords: the shibboleth is valid to authenticate only once.
  - Time-base passwords: they are a special type of one-time password. The shibboleth is valid only once and for a given amount of time, normally a minute.
- Lightweight Directory Access Protocol (LDAP): provides with directory services that can authenticate its registered users [5].
- Challenge-response schemes: the service provider presents a question (challenge) to the user who must answer correctly.

These authentication methods require the use of cryptographic algorithms to secure the system. These algorithms are designed to secure the communication in the potential presence of non-desired third parties. Generally speaking, cryptography is divided in three main families:

- Symmetric functions: both the sender and receiver share the same key to protect the messages (i.e. DES, TDES, RC2, RC4, RC5, IDEA, Blowfish and AES).
- Asymmetric functions: each of the participants has two keys, one to cipher and one to decipher (i.e. Diffie-Hellman, RSA, DSA, ElGammal).
- Hash functions: maps a dataset to a smaller dataset, which is normally used to guarantee the integrity of the messages (i.e. SHA, MD5, and Rabin-Karp).

Depending on the security requirements of a service, these or other techniques can be used in order to ensure the identity of the user, even though the standardisation and imposition of one technique over the others is complex and probably will not happen in the near future.

As mentioned above and despite the difficult stage of homogenisation, some countries are providing their citizens with basic online authentication mechanisms through the use of eID cards.

EID cards are a subset of smart cards. Smart cards have been used in many sectors, such as prepaid telephony, banking, loyalty cards, access cards, and so forth. They contain an Integrated Circuit Card (ICC) which, depending on the chip they have, will provide with different functions.

In this way, smart cards can have memory cards that only offer data storing. They can include micro-processed cards that contain files and applications that are normally used for identification and electronic payments. Finally, there are cryptographic cards that include specific modules to perform cryptographic operations. Since eID cards provide with authentication and signature capabilities, they are considered cryptographic cards.

A. The particularities of the DNIe

In our research we focus on the authentication through the DNIe because it provides with two levels of security. Authenticating with the DNIe implies having the eID card and knowing the card holder's verification password.

The DNIe is an eID card that follows the ISO 7816 standard, which in turn is an evolution of the PKCS#15 standard [12].

These standards determine how the keys, certificates, authentication objects and any other data are stored in the eID card. The data are stored in a hierarchical file system made up of a Master File (MF) and various levels of Dedicated Files (DF) that can store data o perform administration tasks. The bottom level is formed by Elemental Files (EF) that contain the data.

The DNI distributes the user data in three different security areas with specific security policies:

- Public zone: there is no access security control. This zone contains the root Certificate Authority (CA) certificates and the certificates of the CA responsible for validating the user identity.
- Private zone: access is granted with a password. This zone contains user authentication (provides digital signature) and sign (provides non-repudiation) certificates.
- Secure zone: access implies the use of administration privileges. This zone is only

accessible with certain physical devices and contains the user’s personal data, a photograph, an image of the handwritten signature and the user’s fingerprint.

It is worth mentioning that the DNIe has also several physical anti-counterfeiting measures: offset printing, guilloche patterns, iris printing, invisible ink, positive and negative micro-texts, encoded images, silkscreen, ink whose colour changes depending on vision angle, kinegrams and embossed photography and text.

Some of them can be seen with naked eye and others require additional optical and electronic equipment (e.g. ultraviolet light). All of these protections enhance the security of this eID card. Figure 1 shows the physical appearance of the DNIe, both the front and the back.

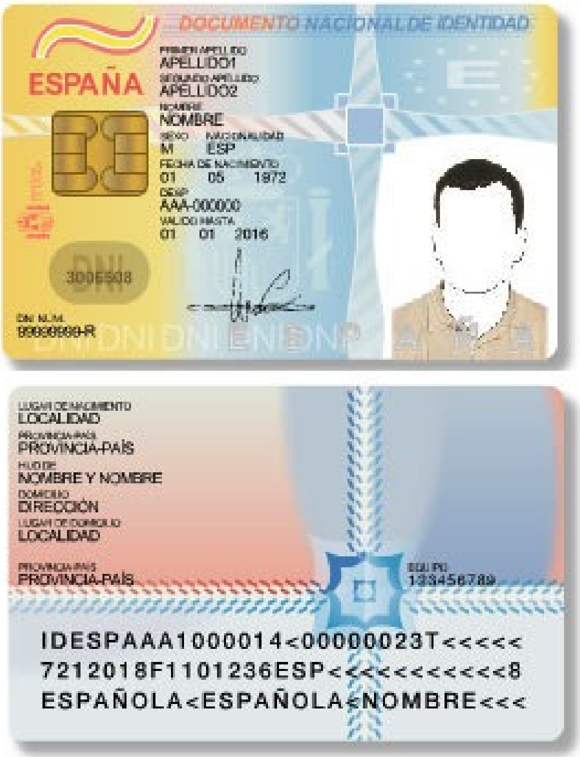

Figure 1. Front and back of a DNIe.

B. *VoIP authentication with eID cards*

To our knowledge, very little work has been done in VoIP authentication using eID cards. There is a theoretical approach to identify the users of a VoIP call by using the German eID card [9]. This approach presents a model that attempts to encrypt the communication between the participants after authenticating them. Furthermore, the direct integration of the authentication certificates in a smart phone has also been achieved [2], although the integration with the applications is not complete. The DNIe has also been integrated in a proprietary VoIP solution that collects the identity of the users and registers them in a central server [14].

III. Service Authentication

Even though eID cards can be applied to many use case scenarios such as information signature, time stamping, data integrity, and so on, the scope of this paper focuses on service authentication.

In most of the authentication scenarios the user has to connect and prove her identity to the service provider prior to the consumption of the desired service.

Traditionally the authentication with an eID card uses a challenge-response authentication scheme [3]. The user has to authenticate against the service provider who checks her identity. Each of the participants (user and provider) have a pair of keys, a private key and a public key, that is used to secure communications. The service provider generates a “challenge” (normally random data) and sends it to the user using a hash function. The user uses her private key to sign this challenge and sends it back. Finally, the provider checks whether the challenge signed by the user is correct and uses the user’s public key to validate her identity. Figure 2 represents the user’s point of view in the authentication process and Figure 3 represents the point of view of the service provider.

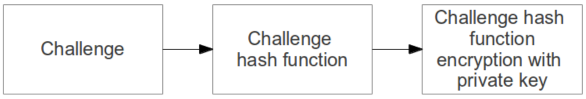

Figure 2. Authentication process from the user point of view.

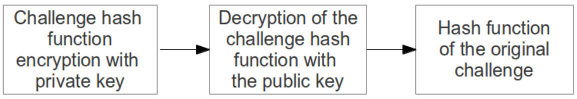
Challenge hash function encryption with private key
Decryption of the challenge hash function with the public key
Hash function of the original challenge

Figure 3. Authentication process from the service provider point of view.

Authentication with the DNIe is based on this schema. Beyond it, authentication with the DNIe includes the steps summarised in Figure 4. The user connects to the card, loads user certificates and selects authentication certificates; next, authentication with the service provider starts. The provider generates an authentication challenge that is sent to the user. The user uses her private key to sign this challenge and sends the signed challenge and her public key to the service provider. The provider checks whether the signed challenge is correct and sends the validation result to the user. If the result is successful, the user service provider can trust the user’s identity and the authentication is finally accomplished.

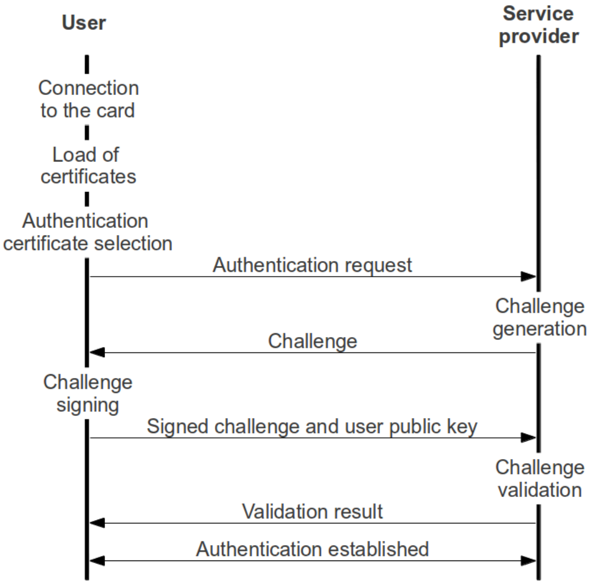

Figure 4. Process of authentication with the DNIe.

A. Connection to the card

In order to establish the connection of the DNIe, the computer, or any other device, requires the use of cryptographic modules and hardware elements.

The cryptographic modules vary depending on the operating system with which the authentication is performed. The corresponding cryptographic modules of the most popular operating systems are the following: Microsoft systems use the Cryptographic Service Provider (CSP) or PKCS#11, UNIX/Linux systems use the PKCS#11 and Mac systems use the Common Crypto or the PKCS#11. As the PKCS#11 module is available in all the main operating systems, we decided to use this option. Figure 5 represents the PKCS#11 operating scheme. This standard offers an Application Programming Interface (API) for the services that require cryptographic functionalities.

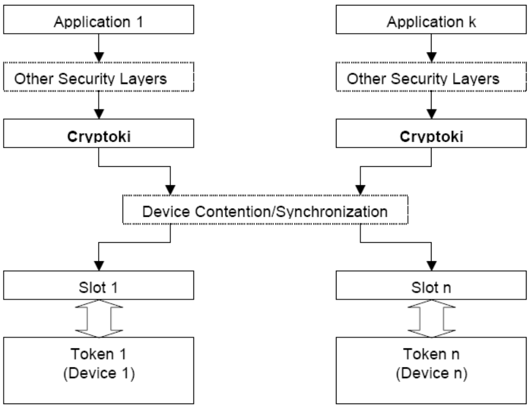

Figure 5. The PKCS#11 operating scheme.

The applications that use the eID card must be executed locally. The card is a physical resource that performs operations that must be connected to the user's equipment.

There have been some attempts to use eID cards remotely or in the cloud. Though, the user's security could be compromised, therefore, its use is not recommended [6].

In order to connect the DNIe to the user's equipment a smart card reader is required. The reader must be compatible with the following standard requirements to recognise and work with the card: it must support asynchronous cards, have a minimum communication capability of 9600 bps and support Personal Computer/Smart Card (PC/SC), CSP and PKCS#11 standards.

Furthermore, cryptographic modules and the smart card reader have to establish a mutual authentication process to create an encrypted tunnel between them. This mutual authentication is performed by using officially supported cryptographic modules.

B. Load of the user certificates

Depending on service security requirements, the certificates used during the authentication process with an eID card have different levels of acceptability: the laxest level accepts the use of any user certificate; a standard level accepts certificates issued by a Certification Authority (CA) that guarantees the user's identity; finally, the highest level accepts only certain specific certificates. The service provider defines who can access the service by using access lists. In the case of the DNIe the identity is guarantied by the police CA.

User certificates must be generated following specific security requirements [7]: the data used to generate the signature must be uniquely produces once and its secrecy has to be protected, the data used in the signature cannot be inferred from the data used in the validation, the data used to sign have to be protected from non-authorise users, and finally, the eID card must not alter the data to be signed.

In the case of the DNIe certificates are generated inside the ICC and all the cryptographic operations are also done there. This procedure ensures that the certificates cannot be extracted from the card.

It is important to highlight that the DNIe contains two different user certificates. One is used in signature operations and the other one is used in authentication operations. The certificates are separated in order to increase the security of signature operations that have implications of legal significance.

Both of them require other certificates to ensure the validity of cryptographic operations. These validation certificates include the national police certificate, CA certificates and Validation Authority (VA) certificates.

Since we want to offer authentication capabilities, we are going to use the authentication certificate. This certificate ensures that the user identity is correct when using a service. Despite the fact that this certificate does not offer non-reputation in the origin, it is successfully used to generate authentication messages and guarantee safe access to services.

This authentication certificate establishes a secure channel between the user and the service provider. It follows the X.509 v3 standard [8] and is configured for Digital Signature. It includes a pair of public and private cryptographic keys that, as aforementioned, are generated inside the ICC eID card.

This certificate can be used to authenticate against a public body or any corporate service that implements this access methodology.

C. Generation of a verification challenge

The generation of a verification challenge is performed by the service provider. The generation of the challenge can be performed in many different ways [16] [13] and is out of the scope of this paper.

The challenge is hashed and submitted to the service user for signing. When the challenge hash is returned to the service provider it is verified against the original challenge.

D. Signing of the verification challenge

The user receives the verification challenge from the service provider. Then, she signs this challenge by using the authentication certificate that was loaded as indicated in Section III.B.

The signature is performed by using the private key of the authentication certificate. Besides this signed challenge, the user must also send the public key of the authentication certificate to the service provider. This public key will be used in the next step to verify the correctness of the signature.

The signature can be requested by using one of the different available cryptographic modules. As indicated before, in our experiment we are using the PKCS#11 module.

E. Verification of the challenge signatures

After the challenge has been signed by the user, it has to be verified by the service provider. For this purpose, the service provider requires the user's certificate and the certificates of the VA.

The signature of the challenge is performed by the user's certificate. That is, it was signed with the private key that corresponds to the public key in the user's certificate. The signed challenge is also compared to the original challenge to ensure that the signed challenge is the one that had to be used. If this is correct, the user has successfully signed the challenge and the service provider just needs to make one last check to trust her identity.

Despite, the certificates themselves must also be validated. The verification process must make sure that the certificates are not out-dated, are not revoked; and that they are signed by a trustworthy CA that is in the trust validation chain.

This validation can be done offline or online. In the offline scenario, the user has a full list of the non-valid certificates and performs the checking locally. On the other hand, the validation is completed remotely by checking each certificate individually.

The online validation provides with better performance (only the required certificates are checked) and is more secure (the revocation list is always updated). Under this method, we can distinguish two different techniques.

On one hand, we have the Online Certificate Status Protocol (OCSP): is the most popular method. The client sends a certificate, or its serial number, to a receiver that will respond by indicating the state of the certificate. The certificate can have one of the following state values: good, revoked or unknown. The response is usually signed to guarantee its content [8].

On the other hand, we have the Server-based Certificate Validation Protocol (SCVP): not only does it provide with the state of a given certificate but it also provide with the optimal validation route through the CA-s trust chain [4].

As aforementioned, nowadays there are many different CAs that provide with identification certificates. As there are many CAs, users may find difficulties determining which one is the correct CA and may need to check against many CAs to verify a certificate. The VAs help simplifying this process and provide with a centralised point to query.

When a certificate validation state is requested, the VA returns three different answers: good (the certificate is correct), revoked (the certificate is revoked) or unknown (the certificate was signed by a CA that does not belong to the trust hierarchy or its state is unknown). The VA performs the required request to all the involved CA through OCSP, SCVP or other validation methods.

Nowadays, the DNIe can only be validated with the OCSP technique. VA and CA activities are performed by different entities. In this way, the CA (i.e. Home Office) can not see the users' transactions and the VA (i.e. Ministry of Public Administration or the National Coinage and Stamp Factory – Royal Mint) cannot access user identity [11]. This separation ensures that the CA does not control the user's behaviour and that the VA does not have any private information from the user when she authenticates certificates.

F. Validation result

If the results of all the previous steps are successful, the authentication will be established. At this point, the user has successfully proven her identity to the service provider and an authenticated connection is established. The user is ready to use the provider's service.

IV. VOIP SERVICE AUTHENTICATION

In order to validate this methodology, we integrate our methodology as a seamless authentication library in a Voice over IP application.

This application can make and respond calls, manage transferences and hold calls. It manages all the user requests and redirects them to a VoIP server. It also has all the standard soft-phone capabilities (e.g. contact list, tone configuration, and so forth).

Currently, this application is being used in call-centres that need to unequivocally validate the identity of the operators in each call and operation they perform.

This authentication mechanism also provides with a track of all the operations. For instance, a manager can validate which operator has done each sale call or check their performance.

V. Conclusion

We have introduced the related work in service authentication using eID cards and focused on the particularities of the DNIe. We have also proposed a service authentication methodology using the DNIe and detailing all the required steps.

We propose and implement a method that integrates the authentication capabilities of the DNIe with a VoIP service application. Future work includes the support of other eID cards and services with the aim of guaranteeing the user's authentication in as many resources and assets as possible.

Acknowledgment

We thank Irontec and Bzero for their collaboration in this project. This research was funded by the Basque Government. We also thank Izaskun Canga-Sanchez for her useful comments and corrections.

References

[1] Brainard, J.; Juels, A.; Rivest, R.; Szydlo, M. & Yung, M. (2006), Fourth-factor authentication: somebody you know, *in* 'Proceedings of the 13th ACM conference on Computer and communications security', pp. 168--178.

[2] Danny, G.; Cock, D. & Schellekens, D., 'Integrating the Belgian e-ID into Android', .

[3] Franks, J.; Hallam-Baker, P.; Hostetler, J.; Lawrence, S.; Leach, P.; Luotonen, A. & Stewart, L. (1999), 'HTTP authentication: Basic and digest access authentication', Technical report, RFC 2617, June.

[4] Freeman, T.; Malpani, A.; Cooper, D.; Polk, T. & Housley, R. (2007), 'Server-based certificate validation protocol (SCVP)', .

[5] Harrison, R. (2006), 'Lightweight directory access protocol (LDAP): Authentication methods and security mechanisms', .

[6] INTECO (2008), 'Formación DNIe', Instituto Nacional de TeconologÃ as de la ComunicaciÃ³n.

[7] Jefatura del Estado (2003), 'Ley 59/2003, de 19 de diciembre, de firma electrónica.'.

[8] Myers, M.; Ankney, R.; Malpani, A.; Galperin, S. & Adams, C. (1999), 'X. 509 Internet public key infrastructure online certificate status protocol-OCSP', Technical report, RFC 2560.

[9] Plies, A.; Massoth, M. & Marx, R. (2010), Approach to Identity Card-based Voice-over-IP Authentication, *in* 'Advances in Multimedia (MMEDIA), 2010 Second International Conferences on', pp. 61--66.

[10] Prabhakar, S.; Pankanti, S. & Jain, A. (2003), 'Biometric recognition: Security and privacy concerns', *Security & Privacy, IEEE* **1**(2), 33--42.

[11] Real Casa de la Moneda. Fábrica Nacional de Moneda y Timbre (2012), 'Fábrica Nacional de Moneda y Timbre'.

[12] RSA Laboratories, 'PKCS #15: Cryptographic Token Information Format Standard'.

[13] Schnorr, C. (1991), 'Efficient signature generation by smart cards', *Journal of cryptology* **4**(3), 161--174.

[14] SecVoID, 'Authentication of telephone calls. Voice calls authentication and encryption with electronic ID'.

[15] Stevens, T.; Elliott, J.; Hoikkanen, A.; Maghiros, I. & Lusoli, W. (2010), 'The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies', .

[16] Suh, G. & Devadas, S. (2007), Physical unclonable functions for device authentication and secret key generation, *in* 'Proceedings of the 44th annual Design Automation Conference', pp. 9--14.