Privacy preserving electronic petitions

Claudia Diaz[1], Eleni Kosta[2], Hannelore Dekeyser[2], Markulf Kohlweiss[1], and Girma Nigusse[3]

[1] K.U.Leuven ESAT/COSIC, Belgium
{Claudia.Diaz, Markulf.Kohlweiss}@esat.kuleuven.be
[2] K.U.Leuven ICRI, Belgium
{Eleni.Kosta, Hannelore.Dekeyser}@law.kuleuven.be
[3] K.U.Leuven CS/DistriNet, Belgium
Girma.Nigusse@cs.kuleuven.be

Received: 30 June 2008, Accepted: 25 February 2009

Abstract. We present the design of a secure and privacy preserving e-petition system that we have implemented as a proof-of-concept demonstrator. We use the Belgian e-ID card as source of authentication, and then proceed to issue an anonymous credential that is used to sign petitions. Our system ensures that duplicate signatures are detectable, while preserving the anonymity of petition signers. We analyze the privacy and security requirements of our application, present an overview of its architecture, and discuss the applicability of data protection legislation to our system.

Keywords: security, privacy, electronic petitions, anonymous credentials, electronic ID

1 Introduction

A petition is a formal request addressed to an authority and signed by numerous individuals. Through petitions, citizens are able to express their support or dissatisfaction with government initiatives, and provide feedback to government institutions. In the physical world, petition signers typically provide a unique identifier (such as the national ID number) together with their handwritten signature, so that fake or duplicate signatures can be eliminated. Given the high cost of collecting and verifying petition signatures by hand, it is not surprising that petitions are increasingly available online. E-petitions present substantial advantages with respect to physical world petitions: it is much easier to reach a large number of people potentially interested on signing them, and the signature verification process can be automated. But they also introduce new security and privacy challenges.

Many of the currently available electronic petitions simply collect the name and national ID number of signers. Given that this information is not secret, it is impossible to check that the petition signer is really providing her own data. In other words, it is not possible to detect cheating, which diminishes the trustworthiness of the petition signature list. To prevent this, some e-petition

servers check the IP address of the signer and allow only one signature per IP address. But this disenfranchises legitimate signers who share the IP address with other people (note that in some organizations thousands of users share the same IP address). To ensure that an electronic petition signature is unique and legitimate, it is necessary to use cryptographic means such as digital signatures. Assuming that citizens possess electronic e-ID cards (as is the case in Belgium), an obvious way to implement e-petitions is to have citizens sign them using the key pair available on their e-ID card. However, such a solution is problematic from a privacy point of view. The e-ID public key certificate (needed to verify the digital signature) contains a lot of information about the holder of the card, such as her name, National Registry Number, and date of birth. Revealing all this information for the purposes of signing a petition would definitely be against the data minimization principle, which is the legal philosophy underpinning data protection regulation. Data minimization constitutes that minimal amounts of personal data may be processed, but only in as far as strictly necessary for legitimate purposes. In other words, processing of data must be adequate, relevant and not excessive in relation to the purposes of collection and processing.

Additional data protection issues arise when the petitions allow sensitive information to be derived about the user, the processing of which is in general prohibited by data protection legislation. As discussed in Sect. 7, such information can relate—among other categories of data—to political opinions, religious or philosophical beliefs, all of which are considered as "sensitive personal data" in the European Directive of Data Protection [EC, 1995].

While signer identification is required in the physical world to ensure the uniqueness and validity of signatures, it is possible to reconcile functional, security and privacy requirements in its electronic version using cryptographic techniques. We propose using the existing PKI-based electronic IDs cards [Cock] in combination with anonymous credential protocols to ensure that (*i*) signatures are legitimate, (*ii*) each citizen can sign a petition at most once, and (*iii*) petition signers are anonymous. Sect. 2 describes in detail the privacy and security requirements that we have identified for this application.

Our e-petition design and implementation uses the Belgian e-ID for initial authentication, and then allows the user to obtain an anonymous credential [Chaum, 1985, Camenisch and Lysyanskaya, 2001, Camenisch et al., 2006] that is used to electronically sign petitions on a server. An introduction to anonymous credentials is presented in Sect. 3. By using anonymous credentials, our demonstrator reconciles two seemingly contradictory requirements: it allows anonymous petition signing, while it imposes restrictions on who is entitled to sign and ensures that each citizen can only sign a particular petition once. Multiple signing of a petition with the same anonymous credential is detectable by our protocols, such that repeated signatures can be eliminated.

Our system architecture comprises two servers and a client run by the citizen. We assume that the client routes its communication through an underlying anonymous communication infrastructure (e.g., readily available networks such as Tor [Dingledine et al., 2004] or JAP [JAP Anonymity & Privacy]), to prevent

identification through IP addresses. In this paper we assume that the servers are run by the government, although in a real deployment they may as well be administrated by other entities. The first e-government server is a *credential issuer*, whose role is to issue anonymous credentials to citizens who have authenticated with the Belgian e-ID card. The second is the *e-petition web server*, which maintains the petition pages and processes the petition signatures. The citizens use the anonymous credential obtained from the credential issuer to interact with the e-petition server. The details of our system architecture and protocols can be found in Sect. 4, while Sect. 5 presents the security analysis of the system, and Sect. 6 provides details on the implementation, including performance measurements.

From a legal point of view, very little regulation exists specifically tailored to e-petitions. The lack of specific rules does not mean e-petitions operate in a legal void, as a number of regulations of a general nature are applicable. In this paper, we focus on the data protection issues related to the proposed e-petition application. Our design for the e-petition server aims at a notable advance in protecting user privacy, by shielding off any and all identifiable information about the users through the use of anonymous credentials and anonymous communications channels. The applicability of data protection regulation to our design is discussed in Sect. 7.

2 Requirements

We assume that the Belgian e-ID registration and issuance process works properly, and that each e-ID corresponds to a person. We also assume that private key material is kept securely, and only available to the entity to which it belongs. This requirement includes private key material held by the user that is not protected by the tamper resistance of the e-ID. If a user is willing to sell this material, he is able to sell his right to vote while still remaining in possession of the e-ID. Removing this requirement is part of ongoing future work. The credential issuer is trusted to function correctly and issue (only) one credential to each valid e-ID. Finally, we assume the user has installed an anonymous communication client[1] and routes its browser requests through it.

Building on these basic trust and operational assumptions, we have identified a number of requirements that our design should comply with to provide its functionality in a secure and privacy-preserving manner.

Strong authentication: The e-government servers have to authenticate themselves towards the user to prevent malicious servers from impersonating legitimate ones. In order to prevent that a citizen obtains multiple credentials, and to ensure that the request is coming from a legitimate user, the application requires strong authentication.

[1] Anonymous communication clients are freely available online, also as extensions that incorporate anonymous browsing to standard web browsers (e.g., FireFox).

Authorization: Only citizens eligible to sign a petition should be able to do so. For example, in some cases petitions may only be signed by citizens of legal age, or by those residing in a certain country or locality.

Data integrity: No entity should be able to modify the data exchanged between the citizen and the e-government servers.

Confidentiality: All the data exchanges between a citizen and the e-government servers must be kept confidential from other entities. Additionally, traffic analysis protection is required so that external observers are not able to determine that a citizen is accessing the e-petition server (or a particular petition in the server).

Signer anonymity: The e-petition server (even in collusion with the credential issuer) must not be able to identify the citizens who have signed the petitions.

Multiple signing prevention: An e-petition application has to be designed in a way it can properly detect and rectify citizen attempts to sign a single e-petition multiple times.

Public verifiability: Finally, an important requirement for the transparency of the e-petition signing is to provide evidence of fair counting of petition signatures.

3 Anonymous credentials

Anonymous credential protocols are an active area of research in cryptography. They were first proposed by David Chaum [Chaum, 1985] as a privacy friendly alternative to public key certificates. Today's anonymous credential protocols [Camenisch and Lysyanskaya, 2001] rely on zero-knowledge proofs [Goldwasser et al., 1985] to reduce to the minimum the amount of information disclosed about their owners. The many options and features introduced in the literature [Camenisch and Lysyanskaya, 2001, 2002, Camenisch et al., 2006] allow users to protect their privacy while at the same time providing the necessary information and security features for building secure applications.

For example, using anonymous credentials a credential issuer can encode a user's age in the credential. Using the credential prove/show protocol together with zero-knowledge range proofs [Boudot, 2000a] it is possible for the user to convince a verifier that her age is above/below some threshold. The verifier does not learn the user's exact age, but it can check that her minimum/maximum age is certified by the credential issuer.

A concern that is often raised about anonymous credentials is that the lack of identification leads to a loss of accountability. Not every application, however, needs the same kind of accountability. For many applications, including e-petitions, it is sufficient to guarantee that every user can use her credential at most once in a given context (e.g., a concrete petition). Credentials that implement this functionality generate a pseudo random serial number as a result of the protocol. If the credential is used only once per context, credential shows in different contexts are unlinkable. Reuse of the credential in the same context, however, results in the same pseudo random serial number, meaning that the double use of the credential is detectable.

Various cryptographic tricks can be used to create credentials that support unlinkable and unique serial numbers. Such credentials can be realized based on the so-called epoch number of direct anonymous attestation [Brickell et al., 2004]. By binding a different tag to every context in which a credential is shown, k-times anonymous authentication [Teranishi et al., 2004] can be used to create unique serial numbers. The schemes in [Damgård et al., 2006] and [Camenisch et al., 2006] even support the identification of the owner of a credential that was shown twice with the same serial number. As [Martucci et al., 2008], our scheme uses the cryptographic techniques of [Camenisch et al., 2006] (i.e., e-tokens). We use a variant of these protocols where the identification feature is disabled, implying that in our design the credential shows cannot be deanonymized.

Assertion-based signatures. We introduce—based on prior work in cryptographic protocols—the concept of *assertion-based signatures* (also known in the literature as "signatures of knowledge" [Chase and Lysyanskaya, 2006]) as a mechanism for enhancing the privacy of petition signers. Assertion-based signatures are signatures associated with an assertion that—if properly defined for the transaction in place—should give the verifier all the information needed for assessing whether or not a signer can be trusted for the purposes of the signature. Our approach is in line with many privacy enhancing primitives.

The assertion contains statements about attributes (of the signer) that have been certified by an issuing organization (as part of a credential). Contrary to third-party-issued assertions (that have a lot in common with traditional PKI-based attribute certificates), the signer can create and prove the assertion in her signature using only secret key material that is in her possession. The signature generation takes as additional input the certified attributes, as being available to the signer in the form of credentials issued by the organization.

The issuing of credentials is a more complex process than the issuance of conventional PKI certificates. Although a lot of important work exists on anonymous credential systems, in this work we focus on using credentials for the purpose of signing documents (in our case, these documents are the petitions). We combine credentials with e-tokens to detect double signing.

Further details on assertion-based signatures can be found in [Camenisch et al., 2007], that describes an XML syntax for assertion-based signatures, and discusses the relation of assertion-based signatures to other cryptographic primitives. For the purpose of this paper it is sufficient to note that assertion-based signatures for various assertion types can be obtained by applying the Fiat-Shamir heuristic [Fiat and Shamir, 1987] to various privacy enhanced authentication systems, such as existing anonymous credentials systems, group signatures, and the e-token scheme used by us.[2] Extending the assertion types supported by the assertion-based signature naturally extends the capabilities of the e-petition system for example to support privacy preserving proofs of age and region codes.

[2] Similarly, an assertion-based signature scheme for general assertions generalizes group-signatures, e-tokens signatures, e-cash, non-interactive anonymous credentials, as well as other privacy enhancing protocols.

4 Privacy-preserving e-petition design

We have implemented a demonstrator that provides the basic cryptographic functionalities for e-petition signing and makes them accessible through a web-based user interface. Our demonstrator uses the 'identity mixer' software as the underlying anonymous credential system.[3] The demonstrator extends 'identity mixer' and implements a privacy preserving protocol between a client and two web server applications: the issuer of the anonymous credential and the e-petition server. It also implements an interface to use the Belgian e-ID card for authentication towards the credential issuer. Both 'identity mixer' and our demonstrator are programmed in Java. We first present the architecture of our e-petition system and then give some detail about the cryptographic functions used.

4.1 Implementation architecture

The demonstrator comprises the issuer of anonymous credentials, an e-petition web server, and a client, as shown in Fig. 1. The user accesses the credential issuer web site to obtain an anonymous credential. First, the user authenticates herself towards the credential issuer using her e-ID card. For this, we use the existing 2-factor authentication provided by the Belgian e-ID card. Users authenticate towards the credential issuer with their e-ID card as follows. They insert the card in a card reader and introduce their PIN number to generate a signature on a challenge generated by the credential issuer (steps 1 and 2 of the protocol). In this way the user proves the possession of the e-ID card and the knowledge of the corresponding PIN number. The credential issuer uses the citizen's e-ID certificate to verify the digital signature on the challenge, and extracts some attributes such as the age of the subject, which are encoded in the anonymous credential as certified attributes. Finally, the user and credential issuer jointly generate the anonymous credential (step 3), which is locally stored by the user (step 4).

In our demonstrator, the *petition signing* and *petition signature publication* processes are managed by the e-petition server, and the user is able to (unlinkably) sign as many distinct petitions as desired with the same credential. First, the user selects the petition that she wants to sign, and obtains its corresponding *petitionID*, which is an input to the protocol. Then, she must prove the possession of a credential certified by the credential issuer. For this, the user reads the credential she has stored (step 5), and runs the credential show protocol (step 6) to create an assertion-based signature. Some of our demonstrator petitions require the user to prove not only the possession of a valid anonymous credential, but also that her certified attributes fulfill specific conditions (additional assertions). For instance, one of the implemented petitions is not meant for minors. If a user wants to sign that petition, she needs to prove that her credential encodes an age that is at least 18 years old. The e-petition server verifies whether

[3] `http://www.zurich.ibm.com/security/idemix/`

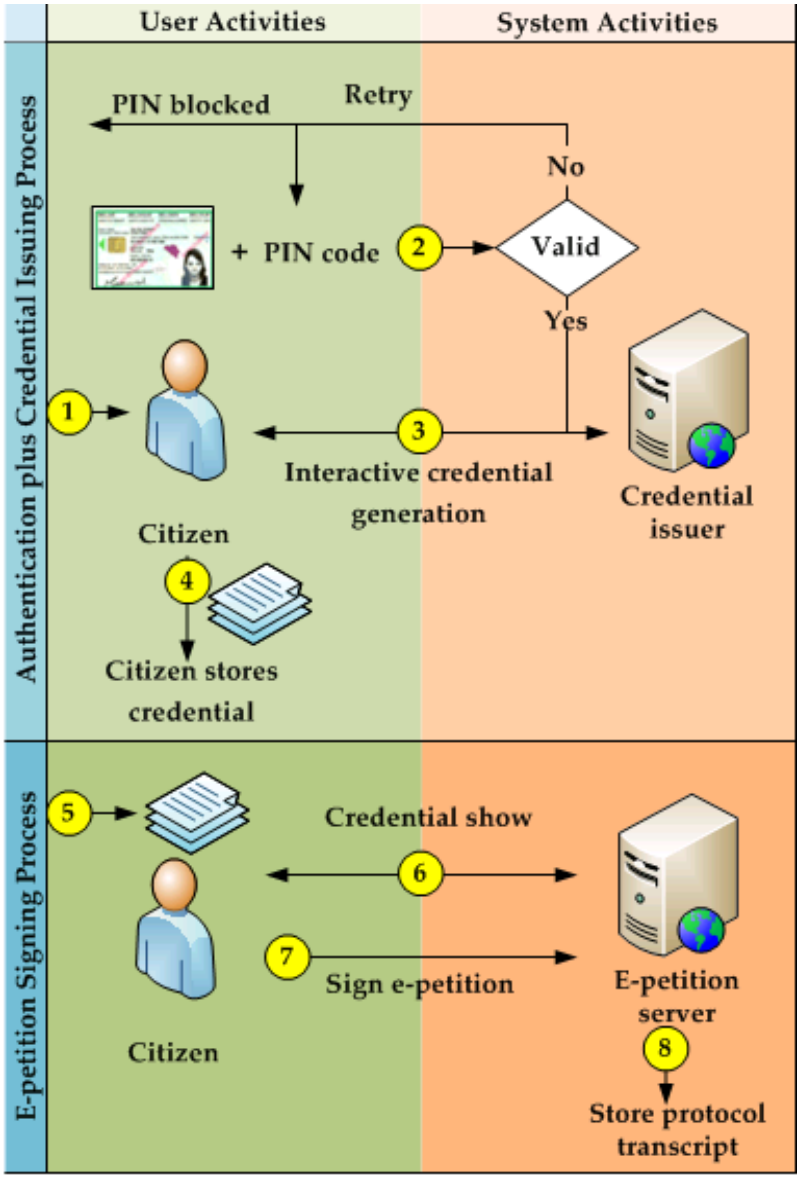

Fig. 1. E-petition system architecture and protocols

the user has already signed the selected petition previously, by comparing the generated pseudo random number to that of previous signatures on that petition. If the verification reveals that the user already signed the selected petition, it automatically rejects the double signing attempt without revealing her real identity. Otherwise the petition signature is accepted as valid (step 7). Finally, the e-petition server publishes the protocol transcripts of every successful petition signature (step 8), so that anyone can verify that their signature has been counted, and additionally check that all transcripts correspond to signatures made by users who possess valid credentials.

4.2 Credential protocols and e-token based signatures

Our anonymous credential protocols use cryptographic constructions with special properties: (*i*) the user is able to prove to a verifier possession of a credential certified by the credential issuer; (*ii*) the user is able to prove conditions on the attributes encoded in the credential (certified by the issuer) without revealing the attributes themselves [Boudot, 2000b]; and (*iii*) the issuer and the verifier (e-petition server), even in collusion, cannot identify which credential issuing corresponds to which credential show, nor can the verifier link credential shows as being related to the same credential, unless the citizen does multiple signing of the same petition [Camenisch et al., 2006].

We use a special assertion-based signature scheme for signing petitions: Camenisch *et al.* have proposed a protocol for periodically spendable e-tokens [Camenisch et al., 2006]. In their application scenario, sensors spend an e-token whenever they report some data. Yet, it is only possible to compute n different e-tokens per time period—from the key material contained in the e-token dispenser. Consequently, sensors can file at most n reports per time period anonymously. Otherwise the sensors have to spend some e-token twice, which allows everyone to compute the sensor's identity from these two e-token show transcripts. The e-token dispenser and the e-token can be seen as a credential and a credential show respectively.

While n-spendable e-tokens provide the necessary main functionality for our proposal, as in [Martucci et al., 2008] we adapt the e-tokens protocol to our application's requirements: (*i*) We transform the e-token authentication scheme into an assertion-based signature by applying the Fiat-Shamir heuristic [Fiat and Shamir, 1987], a cryptographic trick that turns certain interactive proof protocols into signature schemes. (*ii*) Instead of a time period t, we use an e-petition identifier $petitionID$. The value $petitionID$ can be seen as identifying the context in which a signer is allowed to sign only once.[4] (*iii*) We use a version optimized for $n = 1$ and require only detection of double signing (instead of deanonymization of the signer). This eliminates the need for two expensive zero-knowledge proofs: a) a proof that an integer J lies in an interval $[1, n]$, and b) that the double spending tag E was correctly formed.

[4] Contrary to e-cash, which can be used only once, an e-petition credential can be used for signing arbitrary many different petitions.

An e-token based signature scheme as defined in [Martucci et al., 2008] consists of the algorithms *IKg*, *UKg*, *Obtain*, *Issue*, *Sign*, *Verify*. These algorithms are executed by the issuer $\mathcal{I}$ of the e-token dispenser, the user $\mathcal{U}$, and the signature verifier (the e-petition server). *IKg* and *UKg* are executed by the issuer and the user upon initialization of the issuing server and the client respectively. The secret keys need to be secured to assure that e-petitions cannot be forged. *Obtain* and *Issue* are executed in step 3 to obtain the dispenser credential. *Sign* and *Verify* are used in step 6 to sign and verify an e-petition.

- $IKg(1^k)$ and $UKg(1^k, pk_{\mathcal{I}})$ – creates the issuer's key pair $(pk_{\mathcal{I}}, sk_{\mathcal{I}})$ and the user's key pair $(pk_{\mathcal{U}}, sk_{\mathcal{U}})$ respectively. The value k is the security parameter. Let the user's key pair be $(pk_{\mathcal{U}}, sk_{\mathcal{U}})$, where $pk_{\mathcal{U}} = g^{sk_{\mathcal{U}}}$ and g generates a group $\mathbb{G}$ of known order. The issuer's key pair is used for creating and verifying credentials. We use a PRF f_s whose range is the group $\mathbb{G}$.
- $Obtain(pk_{\mathcal{I}}, sk_{\mathcal{U}}) \leftrightarrow Issue(pk_{\mathcal{U}}, sk_{\mathcal{I}})$ – at the end of this protocol between a user and the e-token issuer, the user obtains an e-token dispenser D that can be used to create one e-token based signature per $petitionID$. The dispenser D is comprised of seed s for the PRF f_s, the user's secret key sk_U, and the issuer's credential on $(s, sk_{\mathcal{U}})$. Credentials are issued in a way such that the issuer is prevented from learning anything about s or $sk_{\mathcal{U}}$. I stores $pk_{\mathcal{U}}$ to make sure that users obtain only one credential.
- $Sign(m, D, pk_{\mathcal{I}}, petitionID)$ – shows an e-token from dispenser D in context $petitionID$ to sign a message m. The outputs are a token serial number $S = f_s(petitionID)$, a transcript τ. S, and using the Fiat-Shamir heuristic [Fiat and Shamir, 1987] creates a non-interactive ZK proof τ that S correspond to a valid dispenser for context $petitionID$ (i. e., the user proves in zero-knowledge that S was properly formed from values $(s, sk_{\mathcal{U}})$ signed by the issuer). To sign message m, m is hashed into the challenge together with the first message and the public parameters of the proof.
- $Verify(m, S, \tau, pk_{\mathcal{I}}, petitionID)$ – verifies the zero-knowledge proof τ to check that S was created by a valid dispenser D to sign a message m in context $petitionID$.

Attributes such as a user's age or region code can be added into the system in two ways: either by adding the attributes to the credential in the dispenser D or by showing a separate credential *cred* with D together with a proof that D and *cred* belong to the same user. For simplicity and efficiency our demonstrator followed the first approach for encoding the user's age.

A remark on cryptography. The above mechanisms employ well known techniques from the area of privacy enhancing cryptography. To some extent our choice for the e-token protocol is arbitrary, as other mechanisms for providing similar functionality are known, e.g. direct anonymous attestation [Brickell et al., 2004] and k-times anonymous authentication [Teranishi et al., 2004]. The e-token system is however arguable the most general such system. A credential system that supports e-tokens could for example be used to implement electronic cash

(including compact e-cash [Camenisch et al., 2005]) and electronic petitions using the same building block for limiting the number of credential shows. While other techniques may be slightly more efficient, our implementation efforts have shown that on modern computers the impact on performance is small.

5 Security Analysis

Strong authentication: In our design, the initial authentication of the citizen is achieved through the Belgian e-ID card, which provides 2-factor strong authentication (physical possession of the card and knowledge of its PIN code). The e-government servers also authenticate themselves towards the user to prevent malicious servers from impersonating legitimate ones. As legitimate users show their credentials only towards legitimate servers, strong authentication prevents man-in-the-middle attacks in the natural way. The authentication of the e-government servers is provided through digital signatures and relies on the security of private keys.

Authorization: Our system relies on the Belgian e-ID card as authentic source of user attributes. Petition signers are required to prove that they fulfill the authorization criteria while executing the protocols. The unforgeability of the anonymous credentials prohibits collusions by multiple users that want to combine their attributes.

Data integrity: Our protocols include integrity protection mechanisms that prevent unauthorized modifications of data.

Confidentiality: All the data exchanges between a citizen and the e-government is send through secure (encrypted) communication channels. Anonymous communication channels such as those provided by Tor [Dingledine et al., 2004] or JAP [JAP Anonymity & Privacy] should be used as underlying communication infrastructure to guarantee traffic analysis protection.

Signer anonymity: At the data level, signer anonymity is achieved by the zero-knowledge properties of the anonymous credential protocols. To prevent citizen identification using the IP address, the citizen communicates to the servers through an anonymous communication infrastructure (e.g., Tor [Dingledine et al., 2004]).

Multiple signing prevention: Our protocols provide mechanisms to detect and remove signature duplicates, without compromising signer anonymity.

Public verifiability: In our design, the e-petition server publishes the protocol transcripts of every signature. This information can be used by a citizen to verify that: (*i*) her own signature has been counted; (*ii*) all the transcripts belong to signatures made by citizens who possess valid credentials; and (*iii*) there are no duplicate signatures.

6 Implementation

Our e-petition demonstrator is a Web application coded in Java. It makes use of the idemix code for anonymous credentials and the Belgian eID card middleware software. However, it extends the idemix to accommodate our restricted attribute extraction and verification needs. The middleware facilitates the 2-factor authentication of users towards the e-petition Web server and retrieval of user specific credential attributes.

The demonstrator consists of two simple Web interfaces for issuing anonymous credential and signing e-petitions. Using the issuing server Web site, users can request and save anonymous e-petition credentials into secondary memories. Once they get their credentials, they can consult the e-petition signing server Web site. The signing Web site, let users to select e-petition, explains the objectives of the e-petition, enumerate the requirements of the selected e-petition, and signing of that e-petition. Moreover, the signing Web site publishes the e-petition results and allows users to verify the counting of their signatures.

Table 1 presents sample protocol related performance measures. Since the performance measure given below is an average of ten randomly selected protocol executions, it can give an overview of the overall efficiency estimate of our demonstrator. The performance measures are tested on Intel(R) Core(TM)2 Duo CPU with 2.00 GHz.

Issuing Protocol		Spend proofs	384 ms
Withdraw	1554 ms	Spend certificate	240 ms
Signing Protocol		*Server side*	
Signer side		Verify range proofs	276 ms
Range commitments	166 ms	Verify spend proofs	407 ms
Spend commitments	169 ms	Verify spend certificate	166 ms
Range proofs	245 ms	Earn	850 ms

Table 1. Performance measures, in milliseconds

7 Data protection implications of e-petition

The privacy preserving e-petition system aims at shielding off any identifiable information about the users through the use of anonymous credentials and anonymous communications channels. This is an extremely important element in comparison with the traditional e-petition systems, where no anonymity is ensured. In those systems the user reveals a lot of information, like her name or identification number, which is not really necessary for the needs of the e-petition system. Such systems contradict the data minimization and the proportionality principles, which require that only the absolutely necessary and relevant data shall undergo processing. At this point it is important to be reminded that the

system is designed to run on an anonymous communications layer, which will be taken as a *de facto* requirement in the analysis that follows.

First and foremost it needs to be examined whether the e-petition system entails the processing of personal data and consequently whether the legal framework on data protection—to be precise the Belgian Privacy Act of 1992 [BDP, 1993] and the EU Data Protection Directive of 1995 [EC, 1995]—will apply. According to Art. 2(a) EU Data Protection Directive "personal data" shall mean any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[5] Besides the concept of personal data, the Data Protection Directive provides in Art. 8 (1) for the prohibition of the processing of special categories of data, commonly known as "sensitive data". Such data are the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life. The processing of the aforementioned data, which can be revealed in various petitions, is only allowed on grounds explicitly mentioned in Art. 8 (2)-(7) of the directive.[6]

Before proceeding with our analysis, we need to make a differentiation between the communication among (*i*) the user and the credential issuer on the one hand and (*ii*) the user and the e-petition web server on the other.

In order to obtain the anonymous credential, the user communicates with the credential issuer by using her Belgian ID card. Indisputably, the Belgian e-ID card is a rich source of personal data, as it contains not only the full name of the holder and her nationality, but also the National Registry Number, date and place of birth, noble condition, etc. (see [Cock]).[7] In the current design of the system, the user is fully identifiable by the credential issuer, who in this case is processing personal data of the user in order to ensure authentication and authorization and to issue the anonymous credential that will be used for the e-petition signing. The credential issuer is thus rendered controller of the data; i.e., the one that determines the purposes and the means of the processing of personal data,[8] and has to fulfil the obligations that the data protection legislation foresees for the data controller.

Significant from a legal viewpoint is that our credential issuer does not simply generate a credential file which it then sends to the user. If that were the case, the credential issuer would be able to identify the owner of a given credential. The user and the credential issuer send each other specified data messages from which the user is able to generate a valid and verifiable credential. As such, the credential issuer never sees the resulting credential.

---

[5] Compare with Art. 1 §1 of the Belgian Privacy Act.

[6] Compare Art. 6-8 of the Belgian Privacy Act.

[7] For an overview of the privacy issues concerning the Belgian e-ID card see [Alsenoy and Cock, 2008].

[8] Art. 2 (d) EU Data Protection Directive,compare with Art. 1 §4 of the Belgian Privacy Act.

The communication between the user and the e-petition web server is more complicated when examined from a data protection point of view. A difficult concept that needs to be explained is that a credential can be used without handing it over, like you would hand over a token in the physical world. One way to explain it is that the credential holder is quizzed by the petition server and that only the holder of a genuine credential is able to give the correct answers. As already mentioned, the data protection legislation only applies when the processing of personal data takes place. When the data are anonymous and can not be related to a natural person, their processing does not fall under the provisions of the data protection legal framework. In our e-petition system, it shall be examined whether the data that relate to the anonymous credential are anonymous or whether the user is just pseudonymous towards the e-petition web server and thus the latter processes personal data.

In defining whether the data in the e-petition system are anonymous or simply pseudonymous, Recital 26 of the Data Protection Directive needs to be mentioned. This article stipulates that in deciding whether data could be used to identify a particular person "account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person". Clearly, if the controller is in possession of both the pseudonymized data and the key with which to deanonymize them, the data are identifiable and data protection provisions apply.

The notion of identifiability differs between the European Member States. The German legislation, for instance, has adopted a more pragmatic approach to the notion of identifiability. The German Federal Data Protection Law [BDS, 1990] in Art. 3(6) defines the notion of "anonymization" as follows: "'Rendering anonymous" means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual".[9] The definition of anonymisation allows the deduction of the following *argumentum a contrario*: personal data are information that can be attributed to an identified or identifiable individual without a disproportionate amount of time, expense and labour. The data protection laws of France, Belgium and Sweden, on the other hand, have adopted a broad interpretation of the concept of personal data, rendering any information as personal data, if an individual can be identified, regardless of the technical or legal difficulties in determining the identity of the individual. Thus according to the Belgian legal interpretation of the term personal data and as long as the deanonymization key is out there somewhere, the data are identifiable, no matter how unlikely it is that the controller and the key holder would cooperate.

As supported by the legal scholars "pseudonymous data are still subject to data protection law, since they could be tied to the individual" [Kuner, 2007]. The Article 29 Working Party has adopted a similar position, stating that "[r]etraceably pseudonymized data may be considered as information on individuals which are indirectly identifiable" [Party, 2007]. It is interesting how-

[9] Unofficial translation available at `http://www.bfdi.bund.de`

ever, to mention that the Article 29 Working Party in the same opinion, stated, with regard to key-coded data in statistical and pharmaceutical research, that if all technical measures (e.g., cryptographic, irreversible hashing) have been taken to assure that the identification of the data subject is not expected or supposed to take place under any circumstance, the Data Protection Directive is not applicable. Even more difficult is the situation where seemingly anonymous data becomes identifiable through statistical analysis or cross-referencing.

The Belgian e-ID is by purpose and design a rich source of personal data. Whilst well suited for conventional identity checks (e.g., by the police or government officials), this becomes a disadvantage in any situation that requires both strong authentication and anonymity or at least increased privacy. The data protection legislation in Belgium is based on a very broad concept of identifiable data, encompassing even data that can not be deanonymized without considerable effort or without colluding with others.

However, reverse identifiability is not possible in our e-petition system. Although the Credential Issuer knows the identity of the user that asks for a credential, it does not know which specific credential has been assigned to her. The Credential Issuer just knows that a specific user was given "a" credential with certain attributes encoded. For instance, let us assume the age is the only attribute encoded in the credential and that the proof of knowledge is proving that the age of the credential holder is at least 18 years old (age ≥ 18). When the Credential Issuer issues 10 credentials, 8 of which were given to people with age ≥ 18, he will only be able to verify that the credential holder is actually older than 18 but in no case will he be able to tell which of the 8 possible users she is. Thus, the privacy preserving e-petition system does not allow any kind of reverse identifiability and does not provide any mechanisms for deanonymization.

The proof of knowledge generates a number, deterministically from other parameters such as petition ID. When a user signs the e-petition multiple times, the number will appear several times, meaning that the e-petition web server will be able to tell that two signatures were created by use of the same credential, so that duplicates are removed. However, neither the e-petition web server, nor the certificate issuer, as already discussed above, will be able to define which specific user had this credential and produced these signatures. It shall be noted at this point that even signatures of the same user on different e-petitions are unlinkable. As already mentioned above, Belgium has adopted a broad interpretation of the concept of personal data, rendering any information as personal data, if an individual can be identified, regardless of the technical or legal difficulties in determining the identity of the individual. Even under this broad interpretation, there is no possibility in our system to trace back the identity of the credential holder. Neither the e-petition web server, nor the certificate issuer are able to get back to the identity of the credential holder. Therefore the data that are processed by the e-petition web server are anonymous and the data protection legislation will not apply.

8 Conclusions

We have presented our design of a privacy preserving electronic petition application, which we have implemented as proof-of-concept demonstrator. Our design shows that anonymous credential protocols can be used to extend existing PKI-based national e-ID infrastructures, to achieve a degree of security and privacy protection that PKI alone cannot provide.

Instead of directly signing petitions with the existing Belgian e-ID card, we use it to provide initial strong authentication, and ensure that each user obtains at most one anonymous credential. The use of the anonymous credential in the e-petition signing process ensures maximum privacy protection through data minimization. Our protocol detects multiple signing and thus prevents malicious behavior with no need for identification. We have introduced anonymous credentials, studied the privacy and security requirements of the e-petition application, presented an overview of our design's architecture and protocols, and discussed the applicability of data protection legislation.

Several open issues remain. We have not discussed mechanisms for credential revocation, secure storage of credentials, or practical deployment issues. While the implementation of a system that provides all these functionalities may not be trivial, these are engineering issues that can be overcome.

Bibliography

German federal data protection act of 20 december 1990. Bundesgesetzblatt I S. 2954, December 1990.

Belgian data protection act of 8 december 1992. Moniteur Belge, March 1993.

Brendan Van Alsenoy and Danny De Cock. Due processing of personal data. a case study of the belgian electronic identity card. *Datenschutz und Datensicherheit*, (3), 2008.

F. Boudot. Efficient proofs that a committed number lies in an interval. In *Advances in Cryptology – EUROCRYPT '00*, volume 1807 of LNCS, pages 431–444, 2000a.

Fabrice Boudot. Efficient proofs that a committed number lies in an interval. In Bart Preneel, editor, *EUROCRYPT*, volume 1807 of *Lecture Notes in Computer Science*, pages 431–444. Springer, 2000b. ISBN 3-540-67517-5.

Ernie Brickell, Jan Camenisch, and Liqun Chen. Direct anonymous attestation. In *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, pages 132–145, New York, NY, USA, 2004. ACM Press. ISBN 1-58113-961-6. doi: http://doi.acm.org/10.1145/1030083.1030103.

Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Advances in Cryptology - EUROCRYPT 2001*, volume LNCS 2045, pages 93–118. Springer, 2001.

Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In Moti Yung, editor, *CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 61–76. Springer Verlag, 2002.

Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Compact e-cash. In *EUROCRYPT*, pages 302–321, 2005.

Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, and Mira Meyerovich. How to win the clonewars: efficient periodic n-times anonymous authentication. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM Conference on Computer and Communications Security*, pages 201–210. ACM, 2006.

Jan Camenisch, Markulf Kohlweiss, Bart Preneel, and Dieter Sommer. Assertion-based signatures for xml signatures. Cosic internal report, 2007.

Melissa Chase and Anna Lysyanskaya. On signatures of knowledge. In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 78–96, 2006.

David Chaum. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985. URL `citeseer.nj.nec.com/chaum85security.html`.

Danny De Cock. Non-official information on the Belgian Electronic Personal Identification Card. `https://www.cosic.esat.kuleuven.be/belpic/`.

Ivan Damgård, Kasper Dupont, and Michael Østergaard Pedersen. Unclonable group identification. In *EUROCRYPT*, pages 555–572, 2006.

Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, 2004.

EC. 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 (eu data protection directive). Official Journal of the European Union, November 1995.

Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer Verlag, 1987.

Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems (extended abstract). In *STOC*, pages 291–304. ACM, 1985.

JAP Anonymity & Privacy. `http://anon.inf.tu-dresden.de/`.

Christopher Kuner. *European Data Protection Law - Corporate Compliance and Regulation*. Oxford University Press, 2007.

Leonardo A. Martucci, Markulf Kohlweiss, Christer Andersson, and Andriy Panchenko. Self-certified sybil-free pseudonyms. In Virgil D. Gligor, Jean-Pierre Hubaux, and Radha Poovendran, editors, *WISEC*, pages 154–159. ACM, 2008. ISBN 978-1-59593-814-5.

Article 29 Data Protection Working Party. Opinion 4/2007 on the concept of personal data, June 2007.

Isamu Teranishi, Jun Furukawa, and Kazue Sako. k-times anonymous authentication (extended abstract). In Pil Joong Lee, editor, *ASIACRYPT*, volume 3329 of *Lecture Notes in Computer Science*, pages 308–322. Springer, 2004. ISBN 3-540-23975-8.