eVoting with the European Citizen Card

Gisela Meister[1], Detlef Hühnlein[2], Jan Eichholz[1] and Roberto Araújo[3]

[1] Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81677 München,
{gisela.meister, jan.eichholz}@gi-de.com

[2] secunet Security Networks AG, Sudetenstraße 16, 96247 Michelau,
detlef.huehnlein@secunet.com

[3] TU Darmstadt, Hochschulstrasse 10, 64289 Darmstadt
rsa@cdc.informatik.tu-darmstadt.de

Abstract: As many European countries are about to introduce national ID cards, which are compliant to the European Citizen Card specification prCEN 15480 it is natural to study how those cards may be used to implement secure electronic voting schemes. For this purpose we introduce a modified variant of the electronic voting scheme introduced in [JCJ05] which may be used with European Citizen Cards.

1 Introduction

While there is a rich literature on the use of cryptography for electronic voting and first proposals in which smart cards are used for the secure implementation of such schemes [MaBC01, LeKi03], the application of smart cards for electronic voting purposes is not yet common in practice [KrTV07]. This may be due to the fact that not all citizen are equipped with secure smart cards yet and there is no business case for the creation of secure smart card infrastructures just for voting purposes. With the advent of the European Citizen Card specification [CEN15480-1, CEN15480-2, CEN15480-3, CEN15480-4] and the corresponding national electronic identity card projects this problem may disappear and hence it is natural to investigate how a European Citizen Card may be used for electronic voting purposes.

Among the existing proposals for electronic voting (cf. [Smit05b] for a survey) the scheme proposed in [JCJ05] – together with the variants of it [Smit05a, Webe06, Schw06, WeAB07, AFT08] – seems to be an especially promising approach, because it provides *coercion-resistance*, which is particulary important for secure remote electronic voting systems. Therefore our contribution focusses on modifications, which are necessary to implement this scheme with European Citizen Cards according to prCEN 15480 using Version 2 of the Extended Access Control protocol defined in [BSI-TR-03110(V2.0)].

The rest of the paper is structured as follows: Section 2 provides the necessary background on the basic voting scheme [JCJ05] and European Citizen Cards supporting the Extended Access Control (EAC) protocol [BSI-TR-03110(V2.0)]. Section 3 explains why and how the original voting scheme [JCJ05] needs to be modified such that it can be implemented with said European Citizen Cards. Section 4 will briefly discuss the proposed scheme and Section 5 will finally summarize the main aspects and conclude the contribution.

2 Background

This section contains background information, which is helpful to understand the main contribution in Section 3. While Section 2.1 recalls the main aspects of the basic voting scheme proposed in [JCJ05], Section 2.2 provides some basic information about the European Citizen Card specification.

2.1 Basic voting scheme

Our voting scheme is a variant of the scheme introduced in [JCJ05] and inspired by the modifications proposed in [Smit05a, WeAB07, Schw06, AFT08]. Therefore we briefly recall the main aspects of the voting scheme presented in [JCJ05] and sketch the various modifications proposed so far. As visualized in Figure 1 the system architecture comprises a set of *Election Authorities* EA_i, $1 \leq i \leq k$, a *Registration Authority* (RA), a public *Bulletin Board* (BB) and of course the *Voters* V_j.

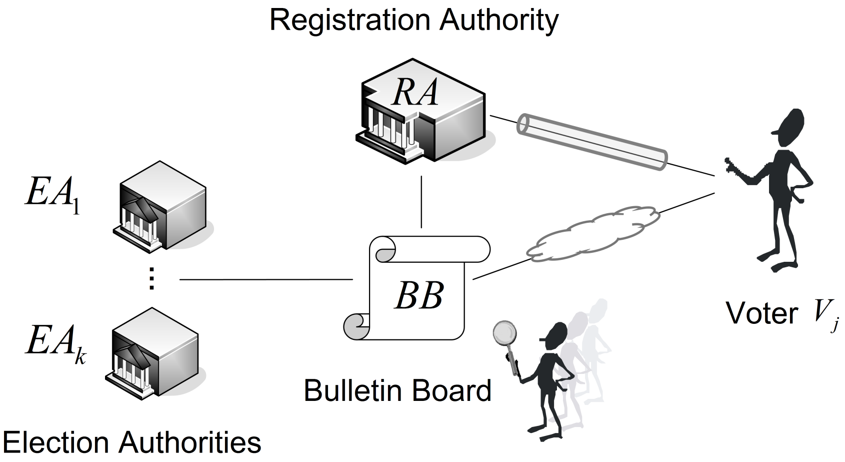

Figure 1: System Architecture

The voting protocol comprises the phases *Setup*, *Registration*, *Voting* and *Tallying*, which are sketched in the following.

2.1.1 Setup

During the Setup phase the system wide domain parameters[1] $\mathcal{D} = \{a, b, p, q, G\}$ are fixed and the Election Authorities EA_i are provided with an individual share SK_{EA_i} of the private decryption key $SK_{EA} = \sum SK_{EA_i}$, which is generated in a distributed manner [GJKR99].

Finally the domain parameters $\mathcal{D}$ and the public encryption key of the distributed Election Authority $PK_{EA} = SK_{EA} \cdot G$ are published on the Bulletin Board BB.

In the modified scheme [WeAB07] the Election Authorities are also equipped with shares of two hash-keys δ and ϵ, which are used calculate deterministic fingerprints of probabilistically encrypted voting credentials such that duplicate and unauthorized votes can be eliminated in the Tallying phase. While the shares of the hash keys δ_i, ϵ_i are kept secret by the Election Authorities, the respective commitments $\delta_i \cdot G, \epsilon_i \cdot G$ are published on BB.

2.1.2 Registration

In the Registration phase each eligible Voter V_j obtains an anonymous secret credential c_j over an ”untappable channel” (cf. [Okam97] for details) from the Registration Authority. The probabilistically encrypted credential $\hat{C}_j = \mathbf{E}(PK_{EA}, c_j)$ is stored on BB. For this purpose [Smit05a, WeAB07] use the classical ElGamal cryptosystem [ElGa85] and [JCJ05] suggests to use a slightly modified ElGamal-variant, which allows to provide a security proof.

In the modified scheme [WeAB07] the encrypted credentials $\hat{C}_j$ are sent through some verifiable MIX-net (cf. [Chau81, FuSa01, Neff01, JJR02]) before a corresponding deterministic fingerprint $h_\epsilon(\hat{C}_j)$ is computed and stored on BB.

2.1.3 Voting

In the Voting phase, which may be performed an arbitrary number of times (indexed by t), the Voter V_j prepares a triple $(B_{j,t}, C_{j,t}, P_{j,t})$ and sends it via an anonymous channel[2] to BB. Here $B_{j,t} = \mathbf{E}(PK_{EA}, b_{j,t})$ is the encrypted ballot, $C_{j,t} = \mathbf{E}(PK_{EA}, c_j)$ is the probabilistic encryption of the secret credential and $P_{j,t}$ is a Zero-Knowledge-Proof, which documents that the ballot is valid (cf. [CrGS97, Section 2.6]), ties together the elements of the triple and documents that the Voter is aware of the plaintexts $b_{j,t}$ and c_j.

Because the Voter may use a fixed but randomly chosen number r instead of the secret credential c_j she may cheat a coercer such that an invalid vote is cast.

[1] While we assume in this paper that the European Citizen Card uses elliptic curve based algorithms and hence the group operations are written additively, the very same voting scheme may of course be used with any other group in which the discrete logarithm problem is believed to be hard (e.g. multiplicative groups in finite fields).

[2] Such an anonymous channel may be implemented using a cascade of MIX-nets [Chau81] for example. The scheme proposed in [Schw06] additionally uses a hardware device, called an observer, to cast the votes.

2.1.4 Tallying

In the Tallying phase all votes in BB are considered and subsequently filtered, mixed and finally decrypted until the final result of the election can be published on the Bulletin Board again. The sequence of steps defined in [JCJ05] and the modifications proposed in [Smit05a, WeAB07, Schw06, AFT08] are briefly summarized in the following:

1. *Checking proofs*
   In a first step all votes in BB with invalid Zero-Knowledge-Proofs $P_{j,t}$ are eliminated. Note that the these proofs prevents the randomization attack, the forced abstention attack (cf. [JCJ05]) and attacks, which make use of the malleability of the classical or modified ElGamal encryption scheme.

2. *Eliminating duplicates*
   In this step all duplicate votes are removed such that only the last casted votes are processed further. In [JCJ05, Schw06] this is realized by pairwise plaintext equivalence tests (PET) [McSJ02, JuJa00], which unfortunately induce a workload, which is quadratic in the number of votes and hence those schemes are not suitable for large scale elections.

   Therefore [Smit05a, WeAB07] propose to replace the PET by the distributed calculation of deterministic fingerprints, which leads to a scheme with linear complexity. As explained below, this change however enables an attacker to generate receipts and hence those schemes may be considered to be broken.

   Finally it was proposed in [AFT08] to use specially formed credentials and the group signature scheme introduced in [CaLy04] instead.

3. *Mixing*
   The remaining votes are sent through an appropriate MIX-net (cf. [Chau81, FuSa01, Neff01, JJR02]) and stored in the Bulletin Board again. This step anonymizes the remaining encrypted ballots $B_{j,\hat{t}}$ and credentials $C_{j,\hat{t}}$.

4. *Checking credentials*
   Now the remaining encrypted credentials are compared to the list of encrypted registered credentials such that unauthorized votes may be eliminated. Similar to the elimination of duplicates above this is realized in [JCJ05] with pairwise PET [McSJ02, JuJa00]. In the variant proposed in [Schw06] this step is not necessary, because the registered credentials are published as plaintexts, which is possible, because a special hardware device, a so called observer, is applied in this scheme. In [Smit05a, WeAB07] the checking of the credentials is performed by a distributed calculation of deterministic fingerprints. While this results in a linear workload, it has been shown in [AFT08, CCM07] that this modification allows a coercer to generate receipts, because he may force the Voter to cast two votes $(B_{j,t}, \mathbf{E}(PK_{EA}, c_j), P_{j,t})$ and $(B_{j,t}, \mathbf{E}(PK_{EA}, c_j^2), P'_{j,t})$, which later on reveal, whether the credential was valid or faked. Therefore the variants in [Smit05a, WeAB07] may be considered to be broken and the only variant of [JCJ05] with linear complexity, which is still secure seems to be [AFT08].

5. *Counting votes*
   Finally the Election Authorities collaborate to decrypt the remaining votes such that the votes can be counted and it is possible to publish the final result of the election in the Bulletin Board.

2.2 European Citizen Card

The CEN technical standard series prTS 15480 [CEN15480-1, CEN15480-2, CEN15480-3, CEN15480-4] describes services, command sets and application contexts of the European Citizen Card (ECC). The Appendix of [CEN15480-4] contains profiles for sector specific applications e.g. for electronic health and/or eID cards. The Extended Access Control protocol, used in the eID profile for device authentication and session key agreement between the ECC and its external partner (local and/or via Internet) is derived from [BSI-TR-03110(V2.0)]. This specification extends the previous version of the EAC protocol [BSI-TR-03110(V1.1)], which is already in use for the second generation of electronic passports.

Both protocols belong to the so called modular Extended Access protocol family (mEAC), which design is described in the basic standard for ESIGN cards [CEN14890-1, CEN14890-2]. The mEAC family comprises the following basic protocol components:

- *Password Authenticated Connection Establishment (PACE)* (cf. [BSI-TR-03110(V2.0), Section 4.2])
  which uses a short password to establish a secure channel between the terminal and the card. This protocol is typically used to protect the communication between a local terminal and a contactless card.

- *Terminal Authentication* (cf. [BSI-TR-03110(V2.0), Section 4.4])
  is a protocol in which the terminal signs a challenge provided by the card in order to be authenticated. Within this protocol the terminal presents a certificate chain to the card, which in particular specifies the authorization of the terminal.

- *Chip Authentication* (cf. [BSI-TR-03110(V2.0), Section 4.3])
  is a protocol in which the terminal and the card use the Diffie-Hellman primitive to agree on a session key, which is subsequently used for authentication purposes. While the terminal typically uses an ephemeral key pair, the card will use its static key pair, which authenticity is verified by Passive Authentication.

- *Passive Authentication* (cf. [BSI-TR-03110(V2.0), Section 1.1 and Annex A.1.2])
  means that sensitive data (e.g. the public key of the card used in the Chip Authentication protocol) are protected by a digital signature according to [RFC3369], which is produced by the so called Document Signer.

- *Restricted Identification* (cf. [BSI-TR-03110(V2.0), Section 4.5])
  is a protocol in which the terminal and the card perform a Diffie-Hellman like protocol in order to produce a sector specific pseudonym of the card.

3 Voting protocol for European Citizen Cards

In this section we will briefly explain why and especially how the original voting scheme [WeAB07] (cf. Section 2.1) needs to be modified to be usable with European Citizen Cards (ECC) supporting the Extended Access Control protocol [BSI-TR-03110(V2.0)].

While it would be an obvious approach to use the ECC for the authentication and identification in the Registration phase and the subsequent storage of the voting credential c_j in a secure manner, there are in particular two issues, which make it necessary to modify the ECC-standards or the voting protocol:

- *ECC does not support the generation of Zero-Knowledge-Proofs*
  While the informative Annex C of [ISO7816-4] contains some information on the use of basic Zero-Knowledge-Proofs for authentication purposes (cf. [ISO9798-5]), it is not yet common practice that smart cards support sophisticated Zero-Knowledge-Proofs as they would be required to implement the original protocol (cf. [CrGS97, Section 2.6]).

- *ECC does not support ElGamal-encryption*
  Because there is usually no requirement for data-encryption functionality on an eID-card and the support of the function `PSO:ENCIPHER` according to [ISO7816-8, Section 11.2] might cause problems with the crypto-policy of some countries, the ECC-specification [CEN15480-2] does purposely not support this functionality.

In the following we will show that the two challenges are no unsurmountable obstacles and that there is a slightly modified version of the original voting protocol, which may be implemented with the European Citizen Card.

As the original scheme our proposal comprises the phases *Setup*, *Registration*, *Voting* and *Tallying*, which are explained in the following.

3.1 Setup

As in the original scheme the Election Authorities (EA_i, for $1 \leq i \leq k$) agree on common domain parameters $\mathcal{D}_{EA}$ and generate a key pair (SK_{EA}, PK_{EA}) in a distributed fashion [GJKR99], which is used to encrypt[3] the credential c_j in the Registration phase (cf. Section 3.2) and the credential and the ballot in the Voting phase (cf. Section 3.3). The domain parameters $\mathcal{D}_{EA}$ and the public key PK_{EA} are published on Bulletin Board BB_0.

The private key SK_{EA} is distributed among the Election Authorities (cf. [GJKR99]) such

[3] Note that our scheme uses the symmetric encryption algorithm – usually AES [FIPS197] – supported by the European Citizen Card for Secure Messaging with a session key, which is agreed within the Diffie-Hellman-like Chip Authentication protocol (cf. [BSI-TR-03110(V2.0), Section 4.3]). Unlike the classical ElGamal scheme [ElGa85], which is used in the original scheme, our encryption scheme does not allow homomorphic re-encryption of cipher texts without knowledge of the session key and consequently prevents corresponding attacks, such as the one mentioned in [AFT08, CCM07] for example.

that a certain subset of the k Election Authorities is required to perform private key operations.

Furthermore we assume that each Voter is equipped with an ECC, which is compliant to the eID profile defined in [CEN15480-4] and contains the additional file listed in Table 2.

DG	Content	R/W	Access
DG.b	Ballot	W	PACE$_\pi$ $+ t_B$
		R	PACE$_\pi$ + PIN$_{voting}$ + TA + CA$_{EA}$

Table 2: Additional File on ECC

The used abbreviations have the following meaning:

- PACE$_\pi$ – is the regular password of the card holder, which is used to protect the communication channel between the local terminal and the contactless ECC,
- t_B – is an election specific template, which defines the syntactical structure of the ballot. This template is loaded onto the ECC in the Registration phase (cf. Section 3.2) and makes sure that only syntactically valid ballots can be stored on the ECC.

  Thus in our scheme we do not require Zero-Knowledge-Proofs to prove that the ballot is syntactically correct in order to guard against randomization and forced abstention attacks, but only trust in the European Citizen Card to reject bogus ballots. Because of the sophisticated Common Criteria evaluation and certification procedures required for those cards this assumption is clearly justified in practice.
- PIN$_{voting}$ – means that one of the voting specific PIN-codes PIN$_{valid}$ or PIN$_{fake}$ (cf. Section 3.2) has been entered correctly and
- TA + CA$_{EA}$ – means that the Terminal Authentication and *double* Chip Authentication protocol (cf. Section 3.3.2) was successfully performed between the ECC and the Registration Authority or the Bulletin Board respectively.

3.2 Registration

As in the original scheme each Voter needs to be equipped with a unique credential c_j to cast a valid ballot. Unlike in the previous schemes however, these credentials are *not* generated by the Registration Authority (RA). Instead, the credential c_j is generated by the ECC using the Restricted Identification mechanism introduced in [BSI-TR-03110(V2.0), Section 4.5].

The interaction of the ECC with the RA is shown in Figure 2.

Thereby the Extended Access Control protocol 2.0 (EAC 2.0, see [BSI-TR-03110(V2.0)]) is processed between the ECC and the RA. After the mutually authenticated connection

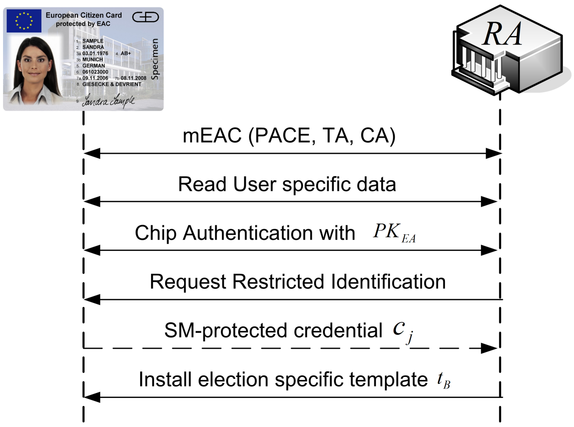
European Citizen Card protected by EAC
Specimen
RA
mEAC (PACE, TA, CA)
Read User specific data
Chip Authentication with PK_{EA}
Request Restricted Identification
SM-protected credential c_j
Install election specific template t_B

Figure 2: Registration Phase

establishment, the RA reads user specific data from the ECC, like the name of the cardholder and the document number for example[4] (cf. [BSI-TR-03110(V2.0), Table E.1]). Since this mechanism identifies the user, the RA can ensure that a Voter registers at most once. After that the Chip Authentication protocol is performed again using PK_{EA} and the Secure Messaging is restarted such that the used encryption key $K_{Enc,EA}$ now is derived from the key agreement with PK_{EA} while the value of $K_{MAC,CA}$ is kept from the initial performance of the Chip Authentication protocol, which used the ephemeral key pair generated during the Terminal Authentication protocol.

Now the Restricted Identification mechanism [BSI-TR-03110(V2.0), Section 4.5] is used to create the ”election specific identifier”

$$c_j = I_{ECC}^{EA} = h\left(I_{ECC} \cdot PK_{EA}\right),$$

which plays the role of the anonymous credential c_j in the original scheme. This credential is computed by the ECC in a Diffie-Hellman key agreement with the public key of the election authorities PK_{EA} and the private identifier I_{ECC} of the ECC and subsequent computation of the hash-value of the x-coordinate of the agreed elliptic curve point ($I_{ECC} \cdot PK_{EA}$). Note that the operating system of the ECC prevents unauthorized access to the identifier I_{ECC} and we require that those identifiers are generated in a manner, which does *not* allow anybody to link the election-specific credentials (cf. [BSI-TR-03110(V2.0), Annex A.5.1]).

The credential c_j is transported from the ECC to the RA using Secure Messaging with $K_{Enc,EA}$ and $K_{MAC,RA}$. The structure of the Response-APDU is depicted in Figure 3 (see [BSI-TR-03110(V2.0), Figure F.3] for more details).

Because the RA knows $K_{MAC,RA}$, which has been generated in the first Chip Authentication, it is able to verify the Message Authentication Code protecting the APDU, which pre-

[4] If the ECC under consideration is an ICAO-compliant travel document, on which biometric characteristics are stored, and the systems of all Voters *would* be equipped with appropriate biometric sensors, the registration procedure could comprise a biometric authentication step (cf. [Hof04]), which may provide even more security.

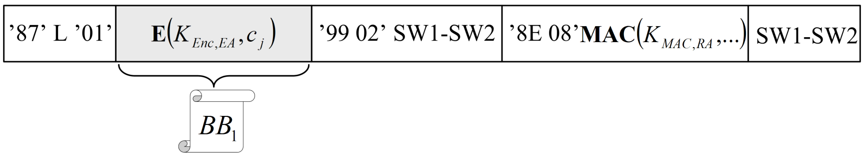
'87' L '01'
$\mathbf{E}(K_{Enc,EA}, c_j)$
'99 02' SW1-SW2
'8E 08'$\mathbf{MAC}(K_{MAC,RA}, \ldots)$
SW1-SW2
BB_1

Figure 3: Response APDU containing protected credential c_j

vents replay attacks. On the other side the RA does *not* (need to) know the key $K_{Enc,EA}$, which depends on a random number r_{ECC} generated by the ECC during the second Chip Authentication (cf. [BSI-TR-03110(V2.0), Section 4.3.1.2]) and therefore provides a probabilistic encryption of the credential c_j. Using this "trick" it is possible to realize the required "ElGamal-like" encryption without having a `PSO:ENCIPHER`-command available on the card.

Next the RA will publish the value $\mathbf{E}(K_{Enc,EA}, c_j)$ and the random number r_{ECC} to the Bulletin Board BB_1 and the RA will install the election specific template t_B on the ECC, which guards against the randomization and forced abstention attacks.

Finally the Voter may[5] choose one or two PIN codes. The first PIN code (PIN$_{valid}$) is used to cast a valid vote, which includes c_j. The second PIN code (PIN$_{fake}$) is optional and may be used to transmit a fake vote, which includes a randomly chosen number r_{fake} instead of c_j. As in the original scheme, this mechanism is of central importance to reach coercion resistance.

It should be noted that we assume that the Voter performs this Registration procedure in a trustworthy environment, which is not controlled or observed by a coercer. Furthermore we also assume that the ECC and the Registration Authority is trustworthy such that only eligible Voters are able to register (at most once) and the Registration process does *not* leak any additional information which may be used to link the personal data read from the ECC during registration to the encrypted credential $\mathbf{E}(K_{Enc,EA}, c_j)$ posted on BB_1. More details on the trustworthy implementation of the Registration step, which is critical for the security of our scheme will be provided in a forthcoming paper.

3.3 Voting

As in the original protocol the Voting phase may be performed an arbitrary number of times. In our proposal however this phase consists of two steps:

1. Casting the vote
2. Transmitting the vote

[5] Note that the Voter should *not* publicly commit that he has chosen the second PIN code, because this would enable a coercer to force him to enter two different PIN codes, which are acceptable by the ECC.

3.3.1 Casting the vote

The voter uses his local PC to complete the ballot form. Afterwards, the voter establishes a local connection to the ECC using the Password Authenticated Connection Establishment (PACE) protocol (cf. [BSI-TR-03110(V2.0), Section 4.2]) together with his individual PACE password (π). After execution of the PACE protocol, a secure channel between the local PC and the ECC has been established and it is possible to store the ballot $B_{j,t}$ inside the file $DG.b$ on the ECC, if it complies with the previously installed election specific template t_B (see Figure 4).

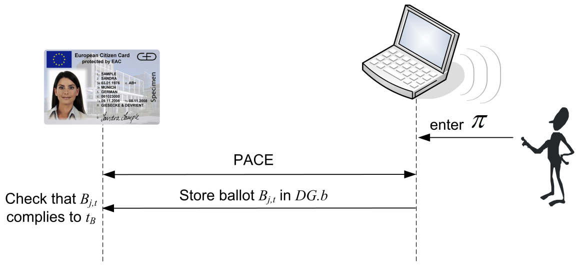
enter π
PACE
Check that $B_{j,t}$ complies to t_B
Store ballot $B_{j,t}$ in $DG.b$

Figure 4: Store the ballot within the ECC

3.3.2 Transmitting the Vote

To transmit the vote v, consisting of the encrypted ballot $b_{j,t}$ and the credential c_j, from the ECC to the Bulletin Board BB_2 the protocol depicted in Figure 5 is executed:

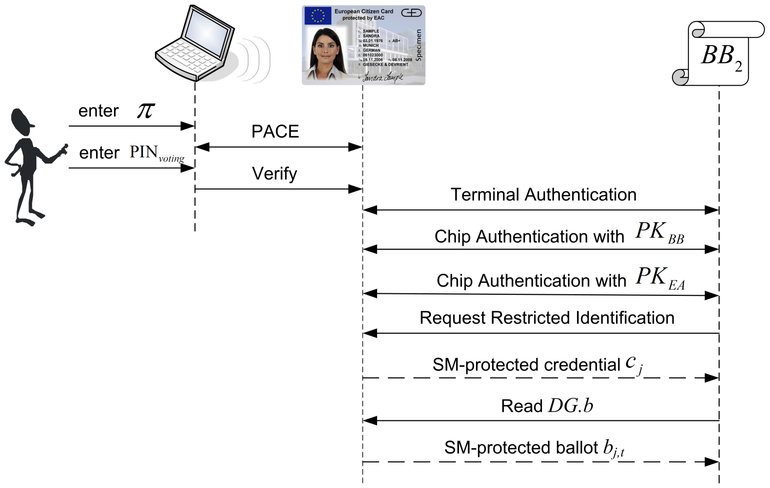
BB_2
enter π
enter PIN_{voting}
PACE
Verify
Terminal Authentication
Chip Authentication with PK_{BB}
Chip Authentication with PK_{EA}
Request Restricted Identification
SM-protected credential c_j
Read $DG.b$
SM-protected ballot $b_{j,t}$

Figure 5: Transmitting the vote

1. To achieve user consent, the PACE protocol is performed locally, which results in a Secure Messaging session between the ECC and the local terminal / PC.

2. The Voter enters his voting PIN. Normally, he uses PIN$_{valid}$, which results in a valid vote. In the case of a coercion, he has the possibility to enter PIN$_{fake}$, which results in an invalid vote, because the ECC is not returning the encryption $\mathbf{E}(K_{Enc,EA}, c_j)$ of the credential c_j, but the encryption $\mathbf{E}(K_{Enc,EA}, r_{fake})$ of the random number r_{fake}, which has been chosen in the Registration phase but has not been registered and hence will lead to an invalid vote with high probability. Note that because $K_{Enc,EA}$ depends on the random number r_{ECC} provided by the ECC in the Chip Authentication protocol (cf. [BSI-TR-03110(V2.0), Section 4.3]), the encryption of c_j (or r_{fake}) is probabilistic and an attacker does not have any means to detect, whether the voter has used PIN$_{valid}$ or PIN$_{fake}$.

3. To authenticate the Bulletin Board BB_2, the Terminal Authentication protocol is performed between the ECC and BB_2. Thereby the ECC validates the correctness of the presented certificate and checks the signature provided by the Bulletin Board. In addition to a challenge provided by the ECC the signature also contains the hash value of the ephemeral public Diffie-Hellman key PK_{BB}.

4. Now the regular Chip Authentication protocol is performed using the ephemeral public key PK_{BB} and the authenticity of the public key PK_{ECC} is checked by Passive Authentication[6].

5. In the next step the Chip Authentication protocol is performed a second time using the public key of the Election Authorities PK_{EA} in order to generate a new Secure Messaging encryption key $K_{Enc,EA}$, which depends on a random number r_{ECC} provided by the ECC. As explained in Section 3.2 this key and the previously generated $K_{MAC,BB}$ is from now on used to protect the responses from the ECC.

6. The Bulletin Board requests the credential c_j from the ECC using the Restricted Identification protocol and receives it in encrypted form $\mathbf{E}(K_{Enc,EA}, c_j)$ (cf. Figure 3).

7. If PIN$_{valid}$ was provided in step 2, the ECC returns the encrypted credential c_j as depicted in Figure 3. If PIN$_{fake}$ was entered, the ECC will return an encrypted random number r_{fake}, which will result in an invalid vote with high probability.

8. Finally the Bulletin Board BB_2 reads the ballot stored in $DG.b$ from the ECC. Similar to the transmission of the credential the ballot $b_{j,t}$ is encrypted with $K_{Enc,EA}$ and the integrity and freshness of the returned APDU is protected with $K_{MAC,BB}$. As the latter key is available to the Bulletin Board, it may readily verify the message authentication code, but it can *not* decrypt the encrypted ballot $\mathbf{E}(K_{Enc,EA}, b_{j,t})$.

9. If the verification of the message authentication code is successful, the data listed in Table 4 is published on BB_2.

[6] Since the ECC keys for Chip Authentication are not unique, this protocol does not reveal the identity of the ECC and hence the card holder. Hence Passive Authentication only ensures that the Bulletin Board communicates with *some* authentic ECC.

Vote Part	Description
$\mathbf{E}(K_{Enc,EA}, b_{j,t})$	Encrypted ballot
$\mathbf{E}(K_{Enc,EA}, c_j)$	Encrypted credential
t	Timestamp of vote transmission
PK_{ECC}	Public Diffie-Hellman key of the ECC
r_{ECC}	Random number used for key generation (cf. [BSI-TR-03110(V2.0), Section 4.3])

Table 4: Contents of a Vote v_j

10. If the verification of the message authentication code fails, the transcript of the communication may be published separately, but the transmitted data are not processed further.

3.4 Tallying

The result of the Tallying phase is to eliminate double or unauthorized votes and count the valid votes in order to determine the result of the election.

We will explain the the different steps of this phase by considering the content of the corresponding Bulletin Boards BB_i:

4 Discussion

In this section we will briefly sketch how the coercion resistance is realized in our proposed scheme and highlight the advantages of our proposal compared to the previously known schemes [JCJ05, Smit05a, WeAB07, Schw06, AFT08]. A more formal and comprehensive security analysis will be the subject of a forthcoming paper.

4.1 Coercion-Resistance

As defined in [JCJ05] a voting scheme is coercion-resistant if it is receipt-free and additionally prevents the randomization, the forced-abstention, and the simulation attack.

Our proposed scheme is *receipt-free* because the decryption of the registered credentials and the comparison with the ones submitted in the Voting phase (cf. Step 6 and 7 in Table 5) is performed after the MIXing step and hence it is not possible for the Voter to produce a receipt. Furthermore it should be noted that the attack presented in [AFT08, CCM07] against the schemes presented in [Smit05a, WeAB07] is not possible in our scheme as the credentials are produced, encrypted and transmitted using the trusted ECC.

i	**Description of step, which fills BB_i**
3	An appropriate subset of the Election Authorities EA_i collaborate in order to decrypt the credentials c_j for all votes v_j stored in BB_2 and publish the votes with decrypted credentials through some robust and verifiable decryption MIX-net (cf. [JJR02]) on BB_3.
4	For all votes v_j in BB_3 with identical credentials c_j, all votes except the vote with the latest time stamp is eliminated and the result is stored on BB_4, such that only the last vote of an eligible voter will be counted.
5	The remaining votes in BB_4 are sent through a robust and verifiable decryption MIX-net (cf. [JJR02]) and stored in BB_5. As in the original scheme this step anonymizes the remaining encrypted ballots $B_{j,\hat{t}}$ and credentials $C_{j,\hat{t}}$.
6	An appropriate subset of the Election Authorities EA_i collaborate in order to decrypt the registered credentials c_j stored in BB_1 and publish the result through some robust and verifiable decryption MIX-net (cf. [JJR02]) to BB_6.
7	The credentials in the votes stored in BB_5 are compared with the registered credentials in BB_6, such that all authorized votes can be published on BB_7.
8	An appropriate subset of the Election Authorities EA_i collaborate in order to decrypt the ballots $b_{j,\hat{t}}$ stored in BB_7 and publish the result to BB_8.
9	Finally it is possible to count the respective votes in BB_8 and publish the final result of the election in BB_9.

Table 5: Description of steps in Tallying phase of ECC-based voting scheme

The *randomization attack* is not possible, because ballots, which violate the syntax defined by the election specific template t_B can not be stored on the ECC. Because of the Secure Messaging employed within the EAC-protocol (cf. Figure 3) it is not possible to "inject" data into an established channel, which has not been stored on the ECC before.

As in the original scheme the *forced abstention attack* is prevented by requiring an "anonymous channel" to cast the vote. As we use the ECC and the EAC-protocol for this purpose (cf. Figure 5) it is in particulary necessary that the certificate of BB_2 only allows to read $DG.b$ and no other data groups, which may contain personal data of the card holder and hence would endanger anonymity.

The *simulation attack* means that the Voter gives away its valid credential c_j to the Coercer, who will subsequently act on behalf of the Voter. As in the original scheme the Voter may simply use PIN$_{fake}$ to export the random r_{fake} instead of the registered credential c_j and hence the simulation attack is not possible. In addition to this the ECC in our scheme even does not allow to export the plain credential, even if the Coercer knows both PIN$_{valid}$ and PIN$_{fake}$. This is due to the fact that in our scheme the credential c_j is produced by the ECC using the Restricted Identification protocol and the secret source identity I_{ECC} together with the public key PK_{EA} of the Election Authorities and subsequently probabilistically encrypted for this public key (cf. Figure 3). In order to obtain the plaintext credential c_j an attacker would either need to decrypt $C_{j,t} = \mathbf{E}(K_{Enc,EA}, c_j)$ or smuggle in his own public key in the second run of the Chip Authentication protocol. The decryption of $C_{j,t}$ is not feasible because the private key SK_{EA} of the Election Authorities is shared among trustworthy parties, which store the key shares in a secure fashion. That an attacker uses his own public key and domain parameters, which may ease the computation of the discrete logarithm I_{ECC} is prevented by the requirement that the hash value of an admissible public key PK_{EA} needs to be included in the certificate of the Bulletin Board (cf. [BSI-TR-03110(V2.0), Annex C.3.2]).

4.2 Advantages of the proposed voting scheme

The main advantage of our scheme compared to the original scheme [JCJ05] is, that our Tallying phase only requires linear work – just as the schemes proposed in [Smit05a, WeAB07]. Those variants however are not receipt-free because of the attack mentioned in [AFT08, CCM07]. On the other hand it is not possible to mount this attack against our scheme, because the credential is produced and securely transmitted by the European Citizen Card.

While the scheme proposed in [AFT08] also has a linear Tallying phase it still requires complex zero-knowledge proofs and much more bandwidth.

An additional advantage of our scheme is that the Voter does not need to remember a long and randomly chosen credential c_j, but only the short PIN codes and hence our scheme seems to have important advantages with respect to usability. While a similar effect could be reached in the scheme proposed in [Schw06], this scheme requires that the Voter will be equipped with special purpose hardware, which clearly is not possible in real world scenarios just because of economic reasons.

5 Conclusion

Based on the discussion in the previous section it seems that our scheme offers many important advantages compared to the previously known schemes [JCJ05, Smit05a, Schw06, WeAB07, AFT08]. As our proposal is based on European Citizen Cards according to prCEN 15480, which support the Extended Access Control protocol and those cards may soon be available to many European citizen, it does not seem to be impossible that our proposal will attain great practical relevance some day.

Acknowledgement

The authors would like to express their sincere thanks to the various people who contributed to this paper by fruitful discussions and valuable suggestions. In particular we would like to thank Johannes Buchmann, Henning Daum, Michael Kreutzer, Dennis Kügler, Rainer Urian, Melanie Volkamer and the anonymous referees.

References

[Hof04] Sonja Hof. *E-Voting and Biometric Systems*. In Alexander Prosser and Robert Krimmer (editors), *Electronic Voting in Europe*, volume 47 of *LNI*, pages 63–72 (GI, 2004). http://www.e-voting.cc/static/evoting/files/hof_p63-72.pdf.

[AFT08] Roberto Araújo, Sébastien Foulle, and Jacques Traoré. *A practical and secure coercion-resistant scheme for remote elections*. In David Chaum, Miroslaw Kutylowski, Ronald L. Rivest, and Peter Y. A. Ryan (editors), *Frontiers of Electronic Voting*, number 07311 in Dagstuhl Seminar Proceedings (Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI), Schloss Dagstuhl, Germany, Dagstuhl, Germany, 2008). http://drops.dagstuhl.de/opus/volltexte/2008/1295/pdf/07311.TraoreJacques.ExtAbstract.1295.pdf.

[BSI-TR-03110(V1.1)] Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik). *Advanced Security Mechanism for Machine Readable Travel Documents - Extended Access Control (EAC)*. Technical Directive (BSI-TR-03110), Version 1.1. http://www.bsi.bund.de/fachthem/epass/EACTR03110_v110.pdf, 2007.

[BSI-TR-03110(V2.0)] Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik). *Advanced Security Mechanism for Machine Readable Travel Documents - Extended Access Control (EAC)*. Technical Directive (BSI-TR-03110), Version 2.0 - Release Candidate, 2008.

[CaLy04] Jan Camenisch and Anna Lysyanskaya. *Signature schemes and anonymous credentials from bilinear maps*. In Matthew K. Franklin (editor), *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 56–72 (Springer, 2004). http://www.cs.brown.edu/~anna/papers/cl04.pdf.

[CCM07] Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. *Civitas: Toward a Secure Voting System*. Technical Report TR 2007-2081, Cornell University. http://www.cs.cornell.edu/people/clarkson/papers/clarkson_civitas_tr.pdf, 2007.

[CEN14890-1] Comité Européen de Normalisation (CEN). *Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services*. Preliminary European Norm, 2008.

[CEN14890-2] Comité Européen de Normalisation (CEN). *Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services*. Preliminary European Norm, 2008.

[CEN15480-1] Comité Européen de Normalisation (CEN). *Identification card systems - European Citizen Card - Part 1: Physical, electrical and transport protocol characteristics*. CEN/TS 15480-1 (Technical Specification), 2007.

[CEN15480-2] Comité Européen de Normalisation (CEN). *Identification card systems - European Citizen Card - Part 2: Logical data structures and card services*. CEN/TS 15480-2 (Technical Specification), 2007.

[CEN15480-3] COMITÉ EUROPÉEN DE NORMALISATION (CEN). *Identification card systems - European Citizen Card - Part 3: European Citizen Card Interoperability using an application interface*. CEN 15480-3 (Working Draft), 2008.

[CEN15480-4] COMITÉ EUROPÉEN DE NORMALISATION (CEN). *Identification card systems - European Citizen Card - Part 4: Recommendations for European Citizen Card issuance, operation and use*. CEN 15480-4 (Working Draft), 2008.

[Chau81] D. CHAUM. *Untraceable electronic mail, return addresses, and digital pseudonyms*. *Communications of the ACM*, volume 24(2):84–88. http://www.freehaven.net/anonbib/cache/chaum-mix.pdf, 1981.

[CrGS97] RONALD CRAMER, ROSARIO GENNARO, and BERRY SCHOENMAKERS. *A Secure and Optimally Efficient Multi-Authority Election Scheme*. In WALTER FUMY (editor), *Advances in Cryptology – EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 103–118 (Springer, 1997). http://www.win.tue.nl/~berry/papers/euro97.pdf.

[ElGa85] TAHER ELGAMAL. *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*. *IEEE Transactions on Information Theory*, volume 31(4):469–472, 1985.

[FIPS197] UNITED STATES OF AMERICA NATIONAL INSTITUTE FOR STANDARDS and TECHNOLOGY (NIST). *Advanced Encryption Standard (AES)*. Federal Information Processing Standard (FIPS) Publication 197. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, November 2001.

[FuSa01] J. FURUKAWA and K. SAKO. *An efficient scheme for proving a shuffle*. In *Advances in Cryptology – CRYPTO '01*, volume 2139 of *Lecture Notes in Computer Science*, pages 368–387 (Springer-Verlag, 2001). http://www.freehaven.net/anonbib/cache/PShuffle.pdf.

[GJKR99] ROSARIO GENNARO, STANISLAW JARECKI, HUGO KRAWCZYK, and TAL RABIN. *Secure Distributed Key Generation for Discrete-Log Based Cryptosystems*. pages 295–310.

[ISO7816-4] *ISO/IEC 7816-4: Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*. International Standard, 2005.

[ISO7816-8] *ISO/IEC 7816-8: Identification cards – Integrated circuit cards – Part 8: Commands for security operations*. International Standard, 2004.

[ISO9798-5] *ISO-IEC 9798-5: Information Technology - Security Techniques - Entity Authentication - Part 5: Mechanisms using zero-knowledge techniques*. International Standard, 2004.

[JCJ05] ARI JUELS, DARIO CATALANO, and MARKUS JAKOBSSON. *Coercion-resistant electronic elections*. In *WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 61–70 (ACM, 2005). http://eprint.iacr.org/2002/165.pdf.

[JJR02] Markus Jakobsson, Ari Juels, and Ronald L. Rivest. *Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking*. In *Proceedings of the 11th USENIX Security Symposium*, pages 339–353 (USENIX Association, 2002). http://www.informatics.indiana.edu/markus/papers/rpcmix.pdf.

[JuJa00] Ari Juels and Markus Jakobsson. *Mix and match: Secure function evaluation via ciphertexts*. In T. Okamoto (editor), *Advances in Cryptology – Asiacrypt 00*, volume 1976 of *LNCS*, pages 162–177 (Springer, 2000). http://eprint.iacr.org/2002/165.pdf.

[KrTV07] Robert Krimmer, Stefan Triessnig, and Melanie Volkamer. *The Development of Remote E-Voting Around the World: A Review of Roads and Directions*. In *E-Voting and Identity, First International Conference, VOTE-ID 2007, Bochum, Germany, October 4-5, 2007, Revised Selected Papers*, volume 4896 of *Lecture Notes in Computer Science*, pages 1–15 (Springer, 2007).

[LeKi03] Byoungcheon Lee and Kwangjo Kim. *Receipt-Free Electronic Voting Scheme with a Tamper-Resistant Randomizer*. In *Information Security and Cryptology – ICISC 2002*, volume 2587 of *Lecture Notes in Computer Science*, pages 581–587 (Springer, 2003).

[MaBC01] Emmanouil Magkos, Mike Burmester, and Vassilis Chrissikopoulosm. *Receipt-freeness in Large-scale Elections without Untappable Channels*. In *Towards The E-Society: E-Commerce, E-Business, and E-Government, The First IFIP Conference on E-Commerce, E-Business, E-Government (I3E 2001), October 3-5, Zürich, Switzerland*, volume 202 of *IFIP Conference Proceedings*, pages 683–694 (Kluwer, 2001). http://thalis.cs.unipi.gr/~emagos/I3E_receipt_freeness.pdf.

[McSJ02] P. MacKenzie, T. Shrimpton, and M.Jakobsson. *Threshold password-authenticated key exchange*. In *Advances in Cryptology – Proceedings of CRYPTO02*, volume 2442 of *LNCS*, pages 385–400 (Springer, 2002). http://web.cecs.pdx.edu/~teshrim/jdp9.pdf.

[Neff01] C. A. Neff. *A verifiable secret shuffle and its application to e-voting*. In *8th ACM Conference on Computer and Communications Security*, SIGSAC, pages 116–125 (ACM, 2001). http://www.freehaven.net/anonbib/cache/shuffle:ccs01.pdf.

[Okam97] Tatsuaki Okamoto. *Receipt-free electronic voting schemes for large scale elections*. In *Security Protocols Workshop*, volume 1361 of *Lecture Notes in Computer Science*, pages 25–35 (Springer-Verlag, 1997).

[RFC3369] R. Housley. *Cryptographic Message Syntax (CMS)*. Request For Comments – RFC 3369. http://www.ietf.org/rfc/rfc3369.txt, August 2002.

[Schw06] Jörn Schweisgut. *Coercion-Resistant Electronic Elections with Observer*. In Robert Krimmer (editor), *Electronic Voting*, volume 86 of *LNI*, pages 171–177 (GI, 2006). http://www.e-voting.cc/static/evoting/files/schweisgut_coercion-resistant_171-177.pdf.

[Smit05a] WARREN D. SMITH. *New cryptographic voting schemes with best-known theoretical properties*. In *Workshop on Frontiers in Electronic Elections (FEE 2005)* (2005). http://www.math.temple.edu/~wds/homepage/jcj.pdf.

[Smit05b] WARREN D. SMITH. *Cryptography meets Voting*. September 10. http://www.math.temple.edu/~wds/homepage/cryptovot.pdf, 2005.

[WeAB07] STEFAN G. WEBER, ROBERTO ARAUJO, and JOHANNES BUCHMANN. *On Coercion-Resistant Electronic Elections with Linear Work*. In *2nd Workshop on Dependability and Security in e-Government (DeSeGov 2007) at 2nd Int. Conference on Availability, Reliability and Security (ARES'07)*, pages 908–916 (IEEE Computer Society, 2007). ISBN 0-7695-2775-2. http://elara.tk.informatik.tu-darmstadt.de/publications/2007/WeberAB07.pdf.

[Webe06] STEFAN WEBER. *A Coercion-Resistant Cryptographic Voting Protocol - Evaluation and Prototype Implementation*. Diplomarbeit. http://www.cdc.informatik.tu-darmstadt.de/reports/reports/StefanWeber.diplom.pdf, 2006.