Electronic Voting Using Identity Domain Separation and Hardware Security Modules

Thomas Rössler

Secure Information Technology Center Austria (A-SIT)
thomas.roessler@a-sit.at

Abstract. E-voting increasingly gains interest in e-Democracy and e-Government movements. Not only the technical security issues of electronic voting systems are of paramount importance, but also the necessity of following an all-embracing approach is challenging and needs to be addressed. This paper discusses e-voting as being a supreme discipline of e-Government. It introduces an innovative e-voting concept using the Internet as the voting channel. The concept introduced is based on Austrian e-Government elements and the Austrian identity management concept in particular. As a result, this paper presents a novel approach of building an e-voting system relying on two core principles: strong end-to-end encryption and stringent identity domain separation.

1 Introduction

Voting is the most important tool in democratic decision making. Therefore, elections and referenda should be accessible to as many people as possible. It is especially difficult for citizens living abroad to participate in elections.

The word e-voting is a general term that refers to any type of voting in electronic form. This work introduces a remote Internet e-voting concept that suits the needs of international election fundamentals—as formulated by the Venice Commission [1] and the Council of Europe in [2] and [3]—and the needs of Austrian elections [4] in particular[1].

Today, the e-Government infrastructure is highly developed in many member states of the European Union. Austria in particular has actively pursued its e-Government strategy since the beginning and thus is today one of leading countries in Europe with respect to e-Government.

E-voting, seen as a special application of e-Government technologies, can be considered as being the supreme discipline of all e-Government applications due to its conflicting priorities of unique identification and perfect anonymity.

The proposed e-voting concept draws upon two principles in order to protect the election secrecy. On the one hand, the proposed e-voting system makes use of strong

[1] In preceding work [5] we worked out an exhaustive and all-embracing set of security requirements by following a standardised methodology (i.e. Common Criteria methodology). The security requirements have been created based on (legal) election fundamentals [1], [2], [3], [4], [6] and existing security considerations [7], [8]. These achievements serve the basis for the e-voting concept presented here.

C. Godart et al. (Eds.): I3E 2009, IFIP AICT 305, pp. 1–12, 2009.

end-to-end encryption between the voter casting her vote and the electronic device responsible for counting. Thus, the cast vote is immediately encrypted by the voter after she has filled in her decision and is only decrypted for the single moment of counting. On the other hand, the proposed e-voting concept introduces a stringent domain separation model that has to ensure unique identification of voters during registration, but also guarantee perfect anonymity of cast votes. A special case in the introduced e-voting concept is that although votes are cast anonymously it is still possible to determine whether a given voter has cast her vote already or not. This mechanism is available during the election event only. This is important and a big advantage of the proposed scheme as it enables a voter to cast her vote conventionally at a polling station although she has decided to vote electronically. This characteristic of the proposed e-voting concept faces problems in connection with the Internet and the voter's local infrastructure as raised by the SERVE-report [9] for instance.

From a technical perspective, the proposed e-voting concept makes use of Austrian e-Government components such as the Citizen Card [10]. Although the core principles of this e-voting concept are versatile, the resulting e-voting concept is tailored to a certain degree for Austrian elections. Thus, the proposed e-voting concept has been named "EVITA" (Electronic Voting over the Internet - Tailored for Austria). The EVITA voting model aims to follow the process model of conventional postal elections which has two phases. In phase one, voters have to register and in phase two the voting process is carried out. Also from a technical perspective EVITA follows tight the model of postal elections. The EVITA scheme requires to encrypt the voter's decision without any identifying information and to attach additional voter related information to the encrypted vote. This corresponds to scenario of postal election scenarios where the vote is put into an inner envelope which itself is wrapped by an outer envelope that contains additional identifying information about the voter.

This paper introduces the core elements of the proposed EVITA-voting concept. The rest of this paper is organised as follows. The next section explains the core principles of the EVITA concept and introduces the dual approach of using strong end-to-end encryption and stringent identity domain separation. Section 3 and 4 further elaborate these core aspects—the creation of the identifiers following the Austrian electronic identity management in particular—in several sub-sections in detail. Section 5 briefly sketches the counting phase. Finally conclusions are drawn.

2 Core Elements of the EVITA Schema

First of all, an e-voting schema (EVS) must guarantee that a voter's decision remains an inviolable secret. To do so, most of them use cryptographic mechanisms and principles. Existing e-voting schemes can be grouped as follows:

- EVS based on Homomorphic Encryption, e.g. [11][12][12]
- EVS based on Mixing Nets, e.g. [14][15][16]
- EVS based on Blind Signatures, e.g. [14][17][18]

To guarantee that a voter's decision remains an inviolable secret, two distinct general approaches seem to be promising. One approach is to have a voting scheme that prevents the vote from being spied on by applying cryptographic methods. Another

approach for protecting the secrecy of the ballots is by removing any form of identifying information from the cast vote thus breaking any link between the voter and her cast vote. Both approaches have drawbacks and advantages. Furthermore, regarding the requirements given by the targeted use-cases neither approach by itself would be satisfactory.

In the first approach, the use of encryption algorithms seems to be adequate. Various strong encryption algorithms exist, so question that remains is how and where to hold the decryption keys needed to decrypt votes. There are several schemes which do not need to decrypt votes in order to count them (e.g. schemes based on homomorphic encryption), but those approaches have limitations regarding write-in votes or they are too complex.

However, the use of strong encryption algorithms in order to protect the secrecy of ballots is no guarantee that these algorithms will be able to resist attack in the future. Due to the ever-increasing power of new computer systems it could become quite easy to crack a given encrypted vote by a brute force attack (e.g. by trying all encryption keys possible).

Therefore, using strong encryption mechanisms in combination with a comprehensive identity management concept in order to keep cast votes anonymous throughout the election and beyond are the key elements of the EVITA e-voting schema. Due to a sophisticated identification and authentication model that is based on the Austrian identity management concept[2], it can be ensured that the identity of a voter cannot be determined based on her cast vote, especially after the election. This eliminates the progressive weakness inherent to encryption algorithms.

3 Encryption Using a Hardware Security Module

From the moment the voter makes her decision there is no more need to reveal it except for the reason of counting. There is no need to uncover the voter's decision, her vote respectively, at any other time. The aim is to achieve an end-to-end encryption of the cast vote between the voter and the counting device. At this point two questions arise. How to provide the voter with the encryption key and how to ensure that only the counting device is able to decrypt the vote. An obvious answer to the first question is to use an asymmetric encryption algorithm and a public key infrastructure. The latter question is more difficult to address as both technical and organisational measurements have to be put in place.

One technical solution for protecting the confidentiality of the private decryption key is to build the counting device on the basis of a hardware security module. Due to this, the private key used for decrypting of cast votes is solely stored in the hardware security module in a very secure way. However, additional organisational and technical measures are required in order to address the process of key generation and distribution. The private key—or any copy of it—must not exist outside the hardware security module without any technical or non-technical security measure.

In order to export, backup and (re-)import the private key of the hardware security module—which is necessary in real election scenarios—an adequate and sophisticated

[2] For further details about the Austrian electronic identity management system see 19 and 10.

key management must be put in place. It would be a desirable to require the hardware security module to provide a key export and import mechanism following a defined shared key schema. If a shared key schema is provided, a dedicated organisational framework has to be defined that states how to distribute the key shares and to whom. The organisational framework as well as the legal framework of an election must state clearly how many shares are required at a minimum to import or reset the decryption key of the hardware security module. Furthermore, it must describe which organisations—or more generally which entities of the election process—are eligible to hold a key share. From an organisational and legal perspective, a shared key schema would be perfect for replicating the legal responsibilities of the participating political parties regarding the election.

The EVITA approach is to decrypt the vote only at the very single moment of counting; a cast vote remains encrypted at any time before and after counting. This contrasts with other e-voting approaches where votes are decrypted before counting. However, the counting device holds the decryption key for decrypting the votes within the counting process. It must meet the requirements of a hardware security module in order ensure that the key cannot be exported or stolen. Furthermore, the counting device must ensure that votes are decrypted only for the purpose of counting. There must not be any chance to learn decrypted votes by accessing the counting device by any means. It is not sufficient to use a hardware security module only for the purpose of securely holding the keys. Additional critical components of the counting device—critical with respect to revealing encrypted votes unintentionally—are the counters used to compute the result. The counting device must not offer any possibility of finding out intermediate results or to observe the current status of the counting process. However, logs for recording information might be put in place throughout the counting process by the counting device in order to collect additional information that confirm the correctness of the count, e.g. for an election audit.

4 Domain Separation and Identification Model

On the one hand, the process requires unique identification of the voter in the course of the registration procedure in order to record who has cast her vote. On the other hand, the cast vote must not be linkable to the voter. Although these requirements seem to be contradictory, the EVITA voting schema meets both requirements by introducing a sophisticated identification concept and domain separation schema (domain separation with respect to identity domains).

The concept of domain separation is based on the need-to-know principle since neither of the involved authorities—usually we have two authorities: a Registration Authority dealing with registration issues and an Election Authority dealing with the election itself—need to know the voter's unique identity (identifier). Usually it is sufficient to identify the voter within a dedicated context. This principle is also the underlying idea of the whole identity management of Austrian e-Government and the Citizen Card concept.

The Austrian identity management concept introduces a unique identifier for each citizen, called Source Personal Identification Number (sPIN), as well as identifiers for sectors of applications, called Sector Specific Personal Identification Numbers

(ssPIN), in order to uniquely identify a citizen within a given sector of applications. It is important to note that a person's sPIN is only stored in her Citizen Card. There exists neither a register of sPINs nor is any authority or application allowed to handle or store them. Applications and authorities are only allowed to work with sector-specific identifiers which are derived from a person's sPIN by applying cryptographic one-way functions (section 0 describes this derivation process in detail).

Since it was the aim to develop an e-voting schema that is fully compliant with Austrian e-Government elements, the EVITA voting schema adopts and extends the concept of sector-specific identifiers.

The EVITA voting schema follows a two phase approach, which differs between registration phase and election phase. Therefore, the identification schema needs to be discussed and developed in two levels. On the first level, the identification schema must handle registration issues. On the second level, the identification schema must offer the possibility to determine whether or not a voter has cast her vote already.

To clarify the requirements for the identification schema, here is a list of scenarios and phases where identification is necessary:

1. **During the registration phase:** The voter requests to vote electronically using her Citizen Card.
2. **During the election phase:** In the event the voter is unable to vote electronically—due to technical problems within the voter's technical environment etc.—the voter should have the possibility to visit a polling station in order to vote conventionally (this is a design requirement for the EVITA concept). At the polling station, the election officials must (electronically) identify the voter in order to determine whether she has already cast her vote via e-voting or not.
3. **During the election phase:** In the course of casting a vote electronically, the voting system should determine whether the voter has already cast a vote or not, in order to prevent double votes.

Although the second and the third scenarios appear to contradict the election secrecy at first glance, the proposed domain separation model is able to solve the problem. Thus EVITA proposes an identification schema that is built on the established identity management concept of Austrian e-Government and makes use of two different identifiers which are loosely bound to each other using cryptographic technologies.

From an organisational point of view, there are two different domains. The registration system has to identify the voter in existing registers and databases, such as the register of voters, the Central Resident Register, etc. The representation of a voter's identity must match existing records of registers and authorities, therefore, the first form of identity is taken directly from the conventional identity management system of the Austrian e-Government, i.e. a conventional sector-specific personal identification number (ssPIN). Since these registers are used for conventional elections as well, they usually contain additional information about the voter, such as her given name, name, date of birth, etc.

The information attached to the encrypted vote must contain some identification information in order to determine whether a voter has already cast her vote and thus prevent double votes. The latter question is important when conducting a conventional election in parallel and allowing e-voters to cast their votes by conventional means as well (in the event of technical problems, etc.).

So, two different domains and two different representations of a voter's identity appear necessary:

1. The first domain is denoted as Registration Domain and it deals with identifiers taken from the conventional Austrian e-Government (such as ssPIN).
2. The second domain is denoted as Election Domain and it deals with identifiers distinct from those of the Registration Domain.

A bidirectional link must not be allowed to exist between the identity representations of both domains. Nevertheless, it must be possible to prove whether or not a given voter has already cast a vote by checking the voter's identity representation in the Registration Domain.

Only in the event that an e-voter is not able to cast her vote electronically for some reason and thus shows up at a conventional polling station to cast her vote it is legitimate to search for the existence of the voter's vote. It must be noted that this is a strict uni-directional query from a given (conventional) identity to the appropriate cast vote. In terms of identity representations, it means that a corresponding identity representation in the Election Domain should be derivable from a given identity representation in the Registration Domain but not vice versa.

The requirement is to define two identity domains and two respective identity representations in which a corresponding identity representation in the Election Domain can be derived from a given identity representation in the Registration Domain. This requirement leads to having a link between identity representations from the Registration Domain and the corresponding personal identifiers of the Election Domain. Creating this link using simple derivation mechanisms—following the mechanism used for deriving a ssPIN from a given sPIN—is not satisfactory since the identity representations of the Registration Domain are conventional e-governmental identifiers and are based more or less on conventional identification information (such as name, date of birth, etc.). Without additional measures it would be too easy to find out a citizen's identity representation in the Registration Domain, and with this information find the corresponding identity representation in the Election Domain.

The EVITA voting schema suggests creating the link between the personal identifiers in the Registration Domain and the corresponding identifiers in the Election Domain as depicted in figure 1. This sketch outlines both domains and the different forms of identifiers.

The Registration Domain deals with conventional electronic identifiers; i.e. sPIN and a sector-specific identifier which is specific to the election event (ssPIN(v)). In the course of crossing domains, the EVITA schema requires that a special personal identification number be derived that is only to be used within the Election Domain—referred to as a vPIN—from a given ssPIN(v). By applying a mathematical one-way function (HASH function), the link between the ssPIN(v) and the derived vPIN is unidirectional, pointing from the Registration Domain to the Election Domain. Furthermore, in order to have no permanent direct link between both identifiers, the derivation procedure applies secret keys.

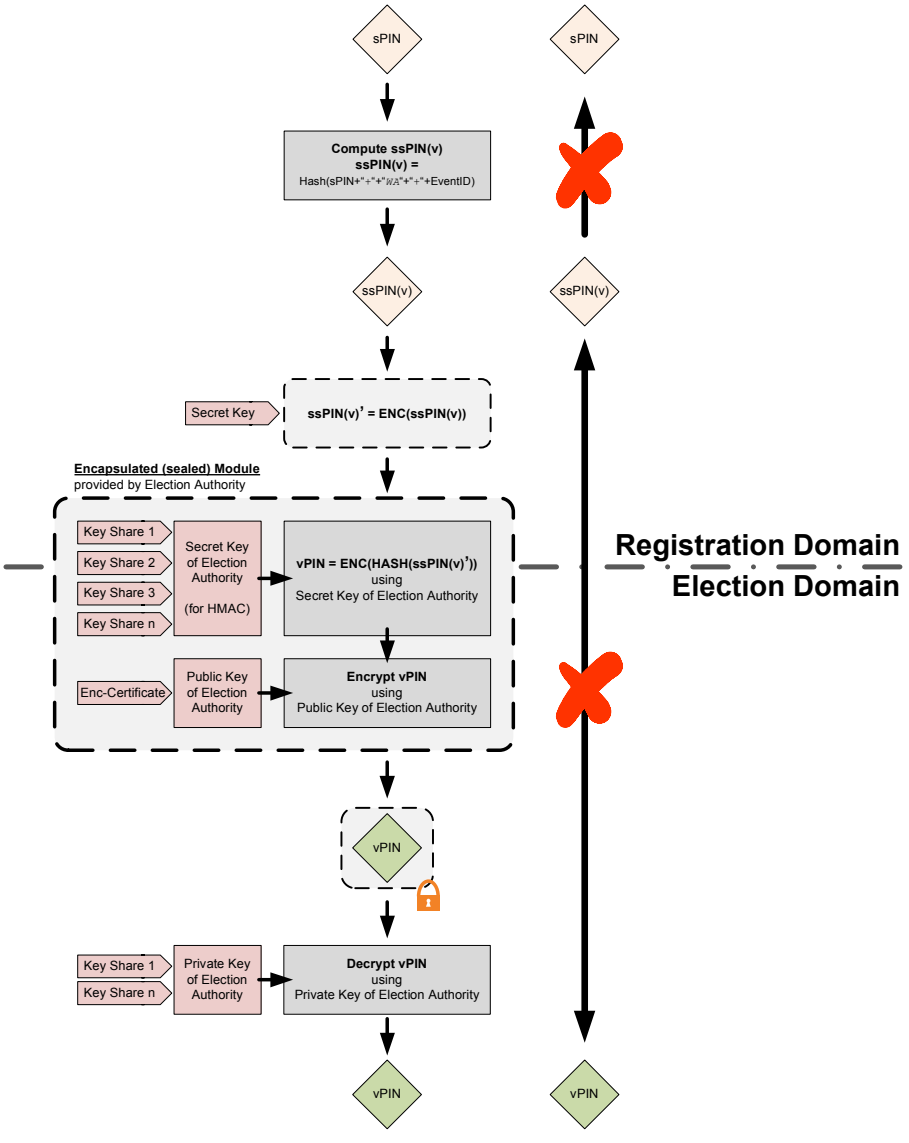

Fig. 1. Cryptographic link between Registration Domain and Election Domain

Since the link between both domains is only necessary during the election event (after election there is usually no need to search for a voter's cast vote after polling stations have been closed), the secret keys that are used to create a vPIN from a given ssPIN(v) are needed during the term of the election event only and have to be destroyed immediately after the election event. This can be ensured on a technical level by using hardware security modules for generating and holding the keys. If the hardware security modules do not provide functionality for exporting the keys, there

would not exist any copy of these secret keys outside the hardware security module, thus there would be no way to create a vPIN from a given ssPIN(v) without using the hardware security module. The link between ssPIN(v) and vPIN can be permanently broken by securely erasing the secret keys or by destroying the corresponding hardware security modules.

In order to prevent any kind of abuse, it is important to log whenever the system is used to transform a ssPIN(v) to a vPIN. The use of hardware security modules means that there is only one single point to control, so it is easy to apply both technical and organisational mechanisms to prevent abuse.

4.1 Registration Domain – Creation and Use of ssPIN(v)

The voter registers for electronic voting using a process provided in the Registration Domain. Since the application for electronic voting requires discrete identity data as well, such as the voter's name, date of birth etc., a conventional sector specific identifier is used.

The registration service usually identifies the voter using her Citizen Card. This means that the registration process has access to the sPIN, and can also find out the application-specific sectoral identifier ssPIN(v). The ssPIN(v) is the conventional sectoral identifier specific to an election. The registration application contacts registers—such as the Central Resident Register or the electronic register of voters—using the ssPIN(v). As the ssPIN(v) conforms to the conventional identification schema of Austrian e-Government, every register is able to resolve the identifier and provide the requested information.

All actions taken in the registration phase correspond to conventional governmental processes. Therefore, the personal identifier used within the Registration Domain is a conventional sector-specific personal identifier. The sectoral identifier is derived from the voter's unique sPIN following the schema defined in the Austrian identification schema [20]. The following expression shows the whole derivation process in detail:

$$ssPIN(v) = HASH(sPIN \oplus "ed")$$

sPIN	the voter's sPIN
'ed'	short-name of the sector, e.g. **e**lection and **d**emocracy (ed)
HASH	cryptographic one way function
$\oplus$	concatenation of two strings

4.2 Election Domain – Creation and Use of vPIN

In contrast to the Registration Domain, the Election Domain does not require any discrete identity information about the voter. It is not even necessary to identify the voter in person within the Election Domain since the processes of the Election Domain do not deal with identification but rather with authorisation. The election process is not interested in the unique identity of the voter. The only thing the voter has to prove is that she is eligible to vote.

There needs to be a way to track which voter has already cast a vote. This is necessary when running a conventional election process in parallel and considering the conventional election process as a fallback scenario for the electronic election. This implies that the officials at the polling station must be able to prove whether or not the voter has already cast a vote. It must be kept in mind that the voter at the polling station might only be carrying a conventional identity card, e.g. a passport, which leads to the requirement of having a link from a voter's conventional identity information through a sectoral identifier (ssPIN(v)) to her corresponding identifier of the Election Domain (vPIN).

The creation of a ssPIN(v) from a set of discrete identity information which is sufficient enough to identify the person uniquely is only possible with the help of the so called Source PIN Register Authority. Thus it is possible to determine a voter's ssPIN(v) based on the information given on her conventional identity card. As a consequence, the algorithm for creating the vPIN has to take the ssPIN(v) as input. Moreover, this creation algorithm must always yield the same vPIN for a given ssPIN(v). Since the link between ssPIN(v) and vPIN is only needed temporarily, there must be a way to remove the link relation permanently, for example, immediately after the election event. The algorithm given in the following equation achieves both requirements:

$$vPIN = HMAC\left(ENC\left(ssPIN(v)\right)_{SK_{RA}}\right)_{SK_{EA}}$$

SK_{EA}	secret key of the Election Authority
SK_{RA}	secret key of the Registration Authority
HMAC	keyed hash function; e.g. realized through ENC(HASH(x))
ENC	symmetric encryption algorithm

The algorithm for creating vPINs is a logical continuation of the ssPIN(v) algorithm. Here again the algorithm makes use of a one-way function (HASH function) in order to ensure uni-directionality. Contrary to the creation of the ssPIN(v), the algorithm for creating vPINs requires a secret security measure for both the Registration Domain and the Election Domain. This measure may be implemented in several ways, for instance by adding secret phrases or by applying cryptographic algorithms such as encryption algorithms or keyed HASH functions.

The proposed algorithm for creating a vPIN takes the previously created ssPIN(v) as input. First, the algorithm adds the secret of the Registration Domain to the ssPIN(v) by applying a symmetric encryption algorithm (e.g. 3DES, AES). Here the encryption algorithm makes use of a secret key which is under the sole control of the Registration Authority (i.e. the authority controlling the Registration Domain/Process). The resulting encrypted ssPIN(v) is further derived by applying a keyed HASH function as a one-way function. This keyed HASH function (HMAC) not only creates the HASH value for the given input but also combines it with a secret by applying a secret key provided by the Election Authority (i.e. the authority controlling the Election Domain/Process).

As a result, the link between a vPIN and the underlying ssPIN(v) cannot be created without knowing both secret keys. Thus both secret keys are important elements of the vPIN-creation algorithm, which leads to a temporary link between the personal

identifiers of both domains. In other words, both authorities have to cooperate to uncover a voter's identifier. Therefore, Registration Authority and Election Authority have to be separated by organisational means, which is common in elections.

Just involving secret keys in the derivation process as a technical measure is not sufficient. Additional organisational measures are required. The management of the secret keys is of crucial importance since possession of both secret keys enables the owner to create vPINs. Therefore, each secret key has to be provided and handled within the respective domain by the according authority and has to be handled appropriately. The use of a hardware security module is not only strongly recommended, but rather should be treated as a requirement for creating and holding the keys securely.

Figure 1 shows the proposed approach for handling both secret keys. This proposal suggests using a shared key schema for the handling of the Election Authority's secret key. The key shares should be held by the members and representatives of the election commission. In order to permanently break the link between the identifiers of both domains, it is sufficient to destroy at least one of both secret keys.

Figure 1 also highlights a second but very important issue in the vPIN creation process. Since a vPIN is created by using a specific ssPIN(v) as input, the creation process should be located within the Registration Domain. The process has to ensure that the vPIN that is created cannot be accessed by any entity in the Registration Domain. Therefore, the schema requires encryption of the vPIN for the Election Authority (Election Domain) immediately after it has been created.

Any technical implementation of the vPIN-creation process must follow the requirements stated above. In addition to all technical measures there is a strong need for organisational measures. Thus it is recommended that the Election Authority provide the technical implementation for dealing with its secret keys for the vPIN creation process by means of a sealed module (e.g. sealed hardware and electronically signed software) that contains a hardware security module holding all keys of the Election Authority (see ``Encapsulated (sealed) Module'' in figure 1).

5 Sketch of the Cast Vote and Counting Phase

For a complete understanding it is important to sketch the cast vote and counting process briefly. In order to cast a vote, the voter has simply to contact a server of the Election Authority which takes the voter's encrypted vote. As mentioned before, a cast vote consists of two parts: the inner part holding the encrypted vote which solely contains the voter's decision; the outer part holding at least the voter's vPIN in order to detect double votes and to mark which voter has cast a vote. During counting—which might take place any time later—the counting module removes the outer part of votes and just takes the encrypted inner part as input for counting. All encrypted parts become mixed up and fed into the counting device (i.e. a hardware security module) which decrypts votes and prepares the final result. The hardware security module of the counting device solely holds the private key to decrypt votes.

The EVITA approach is to decrypt the vote only at the very single moment of counting; a cast vote remains encrypted at any time before and after counting. This contrasts with other e-voting approaches where votes are decrypted before counting. However, when re-counts are considered, keeping votes encrypted is more advantageous. The

counting device holds the decryption key for decrypting the votes within the counting process. It must meet the requirements of a hardware security module in order ensure that the key cannot be exported or stolen. Furthermore, the counting device must ensure that votes are decrypted only for the purpose of counting. There must not be any chance to learn decrypted votes by accessing the counting device by any means. It is not sufficient to use a hardware security module only for the purpose of securely holding the keys. Additional critical components of the counting device—critical with respect to revealing encrypted votes unintentionally—are the counters used to compute the result. The counting device must not offer any possibility of finding out intermediate results or to observe the current status of the counting process. However, logs for recording information might be put in place throughout the counting process by the counting device in order to collect additional information that confirm the correctness of the count, e.g. for an election audit. This information also must not be disclosed to anybody during counting as it can be used to reveal cast votes.

This sketch of the counting phase is very simplified. Important details, such as an additional signature on votes (before casting) to prevent manipulation of cast votes or the mechanism of indirect voter authentication, have been omitted due to length restriction.

6 Conclusions

The proposed e-voting solution relies on two core principles: strong end-to-end encryption and stringent domain separation. Both principles are closely coupled to Austrian e-Government solutions. The latter principle especially is an extension of the Austrian identity management concept. Due to the domain separation concept introduced, the e-voting concept is able to handle unique identification of voters while protecting the anonymity of cast votes with the simultaneous possibility of gaining knowledge about whether a given voter had cast a vote already (during the election event). Thus, the proposed e-voting scenario allows voters to cast their vote conventionally at a polling station on election day even though the voter might have registered for e-voting. Allowing e-voters to cast their vote at the polling station as well—under extenuating circumstances—is an important element of the EVITA's embracing security concept which makes the EVITA concept different from other e-voting schemes. The use of the Internet inherently brings with it some risks that cannot be addressed by technical measures (i.e. network security elements, redundancy, etc.) alone, however they can be tackled by having a comprehensive technical, organisational, and legal security concept. So, allowing e-voters to cast their vote at the polling station is an organisational measure facing a possible break-down of the e-voting channel (e.g. due to DoS, etc).

References

1. European Commission for Democracy through Law (Venice Commission). Code of Good Practice in Electoral Matters (October 2002)
2. Council of Europe Committee of Ministers. Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Council of Europe (September 2004)

3. Multidisciplinary Ad Hoc Group of Specialists (IP1-S-EE). Explanatory Memorandum to the Draft Recommendation Rec(2004) of the Committee of Ministers to member states on legal, operational and technical standards for e-voting. Council of Europe (September 2004)
4. Working-Group "E-Voting". Abschlussbericht zur Vorlage an Dr. Ernst Strasser, Bundesminister für Inneres (November 2004)
5. Rössler, T.: Electronic Voting over the Internet – an E-Government Speciality. PHD-Thesis, Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Austria (September 2007)
6. Council of Europe. Convention for the Protection of Human Rights and Fundamental Freedoms (November 1950)
7. Bundesamt für Sicherheit in der Informationstechnik. Basissatz von Sicherheitsanforderungen an Onlinewahlprodukte (Version 0.18) (May 2007)
8. Gesellschaft für Informatik e.V (GI). GI-Anforderungen an Internetbasierte Vereinswahlen (August 2005)
9. Jefferson, D., Rubin, A.D., Simons, B., Wagner, D.: A security analysis of the secure electronic registration and voting experiment (serve) (January 2004)
10. Rössler, T., Hayat, A., Posch, R., Leitold, H.: Giving an interoperable solution for incorporating foreign eids in austrian e-government. In: Proceedings of IDABC Conference 2005, March 2005, pp. 147–156. European Commission (2005)
11. Cohen, J., Fischer, M.: A robust and verifiable cryptographically secure election scheme. In: Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science (FOCS), pp. 372–382. IEEE, Los Alamitos (1985)
12. Cohen, J., Yung, M.: Distributing the power of government to enhance the privacy of voters. In: Proceedings of 5th ACM Symposium on Principles of Distributed Computing (PODC), pp. 52–62. ACM, New York (1986)
13. Cramer, R., Gennaro, R., Schoenmakers, B.: A secure and optimally efficient multi-authority election scheme. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 103–118. Springer, Heidelberg (1997)
14. Chaum, D.: Untraceable electronic mail, return adresses, and digital pseudonyms. Communications of the ACM 24(2), 84–86 (1981)
15. Juang, W.-S., Lei, C.-L.: A collision free secret ballot protocol for computerized general elections. Computers and Security 15(4), 339–348 (1996)
16. Hirt, M., Sako, K.: Efficient receipt-free voting based on homomorphic encryption. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, p. 539. Springer, Heidelberg (2000)
17. Fujioka, A., Okamoto, T., Ohta, K.: A practical secret voting scheme for large scale elections. In: Zheng, Y., Seberry, J. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 244–251. Springer, Heidelberg (1993)
18. Okamoto, T.: Receipt free electronic voting schemes for large scale elections. In: Christianson, B., Lomas, M. (eds.) Security Protocols 1997. LNCS, vol. 1361, pp. 25–35. Springer, Heidelberg (1998)
19. Leitold, H., Hollosi, A., Posch, R.: Security architecture of the austrian citizen card concept. In: Proceedings of ACSAC 2002, Las Vegas, December 9-13, pp. 391–400. IEEE Computer Society, Los Alamitos (2002)
20. Hollosi, A., Hörbe, R.: Bildung von Stammzahl und bereichsspezifischem Personenkennzeichen (SZ-bPK-Algo -1.1.1). Platform Digital Austria, AG Bürgerkarte (January 2006), `http://www.ref.gv.at` (as seen on May 12, 2007)