IJCSS International Journal of Complex Systems in Science

Int. J. Complex Systems in Science
vol. **6(1)** (2016), pp. 37–57

Development of a Holistic Methodology for the Evaluation of Remote Electronic Voting System

David Yeregui Marcos del Blanco[1,†], Luis Panizo Alonso[1] and Jose Angel Hermida Alonso[2]

[1] *Mechanical, Computing and Aerospace Engineering Department, Universidad de León*

[2] *Mathematics Department, Universidad de León*

Abstract. The implantation of Remote Electronic Voting (REV) Systems to Electoral Processes is taking place at a slower pace than anticipated. One of the most relevant factors explaining that fact is the atomization of the existing solutions, fostered by a lack of harmonization in the field. In this paper, the authors introduce a holistic methodology for the evaluation of remote electronic voting systems based on their direct involvement in the matter over the last 15 years. The aim is to contribute to the establishment of a much needed standardization as a necessary step towards a broader introduction of REV solutions in elections.

Keywords: e-democracy, Internet Voting, Remote Electronic Voting, Standarization.
MSC 2000: 00A06, 00B20, 43A22

† **Corresponding author:** dmarcb01@estudiantes.unileon.es
Received: July 27th, 2016
Published: November 30th, 2016

1. Introduccion

The standardization of the Information and Communications Technologies has brought undeniable progress to countless sectors: from healthcare to leisure, e-commerce, e-banking, logistics or the labor market.

With regards to the e-democracy, the implantation has not been quite as fast as anticipated, especially when it comes to the possibility of exercising the right to vote through electronic means, namely the e-voting. The causes are varied and complex, but among them, the difficulty of reproducing the whole voting process in a verifiable yet privacy-preserving way is definitely one of the most relevant.

In addition, the very intrinsic nature of voting decisively contributes to a slower introduction. Binding elections constitute the backbone of Democracy since they bestow on the political leaders the power and responsibility to pass the bills that will regulate every sector, including the most sensitive ones, such as Defense or Sovereignty. What is at stake is of the utmost importance, and thus a wary approach prevails.

Previous attacks coming from foreign nations during e-voting pilots [1] constantly remind us how important it is to correctly assuring security when it comes to electoral democratic processes. More so in the present times, with mounting geo-political conflicts and crossed interests.

All of the aforementioned leads to a need of very strict operative standards to be applied to the remote electronic voting solutions. Ultimately, an error in an e-commerce shipment or a bank transfer can be reverted. By contrast, for political binding elections, if a fraud is detected after the new cabinet has been established, critical legislative changes may have occurred in the interim until the attack has been discovered, potentially affecting even the core of the country (Constitution, Defense etc.) and being extremely difficult to reverse.

The problems and events that surrounded the 2000 US Presidential Elections [2] were a wake-up call about the necessity to improve the technology applied to the voting processes and also served as a spur for the development of innovative remote electronic voting systems throughout the world.

A. Contribution

The vast variety of systems and lack of standards in the field of e-voting has traditionally shaped a highly atomized landscape with little harmonization. Only in 2015, the IEEE has reactivated the 1622 committee on Voting System Standards [3]. Nevertheless, the majority of solutions currently in use were developed before 2015 and have not been analyzed in a protocolized way. Therefore, it persists the need for an evaluation methodology for Remote Electronic Voting systems (REV hereinafter) firmly based on state of the art cryptographic primitives and previous experiences in binding elections.

The present article introduces a holistic evaluation methodology for REV systems based on traditionally accepted requirements with the addition of the practical expertise acquired through more than 2.000.000 votes cast over the last 15 years in real REV pilots, several of them with a direct involvement of the authors.

B. Structure of this Article

Section I introduces the cybersecurity applied to e-democracy with some relevant unsolved issues. Section II briefly elaborates on the main REV definitions and building blocks to be used in this article.

In Section III, the main requisites applying to REV systems are detailed, drawing a distinction between the *sine qua non* and those that can be assigned a value according to the degree of implementation. In Section IV, a brief review of the most relevant experiences with REV systems in real binding elections is detailed.

Section V defines a set of additional evaluation criteria extracted from the experiences in Section IV as well as other prominent pilots. With the "traditional" requirements from Section III and the additional ones obtained through more than 2.000.000 votes cast with REV systems, the authors, based on their first-hand experience in the last 15 years in e-voting assign a weighing factor to each one of them and configure the holistic review methodology in Section VI.

Lastly, in Section VII the main conclusions of this Article are presented.

2. Definitions and Building Blocks

In this article, a Remote Electronic Voting system is defined as: "A voting system used in a remote, non-controlled environment, through electronic means, in which the vote is sent partially or totally via an internet connection from a personal computer or mobile device which has not been specifically designed as a specialized electronic voting machine".

Therefore and according to the previous definition, in this paper REV does not include e-voting systems in controlled environments and/or using specifically designed machines to vote such as DRE voting devices. For those kind of e-voting initiatives, the authors recommend the research activity by Dr. Luis Panizo [4].

Elements of a REV system

Depending on the REV system implementation, the elements may slightly vary. Therefore, the enumeration is not intended to be exhaustive but rather an approximation to the standard scheme. Every component except the voter can be either a single unit or a distributed system in order to increase security (or attacking capacity for the attacker):

Voter: The person who, upon successfully authenticating, chooses a candidate/s from the candidate list, and casts the vote (preferably encrypted) through his/her personal computer or electronic device.

Electronic Ballot Box: It generally refers to the server(s) receiving the encrypted ballots from all the authenticated voters that have effectively voted. Encryption/Decryption Service: It involves the server(s) receiving the encrypted votes; decrypting and shuffling them in order to break the link vote-voter, and finally counting the votes and publishing the results.

Authority: The entity in charge of controlling that the Election takes place according to the applying laws and procedures. Usually there are several authorities in charge of different aspects in a REV system. The potential risk of collusion among them is a very relevant source of vulnerabilities.

Auditor: It is an external, independent part responsible for the critical role of verifying that the whole Election with its associated procedures and even the authorities operate according to the regulation and the approved protocols.

Bulletin Board: It is the place where all the counted ballots are displayed. In order to protect the voter's privacy, only a hash of the ballots should be published with no additional info that could lead to a security breach. The voter can verify that his/her vote was correctly counted. Nonetheless, it is worth being noted that there have been several cases of REV with Bulletin Boards which showed relevant challenges to achieve coercion-resistance [5], [6], [7].

Attacker: Malicious Entity trying to successfully attack and manipulate the elections in his/her own benefit or on behalf of another attacker without the required technical acumen.

Phases of a REV system

Similarly to the point 2.1, the phases and their implementation may vary depending on each system. Nevertheless, the most common scheme includes to following steps:

Initialization/Preparation: Carried out by the authorities, comprises the execution of the initialization protocol. It includes among other actions: update of the electoral roll, ballot design, delivery of previous information for the authentication procedure, set-up and testing of the system components, human resources training and material means organization, computation of the election's public and private keys etc.

Registration/Authentication: Each voter has to register and authenticate according to the procedure developed for the REV system. Usually, it requires some personal information such as birthday date, ID number etc., a code/PIN/password chosen by the voter and a randomized and unique string received directly from the authorities.

Voting: The voter chooses the candidate(s), encrypts the vote (generally with his/her private key and the election's public one) and sends it to the electronic ballot box.

Tallying: Once the period for REV is over, the valid ballots are counted and the results are published. The actual moment in which the votes are decrypted and counted and how these tasks are performed depends on each particular REV solution and the cryptosystem scheme implemented (refer to subsection 2.3 for details).

Verification: As a critical property to be fulfilled by the REV system, many solutions allow verifiability in one or more of its degrees: individual, universal or end-to-end.

Auditing: External and independent. Serves as a proof of the integrity of the results and the degree of compliance with the existing protocols and specifications applying to the elections and all its components.

Main REV cryptographic schemes

Blind signature: Introduced by D. Chaum in [8] and originally designed to be used in telematic payments. In 1992 Fujioka et al. [9] applied it to a voting system. It implements a type of digital signature in which the authority signs the message without having access to its content. The analogy with the carbon paper exemplifies it: the sender encloses the message in a carbon paper envelope. If the sender is successfully identified, the authority signs the envelope without opening it (hence without access to the message). A message is valid only if it includes the authority's signature. An example of a Blind Signature scheme based on RSA would be [10]:

Let (N, e) and (N, d)be respectively the public and private authority's signature.

The sender generates a random value r such as GCD(r, N) = 1 and sends to the authority:

$$v' = v \cdot r^e \ mod \ N$$

Therefore the value r is used to hide or "blind" the vote v to the authority. The authority signs the blinded vote and returns s'

$$s' = \left(v'\right)^d \ mod \ N \ = \ v^d \cdot (r^e)^d \ mod \ N$$

Since the sender knows r he/she can obtain the signature s by computing:

$$s = s' \cdot r^{-1} \; mod \; N \; = \; v^d \cdot r \cdot r^{-1} \; = \; v^d \; mod \; N$$

Once the sender receives the vote signed by the authority, he/she can send it to a set of mix-nets in order to break the link between vote and voter.

Blind Signature schemes are the most efficient ones but they have serious verifiability limitations and they also demand anonymous communication channels, very hard to obtain in practice. Therefore, blind signature based schemes are currently the least utilized for the development of REV systems [13].

Homomorphic Encryption Schemes In Homomorphic Encryption Schemes (HES), homomorphic properties are utilized in order to perform operation over encrypted votes without having to individually decrypting them first.

Let G be a commutative group of order $|G| = q$. The public key is (G, q, g, h), being g a generator of G, $h = g^x$ and x the secret key.

Let the encryption of a vote v be

$$E(v) = (\alpha, \beta) = (g^r, g^v, h^r)$$

being r a random value r $\in \{0, 1, \ldots, q-1\}$.

Fot two votes v_1 and v_2 encrypted as:

$$E(v_1) = (\alpha_1, \beta_1) = (g^{r_1}, g^{v_1}, h^{r_1})$$

$$E(v_2) = (\alpha_2, \beta_2) = (g^{r_2}, g^{v_2}, h^{r_2})$$

The additive homomorphic property is:

$$E(v_1) \cdot E(v_2) = (\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2) = (g^{r_1}, g^{v_1}, h^{r_1}) \cdot (g^{r_2}, g^{v_2}, h^{r_2}) =$$

$$= \left(g^{r_1+r_2}, g^{v_1+v_2}, h^{r_1+r_2}\right) = E(v_1 + v_2)$$

Among the biggest advantages in the implementation of HES in REV systems, the following can be emphasized: as the scheme operates over encrypted votes, no anonymous channel is required (unlike the blind signature schemes) and hence the tally process is very efficient, since there is no need to decrypt the votes one by one.

Furthermore, it is not necessary to wait until the end of the election to start tallying the votes, which in practice is a big advantage.

Regarding the disadvantages, the scheme requires that the voters provide evidence that their cast votes encode valid votes through Zero Knowledge Proofs (ZKP) [14] [15] [16]. Unfortunately, regular PC's or mobile devices usually don't have the required computational capacity to run such proofs within acceptable timeframes.

Additionally, the verification cost for HES is strongly correlated to the number of candidates and options to vote. Therefore, in elections with a significant amount of them such as in New South Wales, with up to hundreds of candidates, HES are less efficient than the mix-net based ones. One last concern is the fact that for additive schemes, the key distribution is complex because they use factorization as a trapdoor. Even assuming that there are certain relevant drawbacks, HES schemes are currently one of the two main types of implementations used in the development of REV systems (together with the mix-net scheme).

Some of the most relevant examples of HES in REV solutions implemented in political-binding elections are the New South Wales' iVote, the Norwegian system [27] or the very-well known Helios Voting.

Mixed networks or mix-nets: Introduced in 1981 by D. Chaum [17] for anonymous communications, a mix-net defines a sequence of proxy servers in which each one of them takes as input a set of ciphertexts (encrypted votes in the case of a REV system) obtained through Public Key Protocols, re-encrypts them, shuffles them following a secret permutation and sends the output to the next proxy server, which proceeds in the same way.

In real situations, the aforementioned sequence corresponds to a re-encryption mix-net, which is the most popular type in the development of REV solutions. The main reason is that, as opposed to decryption mix-nets, it suffices that

just one server is honest to guarantee the vote's anonymity.

In order to verify that every server is honest, ZKP are performed in each one of them, considerably increasing the computational complexity of the scheme.

As previously pointed out, the mix-net scheme is, together with the HES the two main groups of schemes applied in the development of REV systems.

Two of the most important advantages deriving from the use of mix-nets are that they effectively break the link between voter and vote and they are more flexible with regards to their performance in elections with relevant differences in the number of voting options, as opposed to the case of HES.

On the top of that, the fact that in mix-net based schemes, ZKP are not performed in each server reduces the risk of overloading the voter's device, usually not powerful enough for that task. Lastly, if correctly developed, it is fairly easy to achieve universal verifiability in this scheme since the output of every server is publicly accessible

Regarding the disadvantages, it is worth noting that all the computing burden eased to the voter has to be performed by the REV system. As a consequence, the amount of technical resources in order to build a dependable mix-net based REV solution is higher than that of a HES equivalent. Furthermore, the tallying cannot start until the ballot box is closed (the last server has re-encrypted and mixed the last vote), which in practice can cause important delays for bigger elections. Lastly, the mix-net scheme is more vulnerable against DDoS attacks.

3. Requirements of a Remote Electronic Voting System

After having introduced the REV and succinctly gone over the main components, phases and schemes, the next step is to define the requirements of a REV system.

The first years of the 2000's brought along an important rise in the number of countries experimenting with REV pilots. Nonetheless, the diversity in the way each country approached the experiments, with different requirements and implementations, led to a strongly atomized landscape. Recently, there has been a relative convergence among the different solutions, but there still remain important differences [18], [19].

One of the basic pillars in REV is that the system must simultaneously preserve integrity and privacy, in most cases antagonistic between them [2]. As the Council of Europe stated [22]: "The five key principles of electoral law are: universal, equal, free, direct and secret suffrage and they are at the root of democracy".

Thus, one of the vital tasks in order to formally establish the requirements of a REV system is to define the properties corresponding to the five key principles pointed out by the Council of Europe [22] (universal, equal, free, direct and secret).

The authors of this article believe that the property corresponding to the universal, equal, free and direct attributes is the end-to-end verifiability (E2Ev). With regards to the fifth one (secrecy), it is guaranteed by the privacy.

Regarding the E2Ev [20], the voter has to be able to verify that his/her vote was: i) cast as intended ii) recorded as cast iii) counted as recorded. Moreover, any voter or external verifier should be able to verify those 3 conditions, regardless of the software used [2].

With respect to privacy, the fact that the voting procedure takes place in a remote, non-controlled environment increases the challenges in order to preserve it. Another concern is the vote selling/coercion issue. The REV does not introduce the problem, but it certainly can facilitate the task for the attacker. As a consequence, it is vital that the REV system maintains a privacy protection strong enough to tackle with the threats inherent to politically binding elections.

The privacy safeguarding in REV systems has been thoroughly studied [5], [21], and currently, probably the most accepted categorization is as follows, in ascending order:

1. Vote privacy: A voter's vote is not revealed to anyone. 2. Receipt-freeness: The voter cannot obtain any information that could be used to prove an attacker the way he/she voted. 3. Coercion-resistance (CR): The voter cannot show the coercer the way she voted even if both parts cooperate. Hirt and Sako in [6] were the first demonstrating that receipt-freeness is not enough to guarantee the privacy.

Thus, the required level for a REV in politically binding elections is the highest one, the coercion-resistance.

In summary, the *sine-qua-non* for any REV system are the E2Ev and the CR, since they embody the five key principles of electoral law (universal, equal, free, direct and secret). Because of that, they will be evaluated in terms of "met/not met" for each REV.

Apart from the E2Ev and the CR, there are other required properties which can be implemented to different extents. They will also be taken into account for the evaluation methodology and each one will be assigned a weight coefficient in Section VI.

Based on the 15 year experience of the authors in REV pilots, the requirements that sum up the rest of desirable properties of a REV system are:

a. Inviolability: Referring to the REV system security and implemented through practices such as authentication gates, single-use passwords or firewalls against access through third-party programs (as happened in [32]). There will also be taken into account the following: updated security protocols both at design and implementation levels as well as the distributed and threshold policy, especially in the most critical nodes, in order to minimize the concentration of duties and the risk of collusion between the parties.

b. Usabilility: The council of Europe stated in [22] that one of the main goals of the e-voting implementation is to facilitate the vote to those groups who currently suffer bigger limitations, such as visually/hearing impaired individuals or senior citizens. Acemyan et al. showed in [23] that several of the most popular REV systems are perceived by the users as very complex; leading to an important percentage of them unable to successfully cast their vote. Hence usability remains a relevant issue to be addressed.

c. Monitoring/Auditing: Every binding election implies an authority transfer to the elected party. It reaches its pinnacle at General Elections in democracies, where each voter cedes his/her portion of sovereignty, with the winner gaining very relevant power. Thus, there is a huge temptation for attackers to influence them.

The attacks could potentially aim or even involve the authorities, and therefore the monitoring/auditing tasks are of the utmost importance and must be carried by external, independent parties throughout the whole lifecycle of the project.

To evaluate this point, the existence of auditing/monitoring protocols from the design phase to the implementation will be assessed, as well as the existence of protocolized benchmark tests and the generation of periodical, read-only logs.

d. Software Development: It must not be forgotten that when talking about REV systems, after all we mean a very complex software with several associated operating protocols. Therefore, the way in which all the requirements, policies and attributes are translated into code remains of critical importance.

As a consequence, the items to be considered include: a robust software engineering, an enhanced system compatibility, a correct implementation of the cryptographic primitives, and the access to the source code by the research community (even upon signing a Confidentiality Agreement).

e. Scalability: We refer to both hardware and software scalability (especially for the most critical operations such as user authentication, cryptographic primitives, and vote encryption, decryption and tallying) as well as

for logistic and HHRR resources. In short, the REV system must have been tested under conditions at least as demanding as the elections where it is going to be deployed. Since e-democracy is still a relatively new field, sometimes a system is put into operation without having been fully tested, entrusting the correct operation of the REV system to a theoretical scalability.
To sum up the present Section III, the requisites of a REV system are: The E2Ev and CR as *sine-qua-non* and evaluated in terms of "met/not met" and inviolability, usability, monitoring/auditing, software development and scalability as requirements that can be implemented to a different extent in each REV solution.

4. Relevant REV experiences

REV pilots became increasingly popular in the first 2000's following the US 2000 General Election scandal in Florida. Several countries launched REV pilots such as France, Germany, Holland, the UK or Norway. Each country took a unique and personal approach to the matter, contributing to a still remaining atomization. Some of them have prioritized their non-resident voters, such as the US, France or Switzerland, while others have limited the experiences to the local/regional level as in the case of Canada and Australia. Several of them decided to discontinue the pilots in the following years as happened with Holland, the UK, Norway or Germany. Due to space restrictions, only the 4 most relevant REV cases (based on their size and approach) are reviewed in this article:

Estonia: It is probably the country which has more decisively advocated for the introduction of REV as an option for every binding election since the first pilot in 2005. The generalized adoption of an electronic ID Card system in 2002 was a significant milestone that fostered a quick introduction of the REV system. The utilization rate has steadily increased, reaching a 20 percent of all the votes cast in 2011 and a 30 percent for the 2014 European Elections and the 2015 General Election [24].

The Estonian systems implements a verification system through a second channel (QR codes/mobile phone) in order to enhance security.

Nonetheless, in November 2014 D. Springall et al. released an article summarizing their experience as invited observers to the local elections of 2013 [25]. The article detailed several security flaws involving critical procedures and practices.

The Estonian authorities considered the paper and the way it was published an attack to the reputation of the country in an attempt to discredit

their REV system. They also decided that Estonia will continue offering the REV option in their elections.

To this day, there have not been reported large-scale attacks to the Estonian system, although we recommend that the authorities remain vigilant, accept feedback from experts and keep the system updated in order to avoid future security breaches.

In any case, Estonia's firm commitment to REV together with the very relevant experience accrued make the Estonian REV case a very valuable source of information and data for experts and researchers.

Norway: In the Norwegian case, the authorities decided since the very beginning to invite independent experts and researchers to take part in the design and development of the REV system, also rendering total transparency to the whole tender procedure. Furthermore, the REV pilot was given the necessary time to progress without rushing. It took more than 3 years since a Parliamentary task force was formed to evaluate the possibility of organizing a REV pilot until it effectively started (2004-2008). Subsequently, the first real pilot took place in 2011, consequently spending 3 more years in the process of tendering, designing, developing and deploying the REV system.

Therefore, the Norwegian authorities aimed at developing the best, most reliable tool to the population through total transparency (including independent experts and an open code approach) and free competition by publishing of every step of the tender.

The system itself included a multi-channel security approach with random verification codes sent by postal mail beforehand. After voting, the voter received a SMS with a code which should correspond to the one in the postal mail for the chosen option.

The Norwegian REV system was deployed twice (2011 Local Elections and 2013 Parliamentary Elections) before the project was discontinued in 2014. There is no consensus on the reasons leading to its cancelation. The team in charge and the supporters claim that it has been a political decision (the current ruling party has traditionally opposed to the REV) while the Government stated that the flaws and weaknesses of the tool caused the discontinuation [26], [27].

Be that as it may, the open and transparent approach by the Norwegian authorities has certainly established itself as a very valuable example on how to plan and implement a REV project with the aim of building the best possible system.

Canada: Unlike Estonia or Norway, Canada has not implemented a REV

pilot or even legal framework at the national level. Currently, there is no intention to develop a country-wide legislation on the matter until at least 2019 [28].

With Canada being an administratively decentralized country -with regard to REV-, Regional and Local branches can independently implement REV projects. Markham in Ontario (300,000 inhabitants) and Halifax in Nova Scotia (390.000 inhabitants) are the two biggest counties known to have utilized REV systems in binding elections.

Despite totalizing more than 2 million votes cast by REV means (the most in the world), the great atomization as well as the limited information and data on the pilots make it difficult to draw relevant conclusions. It can be said that in a way, Canada personifies the current challenges that a further implantation of the REV is facing.

As Dr. Goodman et al. states in [29], there is a need for a better standardization and a common framework in order to help the REV reach its full potential in Canada.

Switzerland: The Swiss democracy is very unique, with direct democracy customs such as referendums taking place fairly frequently. On average, a Swiss citizen votes 3-4 times per year.

Unlike Canada or Australia, the Federal Government decided to take a prominent role in the establishment and coordination of the REV initiatives since 2000. Currently, there are 3 co-existing implementations (named after the first three cantons that volunteered to implement REV back in the early 2000s) in 14 cantons: Geneve, Zurich (currently in stand-by due espionage concerns [30]) and Neuchâtel. More than 260.000 votes have been cast through REV means [31], mainly non-resident votes.

In 2014, Switzerland implemented a pioneering state-wide legislation which clearly defines verifiability-related requirements with a maximum percentage of allowed REV use associated. It has been the first such step towards harmonization and the authors of this article hope that it fosters a trend in other countries developing REV systems.

Australia: The country has managed the binding elections with the most REV-cast votes (more than 280.000) in 2015 for New South Wales' (NSW) General Election.

Previously, in 2007 there was a minor pilot involving 2.000 Armed Forces' officers deployed abroad. Nonetheless, a private, military-only network was used and it was cancelled in 2009 due to the high costs associated.

There was another experience in 2011 for NSW's Elections where 44.605

votes were cast through the REV system. Regarding the REV tool itself, NSW's authorities did not consider the coercion risk to be high and therefore coercion-resistance was not a requirement. As a consequence, insecure practices like telephone voting of telephone verification are allowed.

Moreover, although there have not been reported large-scale attacks, in [32] Halderman et. al have discovered a vulnerability that could have potentially compromised the security . We believe that not only the system itself (which has already been fixed accordingly by the vendor) but also de NSW legal framework should be reviewed in order to offer the best possible REV system to its voters.

The following Table I sums up the most relevant figures on the reviewed countries

Table 1. Relevant REV experiences in politically binding elections

Country	Period	No. Elections	Total Votes
Estonia	2003-	8	756.277
Noruega	2008-2014	2	97.644
Canada	2003-	200	2.000.000
Switzerland	2003-	200	260.000
Australia	2007-	3	326.689

5. Additional criteria deriving from relevant REV pilots in politically binding elections

After careful review of dozens of REV experiences over the last 15 years (including the ones in Section IV) and applying the expertise gathered through the direct involvement of the authors in several of the most relevant, 5 further criteria were identified to be included in the evaluation methodology:

Ex-software development: As a vital complement to software development, it encompasses all the non-software components of the REV system (hence ex-software).

Insecure practices such as poor access control, opaque tally procedures or publicly visible authority credentials have been identified [25], [32]. Thus, ex-software protocols must be designed, implemented and updated concertedly with the other criteria. It must cover at least credential policy, surveillance, permission controls and back-up.

Anti-attack protocol: Experience has unavoidably showed that attacks are on the rise. On the top of that, they are becoming more sophisticated and aggravated by geo-political tensions [1], [33].

One of the latest trends are on-demand "zero-day exploit" attacks. It is much more profitable for malicious hackers to exploit vulnerabilities (for themselves or on behalf of another party) rather than communicate the security hole to the developing company and just receive a compensation in return.

In this case, the availability of updated guidelines and preventive measures will be specially taken into account. The adaptation of the anti-attack protocol to the specific architecture and schemes of the REV system is also carefully considered.

Versatility: Comprising two components: i) different versions for different implementation schemes (HES, mix-nets etc.) and election types (referendum, multiple choice, in order etc.) ii) the development of specific versions for the groups which will benefit the most from REV systems (visually/hearing impaired, elderly etc.).

Cost: Similarly to any other project, a REV system has an allocated budget that will have an impact on the quality of the developed system.

Since the implemented solution is responsible for the safeguard of the properties inherent to democratic elections (universal, equal, free, direct and secret) as well as voter's rights, the authors consider that it is a safer option to wait until a sufficient budget has been allocated, rather than starting a project without enough resources. What is at stake is too valuable to be put at risk unnecessarily.

Maintenance: Both as i) constant software and ex-software documented updating, and ii) a robust planning and implementation of the "everlasting privacy".

The additional criteria defined in the present Section V together with the requirements in Section III, the next step is to define the evaluation methodology.

6. Methodology and weighting

The evaluation methodology is based on the requirements and criteria detailed in Sections III and V ("traditional requirements" and experience-based criteria respectively).

Thus, the set of factors to be taken into account are: E2Ev, CR, inviolability, usability, monitoring/auditing, software development, scalability, ex-software development, anti-attack protocol, versatility, cost and maintenance.

Not every criterion has the exact same importance,and the authors, based on their extensive ecperience in REV experiences over more than 15 years give each one a rating between 6 to 12 points, so the most important factors

effectively count twice as much as the least relevant ones.

E2Ev and CR: As previously stated, both conform the *sine qua non* preserving the 5 key properties for democratic elections. Thus, the rating is not in terms of a value but rather as "meets" O or "does not meet" x . In the event that the criterion is met under certain plausible assumptions, there is a third option ($\triangle$) .

Inviolability: The security policy and its implementation has a huge impact over the rest of criteria and is given the maximum weighting: 12 points.

Usability: Following the Council of Europe' guidelines on the matter [22] and since the influence of this item over the system is comparatively less intense, it is given a value of 8 points.

Monitoring/Auditing: They represent the external, independent guarantor of the voting system and its components and protocols. It is also the main source of trustable data and information in the event of an attack. It is assigned the highest weighting 12 points.

Software development: It embodies the tangible technical expression of all the REV system requirements. Its performance plays a critical role in the outcome of the election. It is also given 12 points.

Scalability: A robust scalability policy (both software-wise and resource-wise) can prevent several sources of potential weaknesses, limiting the risk of unwanted operational and logistic malfunctions. The designated weighting is 8 points

Ex-software development: Conforming an indissoluble whole with the software development throughout the whole project lifecycle: design, implementation and update. They also share an analogous level of impact over the whole system, hence the weighting is also the same: 12 points.

Anti-attack protocol: Recent REV experiences have made it clear that the risk of an incidence or attack occurring is high and on the rise [1], [32], [33]. Mounting geopolitical tensions together with a surge of cyberwarfare events and on demand attacks make it more important than ever to have an ad-hoc anti-attack protocol duly updated and hence the assigned weighting the highest one, 12 points.

Versatility: Once a REV system complies with the most critical attributes, versatility gains importance and more resources can be allocated to achieve it. Thus, it is given 6 points.

Cost: Over the last 15 years, experience has shown that even having enough resources does not guarantee success when it comes to REV. Taking into account the critical attributes that a REV system is entrusted to preserve, the associated cost of it is very important but not to the point of other critical

factors. Thus it is assigned 10 points.

Maintenance: To prevent updated attacks and properly address the everlasting privacy issue, a solid maintenance policy must be implemented. Because the anti-attack protocol also covers part of the former, the assigned weighting is 8 points.

Once we have defined the traditional requirements in Section III, added further criteria based on more than 2.000.000 votes cast through REV systems in binding elections since 2000 in Section V and assigned weighting coefficients based on the experience accrued over the last 15 years by the authors in Section VI, the holistic evaluation methodology is completed and can be resumed in the following table:

Criteria	**Weighting**	Helios	Scytl 2
E2Ev	–	△	△
CR	–	X	X
Inviolability	12	0.6*12=7.2	0.8*12=9.6
Usability	8	0.4*8=3.2	0.75*8=6
Monit./Auditing	12	0.4*12=4.8	0.85*12=10.2
SW Development	12	0.75*12=9	0.85*12=10.2
Scalability	8	0.4*8=3.2	0.95*8=7.6
ex-SW Development	12	0.3*12=3.6	0.9*12=10.8
Anti-Attack Protocol	12	0.4*12=4.8	0.8*12=9.6
Versatility	6	0.4*6=2.4	0.8*6=4.8
Cost	10	0.9*10=9	0.7*10=7
Maintenance	8	0.5*8=4.0	0.85*8=6.8
TOTAL	**100**	51.2	82.6

Table 2. Holistic Evaluation Methodology for Remote Electronic Voting Sytems

7. Conclusions

In the present article, the authors aim at contributing to a much needed harmonization of the REV systems addressing one of the main causes: the lack of standardization and evaluation methodologies.

To that end, in this paper the authors introduce a pioneer holistic methodology for the evaluation of Remote Electronic Voting systems based in three pillars: the harmonization and selection of the "traditional" requirements (both *sine qua non* and measurable), the inclusion of additional criteria based

on careful research activity over more than 2.000.000 votes cast in actual politically binding elections since 2000 and finally the accumulated expertise which the authors have gathered in their direct involvement in REV pilots over the last 15 years to assign a weighting coefficient to each factor in order to make the methodology as reliable, accurate and proportional as possible.

The authors hope that the present article can contribute to the harmonization and standardization in the field and ultimately facilitate a faster and safer implantation of Remote Electronic Voting solutions in binding elections.

As future lines of improvement, the authors suggest a further sub-division of the methodology requirements in specific, measurable items as well as its application to the most relevant VER systems to date.

References

[1] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman, *"Attacking the Washington D.C. Internet Voting System" in* **Proc. 16th Conf. on Financial Cryptography and Data Security**, (2012).

[2] U.S. Vote Foundation, *"The Future of Voting"* (2015).

[3] IEEE Voting Systems Standard Committee (VSSC). IEEE VSSC/1622: "Common Data Format for Election Equipment", *http://grouper.ieee.org/groups/1622/*.

[4] L. Panizo, *"Desarrollo de una metodología para el análisis y la clasificación de los sistemas de voto electrónico"* **Departamento de Ingeniería Eléctrica y de Sistemas y Automática, Universidad de León**, (2014).

[5] S. Delaune, S. Kremer and M. Ryan "Coercion-Resistance and Receipt-Freeness in Electronic Voting", *CSFW'06: 19th Computer Security Foundations Workshop*, 28-42 (2006).

[6] M. Hirt and K. Sako "Efficient Receipt-Free Voting based on Homomorphic Encryption", *EUROCRYPT'00* **LNCS 1807**, 539-556 (2000).

[7] D. Achenbach, C. Kempka, B. Löwe and J. Müller-Quade: "Improved Coercion-Resistant", *JETS, The Usenix Journal of Election Technology and Systems* (2015).

[8] D. Chaum. "Blind Signatures for untraceable payments", *Advances in Cryptology - Crypto'82*, 199-203 (1982).

[9] A. Fujioka, T. Okamoto and K. Ohta. A practical secret voting scheme for large scale elections, *ASIACRYPT'92* **LNCS 718**, 244-251 (1992).

[10] RSA Laboratories, EMC Corporation. "What is a Blind Signature Scheme", *http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/what-is-a-blind-signature-scheme.htm* (Acc.: Mar. 2016).

[11] J. Benaloh. "Dense Probabilistic Encryption" Clarkson University, (1994).

[12] T. ElGamal. "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms", *Advances in Cryptology: Proceedings of CRYPTO'84* **196**, 10-18 (1984).

[13] D. Schliebner. "Electronic Remote Voting". Humboldt - University of Berlin., (2011).

[14] A. Fiat and A. Shamir. "How to prove yourself: Practical solutions to identification and signature problems", *CRYPTO'86* 186-194 (1986).

[15] S. Goldwasser, S. Micali and C. Rackoff. "The knowledge complexity of interactive proof systems (extended abstract)", *STOC'85*, 291-304 (1985).

[16] M. Blum, P. Feldman and S. Micali. "Non-interactive zero-knowledge and its applications", *STOC'88* 103-112 (1988).

[17] D. Chaum. "Untraceable electronic mail, return addresses and digital pseudonyms", *ACM* **24(2)**, 84-88 (1981).

[18] S. Popoveniuc, J. Kelsey, A. Regenscheid and P. Voral. "Performance requirements for end-to-end verifiable elections", *EVT/WOTE 2010* (2010).

[19] D. Zissis and D. Lekkas. "Design, Development and Use of Secure Electronic Voting Systems", *IGI Global* **ISBN: 978-1-4666-5823-3**, (2014).

[20] J. Benaloh. "Simple verifiable elections", *Proceedings of the USENIX/EVT'06* (2006).

[21] A. Juels, D. Catalano and M. Jakobsson. "Coercion-Resistant electronic elections", *Cryptology ePrint Archive Report 2002/165* (2002).

[22] Council of Europe. Committee of Ministers. "Legal, Operational and Technical Standards for e-voting, rec (2004)", (2004).

[23] C.Z. Acemyan, P. Kortum, M.D. Byrne and D.S. Wallach. "From error to error: Why voters could not cast a ballot and verify their vote with Helios, Pret a Voter and Scantegrity II", *JETS, The Usenix Journal of Election Technology and Systems* (2015).

[24] S. Heiberg, A. Parsovs and J. Willemson. "Log Analysis of Estonian Internet Voting 2013-2015"., *Starmatic - Cybernetica Centre of Excellence for Internet Voting, Software Technology and Applications Competence Centre, Tartu University* (2015).

[25] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine and J.A. Halderman. "Security Analysis of the Estonian Internet Voting System.", *CCS 2014* **ACM 978-1-4503-2957-6/14/11**, (2014).

[26] Ministry of Local Government and Modernisation. "Internet Voting pilot to be discontinnued", *https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/* (2014. Acc.: Mar 2016).

[27] H. Nore. "Implementing E-Voting in Norwegian Elections", *New Voting Technology Consulting AS* (2015).

[28] N.J. Goodman and J.H. Pammett. "The Patchwork of Internet Voting in Canada.", (2014).

[29] N.J. Goodman, and N. Wellsbury. "Internet Voting in Ontario: Time for Overwatching Standards", *University of Toronto, Town of Ajax* (2015).

[30] Swiss Info. "Hacking fears jeopardize evoting rollout", *http://www.swissinfo.ch/eng/voting-with-a-clickhacking-fears-jeopardise-e-voting-rollout/41635672/* (2014. Acc.: Mar 2016).

[31] Office for Democratic Institutions and Human Rights. "Swiss Confederation: Federal Assembly Elections. 18 October 2015. Final Report.", (2016).

[32] J.A. Halderman and V. Teague. "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election", *VoteID 2015* (2015).

[33] J.A. Green. "Cyber warfare. A multidisciplinary analysis.", *Routledge* ISBN: 978-1-138-79307-1, (2015).