The Swiss Postal Voting Process and its System and Security Analysis

Christian Killer and Burkhard Stiller

Communication Systems Group CSG, Department of Informatics IfI,
Universität Zürich UZH, Binzmühlestrasse 14, CH-8050 Zürich
{killer,stiller}@ifi.uzh.ch

Abstract. The Swiss postal voting system builds on trust in governmental authorities and external suppliers. The federal structure of Switzerland of cantons and municipalities leads to a distributed architecture. Detailed information on the current postal voting procedure are manifested as implicit knowledge within fragmented institutions and are not easily accessible. This work serves (*i*) as an overview of the Swiss remote postal voting system, (*ii*) a detailed insight into the process flow, and (*iii*) a respective risk assessment.

Keywords: Remote postal voting, risk assessment.

1 Introduction

Around the globe, government services are becoming increasingly digitized [1]. Naturally, these efforts include electoral processes. In Switzerland, the federal government defined strategies enabling digitization for public authorities and processes, including Electronic Voting (EV) [32,11]. Private companies collaborate with Swiss authorities to actively define standards across e-Government processes [35]. The Swiss EV typically refers to *Remote* EV (REV) carried out over the internet, which is also often referred to as Internet Voting (I-Voting) [19].

According to recent studies [32], 47% of Swiss citizens would be more likely to vote if EV were available, and almost 70% of Swiss citizens welcome an EV system [21]. Despite the positive sentiment surrounding EV, a current political position proposes a moratorium on EV in Switzerland [15]. According to their initiative [15], a REV system has to be "*at least as secure as the current remote postal voting (RPV) system*". Thus, the key question is: what exactly does such a minimal level of security involve? Which security metrics and mechanisms are mandatory? In the general public perception, EV often provokes a fear of change, presuming the current RPV system to be mostly analog and tamper-proof. However, it can be argued that the current Swiss RPV system is already partially EV, since many steps already involve distributed electronic systems. Thus, defining and comparing the security properties of a REV also requires an analysis of the current RPV system in Switzerland.

Reducing cost and increasing the voter turnout by providing a convenient way to vote are important considerations for Swiss authorities [20]. By 1994,

all cantons accepted votes by postal mail. As of today, RPV is the dominant voting channel, used by approximately 90% of the voters in Switzerland [16]. Most eligible voters in Switzerland show trust in the authorities on the federal, cantonal, and municipal level to handle electoral processes and protect voter privacy [32]. The trust placed in authorities encompasses state-owned companies, which are important stakeholders in the current RPV system.

Due to the federal and decentralized structure of Switzerland, each canton and municipality autonomously manages their respective jurisdictional electoral procedures. Cantons and municipalities execute a degree of independence in decisions on how to handle certain parts of the voting process. Therefore, the current RPV system in Switzerland is neither universally documented or specified, nor homogeneous across entities.

This paper, therefore, summarizes major related work and terminology to formalize the Postal Voting Process Flow (PVPF) in Switzerland. The approach taken formalizes the PVPF in a step-based model, for which major assumptions made, such as trust, people involved, and technology applied, are made explicit, if known. The dedicated interpretation of social trust assumptions is discussed within Sec. 3, along with the risk analysis, weaknesses and strengths of a person-based RPV approach. Finally, the paper performs an overall risk assessment in Sec. 4, providing the basis for discussions of security-relevant comparisons to REV or I-Voting, while Sec. 5 draws main conclusions.

2 Legal Background and Related Work

Switzerland is organized as a decentralized system of municipal and cantonal entities, working together under the umbrella of the Federal Government. The federal structure is also mirrored in the legal framework (*cf.* Figure 1). At the root rests the Federal Constitution of the Swiss Confederation, wherein Art. 39 [6] forms the basis for the Federal Act on Political Rights (BPR) [8]. In turn, Art. 91 BPR [8] is the foundation for the Federal Decree for Political Rights (VPR) [9]. On a cantonal level, the VPR builds the foundation for the Cantonal Decrees (*e.g.*, for the canton of Aargau [7]). Every canton is an independent legal entity and defines its own constitution on the basis of the Federal Constitution.

The political system is under the authority of the cantons, *i.e.*, cantonal laws and ordinances regarding political rights define elements for these processes. Various aspects of those elements are relevant for the RPV system in Switzerland, and each canton has its own decrees regarding political rights. The federal structure is mirrored down to the municipal level: each municipality decides on certain processes, again, aligned to cantonal laws and decrees. For instance, keeping record of the electoral register is under the authority of municipalities, leading to different approaches.

A direct comparison of the Swiss RPV system to REV was performed in [29]. Other countries discuss the usage of RPV critically because the secrecy of the ballot cannot be fully ensured [29]. From a practical standpoint, thorough documentation is the easiest way to achieve verifiability for RPV. Supervisory bodies

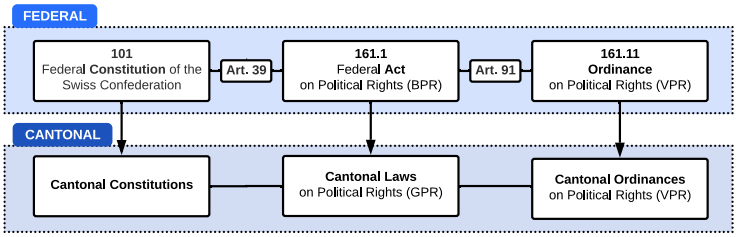

Fig. 1. Swiss Legal Framework

and authorities should check the documentation and verify it [29]. Also, trust is crucial for all voting methods. And the relationship between verifiability and trust is neither linear nor one-dimensional. Technical measures are not sufficient to create trust, sociopsychological aspects also have to be considered carefully. An extended literature review is provided in [18] with a focus on Switzerland, but also outlining the work done in Canada [22], Estonia [19], and Australia [30].

In order to analyze the RPV system with a focus on security aspects, the US National Institute for Standards Technology (NIST) serves as reference, outlining and standardizing terminology on the "Effort, Detection and Impact levels of Threat Events" [26,33,34]. Past work applied such principles to a RPV system used in the United States [25]. To consistently apply terminology, Table 1 defines the corresponding terminology used in Swiss legislation and their English translations.

Tab. 1. Official German Terminology with Corresponding English Translations

German	English
Zwei-Weg Abstimmungskuvert	Two-Way Voting Envelope (VE)
Abstimmungsresultat	Voting Result (VR)
Erwahrung des Abstimmungsresultates	Legally valid determination of VR
Die Schweizerische Post	The Swiss Post (SP)
Stimmkuverts	Paper Ballot Envelope
Stimmrechtsausweis	Voting Signature Card (VSC)
Stimmregister	Electoral Register (ER)
Stimmzettel	Paper Ballot (PB)
Vertrauenswürdiger Dritter	Trusted Third Party (TTP)

3 Postal Voting Process Flow (PVPF) in Switzerland

This section details the illustrated Postal Voting Process Flow (PVPF) in-depth (*cf.* Figure 3), containing an end-to-end process as it is currently implemented in Switzerland. The detailed sub-steps are formalized and vary between cantons and municipalities. However, the general process adheres to the federal laws and

ordinances. The PVPF is divided into six main phases from A to F, each phase containing one or multiple sub-stages from 1 to N (*cf.* Figure 2). The ensuing subsections are structured according to the PVPF within Figure 3 and describe all the different steps in detail.

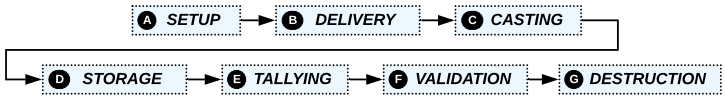

Fig. 2. Paper Voting Process Phases

3.1 Setup Phase

The Setup phase A contains four sub-stages 1-4 describing the production and assembly for dispatch of all necessary ballots and envelopes(*cf.* Figure 4). The two-way Voting Envelopes (VE), the Voting Signature Cards (VSC), the Paper Ballot Envelopes (PBE), and the Paper Ballots (PB) are the physical artifacts produced in the Setup phase. The secure execution of the Setup phase is crucial, since all following phases rely on the sound production and assembly of those artifacts. The main stakeholders of this phase are the municipal and cantonal authorities supervising the process. Due to cost, time, and capability constraints, Trusted Third Parties (TTP) support the authorities during the Setup phase as External Suppliers (ES).

Production of voting envelopes: In Step 1, the certified two-way VEs are produced by an ES. In the canton of Aargau, the municipality secretaries place a centralized buying order [28,17] for the two-way VEs at least a year in advance. After production, the VEs are distributed among the municipalities. In municipalities where Step 3 is outsourced, the VEs are directly delivered to the corresponding ES. The exact process steps are under municipal authority and can differ accordingly. Some cantons contract a single ES to handle the complete Setup phase A, mainly due to the special requirements of EV systems [10].

Production of Paper Ballots and Voting Signature Card: Step 2 consists of the production of the PBs and the VSCs. The printing of VSCs and PBs is predominantly commissioned to an ES. Each political layer in Switzerland (Federal, Cantonal and Municipal) commissions the PBs within their legal responsibility, *i.e.*, the production of federal referendum PBs are commissioned by the federal government, cantonal PBs are commissioned by the cantonal authorities, and municipal PBs are commissioned by the municipal authorities.

A VSC contains the name and address of the eligible voter, embedded within a template customized by the municipality. It is essential that the printed credentials are valid, since the assembled VE is delivered to the credentials printed on the VSC. The voter has to sign the VSC for the ballot to be valid. A substantial amount of ballots are not counted because many VSCs remain unsigned.

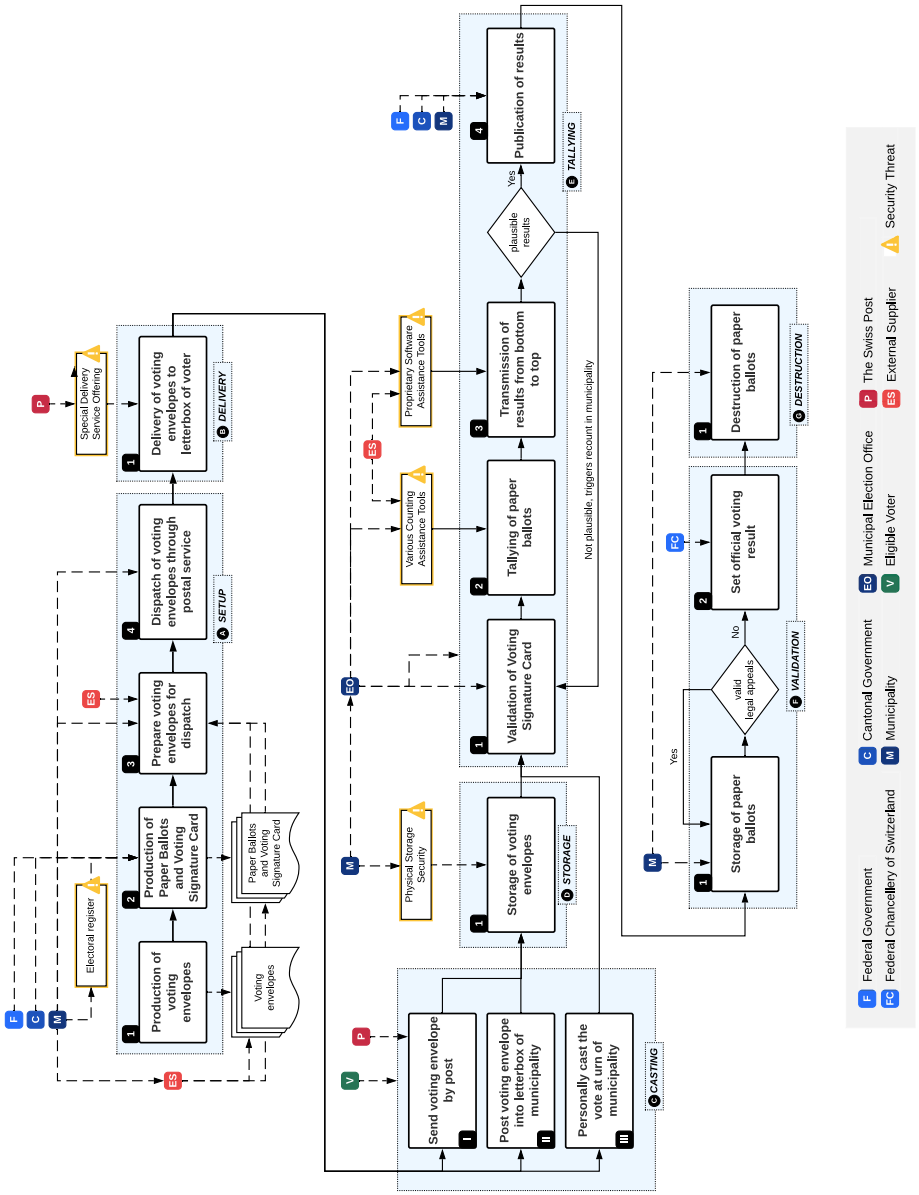

Fig. 3. Paper Voting Process Flow (PVPF)

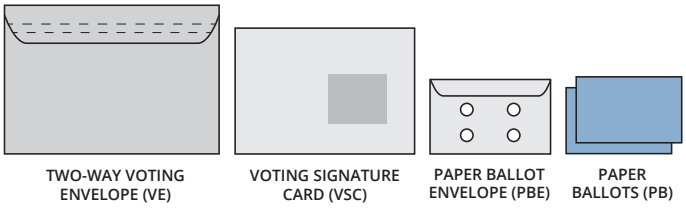

Fig. 4. Abstract representation of the necessary paper artifacts

The individual VSCs are printed according to an electoral register (ER). The ER is a centralized register containing all eligible voters. The ER is under the authority of each municipality. Neither the cantonal, nor the federal authorities have copies of the ER [28].

Since most municipalities contract an ES for the printing of the VSCs, a dataset containing the eligible voters needs to be transferred to the corresponding ES. Most municipalities export a file from the ER (*e.g.*, XLS, CSV) and send the snapshot to the ES directly via email [31,27]. The transmission of an unencrypted, unsigned dataset via standard email is critical, since the dataset could be tampered with (*e.g.*, the creation of fake identities, entries being removed), either after the export, during transmission, or when the export file reached the ES. Most ERs are administered by proprietary software systems provided by companies targeting Swiss public administrations. Some cantons also provide process checklists to municipalities. For instance, the election office (EO) of the Canton of Aargau provides such checklists [17]. These checklists state that the number of VSCs should be identical to the number of eligible voters present in the ER. If issues arise, an *in-depth* manual control should take place. Whether or not to adhere to these checklists is under the authority of the municipality. Also, since printing and assembly of the VE is mostly done by ESs, the ES should verify the integrity of the printed artifacts (*e.g.*, content and amount).

Prepare voting envelope for dispatch: Step 3 concerns the final assembly of the VEs. For each eligible voter (*i.e.*, each VSC), a VE containing the VSC, PBs, and the PBE is assembled (*cf.* Figure 4). The assembly is a monotonous task, often outsourced to ESs or social institutions and foundations [18]. Receiving an incomplete VE increases the possibility of the voter's abstention. According to cantonal checklists [17], handing out new PBs is only allowed if the voter can *make the loss credible*. Then, the voter's credentials should be recorded to check for attempted dual voting in the Tallying phase E [17].

Dispatch of voting envelopes through postal service: The final step involves the dispatch of the assembled VEs. In some municipalities, the VEs are directly dispatched by the ES commissioned with the assembly of the VEs. The Swiss Post (SP) offers a special service [14] for the dispatch and delivery of VEs.

3.2 Delivery

In Switzerland, the postal market was partially deregulated in 2009 [13]. Still, the SP maintains a monopoly on postal letters below 50 gr. Therefore, the SP is a crucial TTP, since the secure delivery to the municipality falls under the responsibility of the SP. When using the special service provided by the SP, VEs can be dispatched on a work day in the week prior to the specified delivery week [14]. Then, the SP guarantees the delivery of the VEs will take place during the specified delivery week [14].

3.3 Casting

Phase C outlines the three different options to cast a vote. The vast majority of ballots are not cast at the urn [16]. Statistics do not indicate whether VEs arrive through postal services (I) or were delivered to the letterbox by the voter (II).

I: The most popular way to cast the vote is to *send the VE by postal mail*. Some cantons pre-stamp the VSCs, which can then be used to return VEs free of charge [3]. For the voter, it is impossible to verify whether the ballot was successfully delivered to the municipal office. The SP offers the ability to track deliveries for an additional cost.

II: Thus, a favoured alternative is to *deliver the VE into the letterbox of the municipality*, which is then emptied by municipal officials and safely stored. According to [12], this option is still a favoured option by many voters.

III: The third option is to *personally cast the ballot at the urn*, which guarantees ballot secrecy. Casting ballots at the urn remains the most secure option to cast a vote, since the PBE (containing the ballot) is directly cast into the urn and separated from the VSC (containing the voter's credentials and signature).

3.4 Storage

Phase D deals with the storage of VEs that were delivered via postal service (I), or directly cast to the municipal letterbox (II). Often, an employee is tasked to fetch the postal mail addressed to the municipal office. During votes, the VEs are collected from the SP and municipal letterbox, and then carried to the safe storage location. Past incidents describe where municipal employees misused that trust [4]. The storage safety varies heavily, depending on the municipality. The Federal Act for Political Rights (BPR) [8] does not specify any security requirements. Additional considerations include the exact definition of an access control for the VE storage, (*e.g.*, Who should have physical access to the VEs?). Also, the definition of a process for incoming VEs can increase process security (*e.g.*, How many ballots arrived at which date and time? Who got the ballots from the letterbox or postal office and transported them where?).

Thus, stricter access control and a secured ballot arrival process can maximize the physical storage security. In practice, physical storage security is not prioritized, since the municipal infrastructure is often not sufficiently equipped [27,31].

3.5 Tallying

Phase E specifies the process of tallying. The main stakeholders of phase E are the municipality and the local EO. The tallying is not regulated on a federal level and is heterogeneous among cantons and municipalities [29].

Art. 14 No. 1 BPR [8] states that every polling station should create a report containing the total number of eligible voters, the total eligible voters living abroad, the total of blank, invalid, and valid ballot papers, and the number of votes in favour and against the proposal [8]. Thus, the BPR serves as a federal guideline, without specific requirements regarding the tallying process.

Approximately 10% [23] of the ballots cast are counted with the help of Electronic Counting (e-Counting) tools, provided by ESs. The parliamentary control of the administration investigated e-Counting and concluded that the federal requirements are neither functional, nor practical, and the control mechanisms of the federal government are not sufficient [23].

Tallying of all ballots: The local EO usually hires paid and elected helpers to assist with the manual counting. In large cities, thousands of helpers are engaged to count the paper ballots [24]. The EO defines the details of the tallying process. Some municipalities use e-Counting solutions or deploy high-precision scales to weigh PBs and derive the tally from averaging the weight of (sometimes pre-counted) batches.

Transmission of results from bottom to top: According to Art. 14 No. 2 BPR [8], the cantonal government is responsible for compiling provisional results from the entire canton and notifying the Federal Chancellery (FC) of the results, and publishing the same result in the Cantonal Gazette (or a special issue thereof) within 13 days of the polling day. As soon as the EO concludes tallying, the result is transmitted from the municipal EO to the cantonal EO, and from there to the FC. Some cantonal EOs deploy dedicated software systems to verify results using statistical methods. Also, most cantons make use of software provided by ESs to transmit the results. Thus, this phase also includes the use of web-based assistance tools [18].

Publication of results: The tallying phase is finalized with the publication of all results on the municipal, cantonal, and federal level. Generally, the FC publishes the collected results from the Cantonal Chancelleries in the Federal Gazette. Cantons publish the results and protocols in their Cantonal Gazettes. Each municipality publishes a final tally and tallying protocol with respect to the cantonal law. Mostly, the publishing process is performed by uploading documents to a public web-server and displaying print-outs outside the municipal offices.

Validation: Art. 15 BPR [8] defines the validation and publication of the results. The official results can only be declared when no valid appeals are in process at the Swiss Federal Court. After that, the official result is published by the FC in the Federal Gazette and can not be appealed anymore.

Storage of paper ballots: Before the results are ascertained, the counted PBs and VSCs have to be safely stored in the municipalities. It is important that the ballots remain unaltered because a recount could be triggered before the

official result is determined. Past cases have shown that premature destruction of the PBs and VSCs made a full re-count impossible [2].

Set official voting result: As soon as no more valid appeals are with the Federal Supreme Court, or as soon as a decision has been made on such an appeal, the legally valid voting result can be determined. According to Art. 15 No. 2 of the BPR [8], the validation decree shall be published in the Federal Gazette. The officiation by the Swiss Federal chancellery finalizes the Validation phase. Since a recount is no longer possible and the result is *untouchable*, the final phase can be started.

3.6 Destruction

The final phase, G, involves the destruction of the stored VSCs and PBs. According to Art. 14 No. 3 BPR [8], "*following validation of the result of the vote, the ballot papers shall be destroyed.*" In practise, the destruction is usually done by physically shredding all PBs and VSCs [27].

4 PVPF Risk Assessment

A risk signifies the level of impact on the operation of an information system's task, given the potential impact of a threat and the likelihood of that threat occurring [5,34]. Therefore, a risk assessment (RA) serves as the identification and determination of the impact of vulnerabilities that an adversary can exploit. A threat covers any event with a potentially adverse impact on the assessed process [26]. With respect to the RPV in Switzerland, threat sources are groups or individuals who could feasibly attack the RPV system. Threat sources can stem from insiders or external adversaries. All Threat Events (TE) in the following RA are general in nature and require multiple co-conspiring hostile individuals or groups to achieve a large-scale effect. The effort for each threat defines the relative level of difficulty of performing a successful attack based on a threat [25]. Three relative levels of effort are defined:

- **Low** (−): An attack requires little / no resources or detailed knowledge of the system.
- **Moderate** (○): An attack requires significant resources (or the ability to obtain these resources) or knowledge of the system. Inside attacks involving a small number of co-conspirators fall into this category.
- **High** (+): An attack requires excessive resources, in-depth knowledge of the system, or even access to the systems. It also requires specific tactics, techniques, and procedures [26]. Insider attacks involving a large number of co-conspirators fall into this category [25]

Detection describes the relative level of difficulty to notice whether a particular threat has been executed in an attack [25]. Thus, attacks are more severe when they remain undetected. Three estimated levels of likelihood of detection exist [25]:

– **Low** (−): An attack is unlikely to be detected without extraordinary resources.
– **Moderate** (∘): An attack may be detectable, but could require a large amount of resources and time. Such attacks are unlikely to be detected during the election.
– **High** (+): An attack would most likely be detected, given proper monitoring.

The impact on PVPF was analyzed according to [26] with the focus on confidentiality (C), integrity (I), and availability (A) as defined in [33]. Some TEs - all are shown in Tab. 2 - are interdependent or can be combined as depicted in Figure 5. The following RA serves as a major discussion of potential TEs that can lead to a loss of voter confidence. The mitigation of identified TEs concerns the actions of establishing trust and confidence in a system.

Tab. 2. Threat Events on the Swiss Postal Voting Process Flow (PVPF)

Phase	TE	Description	Effort	Detection	Impact
A	**TE1**	Delay production of physical artifacts	−	∘	$A+$
A	**TE2**	ER master records	+	∘	$I+$
A	**TE3**	ER data snapshot	∘	∘	$I+$
A	**TE4**	Forge physical artifacts	+	∘	$I∘$
A	**TE5**	Steal assembled VEs before dispatch	∘	+	$I+$
B	**TE6**	Re-route VEs	*unknown*	*unknown*	$A+$
B	**TE7**	Steal VEs from voter letterboxes	∘	+	$A∘$
C	**TE8**	Steal VEs from municipal letterbox	∘	∘	$I∘$
C	**TE9**	Re-route VEs	+	∘	$C+$
C	**TE10**	Cast stolen or forged VEs	∘	∘	$I∘$
D	**TE11**	Access stored VEs	−	−	$I+$
E	**TE12**	Manipulate tallying	+	∘	$I+$
E	**TE13**	Manipulate final tally	+	∘	$I+$
F	**TE14**	Initiate premature destruction	−	+	$I+$
G	*no major threat events identified*				

4.1 Risk Assessment Phase A

The Setup Phase A produces all the necessary artifacts for the secure execution of the whole PVPF.

TE1 describes the *malicious delay* of $A1$ and $A2$ in the PVPF. For instance, delaying the production can be achieved by targeting contracted ESs or directly attacking the municipal information systems.

TE2 describes the *tampering of the ER master records*. Often, the ER is provided and deployed by an ES. A targeted attack of an ES provider or municipal information systems with access to the ERs creates the ability to tamper with ER master records. The modification of master records can damage the integrity of ER data and the exported subset of eligible voters.

TE3 describes the *tampering of ER snapshot data*. Instead of modifying the ER master records, the snapshot used to print the VSCs can be modified. When the snapshot is neither digitally signed nor encrypted, an adversary could modify the data before, during, or after transmission to the ES.

TE4 describes the *forgery of physical artifacts* with (stolen) digital templates. If an adversary gains access to digital templates used to produce the physical artifacts, the adversary can forge VSCs and PBs. Additional information may be necessary to obtain (*e.g.*, weight and type of paper used). PBEs and VEs may also be forged, stolen, or even ordered from an ES. Since most municipalities do not perform a validation of incoming VSCs (by comparing the list of eligible voters with incoming VSCs), the attack can remain undetected. Practically executing TE4 requires a high effort and specific knowledge of the PVPF down to a municipal level.

TE5 describes the *physical theft of the assembled VEs*. By stealing assembled VEs, the adversary can either destroy or cast ballots. The detection of this threat event relies on individual voters noticing that they did not receive their VEs, *i.e.*, the detection probability increases with every voter notifying municipal authorities.

The integrity and availability of ER is crucial for the Swiss RPV. By targeting ERs, substantial damage can be inflicted on data integrity, but also on trust in local authorities and can undermine voters' confidence. Requirements for EV systems can serve as a reference for process improvements [10].

4.2 Risk Assessment Phase B

The Delivery phase B is a black-box. The internal processes of the Swiss Post (SP) are not publicly available. When using the dedicated SP service to dispatch and deliver VEs, the VSC design must adhere to special layout rules to facilitate automatic batch processing [14]. The special layout of VEs could simplify identification of VEs, but requires an adversary to achieve partial control of the SP routing system. To achieve such control, a hostile individual or group can create an Advanced Persistent Threat (APT) within the SP and from there, *e.g.*, identify VEs according to specific attributes and re-route identified VEs, or attempt to delay the delivery deliberately.

TE6 describes the *re-routing of VEs*. This TE requires adversarial access to internal SP systems and the capability to covertly manipulate the postal routing. A re-routing may require a co-conspiring postal employee because re-routing a large number of VEs could raise suspicion. Assuming a successful re-routing of VEs, the adversary is offered multiple options: Either to destroy the VEs, or open, modify, and re-cast them (*cf.* Figure 5).

TE7 describes the *theft of VEs from voter letterboxes* before successful retrieval by the recipient voter. In contrast to TE5, TE7 requires the adversary to steal from individual letterboxes, not only at a single location. Similar to TE5, detection increases with every voter noticing the absence of VEs.

Phase B is characterized by the trust placed in one large entity, the SP. Thus, the effort and detection probability of TE6 can only be analyzed with additional information or access to internal SP systems, operations, and processes. Generally, however, an insider can achieve a low detection with moderate effort.

4.3 Risk Assessment Casting Phase C

TE8 describes the *theft of VEs from the municipal letterbox*. As shown in Figure 5, stolen VEs can either be destroyed or opened and modified.

TE9 describes the *re-routing of VEs (before delivery to the municipality)*. Similar to TE8, re-routing offers two different options: either the adversary can decide to destroy the VEs, or open, modify, and re-cast. Similar to TE6, a co-conspiring postal employee is crucial, since delivering a large amount of VEs to a different location than the authorities may alarm an honest employee.

TE10 describes the *casting of stolen or forged VEs*. An adversary can attempt to cast stolen and modified or forged artifacts to influence the voting result. The interdependence among TEs is visualized in Figure 5.

In official logs provided by the municipalities, there is no differentiation between channels I and II, both count as delivered by the SP. Even though 90% of votes are cast through I and II, keeping III remains crucial: Multiple channels strengthen confidence in results because it enables cross-channel comparison with statistical methods.

4.4 Risk Assessment Storage Phase D

TE11 describes TEs originating from *physical storage security*. Depending on the municipality, one or N employees have access to the cast VEs. The access to VEs offers similar options as presented in Figure 5. Since most municipalities do not log the amount of incoming VEs, the destruction of VEs can remain undetected.

The physical access to the ballots stored allows an adversary to either destroy VEs, modify them, or open VEs and break ballot secrecy. As past incidents show [4], access control to the stored VEs is a again a question of trust.

4.5 Risk Assessment Tallying Phase E

TE12 describes the *risk of manipulation during tallying*. According to [23], over 10% of ballots cast in Switzerland are electronically counted. In 2014, sample checks identified errors in these counting mechanisms and concluded that e-Counting is neither more exact nor more secure than manual counting [23]. The manipulation of e-Counting requires an adversary to write targeted malware to influence the counting mechanism in his favor.

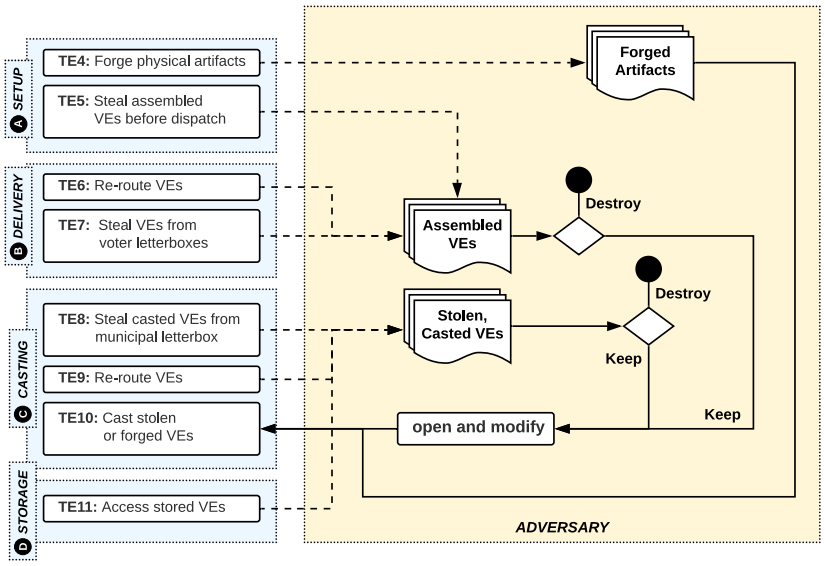

Fig. 5. Threat Event Interdependencies

TE13 describes the possible *manipulation of the final tally*. Some cantons use proprietary software to handle vote transmission from municipalities to the cantonal EO [18].An adversary with access to these tools can tamper with the final tally. Since the manual tallying process produces logs published on a municipal level, large discrepancies can be detected by attentive observers. However, a sophisticated adversary can anticipate that and tamper with all digital traces to further obfuscate detection. Hence, the risk increases when PBs were exclusively counted electronically, without any redundancy from manual counting.

The tallying phase E builds on the integrity of each and every individual member of the municipal Election Offices (EO). The distribution of trust builds the cornerstone of the Swiss RPV system.

4.6 Risk Assessment Validation Phase F and Phase G

TE14 describes the *prematurely initiated destruction* of the PBs and VSCs. The destruction of PBs and VSCs before validation by the FC makes full recounts impossible, which already occurred in 2011 [2].

Since the validation finalizes and validates the official result within Phase G, a recount is no longer an option. Also, PBs are now irrelevant, since legal appeals are impossible at this point.

5 Conclusions

The Swiss postal voting system is highly successful, because substantial trust is placed in third parties, which includes a wide range of governmental authorities, state-owned companies, and various private companies and suppliers, and the individual voter. The current Remote Postal Voting (RPV) system is inherently built on external suppliers and trusted relationships among all parties involved. For a regular citizen, the current process is hard to decipher. Thus, this paper provides a coherent insight into the Postal Voting Process Flow (PVPF) and identifies its weaknesses as well as strengths with practical examples.

The main advantage of the current RPV system is its physical decentralization, which is undercut by using centralized information systems to administer or transfer crucial data (*e.g.*, Electoral Registers (ER) or Web-based assistance tools to transmit votes). Many aspects regarding the ER, assistance tools, the Voter Signature Card (VSC), or the physical storage of voting envelopes offer room for improvements from a security perspective.

The deployment of a Remote Electronic Voting (REV) system potentially decreases the necessary amount of trust placed in institutions and people, shifting trust to verifiable processes instead [29]. As this work showed, assessing the risks of the Swiss RPV system is reliant on the specific process across governmental entities. This work identified crucial Threat Events (TE) and showed that the system cannot serve as a suitable reference for electoral processes [15].

Furthermore, the Swiss federal structure leads to fragmented processes across jurisdictional barriers, from federal to cantonal, down to municipal authorities. The real-world deployment of the threat events identified requires a group of hostile individuals with specific knowledge. In small municipalities, authorities and citizens are intertwined and manipulations would either be not widely effective or detected rather swiftly. In large municipalities or large cities, processes are secured. Releasing an attack would require substantial effort from an attacker. Hence, an attack on the RPV is most likely to be successful in medium-sized municipalities, *e.g.*, where processes have not yet adapted to the larger size of the formerly smaller municipality.

Apparently, federal laws are not complete yet in guiding the deployment of secure e-Counting tools [23]. Thus, the compilation of an open and transparent list of all the electronic tools in use in the current PV flow can help to identify further threat events and enable the design of mitigation measures to handle risks better. Further, the Risk Assessment (RA) needs to be extended and ultimately applied to full real-world processes of cantons. In turn, TEs identified can be assessed in more detail and improvements can be provided to act as a comparison to EV systems.

Acknowledgements

The authors would like to thank Anina Sax, Annina Zimmerli, Dr. Christian Folini, Marco Sandmeier, and Dr. Benedikt van Spyk for their valuable input.

This paper was supported partially by (a) the University of Zurich UZH, Switzerland and (b) the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement No. 830927, the Concordia project.

References

1. Andersen, K., Medaglia, R., Vatrapu, R., Zinner Henriksen, H., Gauld, R.: *The Forgotten Promise of E-Government Maturity: Assessing Responsiveness in the Digital Public Sector*. Government Information Quarterly, Vol. 28, Issue 4 , October 2011, pp. 439–445
2. Berner Zeitung: *Stimmzettel fehlen, Nachzählung über Motorfahrzeugsteuern ist gefährdet*, August 2011, [Online] `http://pvpf.ch/bz-pb`, last visit July 9, 2019
3. Bühlmann, M.: Schweiz am Sonntag, Aargauer Zeitung: *Das Stimmcouvert per Post verschicken - ein Gratisangebot, das viele Aargauer ausschlagen*. [Online] `http://pvpf.ch/az-ve`, February 2016, last visit July 9, 2019
4. Bumbacher, B.: Neue Zürcher Zeitung: *Hauswart fälscht aus Frust Stimmzettel bei Gemeindewahl*, October 2005, [Online] `http://pvpf.ch/nzzfraud`, last visit July 9, 2019
5. Computer Security Division, Information Technology Laboratory: *Minimum Security Requirements for Federal Information and Information Systems*. (FIPS PUB 200), US Department of Commerce, NIST, March 2006
6. Der Regierungsrat des Kantons Aargau: *101 -Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (Stand am 23. September 2018)*. [Online] `http://pvpf.ch/bv`, last visit July 9, 2019
7. Der Regierungsrat des Kantons Aargau: *131.111 - Verordnung zum Gesetz über die politischen Rechte (VGPR) in Kraft seit 01.01.2013, Beschlussdatum: 30.05.2012)*. [Online] `http://pvpf.ch/vgpr`, last visit July 9, 2019
8. Der Schweizerische Bundesrat: *161.1 Bundesgesetz über die politischen Rechte (BPR) (Stand am 1. November 2015)*. [Online] `http://pvpf.ch/bpr`, last visit July 9, 2019
9. Der Schweizerische Bundesrat: *161.11 Verordnung über die politischen Rechte (VPR) (Stand am 15. Januar 2014)*, [Online] `http://pvpf.ch/vpr`, last visit July 9, 2019
10. Die Schweizerische Bundeskanzlei: *Anforderungskatalog Druckereien fur Vote électronique*, [Online] `http://pvpf.ch/bkreq`, last visit July 9, 2019
11. Die Schweizerische Bundeskanzlei: *Vote électronique*, [Online] `http://pvpf.ch/ve`, last visit July 9, 2019
12. Die Schweizerische Bundeskanzlei: Änderung des Bundesgesetzes über die politischen Recht). Erläuternder Bericht zur Vernehmlassung, December 2018
13. Die Schweizerische Post AG: *Das Briefrestmonopol - Finanzierungspfeiler für die Grundversorgung*, [Online] `http://pvpf.ch/spmon`, last visit July 9, 2019
14. Die Schweizerische Post AG: *Factsheet, Briefe Wahl- und Abstimmungssendung*, [Online] `http://pvpf.ch/spfs`, last visit July 9, 2019
15. E-Voting-Moratorium: *Initiativtext*, [Online] `http://pvpf.ch/evmor`, last visit July 9, 2019
16. Grühnenfelder, P.: Neue Zürcher Zeitung: *Digitale Demokratie verlangt Pioniergeist*, September 2015, [Online] `http://pvpf.ch/nzzpio`, last visit July 9, 2019
17. Kantonales Wahlbüro Aargau: *Wahlen und Abstimmungen, Checkliste Allgemeine Arbeiten (Rahmenorganisation)*, November 2017

18. Killer, C., Stiller, B.: A Flow Analysis of Today's Swiss Postal Voting Process and a Respective Security Scrutiny. IfI Technical Report No. 2019-02, Department of Informatics IfI, University of Zurich, April 2019
19. Krimmer, R., Triessnig, S., Volkamer, M.: *The Development of Remote E-Voting Around the World: A Review of Roads and Directions*. First International Joint Conference on Electronic Voting and Identity (E-VOTE ID 2007). Bochum, Germany, October 2008 , pp. 1–15
20. Luechinger, S., Rosinger, M., Stutzer, A.: *The Impact of Postal Voting on Participation: Evidence for Switzerland*. Swiss Political Science Review , January 2007, pp. 167–202
21. Milic, T., McArdle, M., Serdült, U.: *Haltungen und Bedürfnisse der Schweizer Bevölkerung zu E-Voting = Attitudes of Swiss Citizens Towards the Generalisation of E-Voting*. Studienbericht, Aarau, September 2016
22. Pammet, H. Jon and Goodman, Nicole: *Consultation and Evaluation Practices in the Implementation in the Implementation of Internet Voting in Canada and Europe*. Research Study, November, 2013
23. Parlamentarische Verwaltungskontrolle (PVK): *Elektronische Auszählung von Stimmen (E-Counting) Bericht der PVK zuhanden der Geschäftsprüfungskommission des Nationalrates*, Februar 2017
24. Pauchard O. - Swissinfo: *Tausende beim Zählen der Wahlzettel*. [Online] `http://pvpf.ch/swi`, October 2003, last visit July 9, 2019
25. Regenscheid, A., Hastings, N.: *A Threat Analysis on VOCAVA Voting Systems*. Threat Analysis, US Department of Commerce, NIST, December 2008
26. Regenscheid, A., Hastings, N.: *Guide for Conducting Risk Assessments*. NIST Special Publication 800-30, US Department of Commerce, NIST, September 2012
27. Sandmeier, M.: Stadtschreiber und Leiter Stadtkanzlei Baden, February 22, 2019. Personal Conversation, Stadtkanzlei, Baden
28. Sax, A.: Leiterin Wahlen und Abstimmungen, February 20, 2019. Personal Conversation, Staatskanzlei, Generalsekretariat, Kanton Aargau, Regierungsgebäude, Aarau
29. Serdült, U., Dubuis, E., Glaser, A.: *Elektronischer versus brieflicher Stimmkanal im Vergleich. Überprüfbarkeit, Sicherheit und Qualität der Stimmabgabe*. Jusletter IT, September, 2017
30. Smith, R.: *Implications of Changes to Voting Channels in Australia*. Research Report comm. by the Electoral Regulation Research Network, December, 2018
31. van Spyk, B.: Vizestaatssekretär Kanton St. Gallen, February 27, 2019. Personal Conversation, Staatskanzlei, Recht und Legistik, Regierungsgebäude St. Gallen
32. Staatssekretariat für Wirtschaft SECO, Schweiz: *Nationale E-Government Studie 2019*. [Online] `http://pvpf.ch/egov19`, last visit July 9, 2019, March 2019
33. Stine, K., Kissel, R., Barker, W.C., Fahlsing, J., Gulick, J.: *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*. NIST Special Publication 800-60, Vol. I, Rev. 1, US Department of Commerce, NIST, August 2008
34. Stine, K., Kissel, R., Barker, W.C., Lee, A., Fahlsing, J.: *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*. NIST Special Publication 800-60, Vol. II, Rev. 1, US Department of Commerce, NIST, August 2008
35. Verein eCH: *eCH-Standards*. [Online] `http://pvpf.ch/ech`, last visit July 9, 2019