E-Collecting in Switzerland: Status Quo, Setting & Proposals

Florian Moser

October 2025

Abstract

This document has been written for the E-Collecting Hackathon organized by the Federal Chancellery of the 31.10. - 01.11. It drafts the setting, the properties to be reached, and possible solution approaches. A practical solution based on digital signatures achieves participation privacy and reasonable correctness guarantees. A more advanced cryptographic solution is able to further distribute the trust, and avoids assuming the internet as an anonymous channel. It represents work in progress, and its claims have not been formally stated nor verified, and therefore need critical reflection.

1 Introduction

In Switzerland, signature collections are means of direct democratic participation [1]. An initiative, which proposes a change of law, requires 100,000 signatures within 18 months. Further, a referendum, which is launched against a recently passed law by parlament, requires 50,000 signatures within 100 days. To organize such a *collection*, one or multiple committees are formed, often with members from different political parties and interest groups.

Collecting signatures on paper At the time of writing, signatures (*i.e.,* declarations of support) must be collected on paper. The signee must complete the declaration in handwriting, including their name, address, municipality, and signature. These signatures are collected by the collection committee.

The declarations of support are then sent to the municipalities. Municipalities verify the declarations and certify them if the signatory is listed in the electoral register. In this step, the municipality checks whether the specific signee is eligible to vote (but not whether the signature is valid, as there is no signature register). It is important to note that 80% of municipalities verify less than 100 signatures. Common rules for invalidating signatures are double-declarations of support (signing twice) and the lack of eligibility to vote.

The municipalities return the certified lists to the collection committee. Once the committee has collected a sufficient amount of signatures (*e.g.,* 100,000 for federal popular initiatives) they are submitted to the Federal Chancellery. The Federal Chancellery verifies the certification and compliance with formal requirements and then counts the declarations of support [1].[1]

The costs for professional signature collection firms generally range between 3 and 7 francs per signature [2], but this depends on the specific conditions of the initiative (variation of 2.50 - 20 francs per signature). For instance, the faster the signatures need to be collected (*i.e.,* toward the end of the collection period), and the more complex the issue, the higher the rate charged by professional collection firms per signature.

The political process towards E-Collecting Over the years, there have been multiple motions by members of the parlament to digitize collecting. These were initially not successful; with the federal chancellary arguing that the introduction of E-Voting has precedence. However, in 2021, the motion 21.3607 is passed which commissions the federal administration to investigate.[2] The corresponding report is published in 2024 [3], where the Federal Council outlines the legal and technical prerequisites for E-Collecting. The report stresses security, data protection, and recommends pilot projects using the E-ID infrastructure before broader implementation.

Coincidentially, at the end of 2024, a report by a newspaper highlighted a steep rise of invalid signatures and shady business practices, with probably a large part of the abuse uncovered.[3] This lead to a sudden increase in political pressure to harden this process immediately[4], leading notably to a motion which has

[1] Double-signatures (e.g. because relocating in between cantons during the collection phase) are not systematically checked.
[2] `https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20213607`
[3] `https://www.tagesanzeiger.ch/unterschriften-betrug-bei-initiativen-fiasko-fuer-demokratie-304329075925`
[4] `https://anneepolitique.swiss/prozesse/68174`

been resubmitted by members from all parties but one.[5] This motion (e.g. 24.3905) commissions the fast introduction of a trial phase for E-Collecting, based on the E-ID infrastructure.[6]

Acknowledgements We thank Christian Killer, Audhild Høgåsen, INRIA Nancy, and E-Voting BFH for their helpful feedback (feedback represents no endorsement, mistakes in this document are my own).

2 Related Work

Based on the motion of 2021, the federal chancellery contracted two studies. Bühlmann and Schaub [2] analyze the potential political implications of introducing E-Collecting in Switzerland. Their study finds that E-Collecting is unlikely to cause a surge in initiatives or referenda but may slightly strengthen resource-poor actors. They emphasize that while digital collection could enhance inclusivity and efficiency, its overall impact on political participation and agenda-setting would remain moderate. Further, [4] analyse the legal constraints, of which they do not find any.

Given this two studies, and studying internally organizational and technical constraints, the federal chancellery created a comprehensive report of the legal and technical challenges for E-Collecting [3]. The report documents the current process, and sets some fundamentals of the E-Collecting setting (notably the preservation of the paper channel, pilot phases). However, it on purpose leaves most of the details open (e.g. trust assumptions, involved components), and declares them to be defined over the next phase of the project.

There are other works which investigate the topic, of which we mention two. Gfeller et al. [5] analyze the legal requirements of E-Collecting in Switzerland, and discuss concrete technical and political measures to implement it. This includes arguments for a central collection platform, the use of an E-ID infrastructure with the AHV-number as a unique identifier, and the necessity of an efficiency-win for the municipalities to introduce such a system. Scalco et al. [6] describe how the current collection process works, notably highlighting the current lack of reliable detection of double-signatures or forged signatures, and the various privacy issues (signees see others who have signed on same sheet, signees need to be stored by municipality to detect double-signatures, committee and municipality learn all signees). Then, implementation variants of E-Collecting are proposed, relying on digital signatures (QES by Art. 14 OR) or a centralized portal. The essential points of this work are then again repeated in a study commissioned by the canton Basel-Land [7].

eCollecting Solution of St. Gallen The system is actively being developed and will be made public in december. So far there are no public documents that describe their architecture.[7] Based on the Vernehmlassungsvorlage, the document presented to the cantonal parliament when passing the necessary legislative changes, some details can however be guessed.[8] There are three services that interact: AGOV for the login (provided by the federal administration), the eCollecting solution **eC**, and the electoral roll system **ER** (both developed by the canton). When the user logs in to AGOV, AGOV transmits the authenticated AHV-number (AHV = state pension fund) to eC. This checks whether the voter is eligible according to ER, and if yes, stores the ER user-id (!= AHV-Number) in an encrypted form.[9] The voter is informed that their signature has been registered, and eC increases the (publicly visible) number of signatures it has already received for the corresponding proposal. When the municipality receives physical signatures, it logs into the E-Collecting system, and marks the voters that have signed (if they have not yet signed).

It is unclear whether ER is really an independent component, or simply a database attached to eC.[10] Further, the encryption might actually be a hash (with a fresh seed per proposal), to easily derive who has already voted, which is necessary for the municipality use-case.

Comparison to E-Voting There are strong parallels to the internet voting setting, notably in terms of privacy and verifiability targets, however there are important conceptual differences:

- The participation in a collection already exposes the voting preference (no vote privacy), and the signatures are continuously counted (no fairness). Hence the usual solution to the authentication-privacy dilemma, resolved by verifiable shuffles and homomorphic aggregation, does not apply.
- Compared to election periods, the collection period is much longer (months). This necessitates that the list of eligible voters is continuously updated (naturalization, coming of age, relocation, death), but past participations remain valid (i.e. if signed while eligible, a signature remains valid).

[5] `https://anneepolitique.swiss/prozesse/68241`
[6] `https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20243905`
[7] Source: Sebastian.Fust@sg.ch
[8] Source St. Gallen (de).
[9] For each proposal, the key is rotated.
[10] Based on the relatively low cost of the solution (CHF 150k) [7, Anhang 1], it is likely the latter.

- Multiple collections generally run at the same time, while each collection has different start- and end-dates. This notably renders a setup for the voter *per collection* impractical, i.e. no secret channel to the voter with collection-specific secrets can be assumed.

3 E-Collecting Setting

As there is no official definition of the setting by the Federal Chancellery yet, this is our work. A realistic setting reuses the existing responsibilities, capabilities and infrastructure.

Given this, we assume the following parties, which can all be assumed independent:

- *E-Collecting Platform*: Operated by the federal administration, it stores the signatures.
- *Electoral Rolls*: Operated by the canton or municipalities, it manages who is eligible. There are multiple electoral rolls, at least one per canton. Each voter is only on a single electoral roll (at any given time).
- *E-ID Infrastructure*: Operated by the federal administration, and used by the voter, it provides a way to exchange signed attestations.[11] It is important to note that the Swiss E-ID infrastructure does not (yet) provide a signature private key to the end-users; the end-users merely stores and forwards attestations. However, it is realistic to propose changes to the E-ID infrastructure in the context of E-Collecting.
- Further roles are sketched, and may or may not be needed. Concretely, the voter may have a second device to check a bulletin board and the federal chancellery may perform an audit at the end.

Further, we aim for the following properties:

- *Participation Privacy*: The adversary cannot tell who has participated or not. This is stronger than the notion of vote privacy of internet voting, as the participation already reveals the vote.
- *E2E-Verifiability of Participation*: Each counted participation is cast by an eligible voter (eligible at the time of participation). Honest voters indeed are aware of their participation, and all participations of honest voters that verified their participations are included. All voters, including attacker-controlled voters, may only participate once. Together, this corresponds to a weak notion of E2E-Verfiability of internet voting; weak as the participation already expresses the vote, and therefore the adversary can by design not change votes.

To aid intuitive reasoning about participation verifiability of a given system, we analyse subproperties instead. This further allows us to define different trust assumptions per subproperty. We decompose as follows:

- *Participation-as-Recorded*: Voters may check that their participation has been recorded.
- *Authenticated-Participation*: Each recorded participation belongs to an eligible voter who has initiated this participation.[12] Note that the voter needs to be eligible when they sign, but this eligibility may change over time (e.g. voters that relocate must not have their signatures revoked, but must also be prevented to participate again via their new electoral roll).
- *Counted-as-Recorded*: All recorded participations are counted.

Further, the following requirements are given in the setting:

- *No second thoughts*: Signing a collection is final, and cannot be reverted.
- *Double-channel*: Both paper and digital signatures need to be supported (but double-participation must be prevented, including in between the channels).
- *Motivating collection committees*: Collection committees need to know how many voters have already signed, and from which municipality they are.

4 Proposals

As in internet voting, constructing solutions that provide either no privacy or no verifiability is simple. A good solution however manages to have both properties to some reasonable extent. The target is therefore to create proposals of the following two kinds:

- *Basic*: The target is political acceptability and technical simplicity. The reason is that *some* solution will be implemented, and if the "secure" solutions are all very complicated, some trivial implementation (or worse, e.g. a security-theater solution) will be chosen instead. For optimal acceptability, this solution needs to incorporate the E-ID infrastructure, uses off-the-shelf crypto, and should incorporate the existing roles (E-ID infrastructure, Electoral Roll and E-Collecting Platform).
- *Secure*: The target is to sketch a system granting maximal security guarantees achievable, using optimized crypto and proposing fundamental changes to roles if necessary. This will both motivate further research, and but also inform architecture choices of the Basic solution, to prepare a latter upgrade.

[11] For example, a cantonal authority signs the driver's license, or the attribute "I am over 18".
[12] Note that this includes that participations cannot be added by the adversary (i.e. no ballot stuffing).

Each solution must cover the following use-cases:

- *Sign online*: The voter signs a collection online.
- *Sign on paper*: The voter signs a collection on paper.
- *Electoral roll change*: The voter enters or exits a given electoral roll (relocation, death).
- *Credential regeneration*: The voter regenerates their credential (e.g. because of loss of the previous one).

We assume a PKI between the components, and that they authenticate all their messages appropriately.

4.1 Anonymous credentials

The basic idea is that the electoral roll publishes a whitelist of public keys of the eligible voters. This is a weak proposal, with only approximate privacy and correctness, but simple to implement. Concretely:

- The voter generates a signature key-pair, and authenticates the public key towards their electoral roll. This will be done over the E-ID infrastructure, and is assumed trustworthy (*hand-waving*). The voter can repeat this process to replace the authenticated public key.[13]
- The electoral roll sends for each collection a set of `pks` to the E-Collection platform. Each `pks` represents a voter, and contains (optionally) a public key `pk` eligible to sign at this point in time, a (possibly empty) list of expired public keys, and a mark whether the voter has singed offline. The `pks` does not contain any identification of the voter, hence the E-Collection platform cannot attribute it to some voter.

Now, to cover the different use-cases:

- *Sign online*: The voter sends the signature to the E-Collection platform over an anonymous channel. The platform checks that its corresponding public key is eligible according to some electoral roll, and forwards the signature to the trustees. The trustees respond with a signature over all timestamps of valid signatures of this electorate. This includes all signatures that had an eligible public associated at their time of creation, and excludes all doubles, either digitally (i.e. signed towards public keys in the same `pks`) or paper (i.e. signed towards a public key in a `pks` which is marked correspondingly).
- *Sign offline*: The physical signature will eventually reach the electoral roll. The electoral roll certifies the physical signature, and sets the participation-mark in `pks` corresponding to that voter to 1.
- *Electoral roll change*: The municipality invalidates all keys per the exit date (death, relocation). For relocation, the municipality may send *pks* to the new municipality for re-authentication (in that case, the voter can keep using the same public key, and double-signatures are detectable).
- *Credential (re-)generation*: The public key is set to be eligible in the `pks` of this voter, an eventual old key is put into the list of expired public keys.

To implement verifiability:

- *Participation-as-Intended*: The E-Collecting platform publishes per municipality the (signed by the trustees) timestamps of the received signatures. The voter uses an audit device which checks the signature is valid, and then the voter verifies one of the timestamps corresponds.[14]
- *Authenticated-Participation*: The E-Collecting platform has for each collection and electoral roll some other auditing electoral roll defined (e.g. using some deterministic hashing procedure). When the platform receives a new signature, it finds the electoral roll that authenticates this signature. Then, it sends all signatures it received for this electoral roll to the corresponding auditing electoral rolls together with the set of authenticated public keys. The auditing electoral rolls verify the signatures, and sign the list of timestamps of these valid signatures.
- *Counted-as-Recorded*: Each auditing electoral roll stores all signatures it received over time. Once the collection period ends, and the result is announced, the auditing electoral roll verifies that the number of published participations is correct (and could prove deviations). During the final audit, double-signatures are detected over all electoral rolls, by removing signatures attributable to `pks` with matching public keys.

Easy to understand claims (see table 1 for details):

- *Privacy*: Trust in either the electoral roll or the E-Collection platform (internet = anonymous channel).
- *Correctness*: Guaranteed by the trustees (no trust in E-Collection platform necessary). However, the electoral roll needs to be trusted to not add fictive voters in their jurisdiction.

Variants of this scheme:

- *Opt-in*: Once a voter has signed up for E-Collecting, their paper signatures are automatically invalid.

[13] *Replacing* instead of activating multiple, to avoid a ballot stuffing attack where additional public keys are added by the adversary.

[14] As there are only few signatures per municipality, clash attacks are negligible. To harden this, a nonce may be added, or even a hash over the submitted signature; while the latter would need a channel between voting and audit device.

Table 1: Trust assumptions per property, given the E-Collecting platform EC, for some voter registered in electoral roll ER. There are trustees TR assumed (could be four other electoral rolls). The collection committee is denoted CC. We assume a trustworthy PKI in between the system components, and an authenticated channel from VD to ER.

	Online signatures	Paper Signatures
Privacy		
Participation Privacy	$(\mathsf{ER} \vee \mathsf{EC}) \wedge \mathsf{AC}$	$\mathsf{CC} \wedge \mathsf{ER}$
Verifiability		
Participation-as-Intended	$\mathsf{EC} \vee \mathsf{TR}$	none
Authenticated-Participation	$(\mathsf{EC} \vee \mathsf{TR}) \wedge \mathsf{ER}$	$\mathsf{CC} \wedge \mathsf{ER}$
Counted-as-Recorded	$\mathsf{EC} \vee \mathsf{TR}$	$\mathsf{CC} \wedge \mathsf{ER}$

This simplifies the schemes considerable, as signatures online no longer need to be invalidated.

- *No privacy towards* ER: The EC exposes the signatures towards the ER. Then, the electoral roll can invalidate paper signatures instead, if already signed online. However, electoral roll could abuse this lookup, notably a problem as electoral roll may know voters personally.
- *Multiple devices*: The voter may activate multiple public keys (to sign on multiple devices). This usability improvement may however may it easier to stuff valid public keys (as it is no longer concerning when a voter has two authenticated public keys, possibly one belonging to the adversary).

4.2 Using non-standard crypto

Mechanisms:

- *Encrypted participation* As there are multiple collections active at the same time, as a way to avoid the anonymous channel assumption, the voter can encrypt the signature. Trustees then decrypt this, and publicly claim how many valid signatures they found for each collection. Parameter setting is non-trivial (intervals to perform the count? who are the trustees? how to rotate keys but have a high anonymity set?), and individual verification is harder / impossible (at least delayed, as signatures do not appear immediately anymore). Further, note that the anonymity is not perfect (can still make statistical links with who has submitted something, and which initiatives increased in number of signatures).
- *Anonymous two-factor authentication* The voter sends a public key along with real-world authentication to both the E-Collection platform as well as to the electoral roll. Then, both public keys are verifiably randomized by trustees (possibly by collection), and the randomization factor is returned to the voter (encrypted using their public key). To sign a collection, the voter uses both (rerandomized) secret keys.
- *PETs* Voter proves that in possession of a secret key belonging to a set of valid public keys, and that not signed yet (see proposal of [8]).

We can compose the first two mechanisms to get the strongest scheme we deem cryptographically feasible at this point in time. The voter authenticates two public keys, with the E-Collecting Platform and the Electoral Roll each (avoids trusting single authority for eligibility). These public keys are verifiably rerandomized[15] per collection (avoids trusting single authority for privacy). The voter signs (collection, nonce) with both rerandomized keys, encrypts and then sends them to the E-Collecting platform, where they are verifiably shuffle-decrypted in regular intervals (avoids anonymous channel). The signatures are then published, and the voter checks whether their nonce appears on the bulletin board on another device (for IV).

Easy to understand claims (see table 2 for details):

- *Privacy*: Guaranteed by the trustees (notably no anonymous channel).
- *Correctness*: Guaranteed by the trustees. Either the electoral roll or the E-Collecting platform needs to be trusted to not add fictive voters.

See trust assumptions in Table 2.

4.3 General considerations

Considerations when reaching the properties:

[15]Given signature key $h = g^x$, pick random r, and generate $h' = h \cdot g^r$. Do this for all public keys, and randomly permute them (shuffle-like proof). Publish the list of re-randomized and permuted public keys, and send the corresponding r to the voter (encrypted under their public key). Complicated, but seems possible.

Table 2: Trust assumptions per property, given the E-Collecting platform EC, for some voter registered in electoral roll ER. There are trustees TR assumed (could be four other electoral rolls). The voter has a voting device VD and an audit device AD. We assume a trustworthy PKI in between the system components, and an authenticated channel from VD to both EC and ER (to authenticate the public keys).

	Online-Signatures
Privacy	
Participation Privacy	$\mathsf{VD} \wedge \mathsf{TR}$
Verifiability	
Participation-as-Intended	$\mathsf{VD} \vee \mathsf{AD}$
Authenticated-Participation	$\mathsf{EC} \vee \mathsf{ER}$
Counted-as-Recorded	$\mathsf{EC} \vee \mathsf{TR}$

- *Scalability* Attacks on privacy and correctness scale better against the E-Collecting Platform than to the distributed Electoral Rolls. However, attacks on the Electoral Roll may be more motivated (e.g. cleck knows the voter personally) and feasible (as municipality less capabilities to own/operate system).
- *Distribution* It can be assumed that multiple independently operated Electoral Rolls are active, that have no stakes in auditing (e.g. as audits for initiatives that do not apply to them).

Thoughts about achieving simple schemes:

- *Constant eligibility* If the eligibility needs only checked once for the signature, then the schemes becomes simpler (i.e. no removal of once-valid digital signatures because of a paper signature). Instead, if voter has signed up for E-Collecting and paper signature has been received, send physical letter to them informing them that a digital signature is required instead?
- *Secure E-ID infrastructure* If the E-ID infrastructure guarantees an authenticated public key of the voter, the electoral roll needs not to be trusted for authentication-participation. This allows simpler schemes, as no distribution of trust in the electoral roll needs to be considered.

References

[1] Schweizerische Bundeskanzlei, "E-Collecting," https://www.bk.admin.ch/bk/de/home/politische-rechte/e-collecting.html.

[2] Marc Bühlmann and Hans-Peter Schaub, "Staatspolitische Auswirkungen von E-Collecting: Studie im Auftrag der Bundeskanzlei," Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern, Bern, Tech. Rep., Jan 2023, study commissioned by the Swiss Federal Chancellery. [Online]. Available: https://www.newsd.admin.ch/newsd/message/attachments/90666.pdf

[3] Bundesrat, "Elektronische Unterschriftensammlung für eidgenössische Volksbegehren (E-Collecting): Bericht des Bundesrates in Erfüllung des Postulates 21.3607 Staatspolitische Kommission NR vom 27. Juni 2021," https://www.parlament.ch/centers/eparl/curia/2021/20213607/Bericht%20BR%20D.pdf, Bundesrat der Schweizerischen Eidgenossenschaft, Bericht e-parl 21.11.2024 09:19, Nov 2024, bern, 20. November 2024.

[4] Lorenz Langer, Irina Lehner and Kristina Hoffet, "E-Collecting für eidgenössische Volksinitiativen und Referenden," Zentrum für Demokratie Aarau, Arrau, Tech. Rep., 2023, study commissioned by the Swiss Federal Chancellery. [Online]. Available: https://www.bk.admin.ch/dam/bk/de/dokumente/pore/E-Collecting/Rechtsgutachten%20von%20Langer,%20Lehner%20und%20Hoffet.pdf.download.pdf/Rechtsgutachten%20von%20Langer,%20Lehner%20und%20Hoffet.pdf

[5] K. Gfeller, A. Glaser, and I. Lehner, "E-Collecting: Umsetzungsvarianten und Rechtsetzungsbedarf," *LeGes – Gesetzgebung & Evaluation*, vol. 32, no. 1, pp. 1–15, 2021. [Online]. Available: https://leges.weblaw.ch/legesissues/2021/1/e-collecting--umsetz_4ac1c3bc14.html

[6] S. Scalco and R. Rauschenbach, "Vom unterschriften sammeln auf papier zum e-collecting: Digitale transformation der auslösung von volksbegehren," in *Digitale Transformation der öffentlichen Verwaltung in der Schweiz: Stand, Entwicklungslinien und Praxisbeispiele*. Springer, 2022, pp. 119–149.

[7] K. Basel-Landschaft, "Studie zum thema e-collecting." Kanton Basel-Landschaft, study written by liitu consulting gmbh, owned by Sandro Scalco.

[8] P. Locher and R. Haenni, "Verifiable internet elections with everlasting privacy and minimal trust," in *International Conference on E-Voting and Identity*. Springer, 2015, pp. 74–91.