Balancing *Security* and *Usability* in the Swiss Post *E-Voting* Protocol

Audhild Høgåsen, Chiara Spadafora

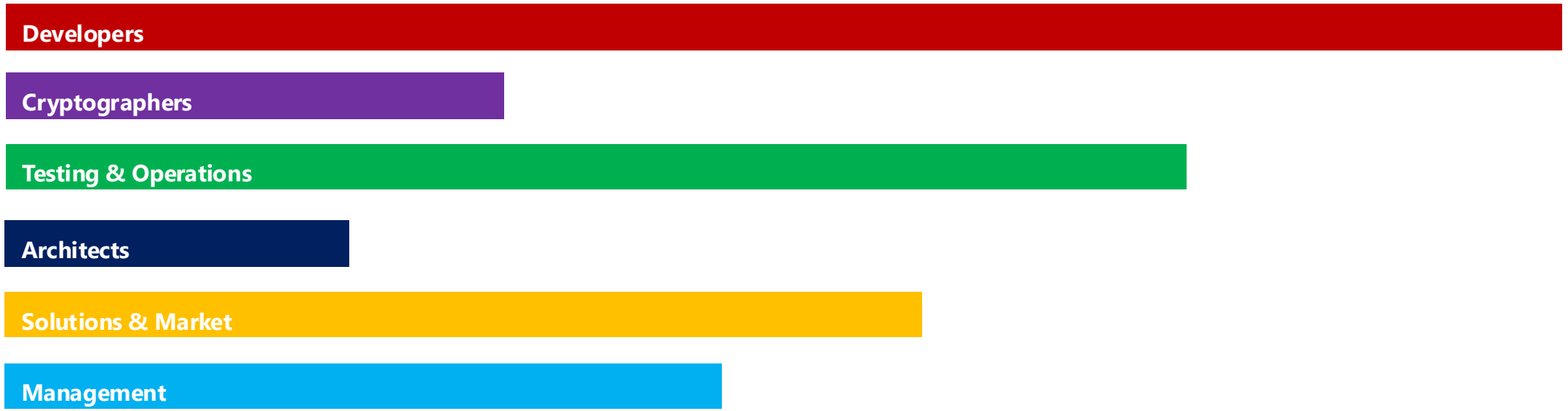
Meet the Presenters

Audhild Høgåsen
audhild.hoegaasen@post.ch

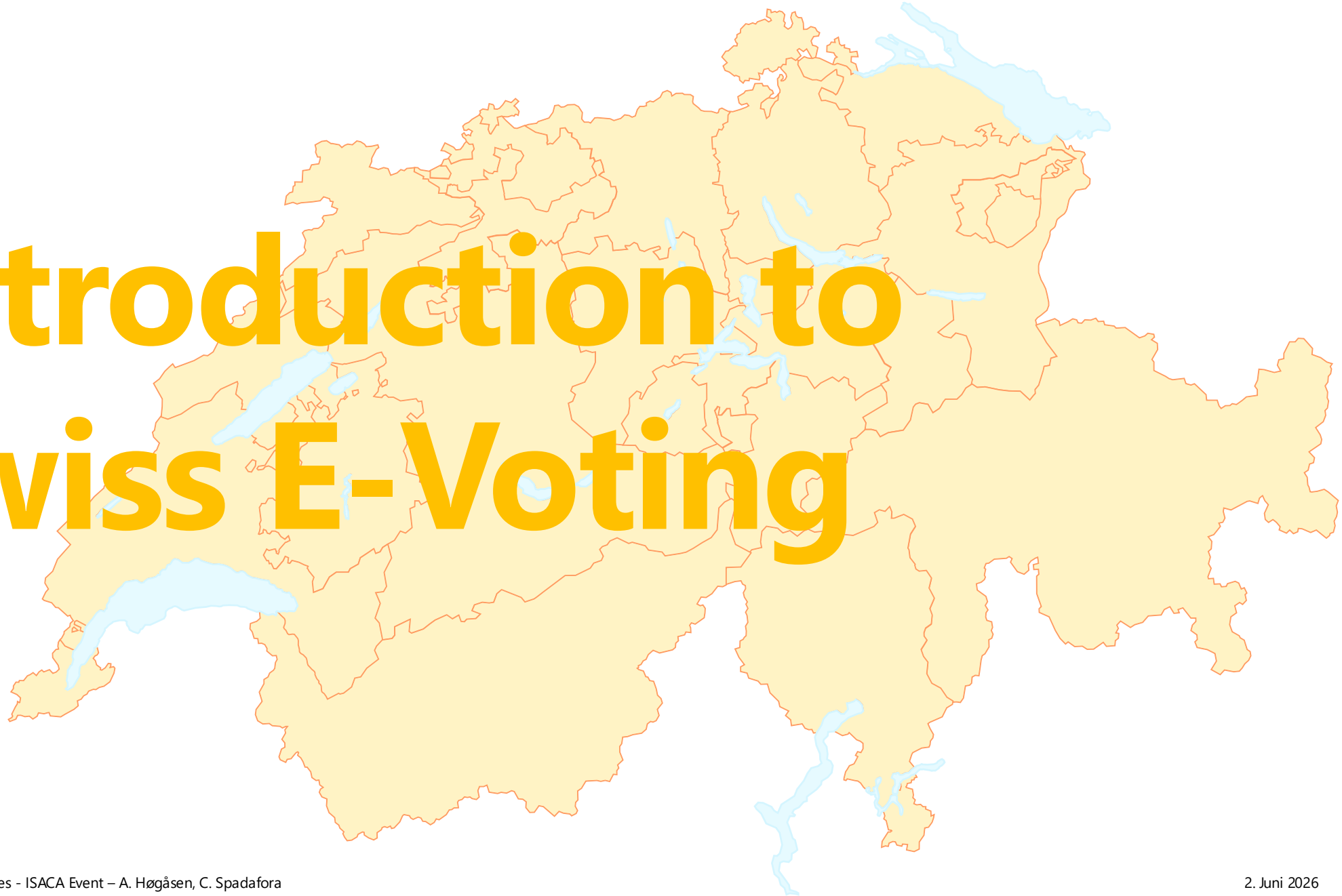
Chiara Spadafora
chiara.spadafora.1@post.ch

Cryptographers in the Swiss Post E-Voting Team

Our Team at a Glance



Introduction to Swiss E-Voting



E-Voting: why Swiss Post?

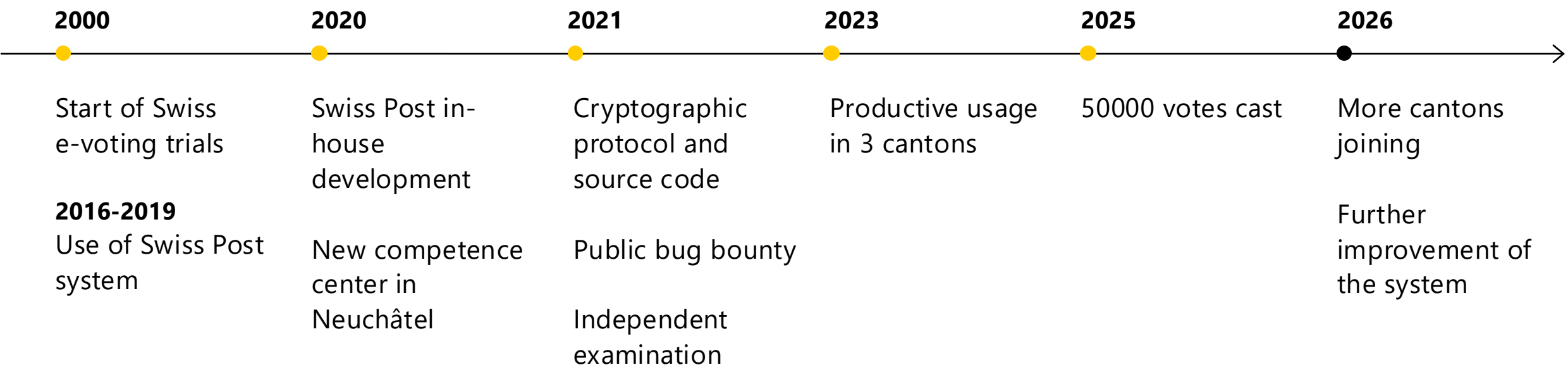
As a provider, Swiss Post offers cantons an electronic voting system that complies with legal requirements from the Confederation

The cantons decide whether they wish to offer electronic voting, and which system to use, based on the legal framework

Swiss Post is digitalizing what it already does best: the secure transport of confidential information.

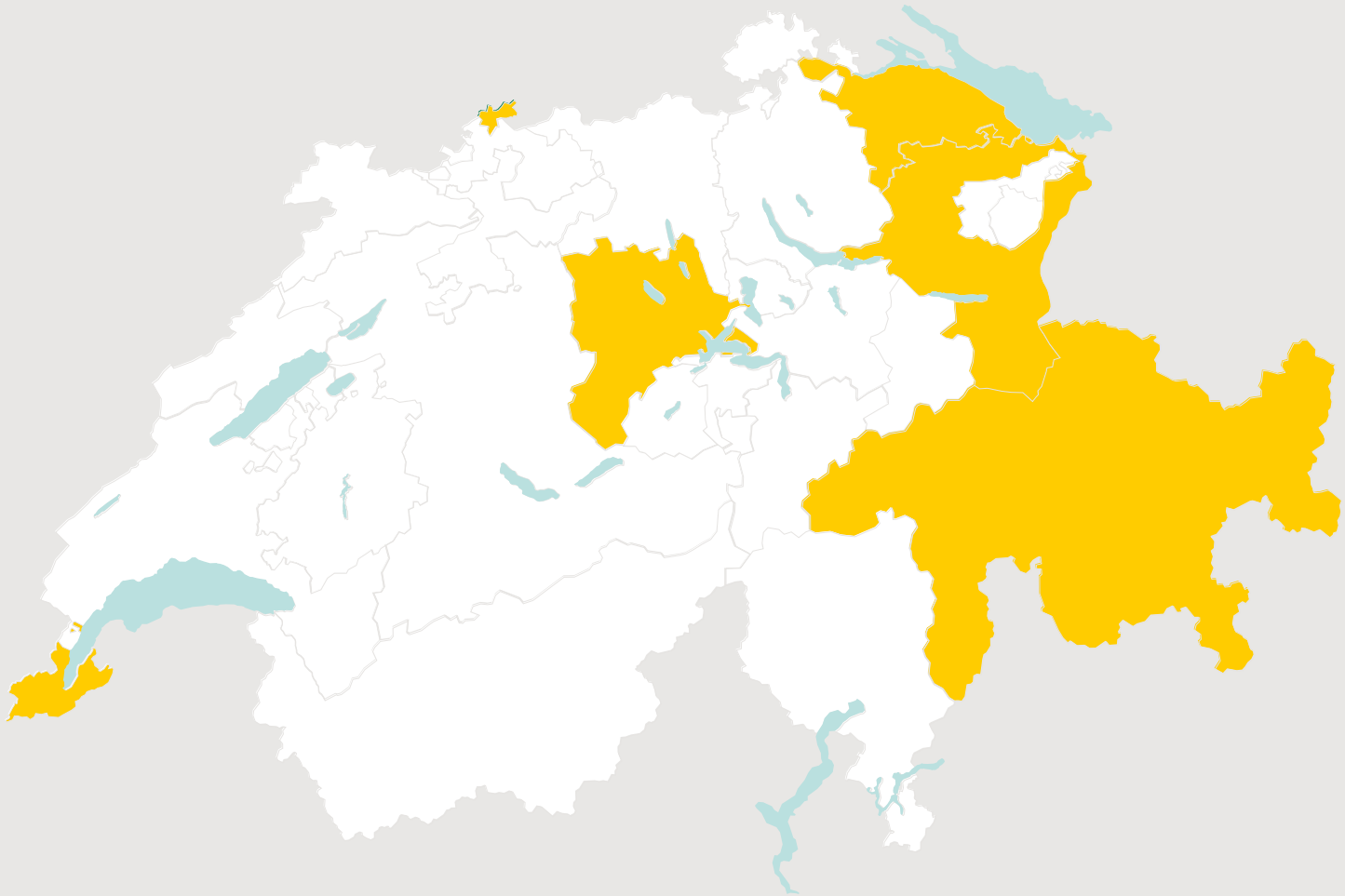
How many votes were cast electronically in 2025 with the Swiss Post Voting System?

Swiss E-Voting Timeline: Past and Present



Status May 2026

14 successful voting events since the relaunch of E-Voting in June 2023



Canton of Thurgau
- Since 06/23
- Swiss living abroad
- Extension to Swiss residents in 2026

Canton of St. Gallen
- Since 06/23
- Swiss living abroad and Swiss residents
- 66 out of 75 municipalities

Canton des Grisons
- Since 03/24
- Swiss living abroad and Swiss residents
- 23 out of 100 municipalities

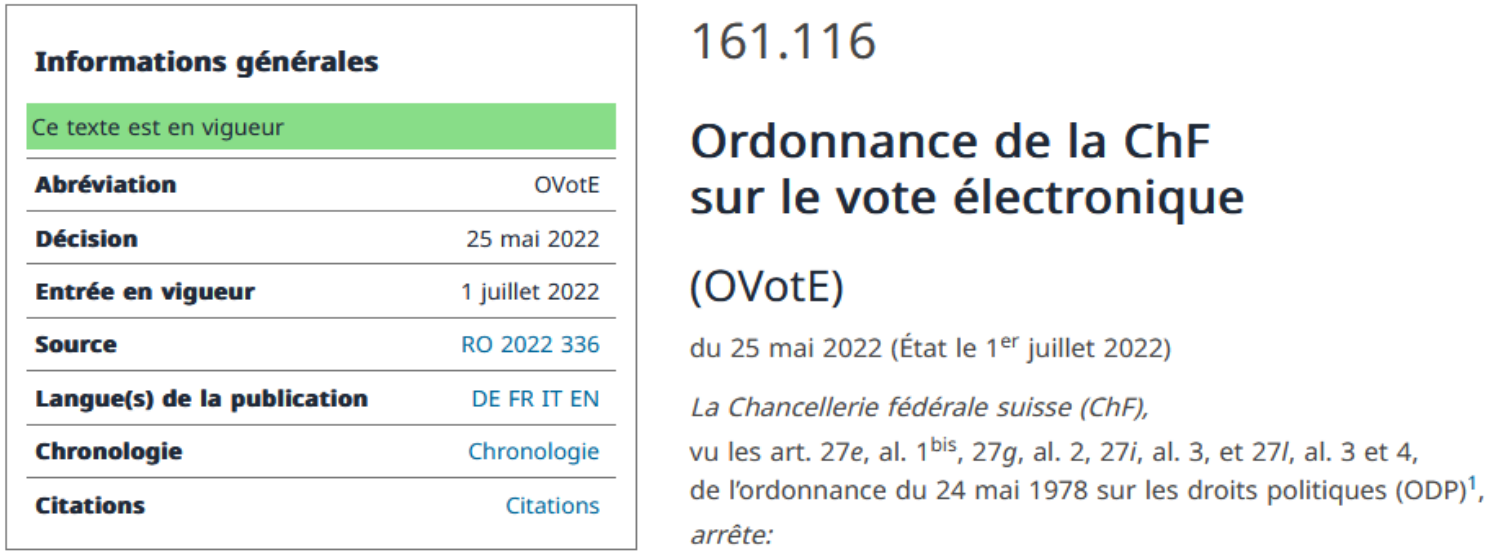
Canton of Basel-City
- Since 06/23
- Swiss living abroad and people with disabilities
- Extension to Swiss residents in 2026

Canton of Lucerne
- Goal: from the **09/26** ballot
- Swiss living abroad
- Extension to Swiss residents in 2028

Canton of Geneva
- Goal: from the **06/27** ballot
- Swiss living abroad and Swiss residents

2022: Ordinance on Electronic Voting Revision

New Swiss Legislation comes into force, including a total revision of the Federal Chancellery Ordinance on Electronic Voting



Informations générales

Ce texte est en vigueur

Abréviation	OVotE
Décision	25 mai 2022
Entrée en vigueur	1 juillet 2022
Source	RO 2022 336
Langue(s) de la publication	DE FR IT EN
Chronologie	Chronologie
Citations	Citations

161.116

Ordonnance de la ChF sur le vote électronique

(OVotE)

du 25 mai 2022 (État le 1er juillet 2022)

La Chancellerie fédérale suisse (ChF),

vu les art. 27*e*, al. 1bis, 27*g*, al. 2, 27*i*, al. 3, et 27*l*, al. 3 et 4,
de l'ordonnance du 24 mai 1978 sur les droits politiques (ODP)[1],

arrête:

2022: Ordinance on Electronic Voting Revision

New Swiss Legislation comes into force, including a total revision of the Federal Chancellery Ordinance on Electronic Voting

The Ordinance requires that any e-voting system used for governmental elections in Switzerland must provide the following security properties.

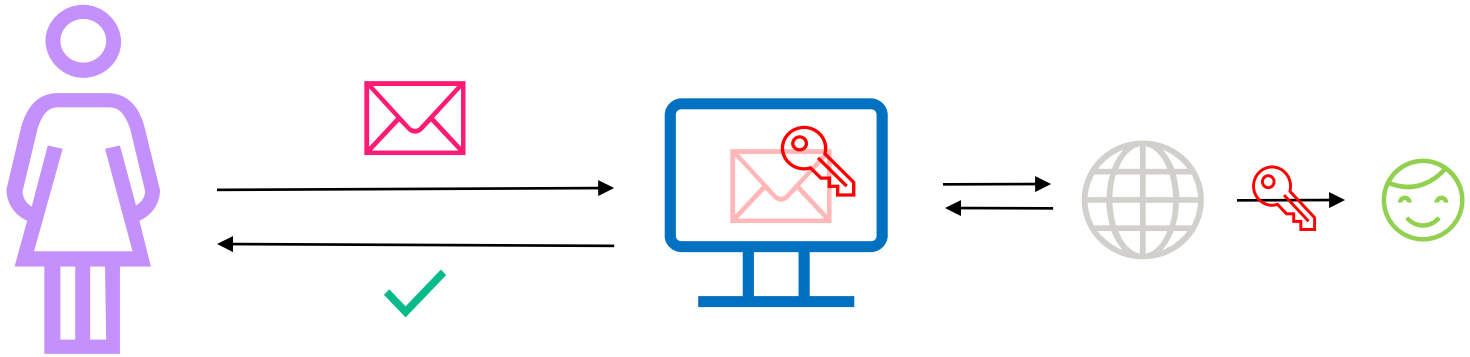
- individual verifiability
- universal verifiability

Verifiability

- vote secrecy and exclusion of premature results

Privacy

A Naïve Voting System



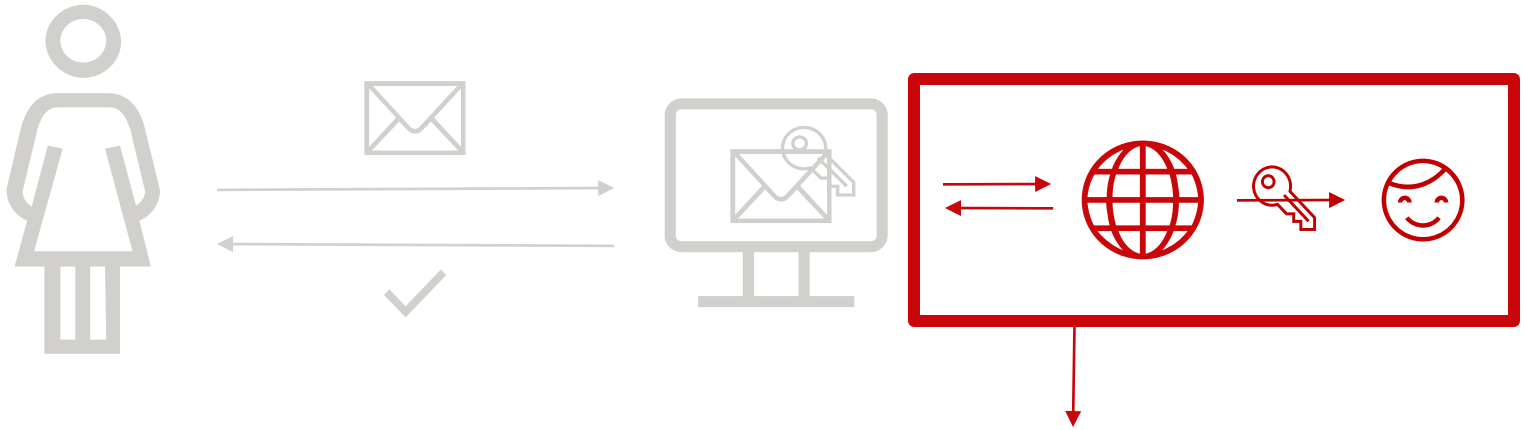
Usability 👍

Performance 👍

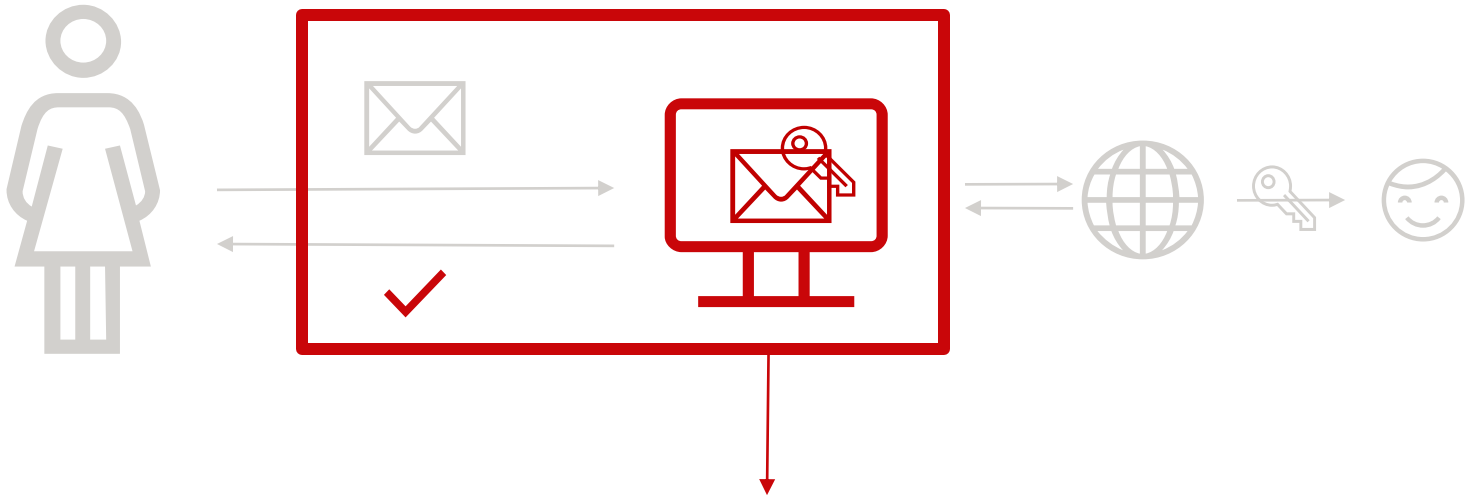
Privacy 👎

Verifiability 👎

How NOT to design a voting system

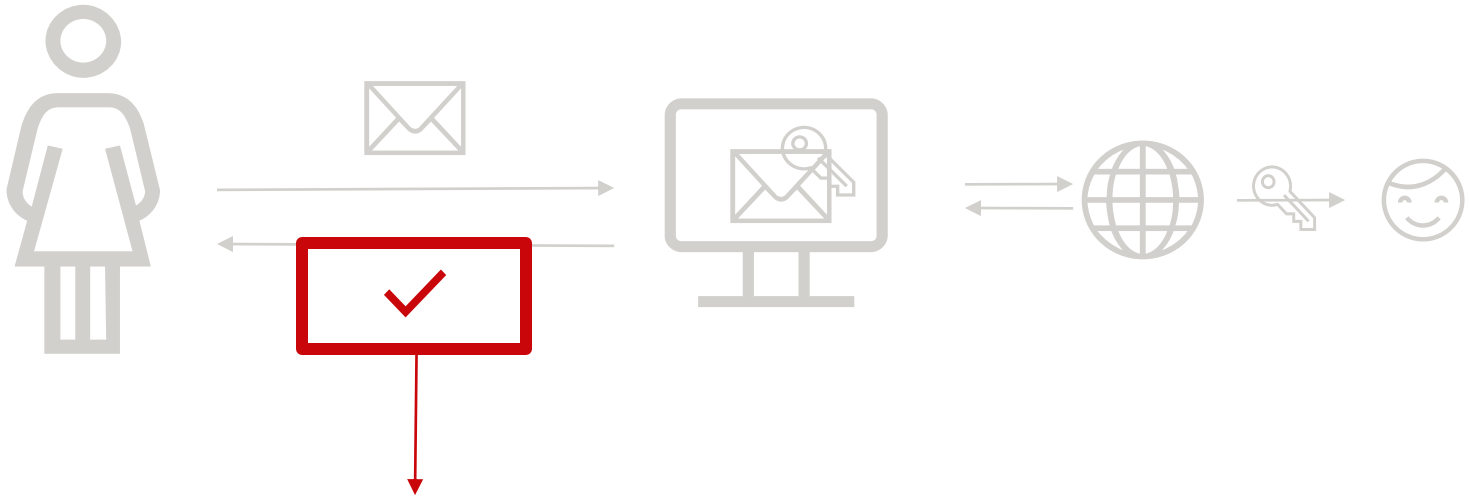


How NOT to design a voting system



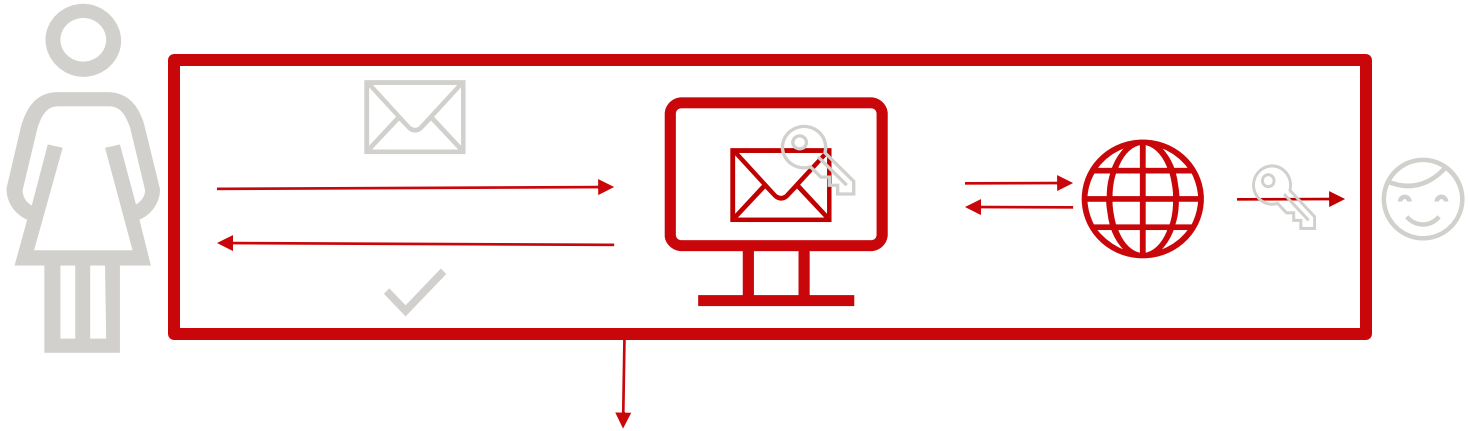
A malicious voter portal can modify the vote without the voter noticing

How NOT to design a voting system



The voter has no proof that their vote was registered in the online ballot box

How NOT to design a voting system

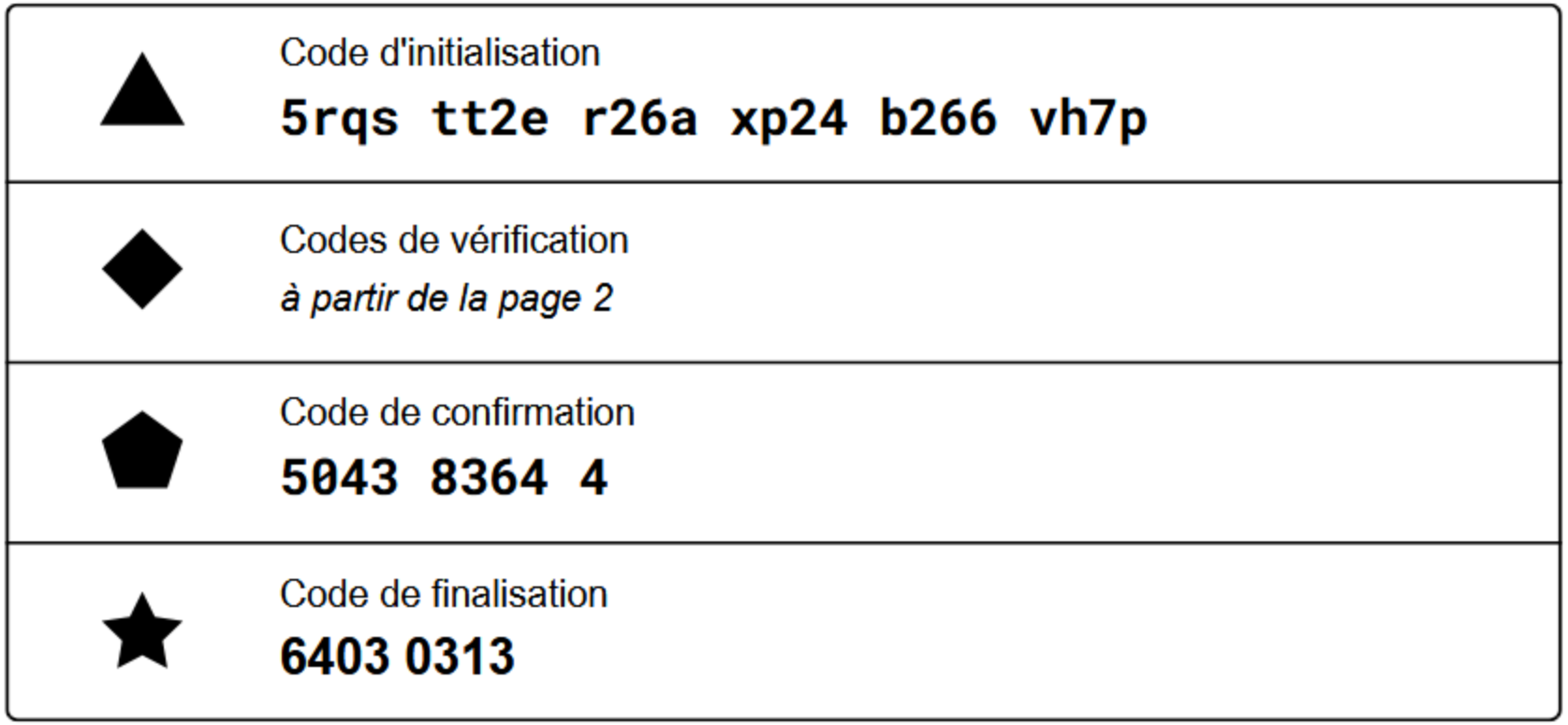


No external auditor can independently verify that every vote was recorded as cast, stored without alteration, and included in the final tally

The Swiss Post Voting System

Image created with Copilot AI

Two-Round Return Code Scheme



The Voting Card

Codes de vérification

Démo Votation

1. Temps ensoleillé

Oui **6715** Non **7336** Blanc **9080**

2. Temps pluvieux

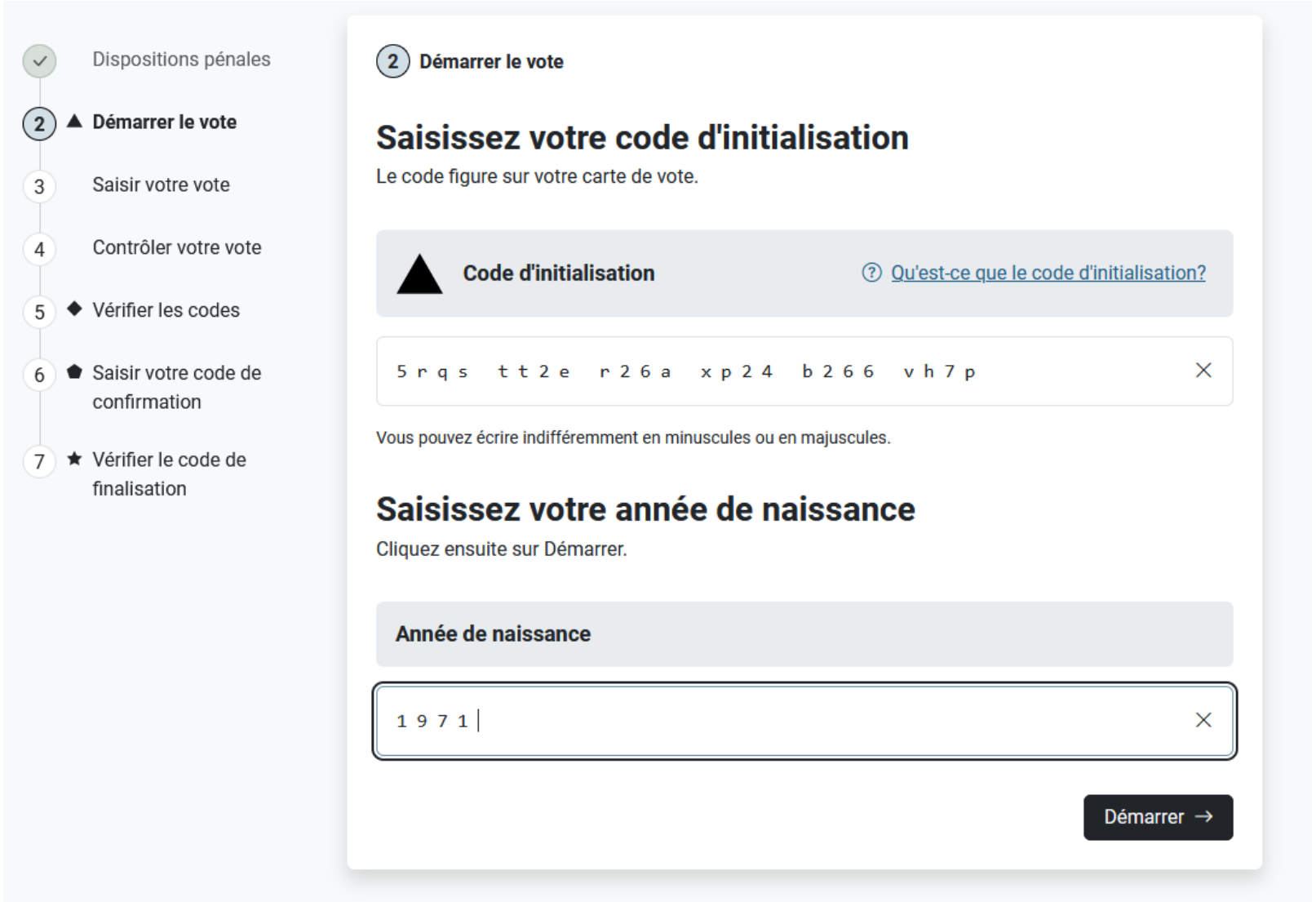
Oui **7618** Non **1018**

Élection proportionnelle

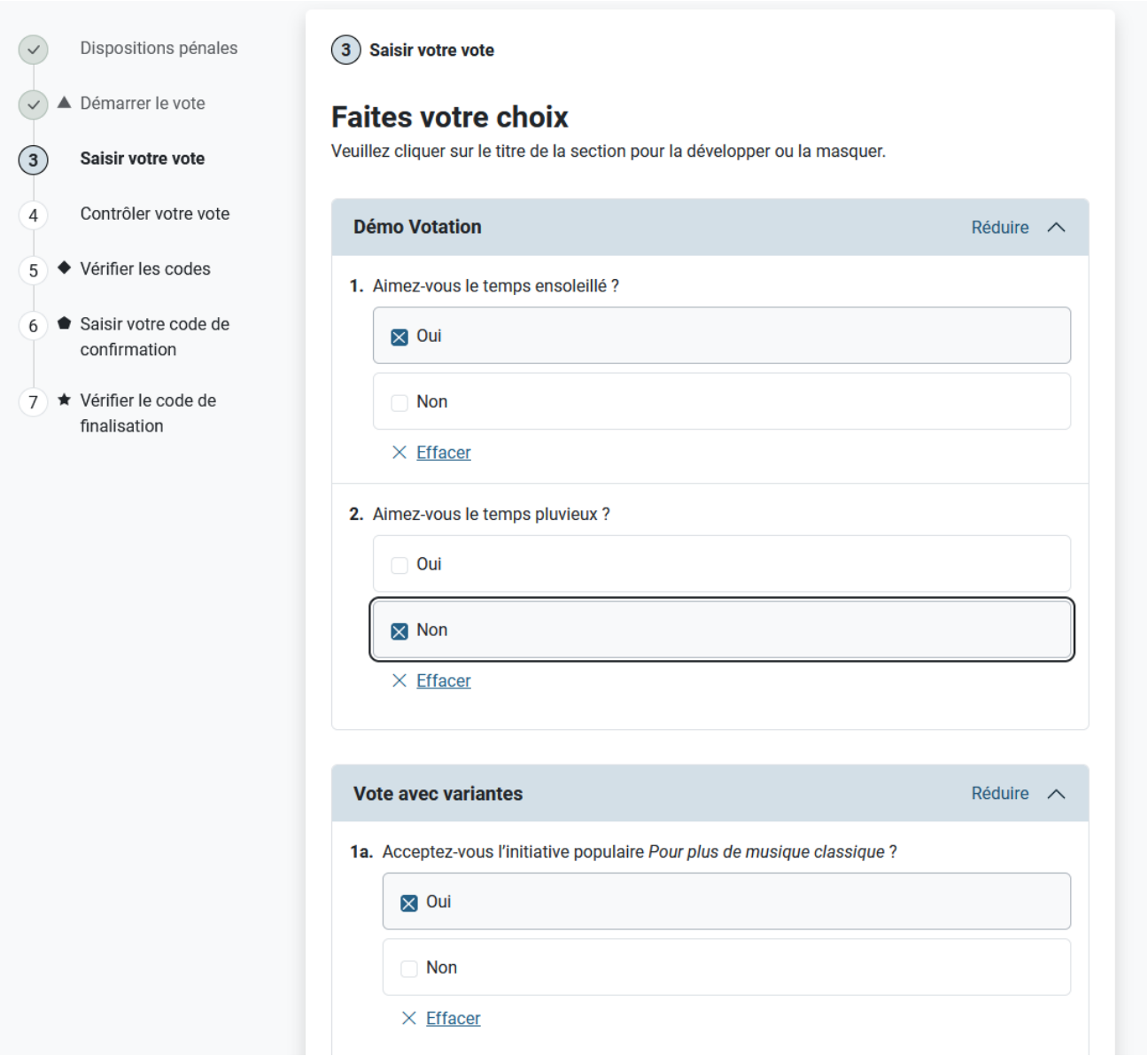
Codes des candidats
«1x» = inscrit une fois
«2x» = inscrit une deuxième fois (cumul)

N°	Nom	1x	2x
1	**Liste 1: Compositeurs/Compositrices**	**7689**	
1.1.1	Chopin Fréderic	**5914**	**3109**
1.1.2	Vivaldi Antonio	**1769**	**3073**
2	**Liste 2: Écrivains/Écrivaines**	**6451**	
1.2.1	King Stephen	**6311**	**9927**
1.2.2	Rowling Joanne	**3998**	**1178**
99	**Blanc**	**5316**	
Aucun nom sélectionné		**4214**	
Aucun nom sélectionné		**0289**	
Aucun nom sélectionné		**7058**	
Aucun nom sélectionné		**9849**	

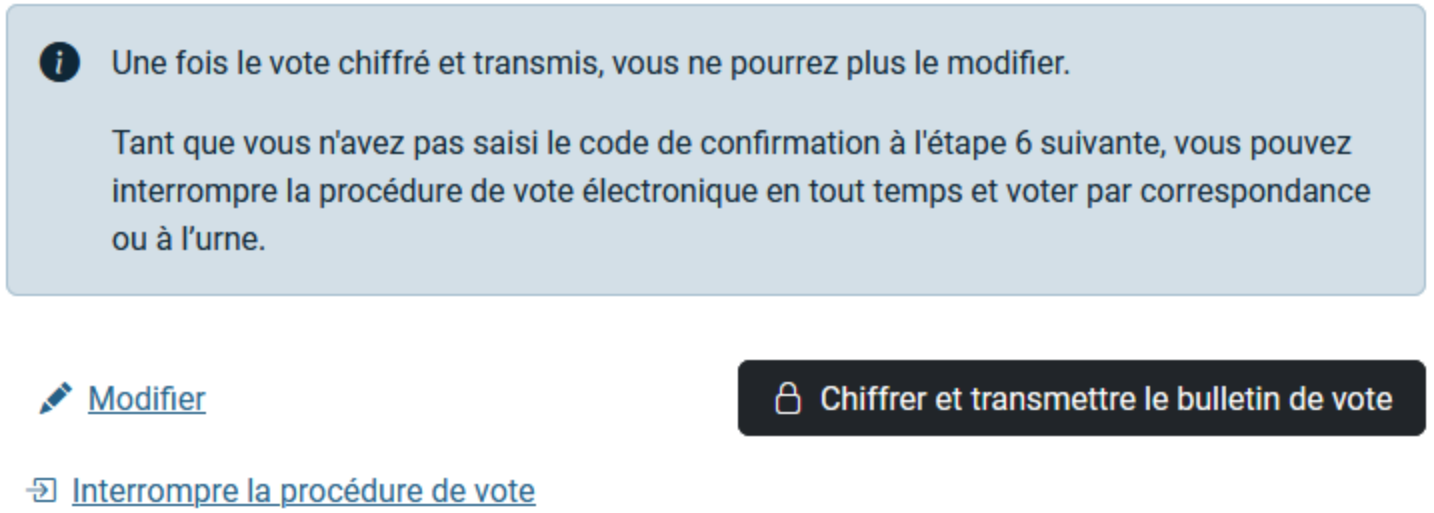
The Voter Portal



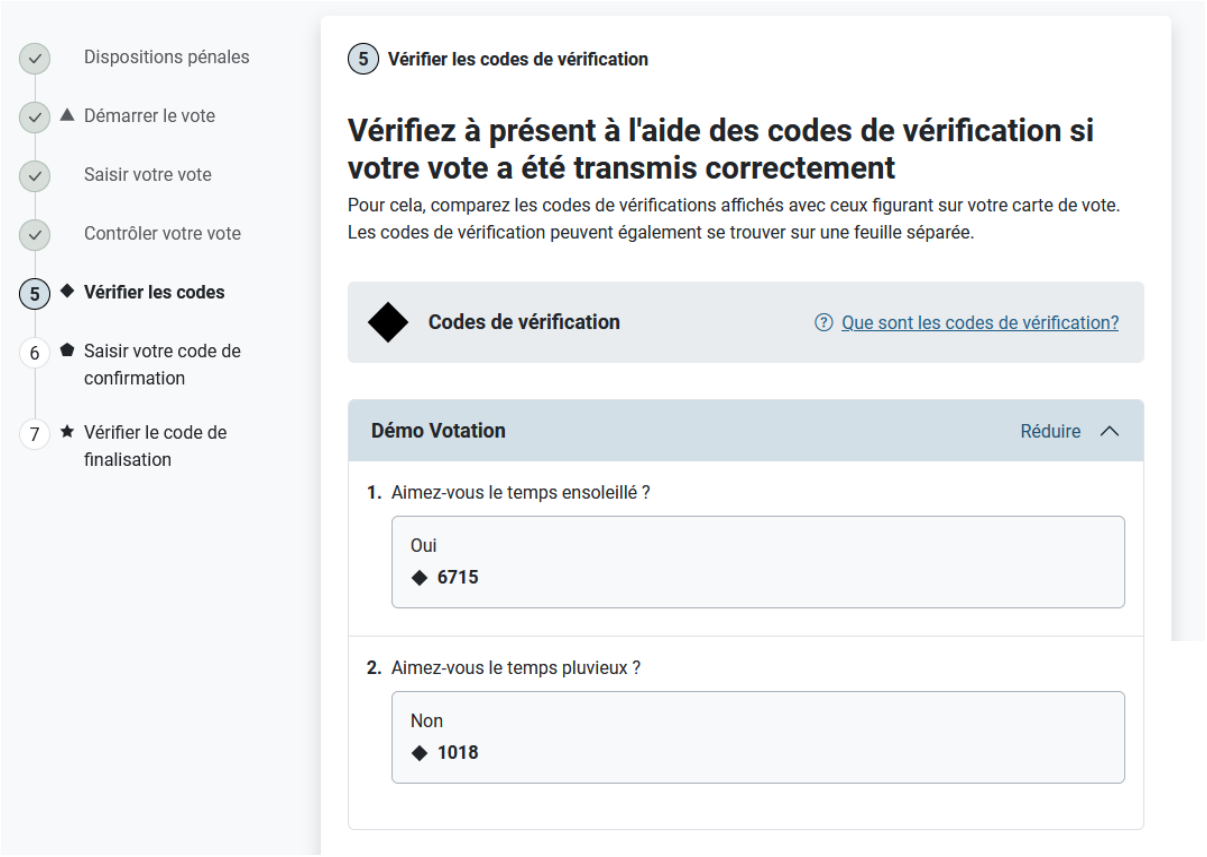
Voting Choice Selection

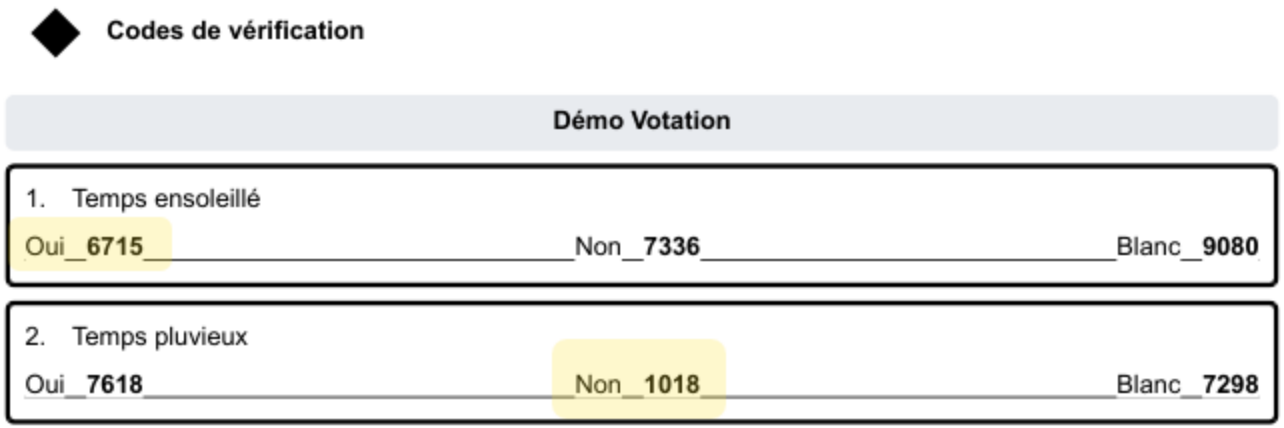


Voting Choice Encryption



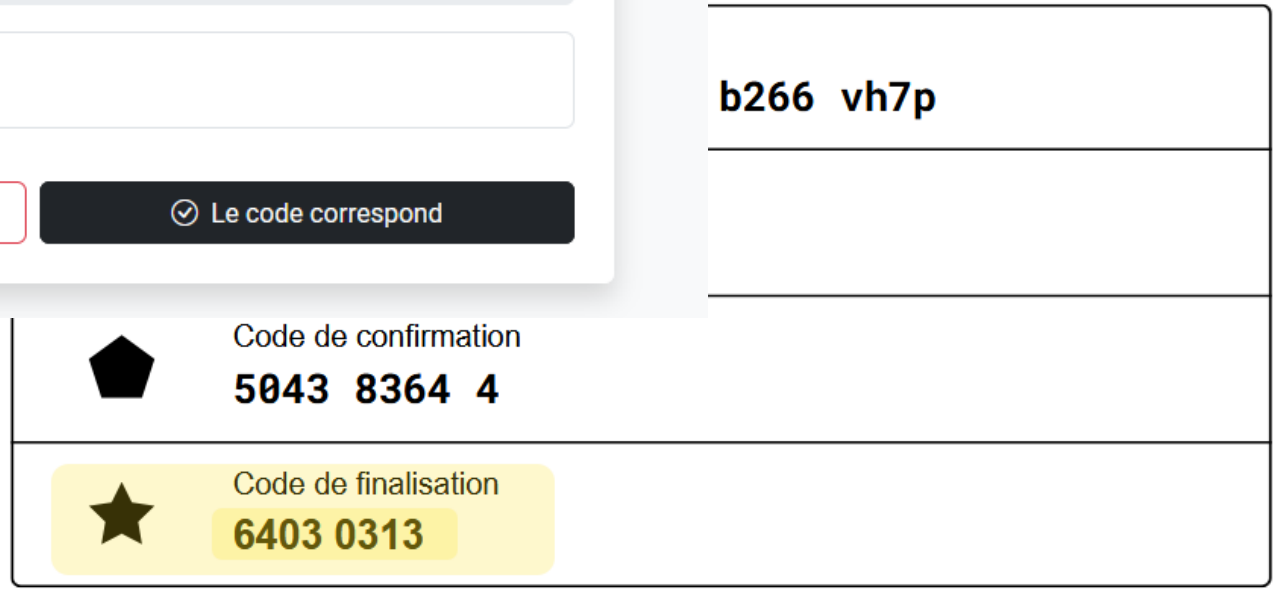
Ballot Verification





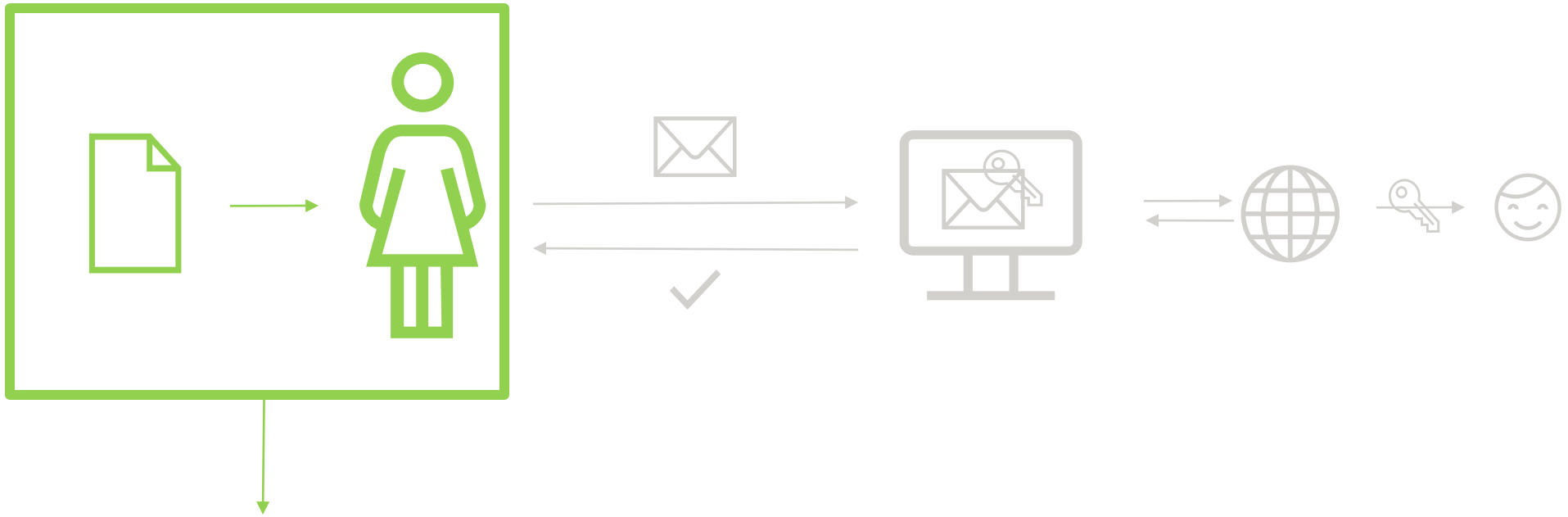
Ballot Confirmation

Ballot Finalization



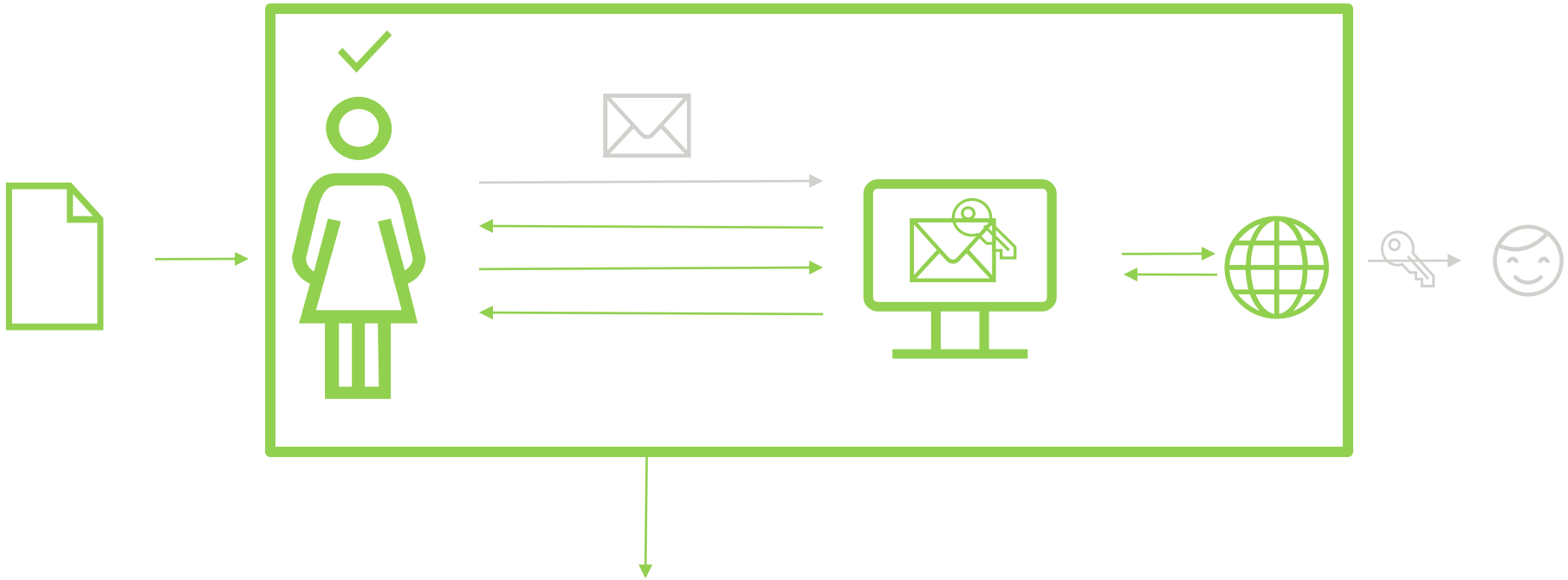
Individual Verifiability

Individual Verifiability



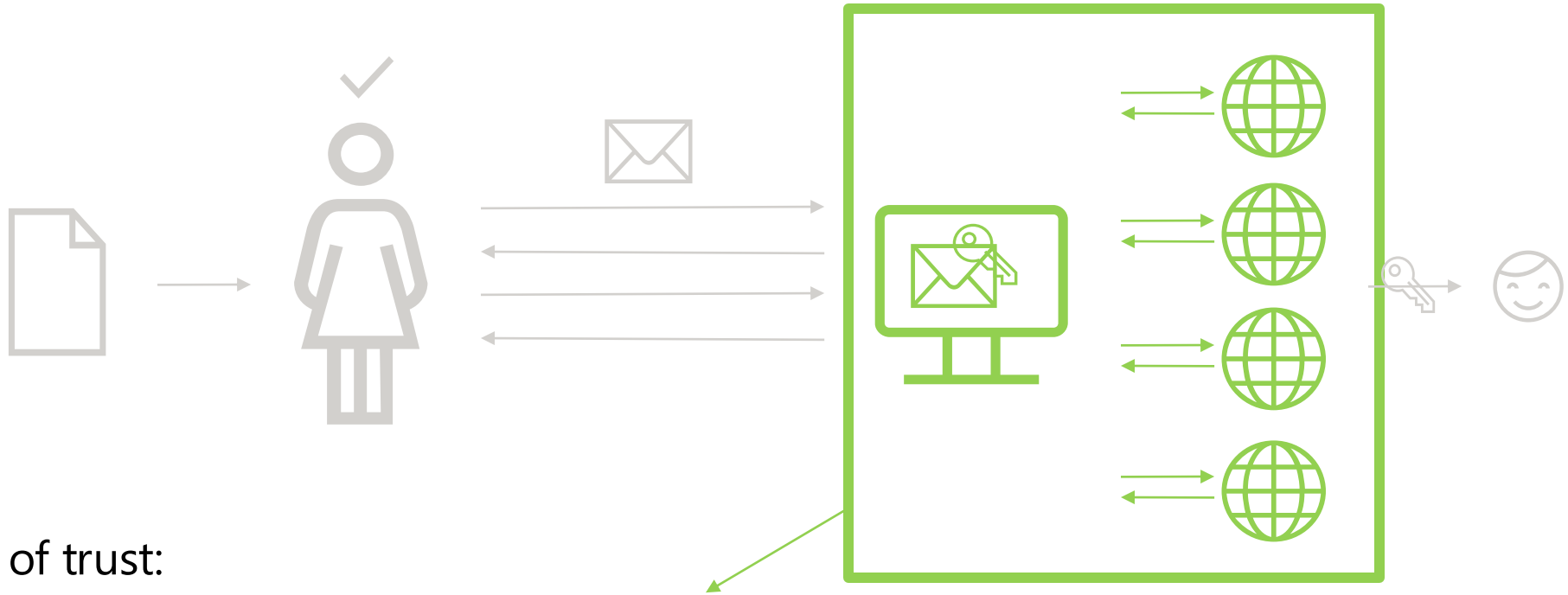
The voter receives a voting card by postal mail, containing codes that are unique to both the voter and the specific election

Individual Verifiability



After submitting the vote, the voter receives a set of return codes.
If these codes match the ones printed on the voting card, this confirms that the vote was transmitted and recorded without any modification

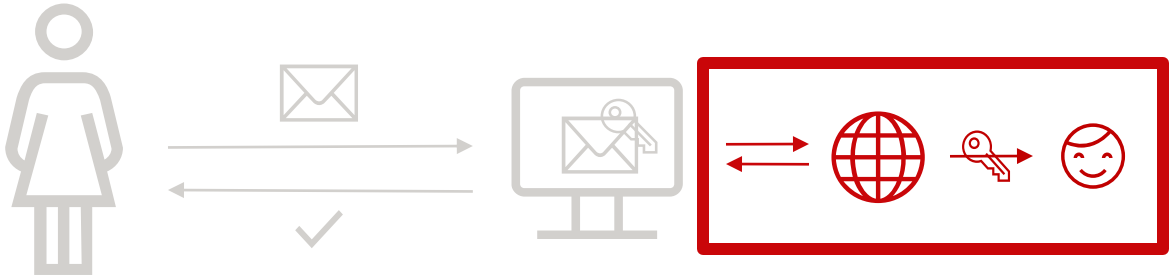
Individual Verifiability



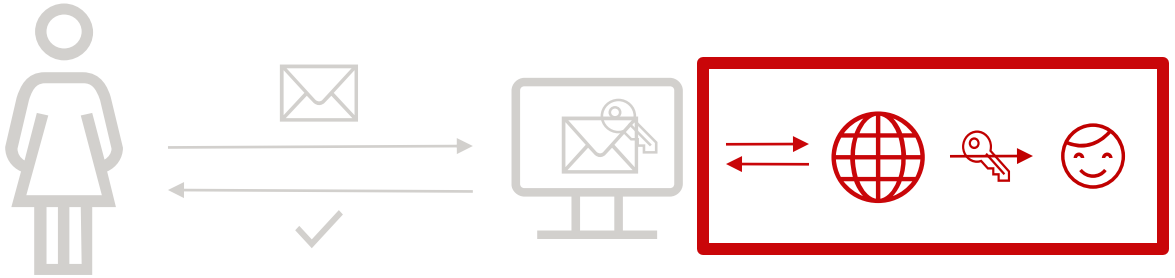
Distribution of trust:

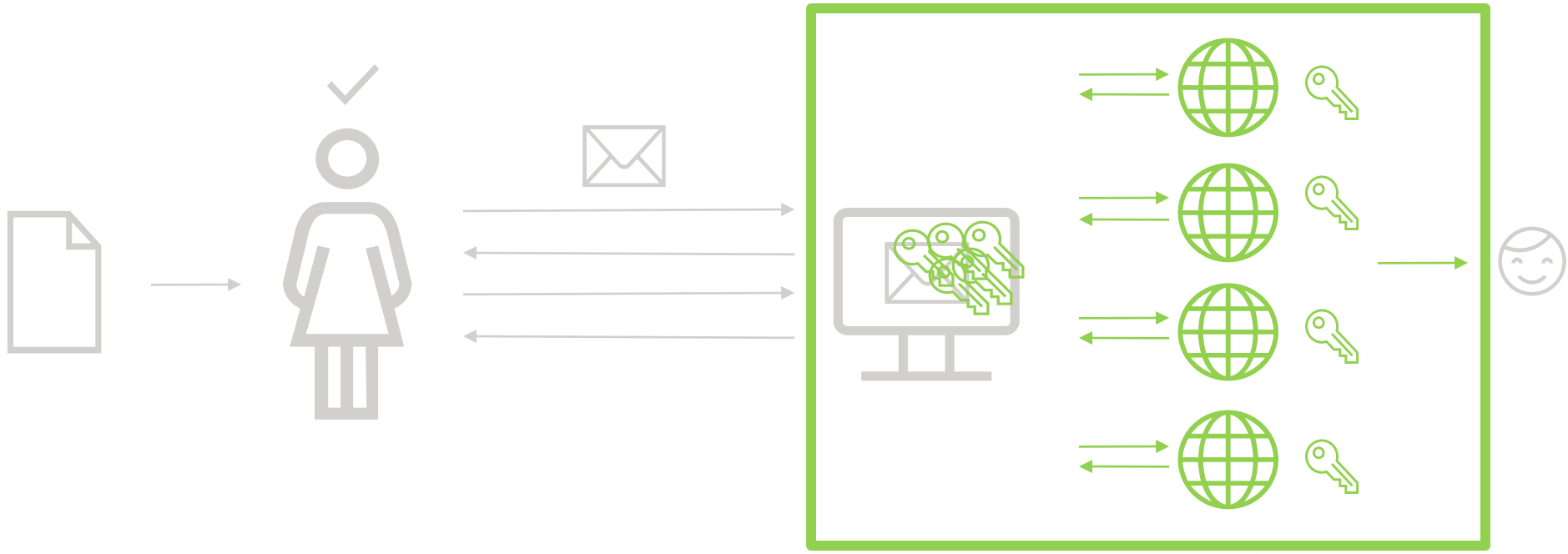
- No online authority knows the return codes
- Shared verification and generation of the confirmation and finalization codes

Vote Privacy



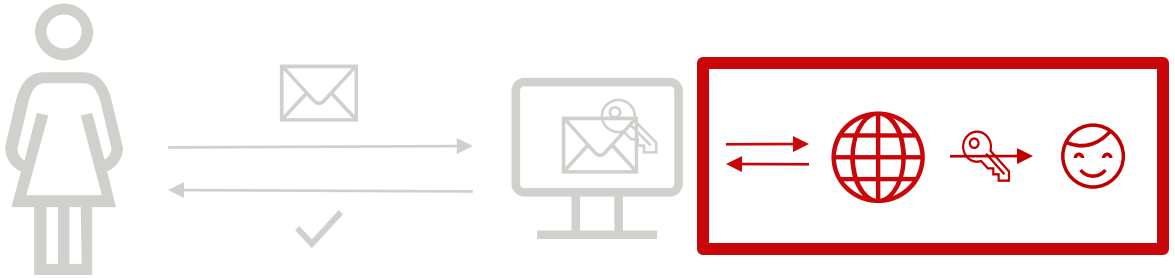
Vote Privacy

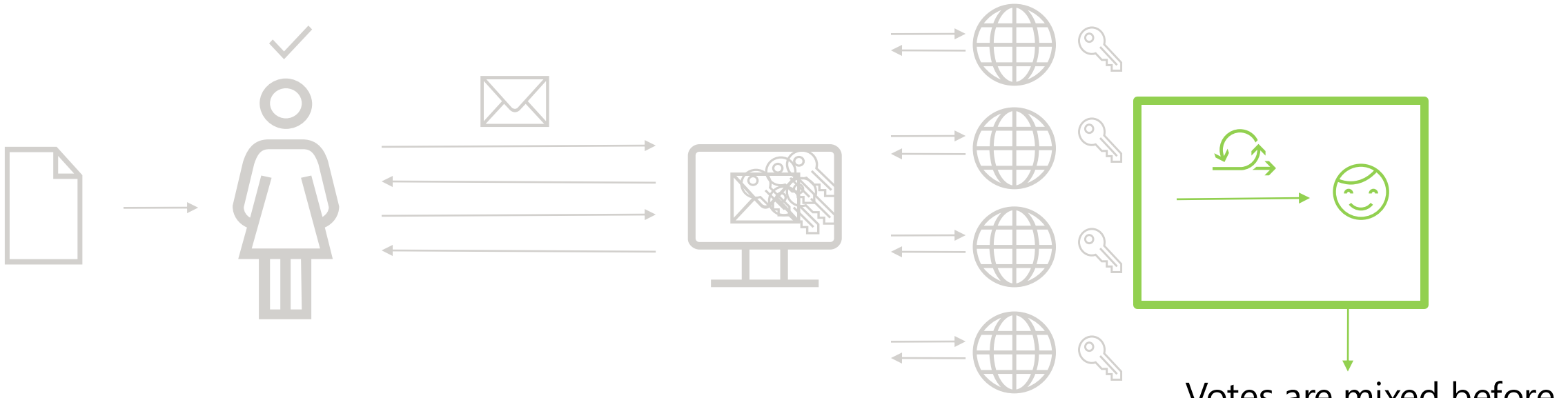




No single authority is able to decrypt the votes

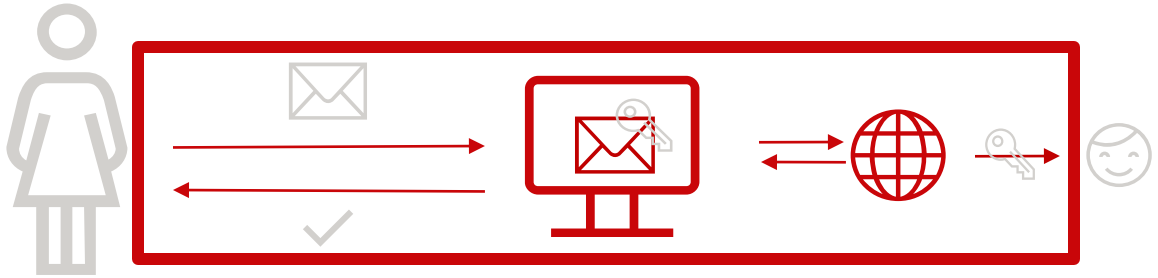
Vote Privacy



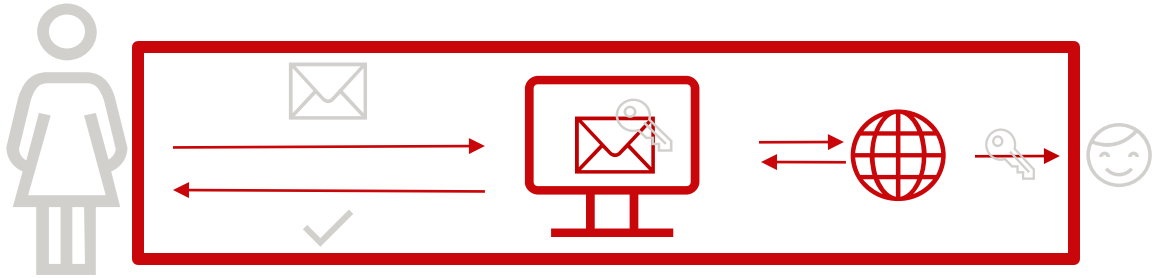


Votes are mixed before being decrypted

Universal Verifiability



Universal Verifiability



Each interaction can be independently verified thanks to the use of a cryptographic technique known as a zero-knowledge proof

TRUE or FALSE

It is possible to stop the voting process and resume on a different device at any time in the voting period

One voting card can only be used to cast one single vote.
No re-voting possible

If a voter forgets to type the confirmation code, their vote will still be counted

Simultaneously with the productive election event, we run a public intrusion test, where anyone can try to cast a vote and try to hack the e-voting system

The zero-knowledge proofs included in the mixnet are needed to guarantee vote privacy

Even if your voting device is hacked, you can be sure that your intended ballot was recorded in the ballot box

Challenge: Maintenability

Image created with Copilot AI

Code and Specification Maintenability

System complexity makes maintenance challenging, ~200,000 lines of code
All code must be fully auditable and publicly available together with:

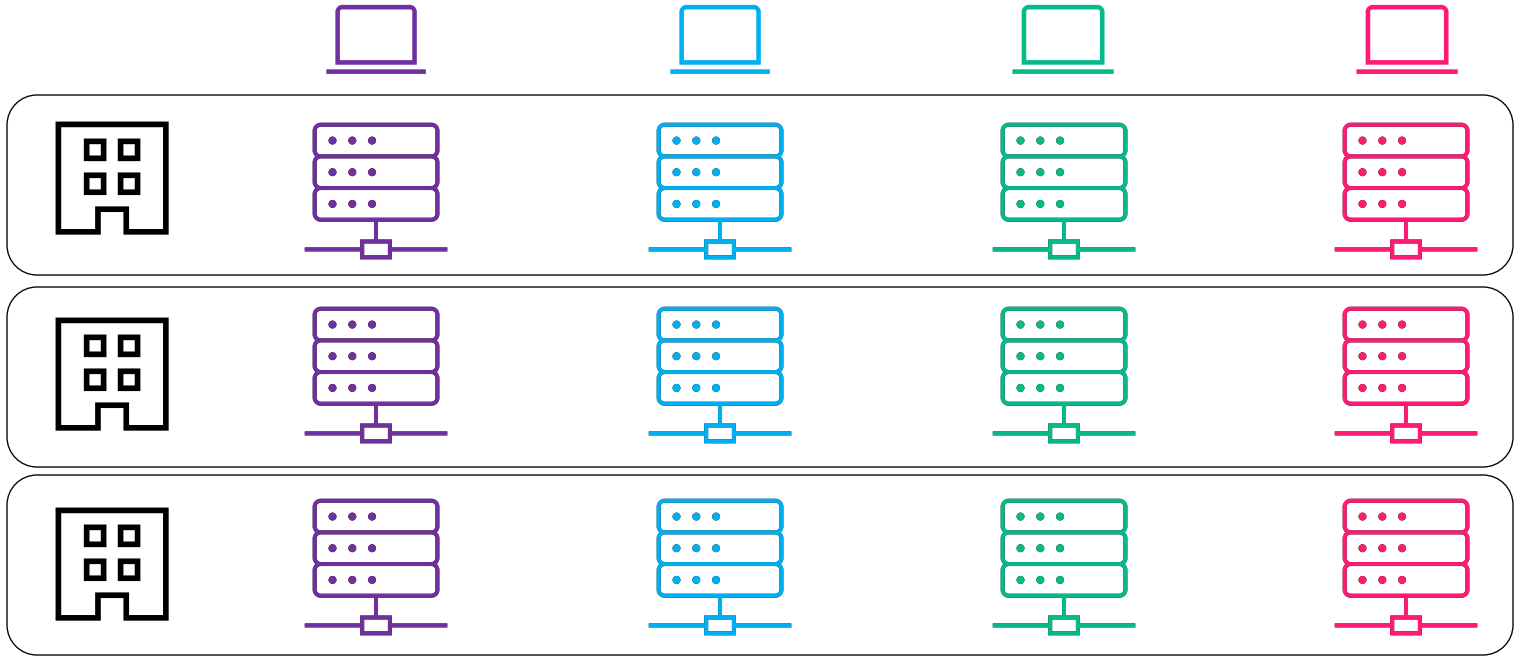
- Specifications and pseudocode
- Computational and symbolic proofs
- Architecture and design documents

Clear alignment between all artefacts is crucial for auditability

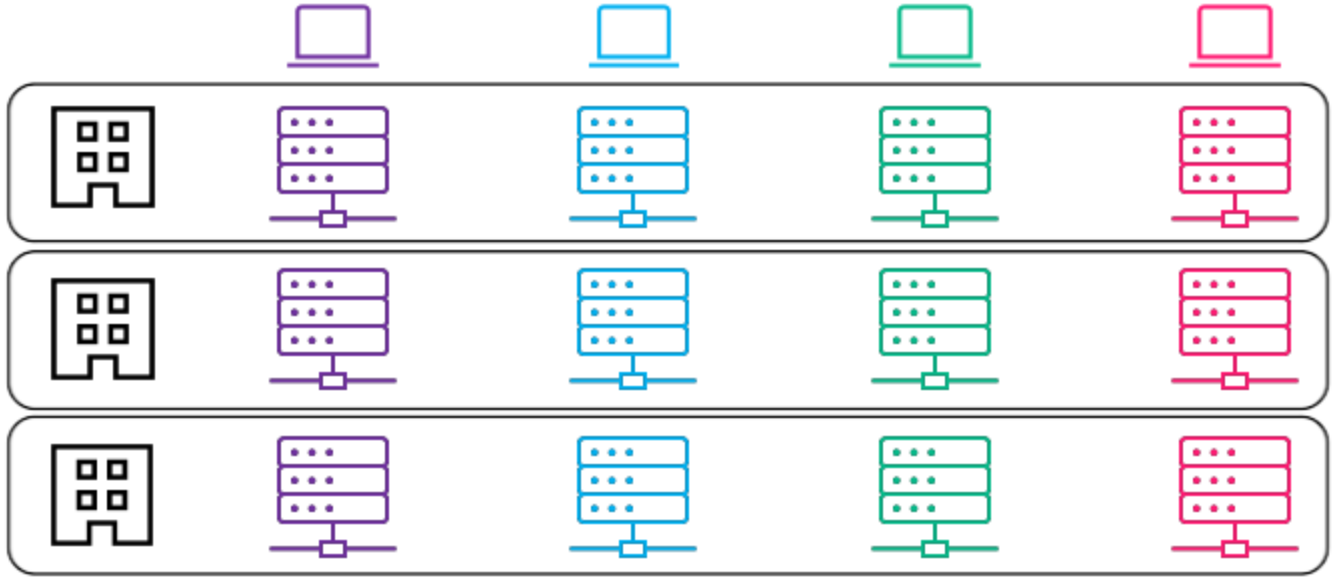
Documentation helps understanding and auditing

But updates require time and effort

Hardware Maintenability



How many servers (at least) must be up and going during the election, to ensure availability?



Challenge: Usability

Image created with Copilot AI

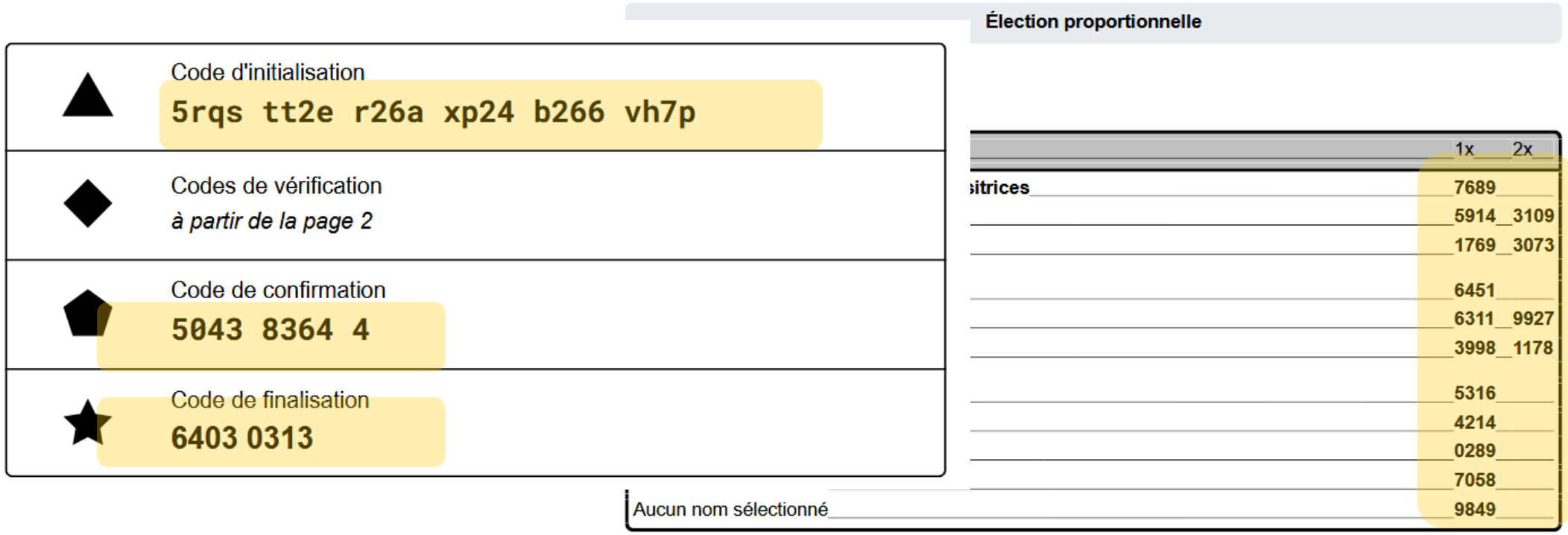
Usability for the Voter

For codes that have to be entered by humans, it is important to choose a user-friendly alphabet. The alphabet used should include only letters and numbers easily found on any keyboard, and the chance of misspelling should be minimized by excluding letters and/or numbers that look similar

(a, b, c, d, e, f, g, h, i, j, k, m, n, p, q, r, s, t, u, v, w, x, y, z, 2, 3, 4, 5, 6, 7, 8, 9)

Usability for the Voter

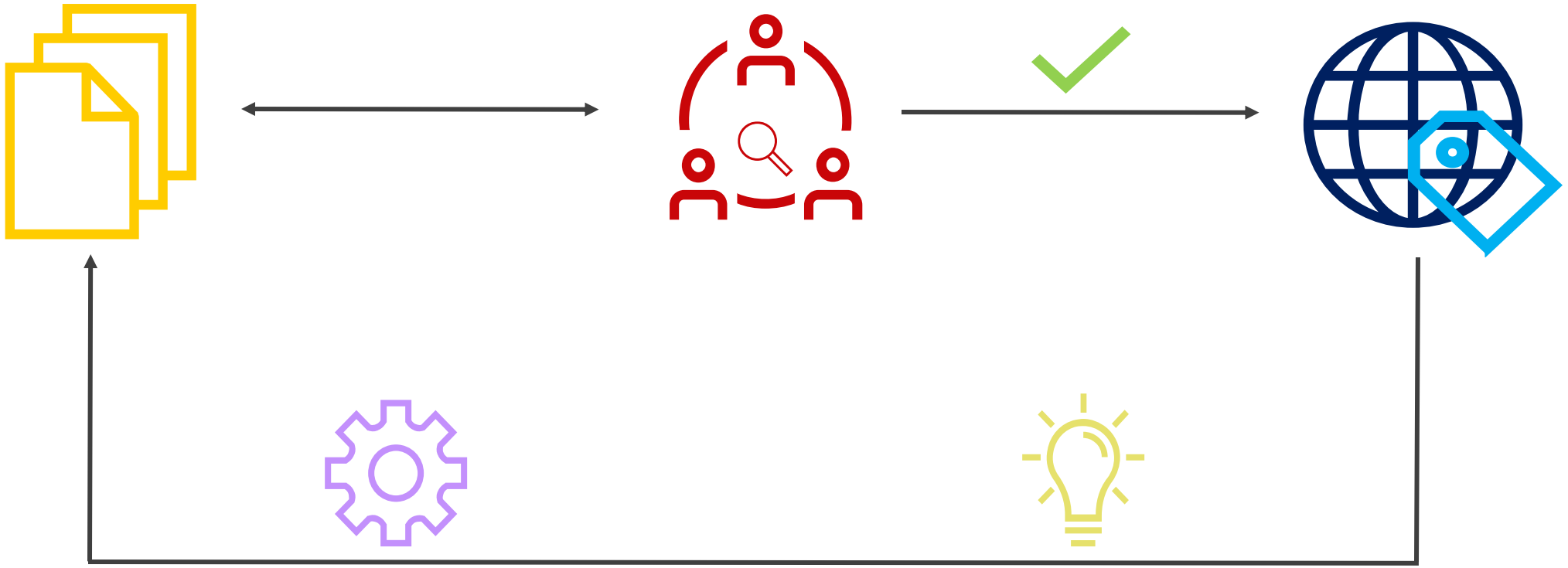
- The length of each code is carefully selected.
- Long codes are harder to copy, increase the chance of typing mistakes.
- If codes are too long, users may skip verification or make errors during the check.



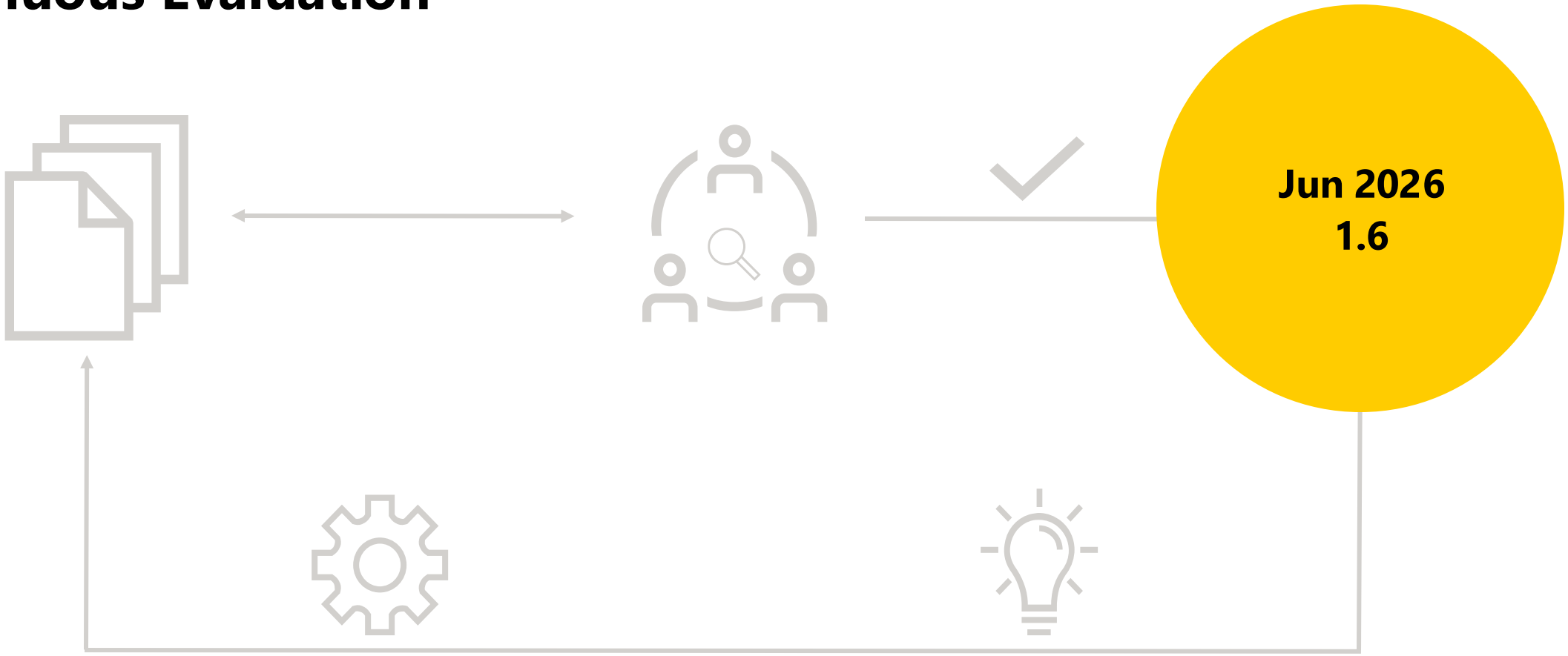
Continuous Improvement

Image created with Copilot AI

Continuous Evaluation



Continuous Evaluation



Community Involvement

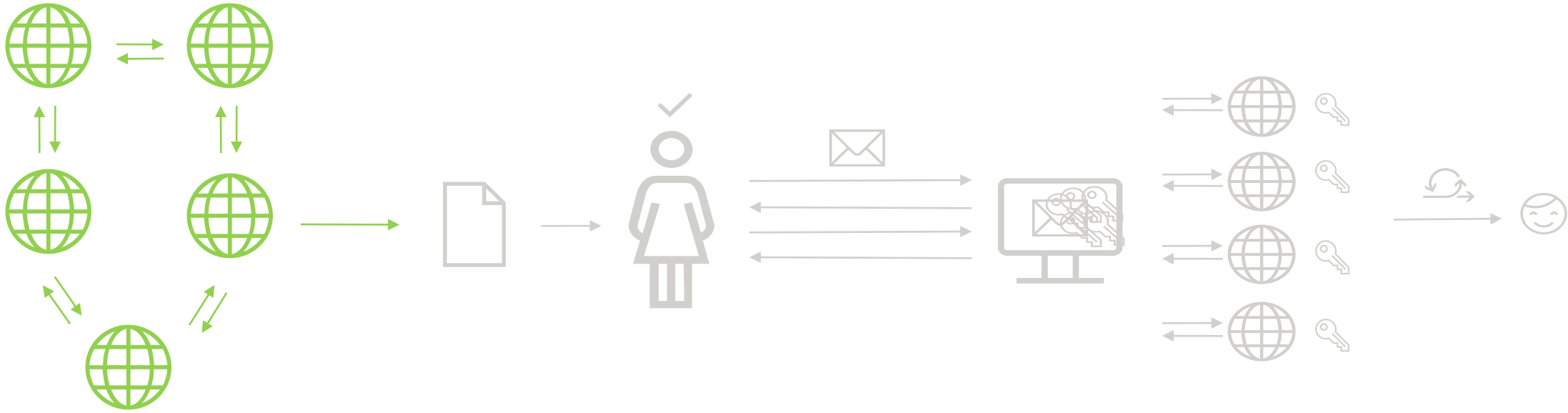
Bug Bounty Programme

Total reports	1108
Findings of "critical" severity	0
Findings of "high" severity	6
Findings of "medium" severity	38
Findings of "low" severity	101
Findings classed as "informative"	137
Total rewards paid out	€ 244 900

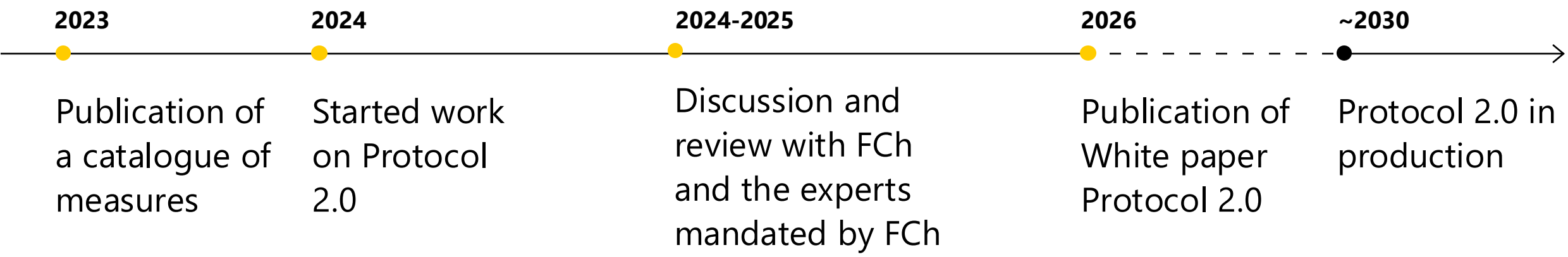
Events and Conferences:

- E-Vote-ID Conference (since 2016)
- Voxxed Days 2026
- Bärnhäckt 2025
- Academic seminars at universities
- … and much more!

Towards Protocol 2.0



Roadmap towards Protocol 2.0



What about post-quantum security?

- Currently, the security of the protocol relies on the hardness of the discrete logarithm which is not a post-quantum assumption
  - Post-quantum primitives are not yet usable and performant for e-voting systems

- Stronger requirement: not only the network, but even the system must not learn the vote

What can we do now?

- Hybrid post-quantum TLS
- No publication of encrypted ballots
- Voters use pseudonyms

Audhild Høgåsen
audhild.hoegaasen@post.ch
Chiara Spadafora
chiara.spadafora.1@post.ch

Grazie, Takk, Merci, Danke, Thank you

https://demo.evoting.ch/

https://gitlab.com/swisspost-evoting

https://swisspost-digital.ch/en/evoting-community/contributions