

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

Developers

Cryptographers

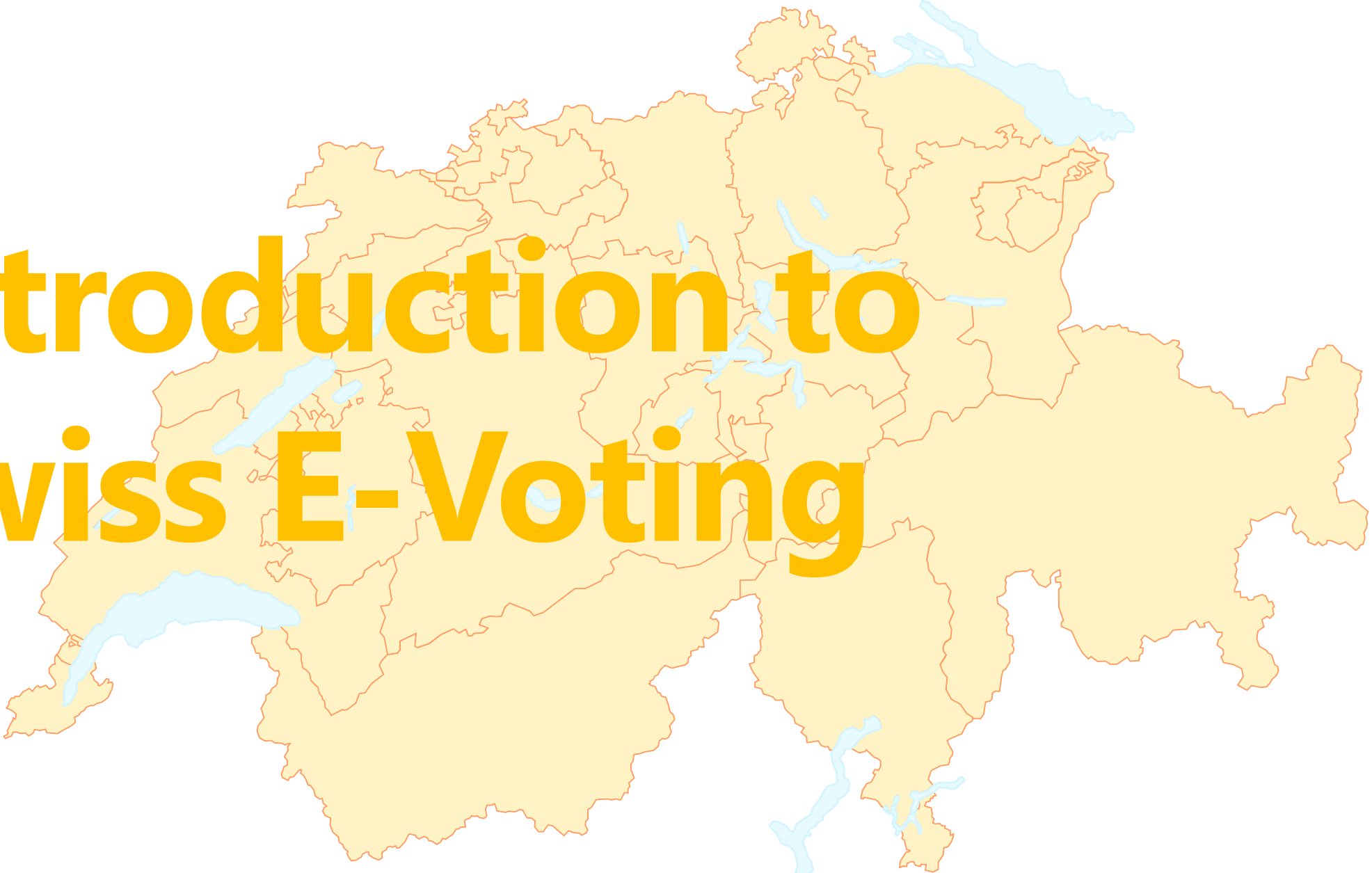
Testing & Operations

Architects

Solutions & Market

Management

Introduction to Swiss E-Voting

A map of Switzerland showing the boundaries of its 26 cantons. The landmass is colored in a light yellowish-orange, and the water bodies (lakes and rivers) are colored in a light blue. The map is centered on the Swiss territory.

E-Voting: why Swiss Post?

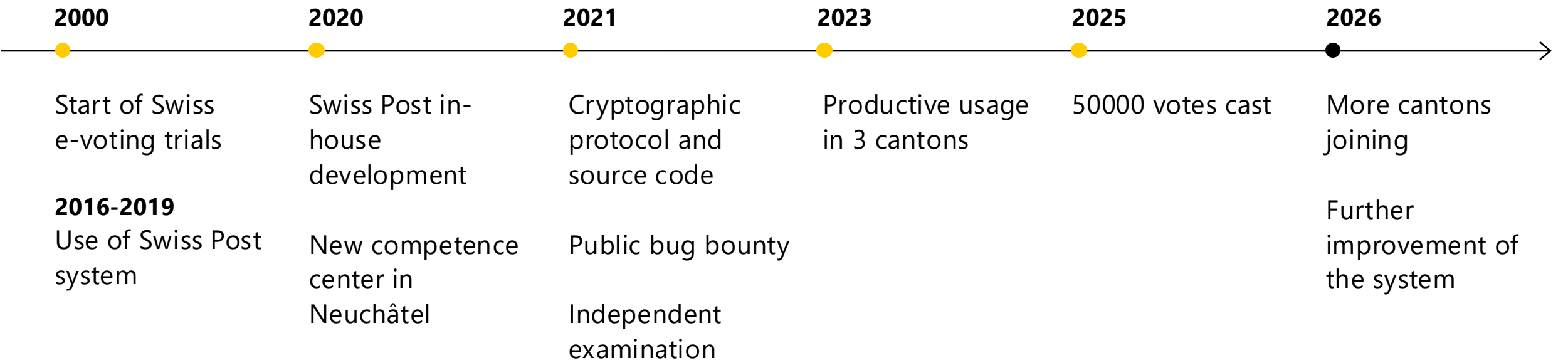
As a provider, Swiss Post offers cantons an electronic voting system that complies with legal requirements from the Confederation

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.

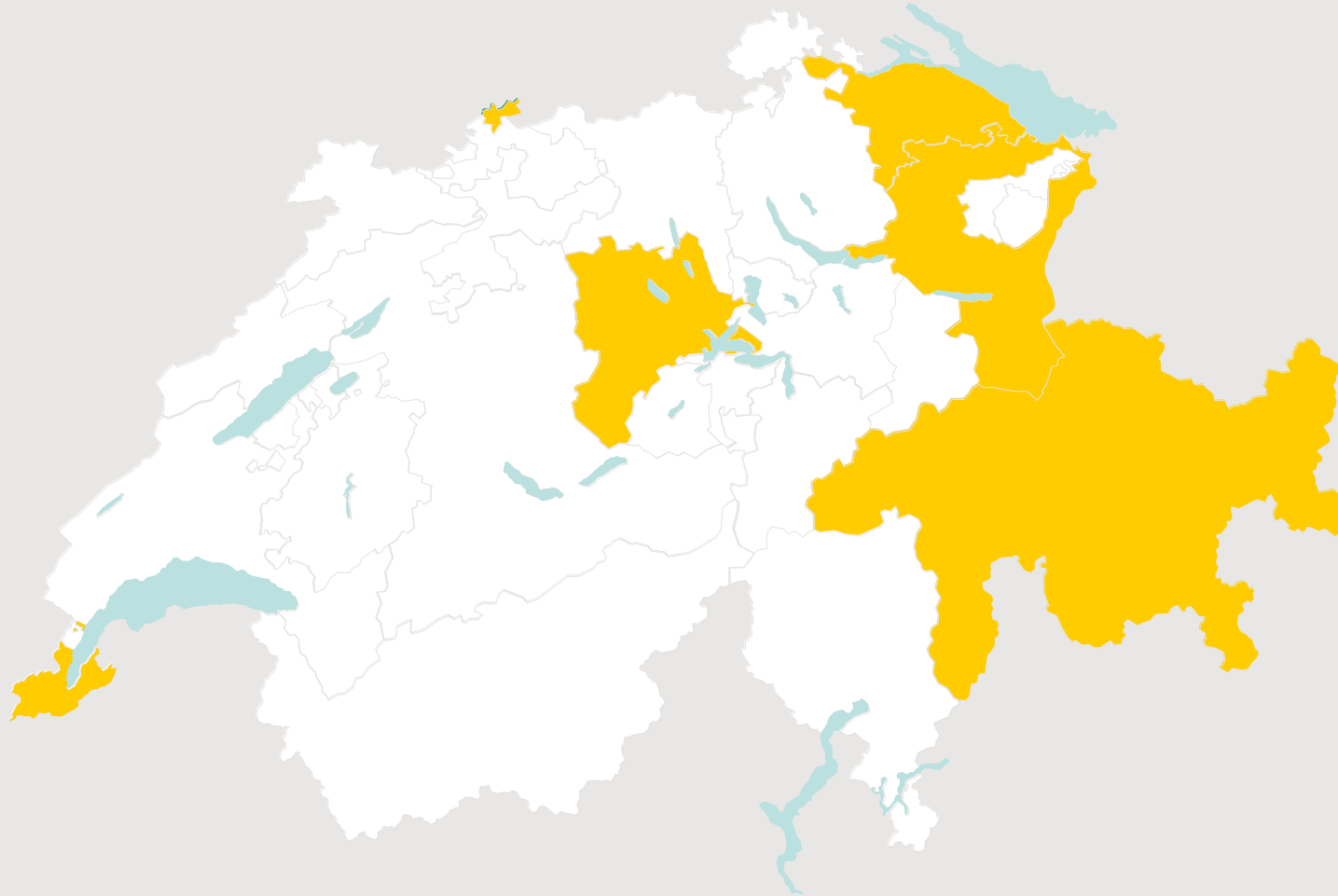
**How many votes
were cast electronically
in 2025 with the
Swiss Post Voting System?**

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 1^{er} juillet 2022)

La Chancellerie fédérale suisse (ChF),

vu les art. 27e, al. 1^{bis}, 27g, al. 2, 27i, al. 3, et 27l, 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.

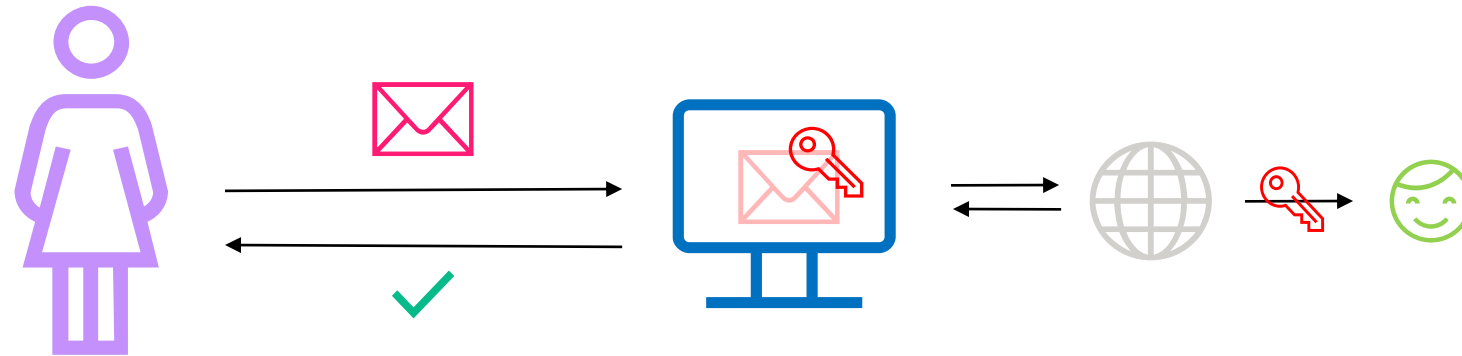
- individual verifiability
- universal verifiability

Verifiability

- vote secrecy and exclusion of premature results

Privacy

A Naïve Voting System



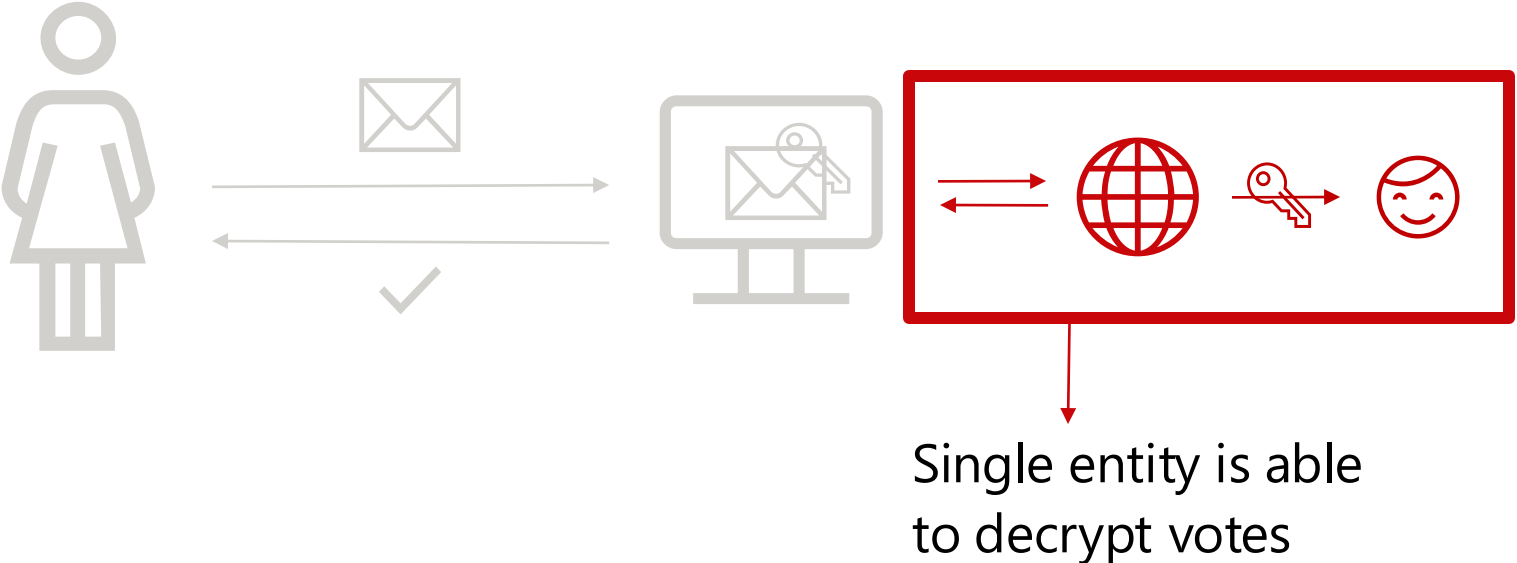
Usability 

Performance 

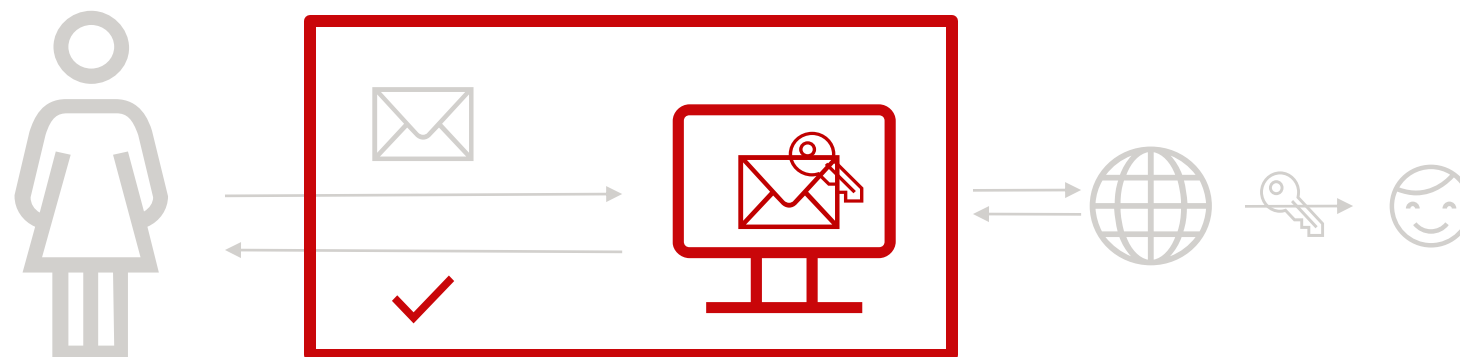
Privacy 

Verifiability 

How NOT to design a voting system

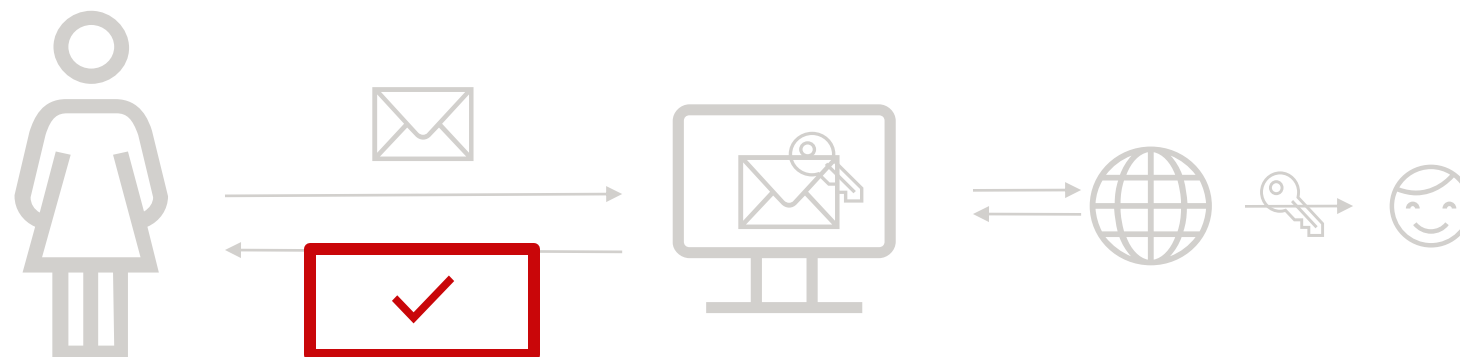


How NOT to design a voting system



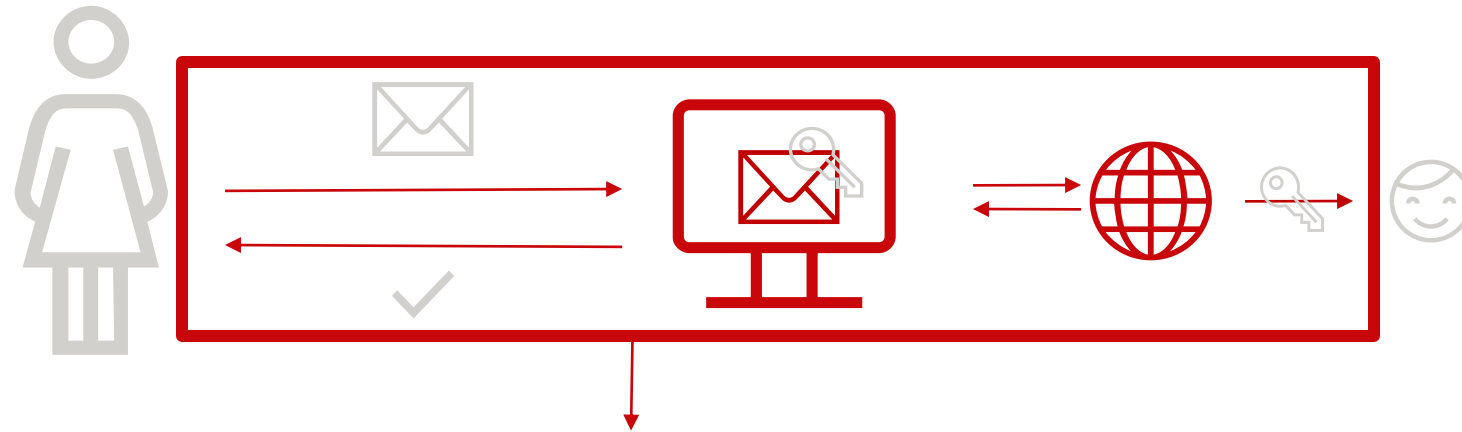
A malicious voter portal can modify the vote without the voter noticing

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

Two-Round Return Code Scheme

	Code d'initialisation 5rqs tt2e r26a xp24 b266 vh7p
	Codes de vérification <i>à partir de la page 2</i>
	Code de confirmation 5043 8364 4
	Code de finalisation 6403 0313

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 Frédéric	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

- ✓ Dispositions pénales
- 2 ▲ Démarrer le vote**
- 3 Saisir votre vote
- 4 Contrôler votre vote
- 5 ◆ Vérifier les codes
- 6 🏠 Saisir votre code de confirmation
- 7 ★ Vérifier le code de finalisation

2 Démarrer le vote

Saisissez votre code d'initialisation

Le code figure sur votre carte de vote.



Code d'initialisation

[? Qu'est-ce que le code d'initialisation?](#)

5 r q s t t 2 e r 2 6 a x p 2 4 b 2 6 6 v h 7 p



Vous pouvez écrire indifféremment en minuscules ou en majuscules.

Saisissez votre année de naissance

Cliquez ensuite sur Démarrer.

Année de naissance

1 9 7 1 |



Démarrer →

Voting Choice Selection

- ✓ Dispositions pénales
- ✓ ▲ Démarrer le vote
- 3 Saisir votre vote**
- 4 Contrôler votre vote
- 5 ◆ Vérifier les codes
- 6 🏠 Saisir votre code de confirmation
- 7 ★ Vérifier le code de finalisation

3 Saisir votre vote

Faites votre choix

Veillez cliquer sur le titre de la section pour la développer ou la masquer.

Démo Votation

Réduire ^

1. Aimez-vous le temps ensoleillé ?

Oui

Non

× [Effacer](#)

2. Aimez-vous le temps pluvieux ?

Oui

Non

× [Effacer](#)

Vote avec variantes

Réduire ^


1a. Acceptez-vous l'initiative populaire *Pour plus de musique classique ?*

Oui


Non


× [Effacer](#)

Voting Choice Encryption

 Une fois le vote chiffré et transmis, vous ne pourrez plus le modifier.

Tant que vous n'avez pas saisi le code de confirmation à l'étape 6 suivante, vous pouvez interrompre la procédure de vote électronique en tout temps et voter par correspondance ou à l'urne.

 [Modifier](#)

 Chiffrer et transmettre le bulletin de vote

 [Interrompre la procédure de vote](#)

Ballot Verification

- Dispositions pénales
- Démarrer le vote
- Saisir votre vote
- Contrôler votre vote
- 5 Vérifier les codes**
- Saisir votre code de confirmation
- Vérifier le code de finalisation

5 Vérifier les codes de vérification

Vérifiez à présent à l'aide des codes de vérification si votre vote a été transmis correctement

Pour cela, comparez les codes de vérifications affichés avec ceux figurant sur votre carte de vote. Les codes de vérification peuvent également se trouver sur une feuille séparée.

Codes de vérification [? Que sont les codes de vérification?](#)

Démo Votation Réduire ^

1. Aimez-vous le temps ensoleillé ?

Oui
◆ 6715

2. Aimez-vous le temps pluvieux ?

Non
◆ 1018

Codes de vérification

Démo Votation		
1. Temps ensoleillé	Oui 6715	Non 7336 Blanc 9080
2. Temps pluvieux	Oui 7618	Non 1018 Blanc 7298

Ballot Confirmation

The screenshot shows a web interface for ballot confirmation. On the left is a vertical progress bar with seven steps. Step 6, 'Saisir votre code de confirmation', is highlighted with a blue circle and a house icon. The main content area is titled '6 Saisir le code de confirmation' and contains the instruction 'Saisissez votre code de confirmation pour transmettre votre vote électronique'. Below this is a label 'Code de confirmation' with a question mark icon and a link 'Qu'est-ce que le code de confirmation?'. A text input field contains the digits '5 0 4 3 8 3 6 4 4' and a clear button 'X'. An information box below the input field states: 'Une fois que vous l'avez confirmé, votre vote est enregistré et vous ne pouvez plus voter par correspondance ou à l'urne.' At the bottom, there are three buttons: 'Interrompre la procédure de vote' (with an external link icon), 'Retour', and 'Confirmer le vote' (with a download icon).

✓ Dispositions pénales

✓ ▲ Démarrer le vote

✓ Saisir votre vote

✓ Contrôler votre vote

✓ ◆ Vérifier les codes

6 🏠 **Saisir votre code de confirmation**

7 ★ Vérifier le code de finalisation

6 Saisir le code de confirmation

Saisissez votre code de confirmation pour transmettre votre vote électronique

Code de confirmation [? Qu'est-ce que le code de confirmation?](#)

5 0 4 3 8 3 6 4 4 X

i Une fois que vous l'avez confirmé, votre vote est enregistré et vous ne pouvez plus voter par correspondance ou à l'urne.

[↗ Interrompre la procédure de vote](#) [Retour](#) **Confirmer le vote** ↓

Ballot Finalization

- ✓ Dispositions pénales
- ✓ ▲ Démarrer le vote
- ✓ Saisir votre vote
- ✓ Contrôler votre vote
- ✓ ◆ Vérifier les codes
- ✓ ⬛ Saisir votre code de confirmation
- 7 ★ Vérifier le code de finalisation**

7 Vérifier le code de finalisation

Veillez comparer le code de finalisation avec celui qui figure sur votre carte de vote

★ Code de finalisation [? Qu'est-ce que le code de finalisation?](#)

6403 0313

Le code ne correspond pas Le code correspond

b266 vh7p

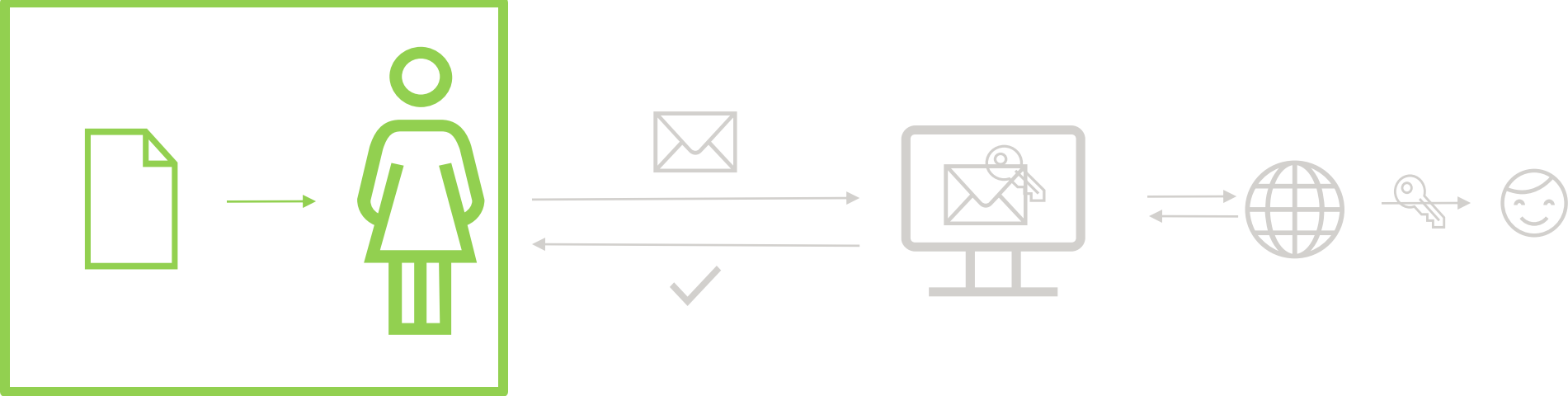
⬛ Code de confirmation
5043 8364 4

★ Code de finalisation
6403 0313

Individual Verifiability

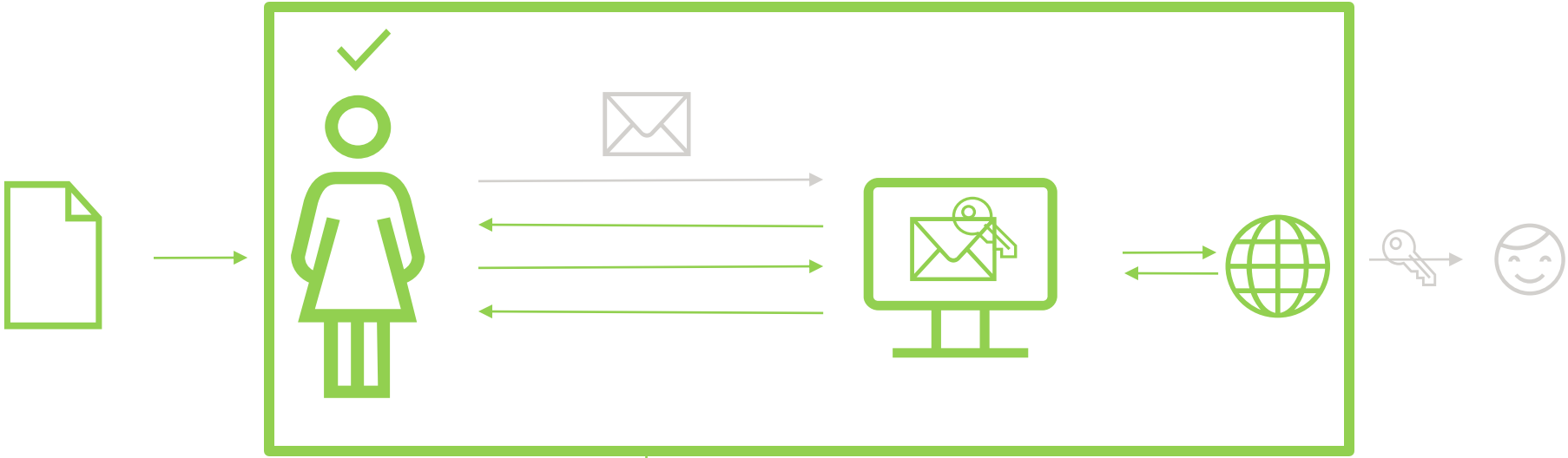


Individual Verifiability



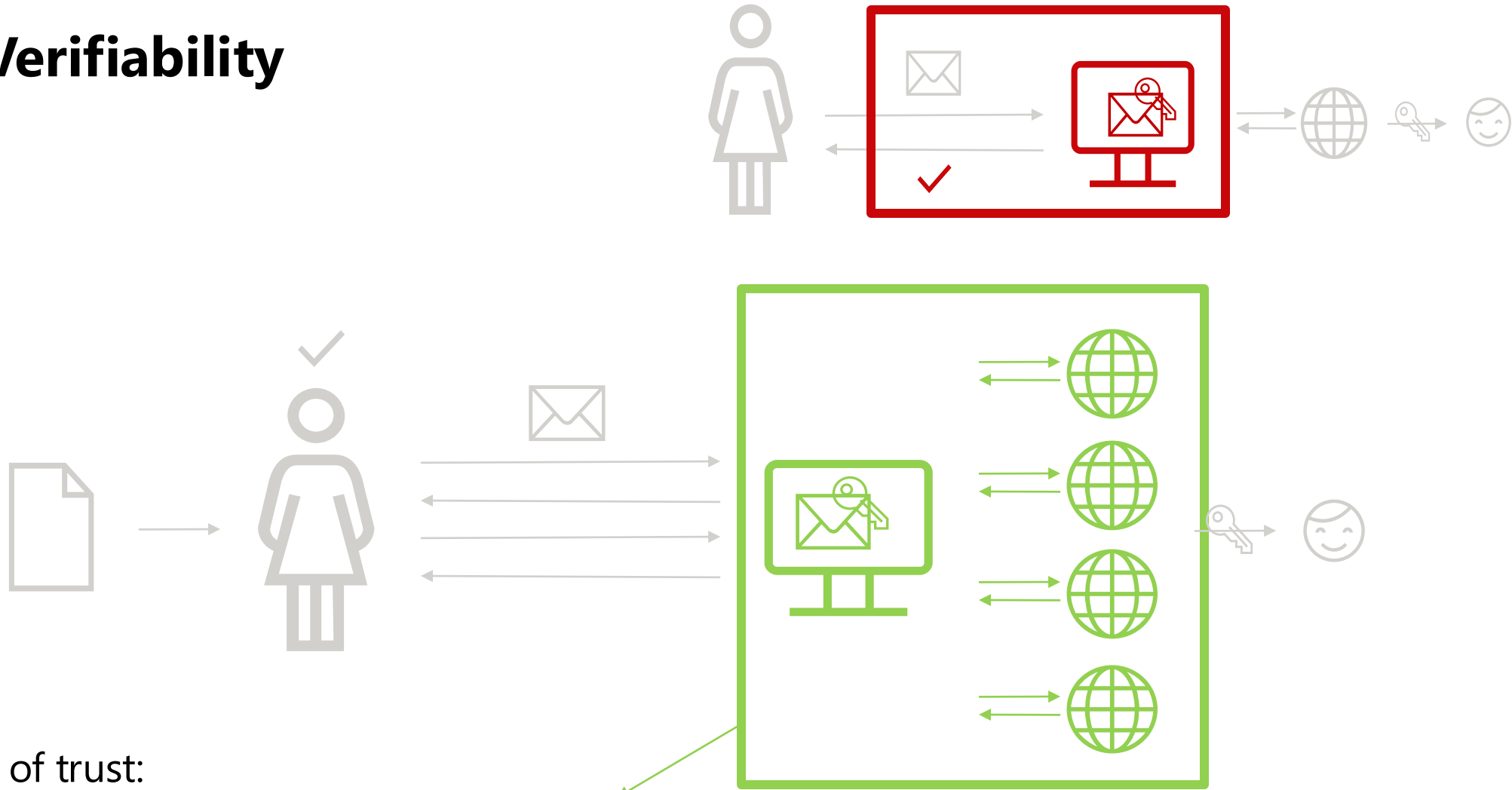
The voter receives a voting card by postal mail, containing codes that are unique to both the voter and the specific election

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

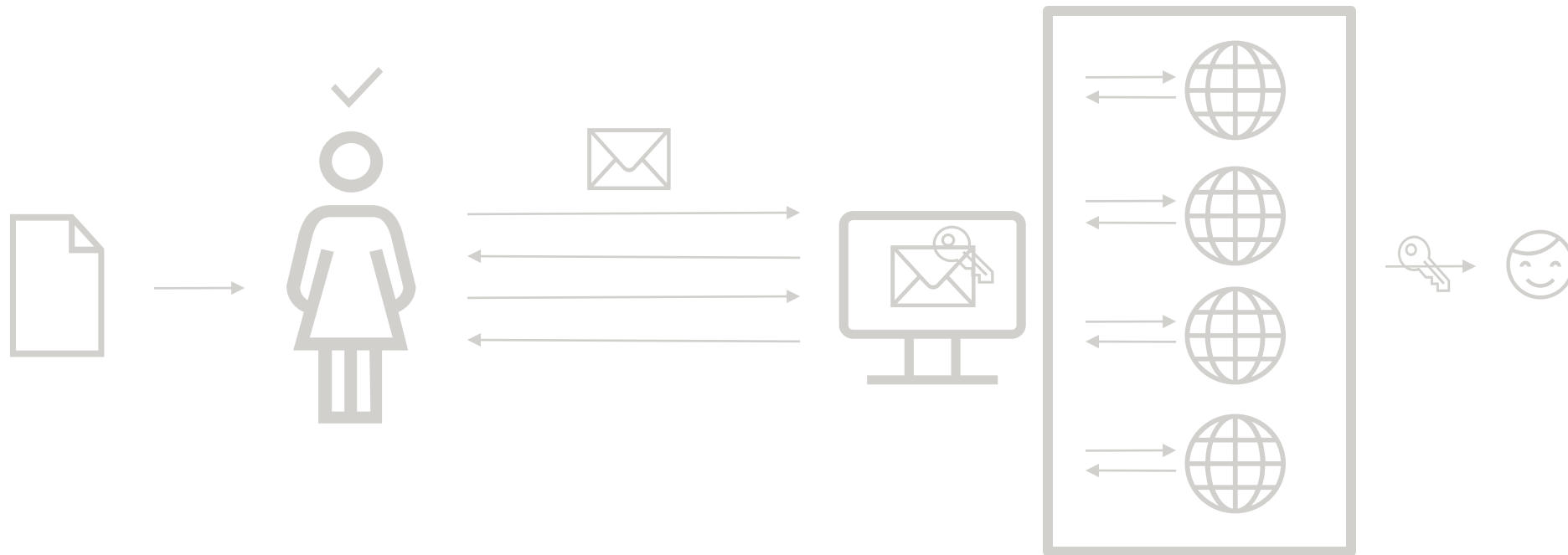
Individual Verifiability



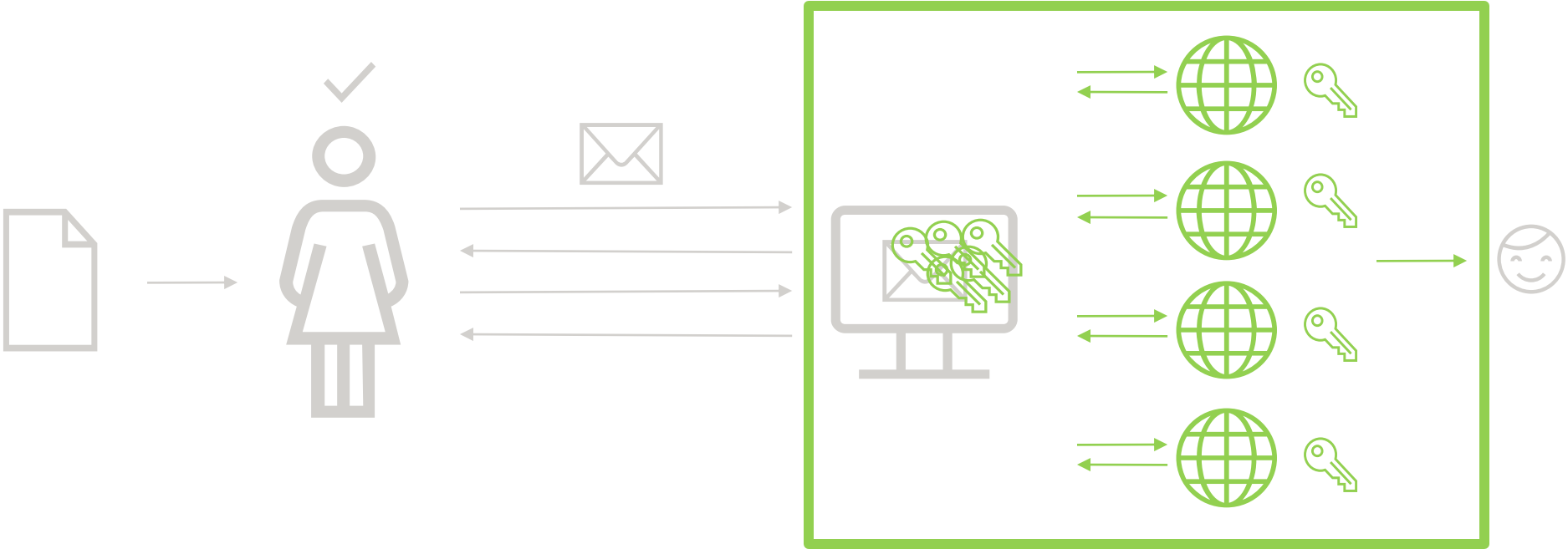
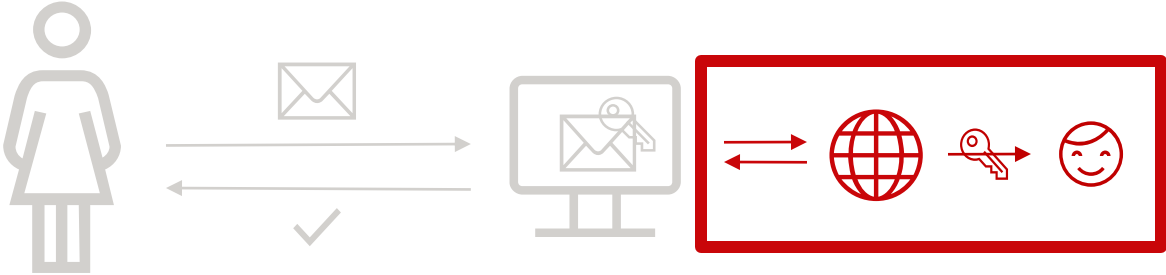
Distribution of trust:

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

Vote Privacy

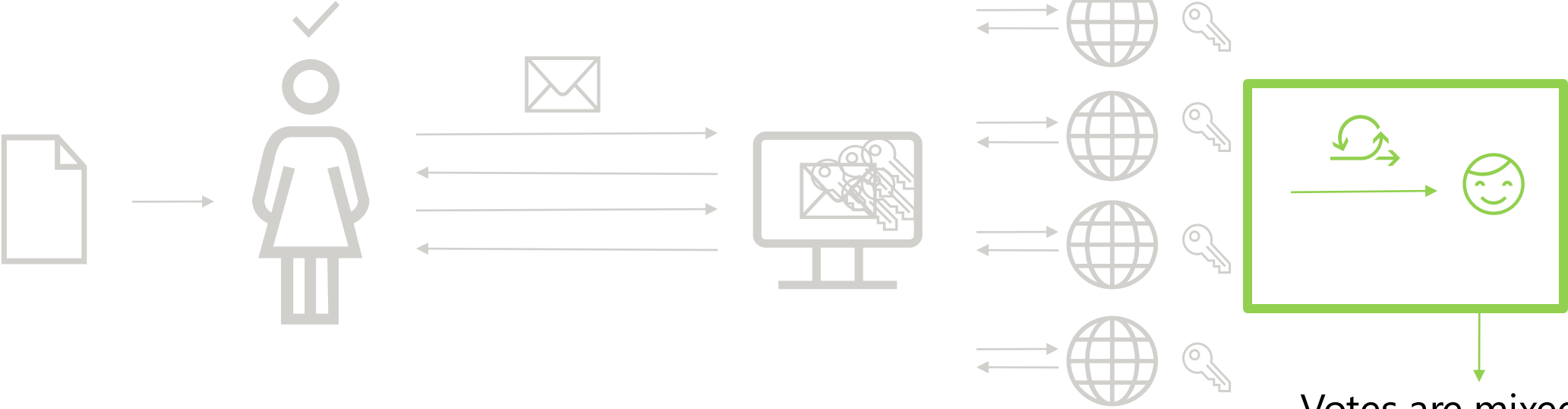
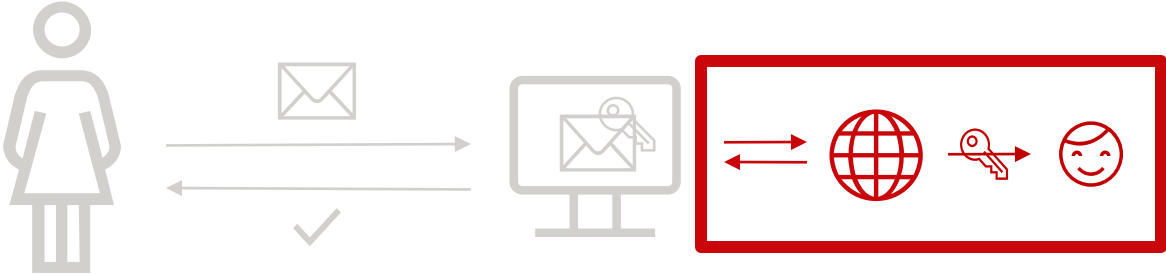


Vote Privacy



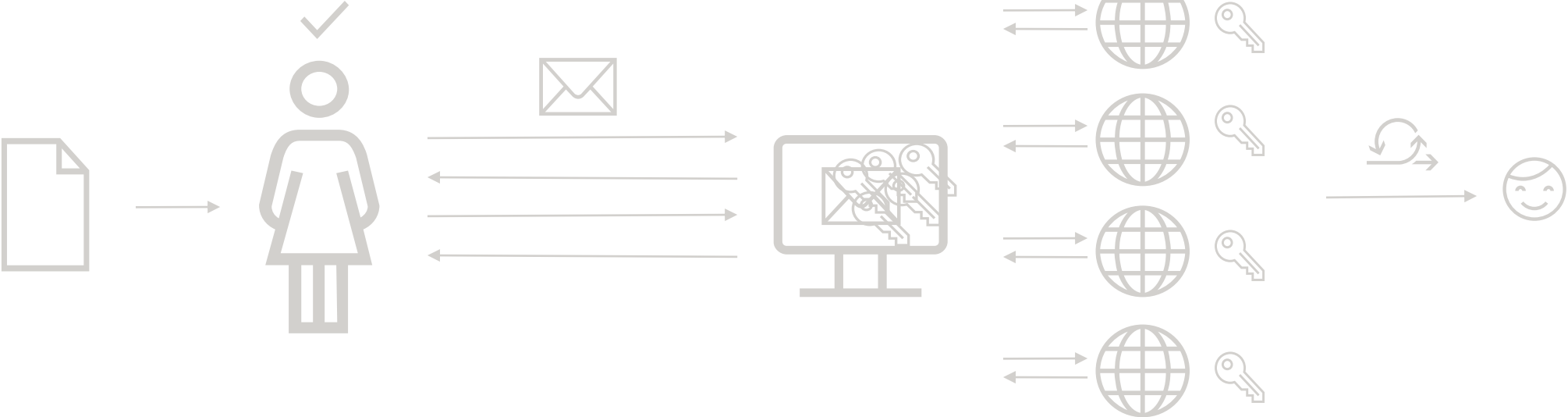
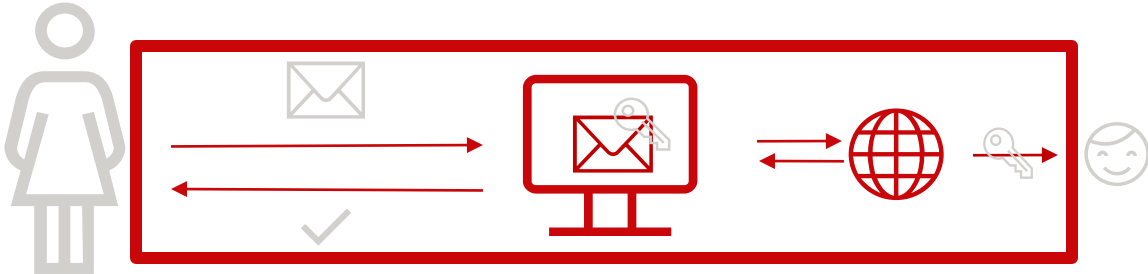
No single authority is able to decrypt the votes

Vote Privacy

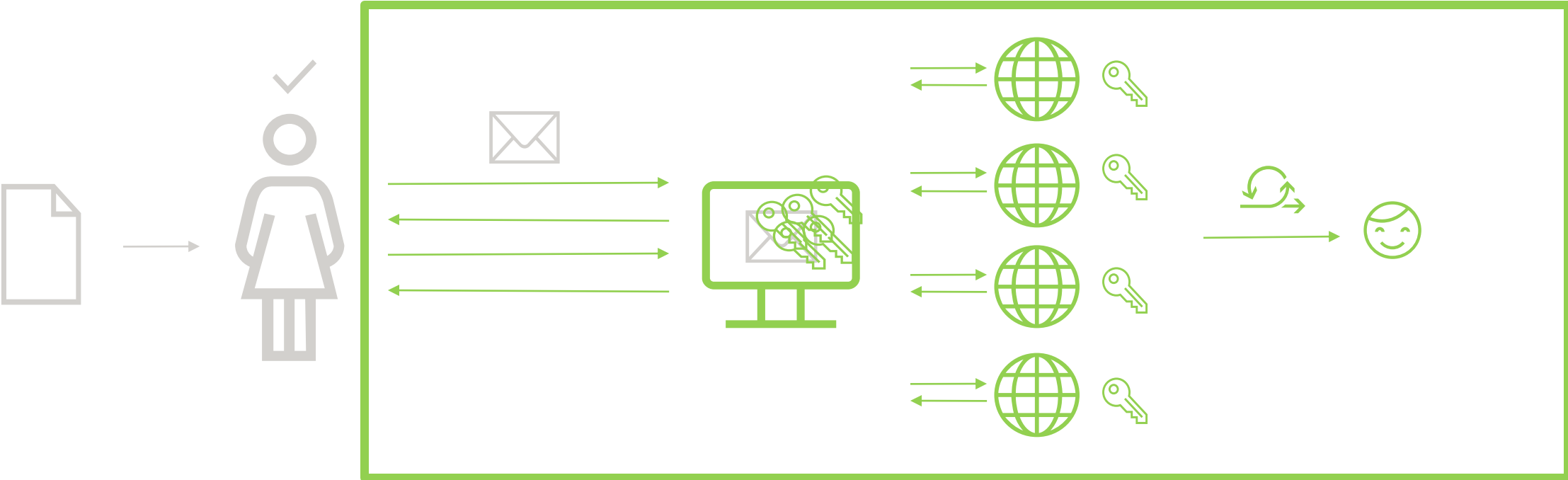
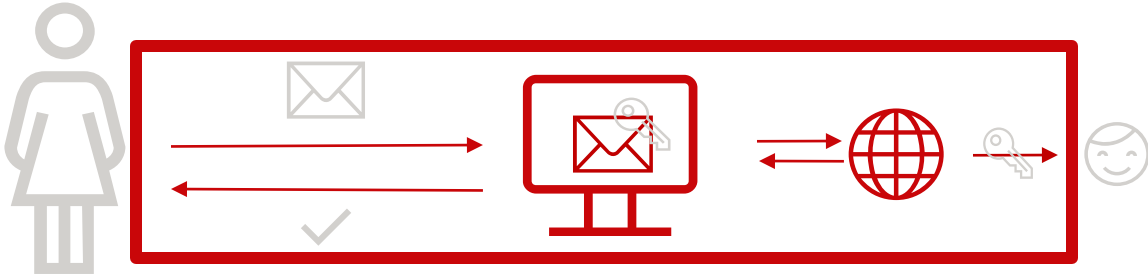


Votes are mixed before being decrypted

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

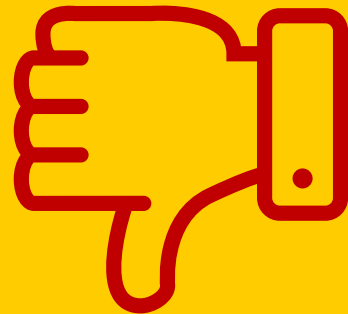
**It is possible to stop the voting process
and resume on a different device at any
time in the voting period**



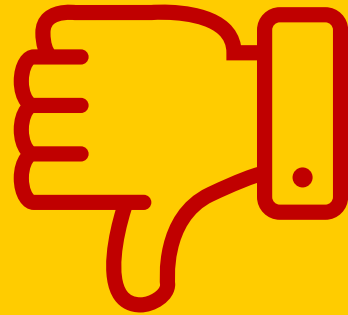
**One voting card can only be used to
cast one single vote.
No re-voting possible**



**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: Maintainability

Code and Specification Maintainability

System complexity makes maintenance challenging, ~200,000 lines of code

All code must be fully auditable and publicly available together with:

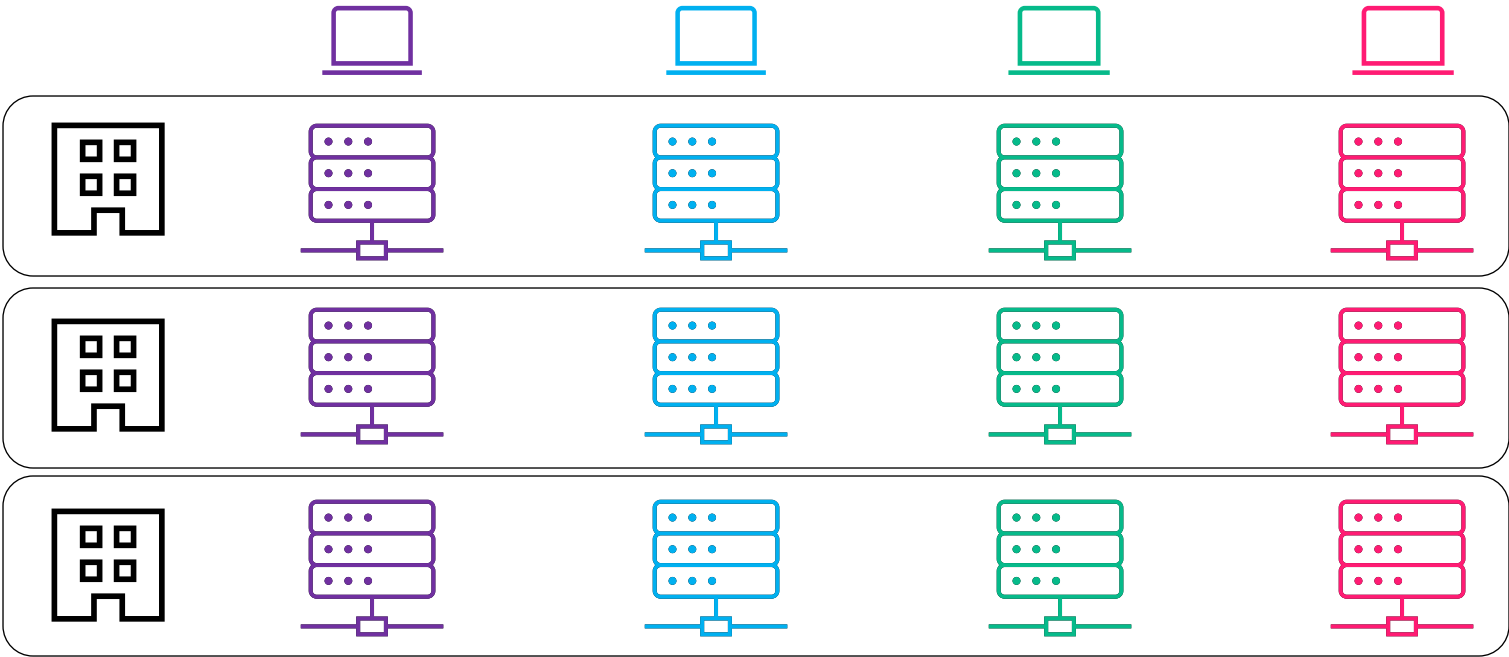
- Specifications and pseudocode
- Computational and symbolic proofs
- Architecture and design documents

Clear alignment between all artefacts is crucial for auditability

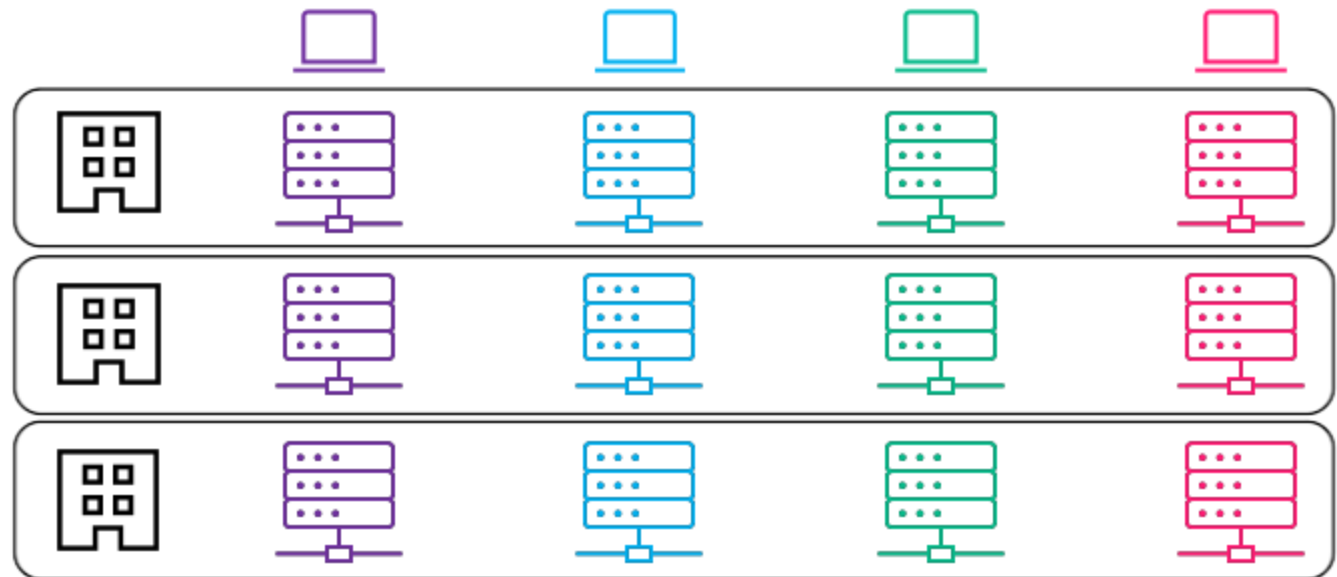
Documentation helps understanding and auditing

But updates require time and effort

Hardware Maintainability



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



A high-angle photograph of a large, intricate maze constructed from green hedges. The maze is composed of many rectangular paths and dead ends, creating a complex, winding pattern. The hedges are a vibrant green color, and the ground between them is a dark, shadowed brown. The lighting is dramatic, with strong highlights on the top edges of the hedges and deep shadows in the recesses, emphasizing the three-dimensional structure of the maze. The overall atmosphere is one of complexity and challenge.

Challenge: Usability

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.

Élection proportionnelle

▲ Code d'initialisation	5rqs tt2e r26a xp24 b266 vh7p	
◆ Codes de vérification <i>à partir de la page 2</i>		
⬠ Code de confirmation	5043 8364 4	
★ Code de finalisation	6403 0313	

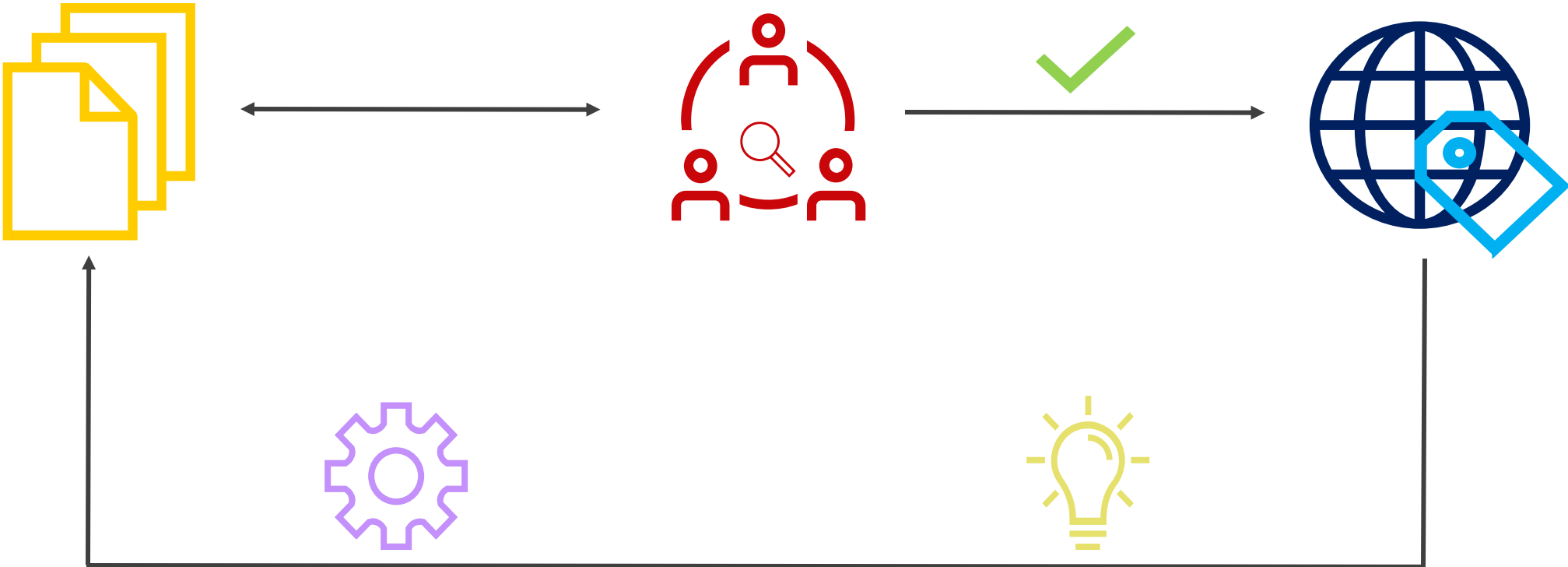
	1x	2x
siatrices	7689	
	5914	3109
	1769	3073
	6451	
	6311	9927
	3998	1178
	5316	
	4214	
	0289	
	7058	
	9849	

Aucun nom sélectionné

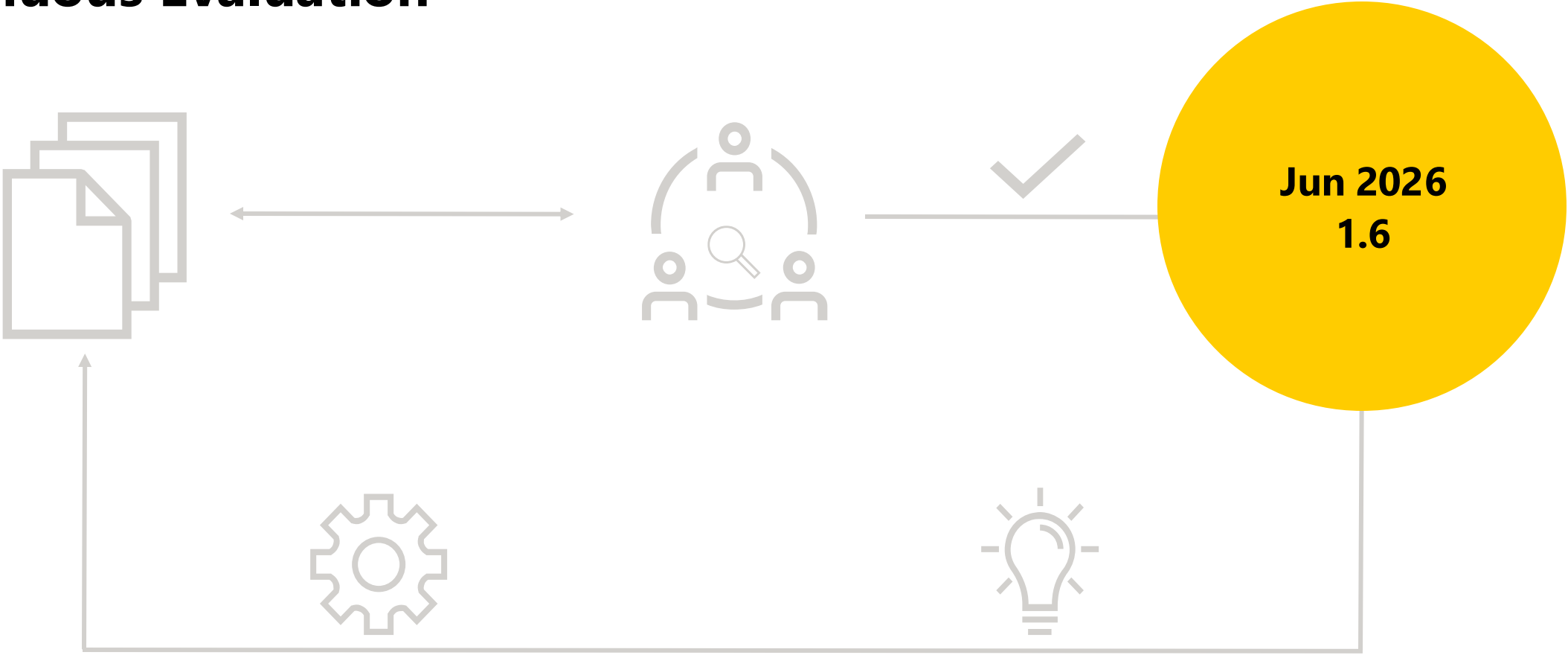
Continuous Improvement



Continuous Evaluation



Continuous Evaluation



Community Involvement

Bug Bounty Programme

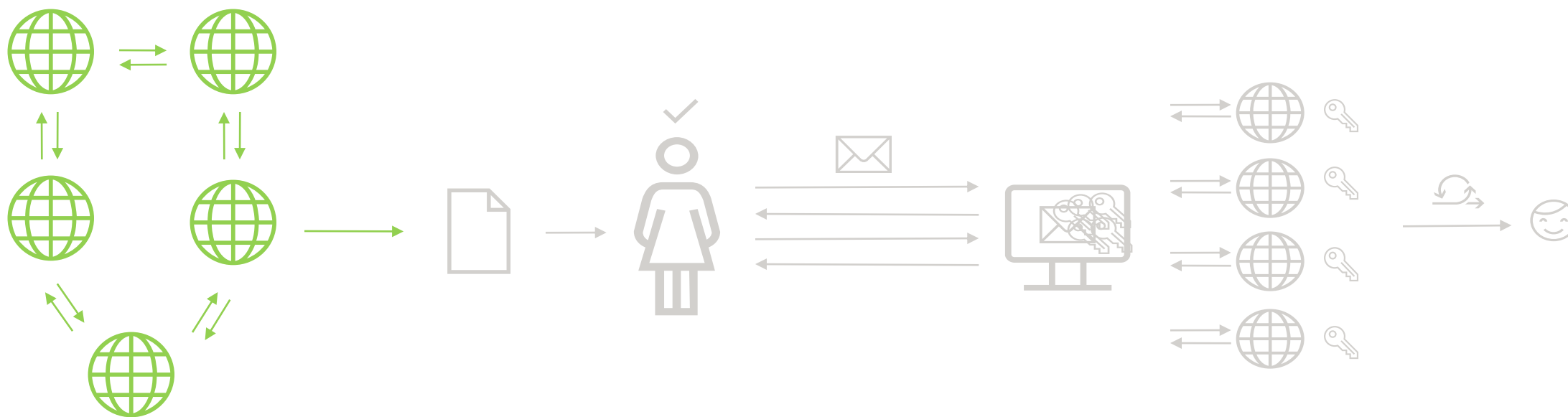
Total reports
Findings of "critical" severity
Findings of "high" severity
Findings of "medium" severity
Findings of "low" severity
Findings classed as "Informative"
Total rewards paid out

1108
0
6
38
101
137
€ 244 900

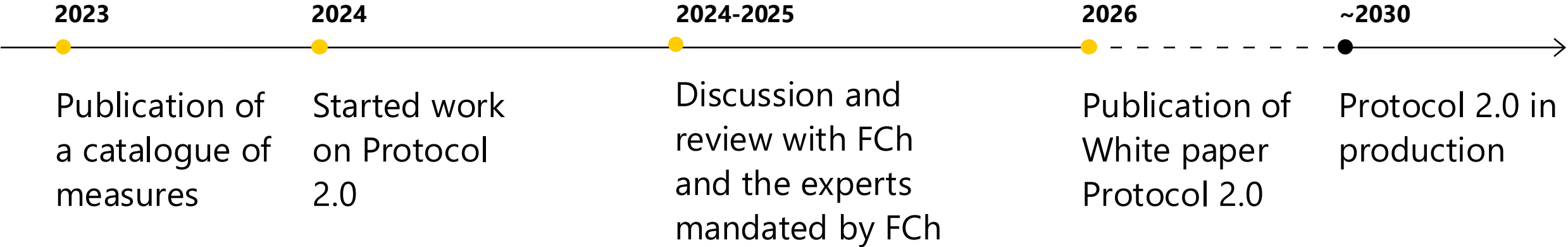
Events and Conferences:

- 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



Grazie, Takk, Merci, Danke, Thank you

Audhild Høgåsen

audhild.hoegaasen@post.ch

Chiara Spadafora

chiara.spadafora.1@post.ch

<https://demo.evoting.ch/>



<https://gitlab.com/swisspost-evoting>



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

