Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

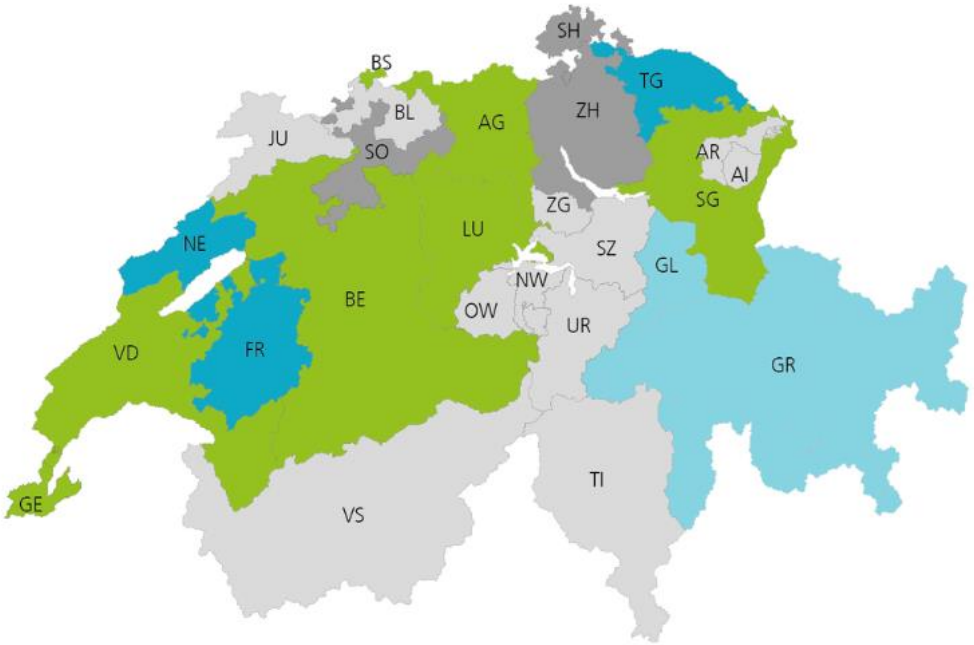
Bundeskanzlei BK
Sektion Politische Rechte

Trust in E-Voting

Oliver Spycher at Swiss Cyber Storm

Bern, 30th October 2018

E-Voting introduced by Cantons



- CHvote system: developed by GE; AG, BE, BS*, LU, SG and VD have joined.
- Swiss Post solution: FR, NE, TG. GL and GR are planning reintroduction in 2019 respectively 2020.
- These cantons carried out electronic voting trials up to the end of 2015.
- These cantons have not yet carried out any electronic voting trials.

*BS will change over to the Swiss Post system (probably in 2019).

Moving ahead step by step

- Trials since 15 years
- Open to 3.8% of the overall electorate (September 2018)
- Security first

Eckdaten zum Einsatz der elektronischen Stimmabgabe am 23. September 2018

Bedingungen / Kantone	Zugelassenes Elektorat Anzahl Stimmberechtigte (A)			Stimmbeteiligung zugelassenes Elektorat alle Kanäle (B)		Anteil elektronischer Stimmkanal (C)		
	Inland	Ausland	Total	Anzahl Stimmende	in %	Anzahl Stimmende	in % am zugelassenen Elektorat (A)	in % an allen eingegangenen Stimmen (B)
Bern	-	17 742	**17 742**	k.A.*	k.A.*	3 380	19.05	k.A.*
Luzern	-	4 944	4 944	1 461	29.55	919	18.59	62.90
Freiburg	1 025	6 040	**7 065**	2 198	31.11	1 047	14.82	47.63
Basel-Stadt	37	8 384	**8 421**	2 304	27.36	1 469	17.44	63.76
St. Gallen	37 778	8 096	**45 874**	18 038	39.32	4 377	9.54	24.27
Aargau	-	9 720	**9 720**	2 292	23.58	1 448	14.90	63.18
Thurgau	-	3 649	**3 649**	1 017	27.87	527	14.44	51.82
Neuenburg	29 059	566	**29 625**	k.A.*	k.A.*	4 643	15.67	k.A.*
Genf	48 171	26 406	**74 577**	***	***	19 461	26.10	***
Total	**116 070**	**85 547**	**201 617**	**27 310**	***	**37 271**	**18.49**	***

www.bk.admin.ch

People need to trust that…

- Result reflects the voters' intentions
- Secrecy of the vote is respected

→ …**even if they're not an observer**

Trust in Will and Ability

Trust One Trustee

…out of many

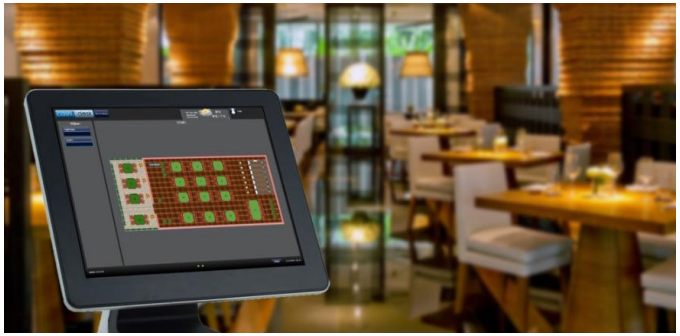
Trust in Will and Ability

E-Voting cannot be trusted…

- Transparency…
  - …inherently impossible
  - …only towards experts
  - …eats secrecy
- No meaningful recounts
- And anyhow, administrations will fail

Sure about that?

Trust through verification



[redacted]

RECHNUNG 9125
Tisch 27

1 2,5dl Lager	5,20	0201
2 geb.Crevetten	58,80	0004
2 Rindsf.Madagask	95,60	0024
2 Beilage Mais Kr	19,60	0042
1 Fl.Poggio	52,00	0461
1 5dl Min.mit	7,00	0223
1 Flan Caramel	10,50	0083
1 Coupe Waldbeere	12,50	0085
2 Kaffee Träsch	12,20	0278

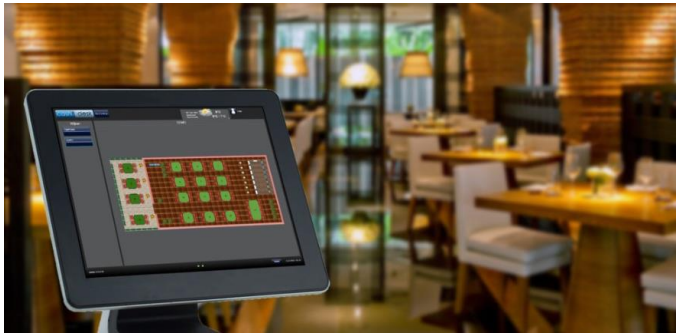
SUMME FR. 273.40

NETTO 08.0%	253,15
MWST 08.0%	20,25

Datum: 06.12.2016 Beat 2
MWST CHE-112.433.949

BESTEN DANK

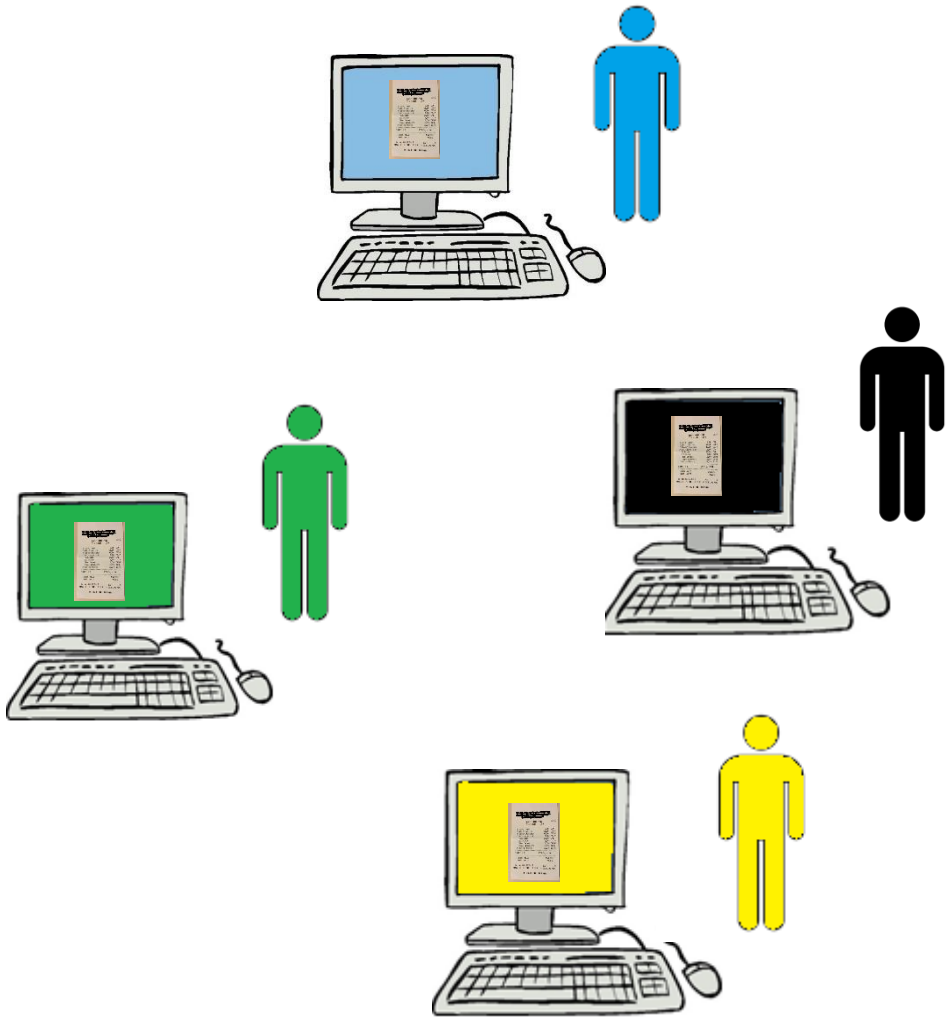
Trust through re-verification



Trust through verification

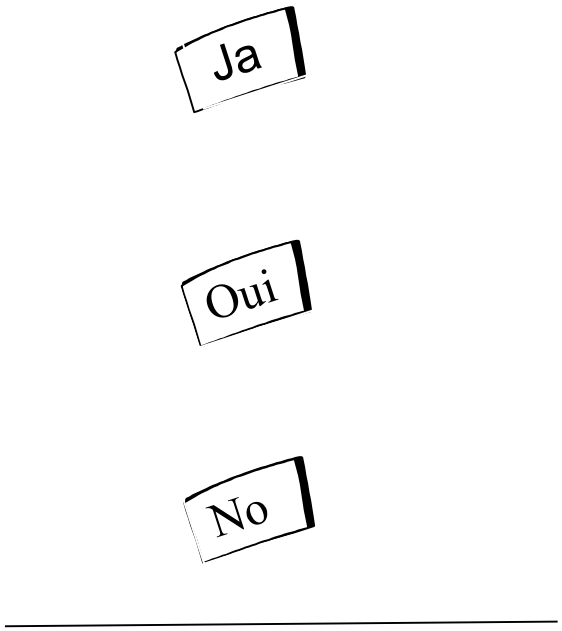
e-mail

Trust through re-verification



Summing up votes is verifiable…

…by checking equations



Ja : 2
Nein: 1

Full Verifiability

Voters or observers verify that votes have been

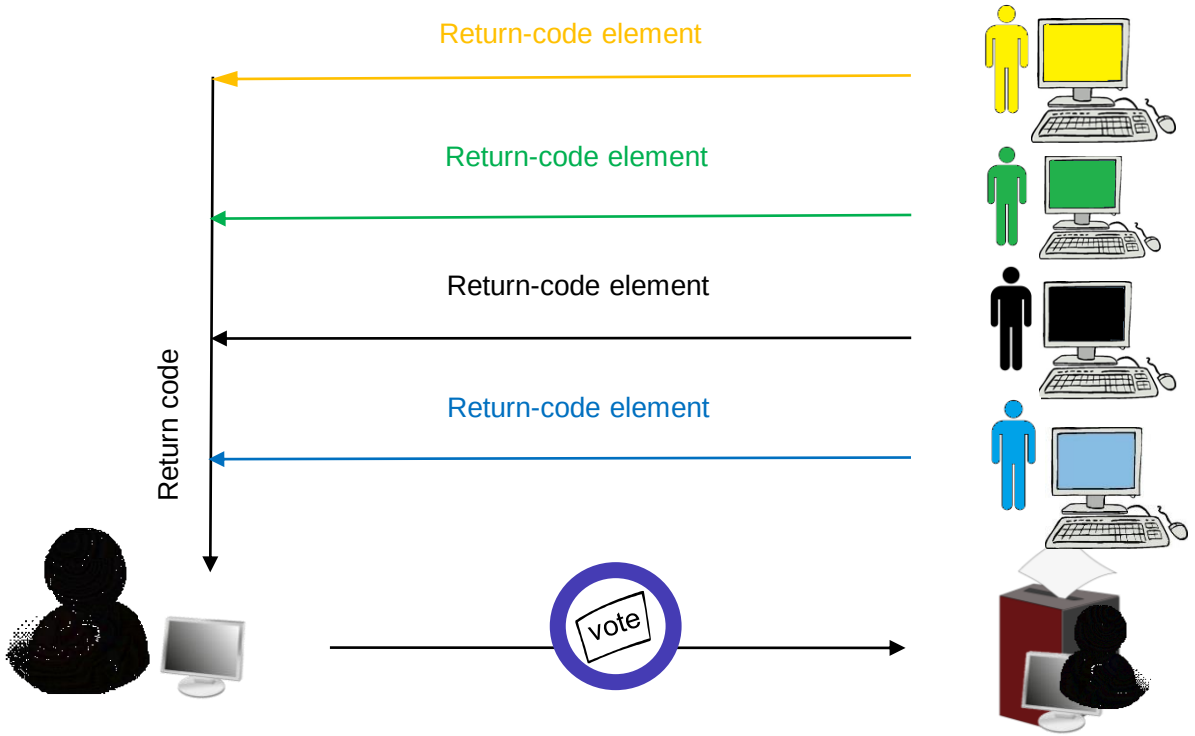
- cast as intended
- recorded as cast
- tallied as recorded

Cast as intended

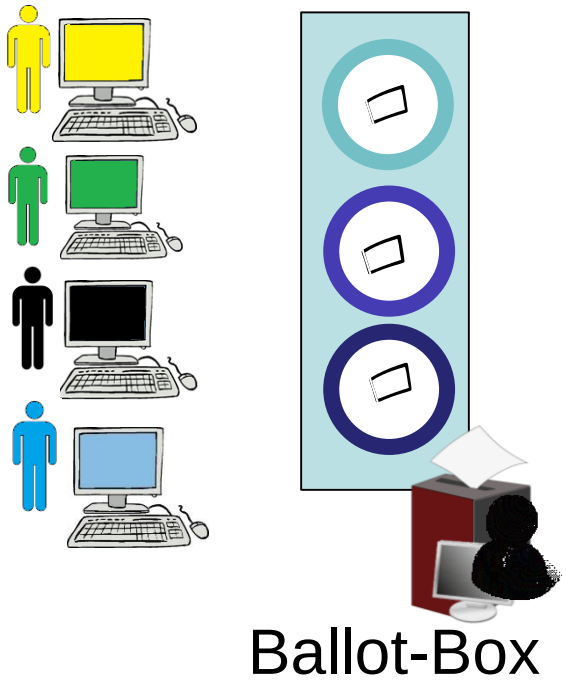
N°	Démo Votation populaire fédérale / Demo Eidgenössische Volksabstimmung	Codes de vérification / Prüfcodes				
		Oui / Ja	Non / Nein	Blanc / Leer	Initiative / Initiative	Contre-projet / Gegenentwurf
1a	Initiative populaire: Acceptez-vous «l'initiative populaire A»? *Volksinitiative: Wollen Sie die «Volksinitiative A» annehmen?*	1299	2023	1610		
1b	Contre-projet: Acceptez-vous le contreprojet de l'Assemblée fédérale «Contre-projet B»? *Gegenentwurf: Wollen Sie den Gegenentwurf der Bundesversammlung «Gegenentwurf B» annehmen?*	0027	4701	8186		
1c	Question subsidiaire: Si le peuple et les cantons acceptaient à la fois «l'initiative A» et «le contre-projet B»: Est-ce l'initiative populaire A ou le contre-projet B qui doit entrer en vigueur? *Stichfrage: Falls sowohl die «Volksinitiative A» als auch der «Gegenentwurf B» von Volk und Ständen angenommen werden: Soll die Volksinitiative A oder der Gegenentwurf B in Kraft treten?*			3009	9991	9194
2	Acceptez-vous l'arrêté fédéral «C» du 28 février 2017? *Wollen Sie den Bundesbeschluss «C» vom 28. Februar 2017 annehmen?*	5040	7313	0619		

Taken from the online demo-system by Swiss Post at e-voting.ch

Cast as intended

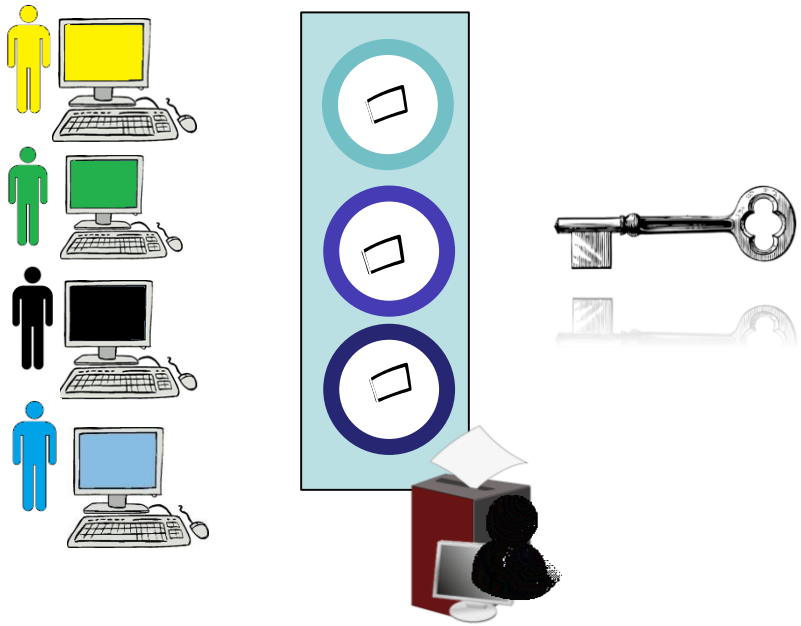


Recorded as cast



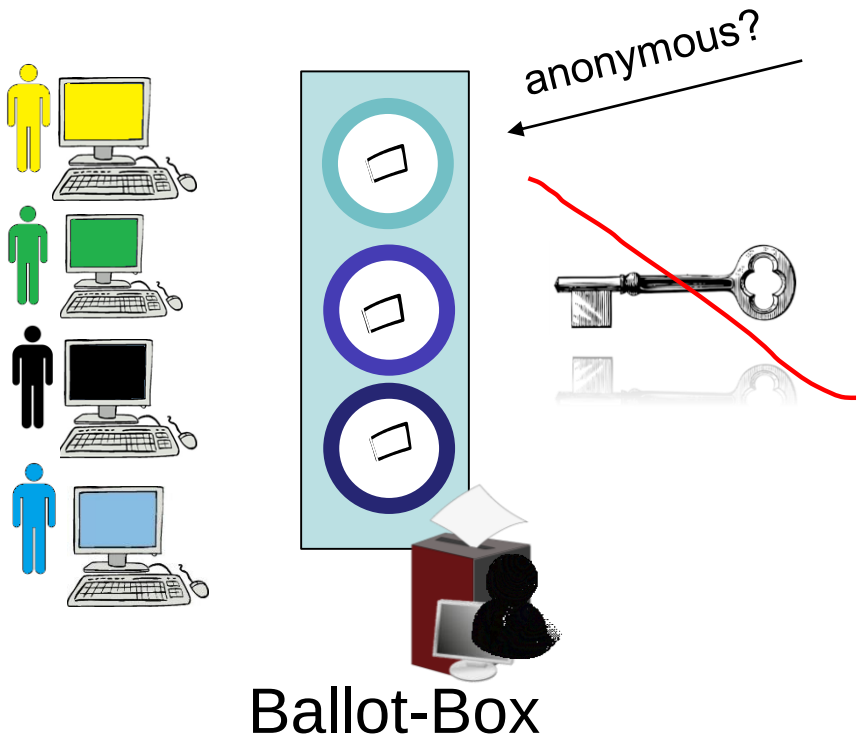
Ballot-Box

Tallying

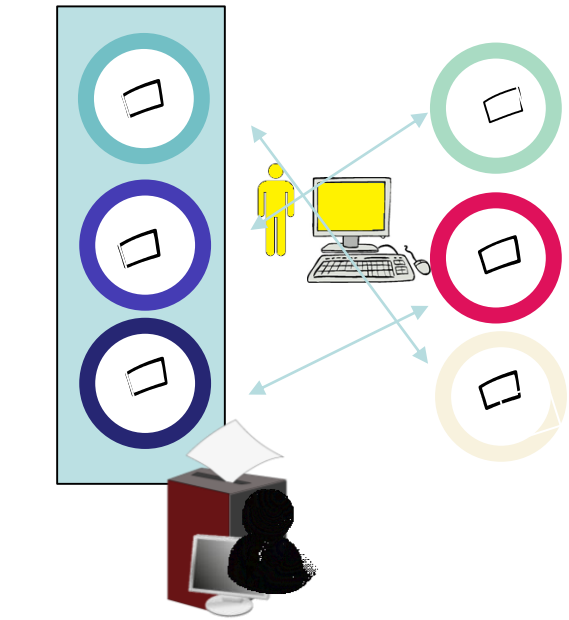


Ballot-Box

Tallying



Secrecy

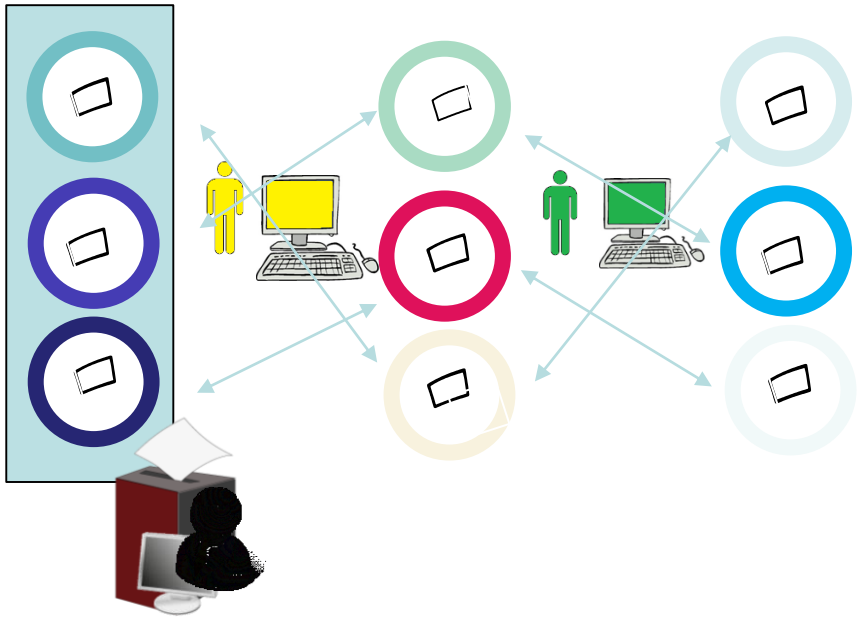


Ballot-Box

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

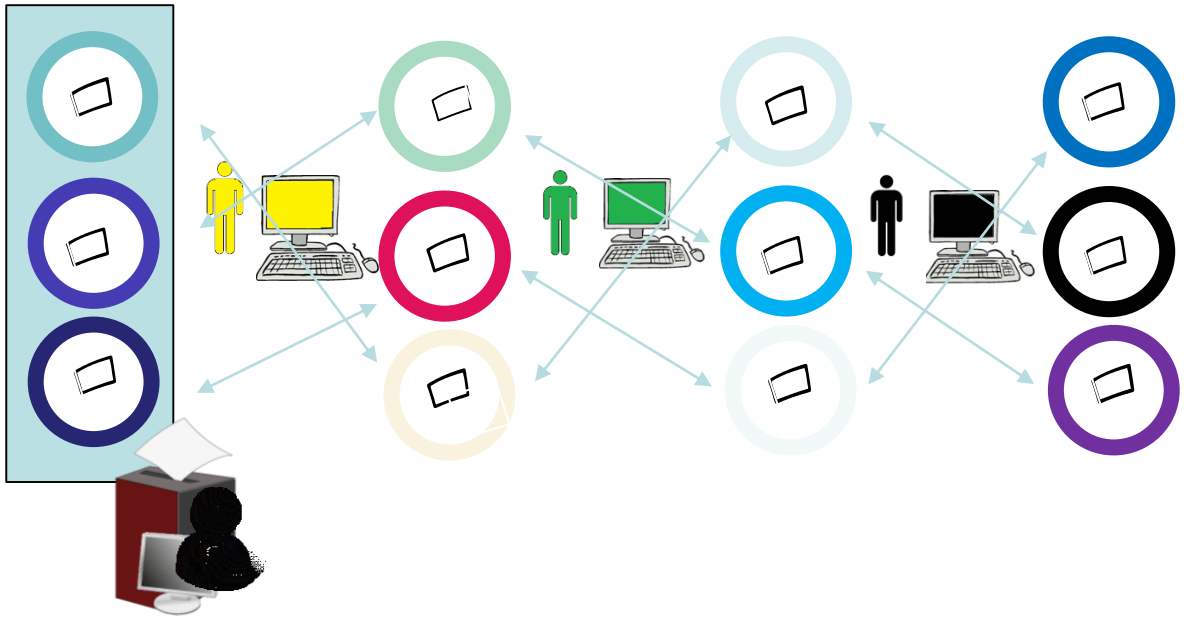
Bundeskanzlei BK
Sektion Politische Rechte

Secrecy



Ballot-Box

Secrecy

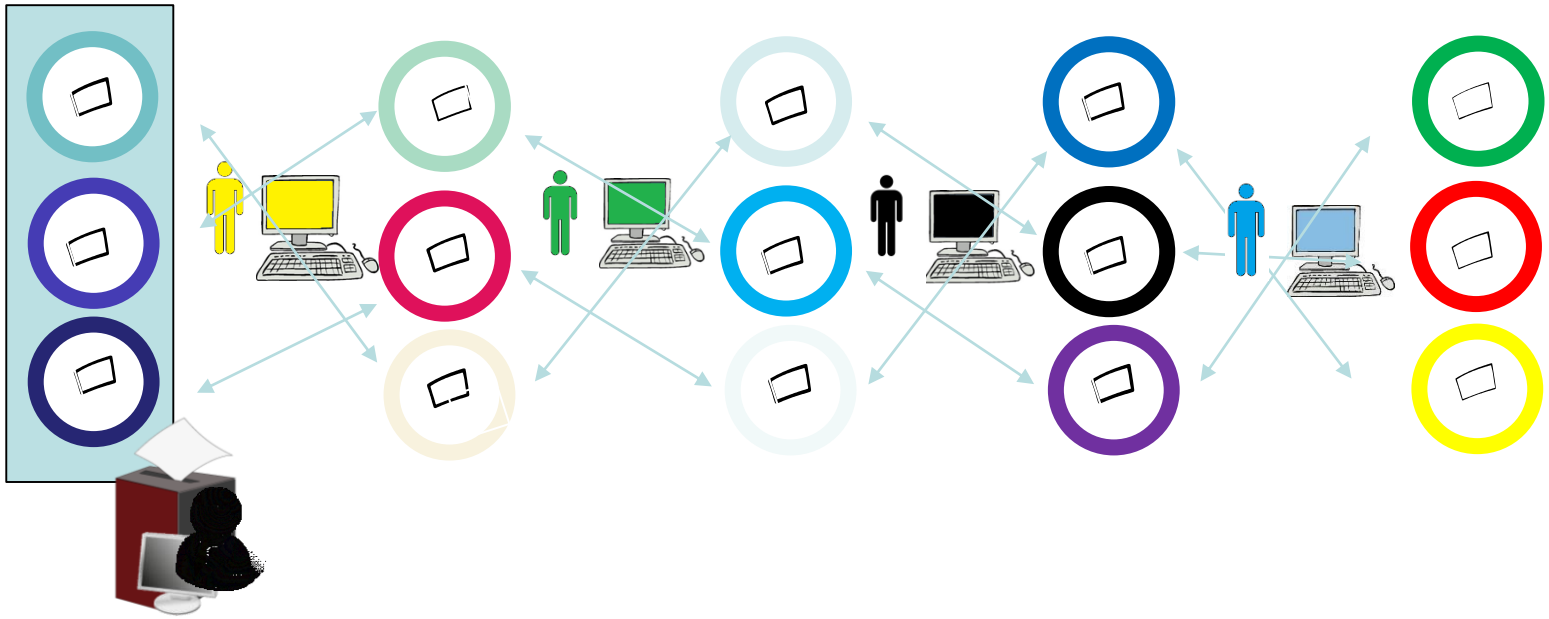


Ballot-Box

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Sektion Politische Rechte

Secrecy

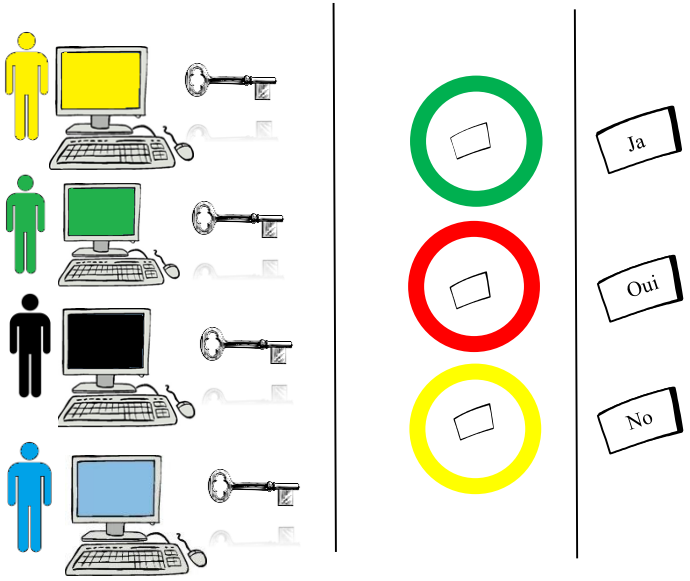


Ballot-Box

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Sektion Politische Rechte

Secrecy

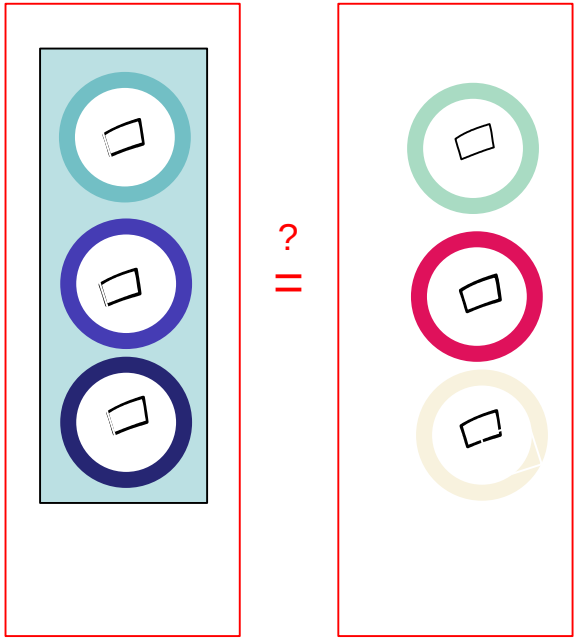


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

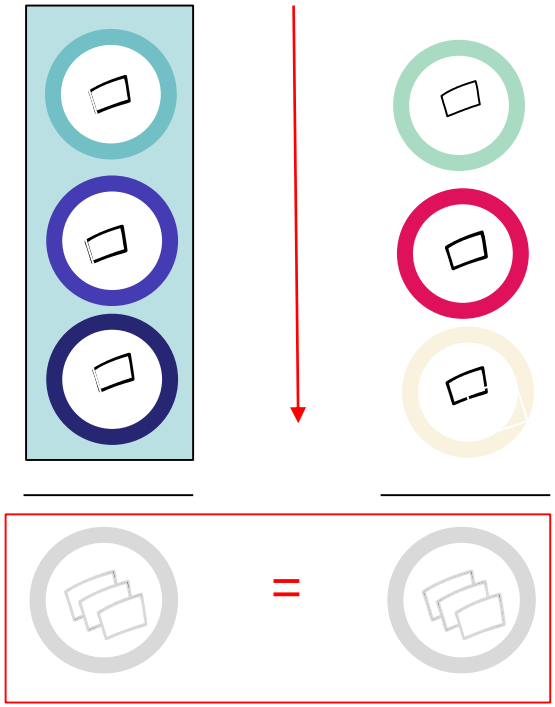
Bundeskanzlei BK
Sektion Politische Rechte

Tallied as recorded

Tallied as recorded

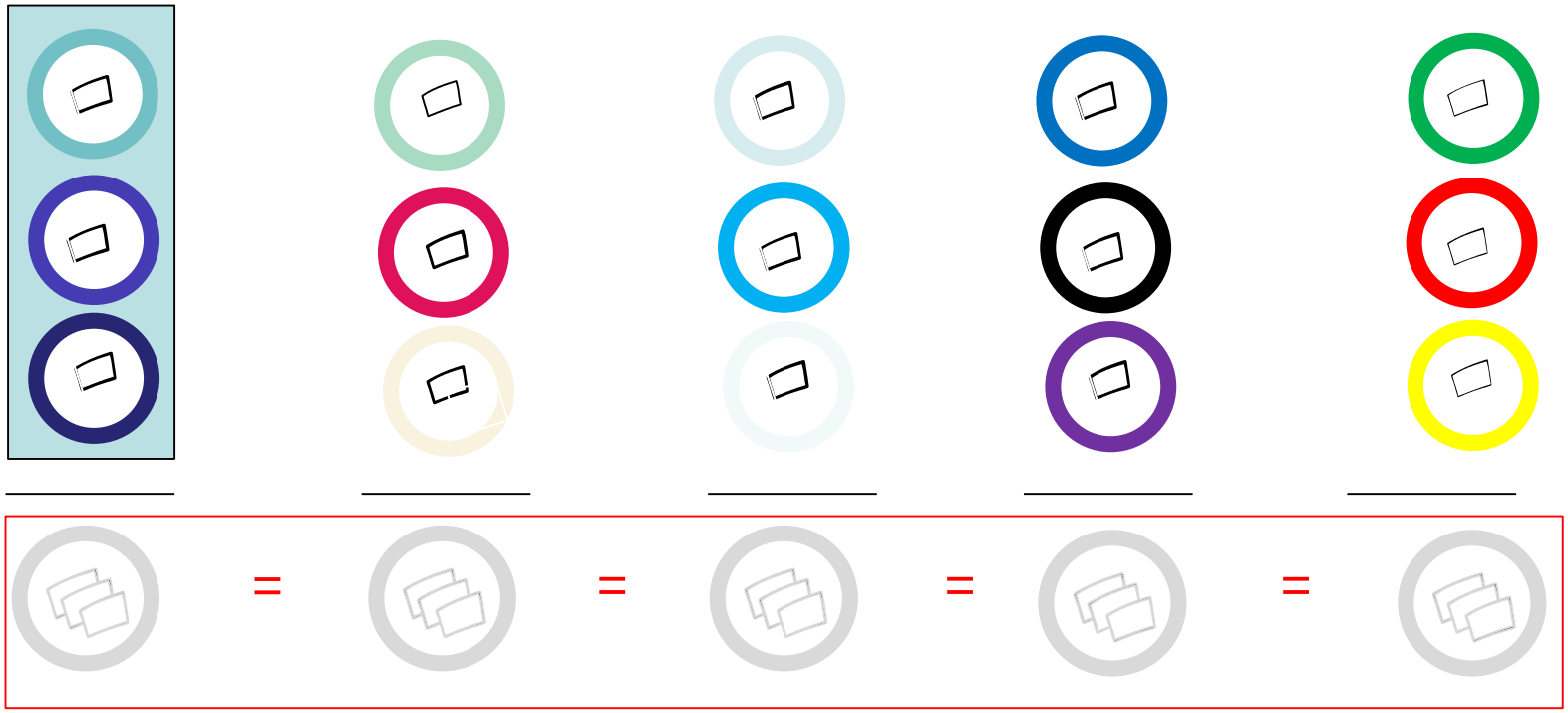


Tallied as recorded



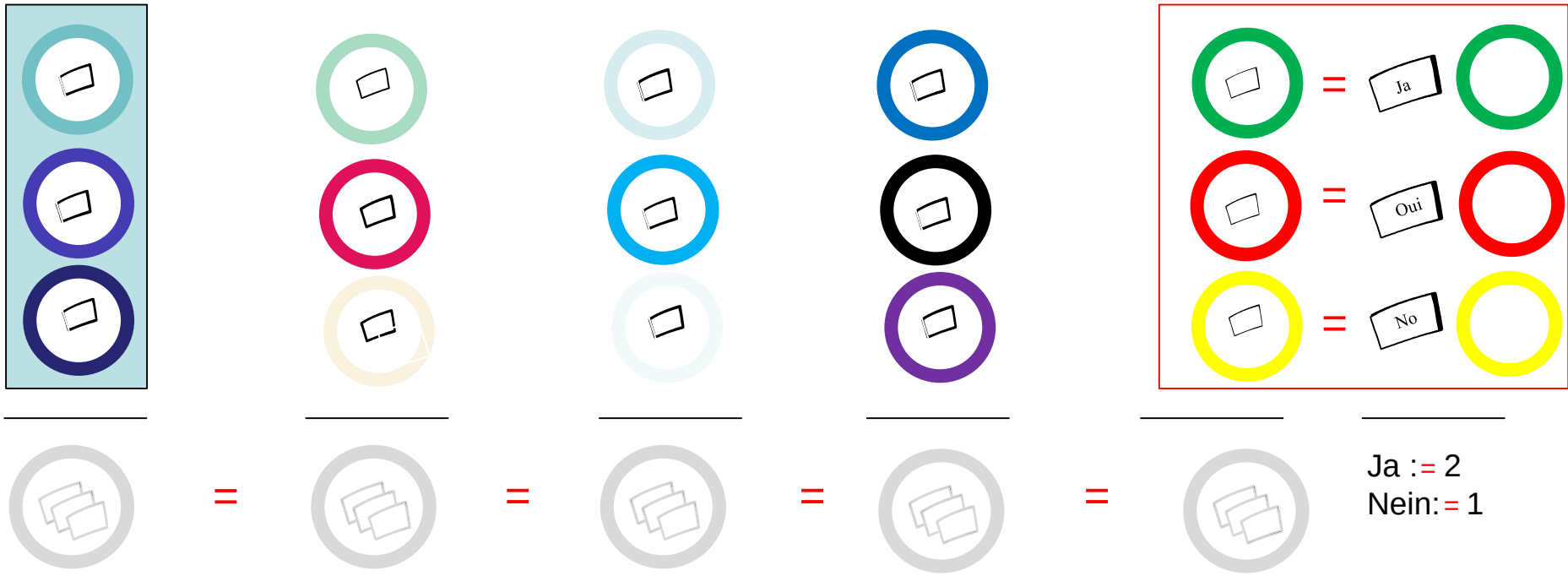
Can be verified and re-verified
By checking equations

Tallied as recorded



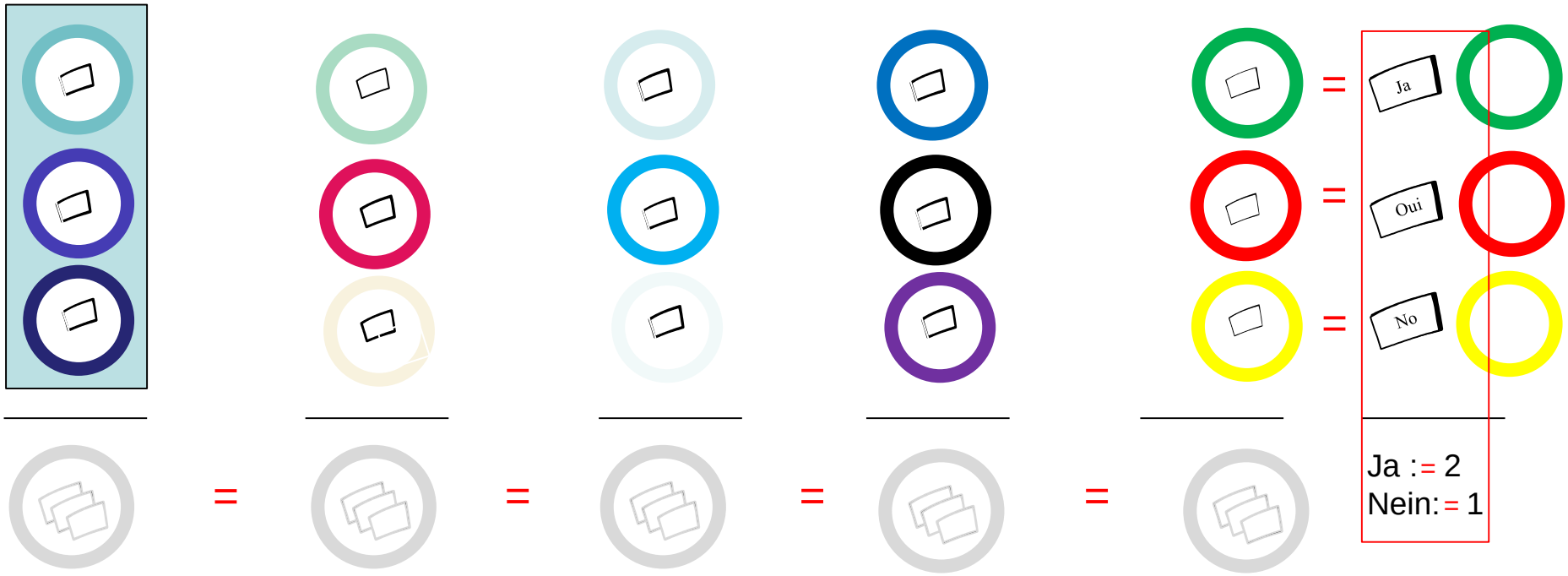
Full chain can be verified and re-verified
By checking equations

Tallied as recorded



Full chain can be verified and re-verified
By checking equations

Tallied as recorded



Full chain can be verified and re-verified
By checking equations

Ordinance of the FCh on E-Voting

Voters or obervers need to be able to detect fraud, assuming that

- 1 out 4 trustees is behaving correctly
- Printing office does not leak codes

Ordinance of the FCh on E-Voting

- Crypto-Protocol
  - Proof of compliance
  - Audit of proof
- Certification
  - Accredited by Swiss Accreditation Service
  - Software EAL2 / EAL4
  - ISO27001
- Source Code Publication

Public Intrusion Test

- Decision by Confederation and Cantons
- 1.Q 2019 enabled by Swiss Post
- Pre-Register: https://pit.post.ch/

Tell your friends!

Conclusion

- Verifiability as a foundation of trust
- Required by the FCh ordinance
- Assessed through certification
- Documented towards the public

Contact:

Oliver Spycher
Dep. Project Leader Vote électronique
oliver.spycher@bk.admin.ch

www.bk.admin.ch