E-Voting im Kanton St.Gallen

St.Gallen, 14. März 2019

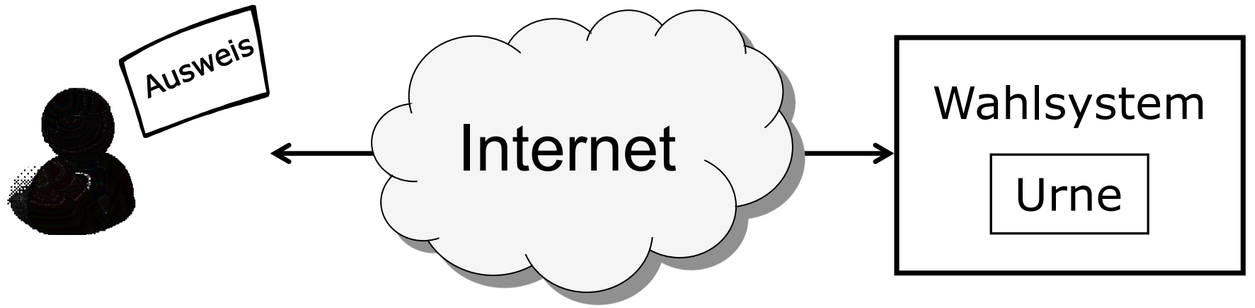
Dr. Benedikt van Spyk, Vizestaatssekretär

Programm

	Programmpunkt	
	Was ist E-Voting?	
	Gründe für E-Voting	
	E-Voting im Kanton St.Gallen: Stand der Dinge	
	E-Voting und Datenschutz	
	Fragen und Antworten	

Was ist E-Voting?

- E-Voting ist die Möglichkeit der Stimmabgabe bei politischen Wahlen und Abstimmungen ausserhalb des Wahllokals über das Internet.



- Abgrenzung zu E-Voting in den USA
- Abgrenzung zum Einsatz von E-Voting an Wahlen in anderen Ländern (Deutschland, Frankreich, Norwegen)

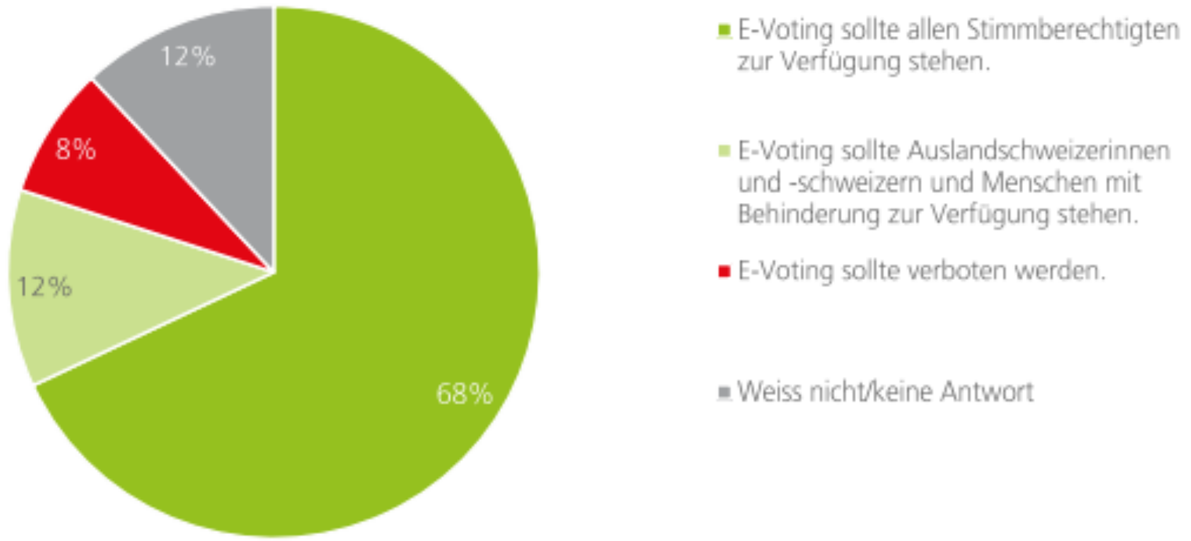
Gründe für E-Voting

- E-Voting verhindert ungültige oder verspätete Stimmabgaben

  (z.B. Stadt Zürich 26 Prozent und Stadt Winterthur 12 Prozent ungültige Stimmen bei den Wahlen im März 2018)
- E-Voting ist ein barrierefreier Stimmkanal
- E-Voting verbessert die Nachvollziehbarkeit der Stimmabgabe
- E-Voting ist ein zusätzlicher Stimmkanal, der die bestehenden und bewährten Stimmkanäle ergänzt

Gründe für E-Voting

- E-Voting wird von den Stimmberechtigten gewünscht

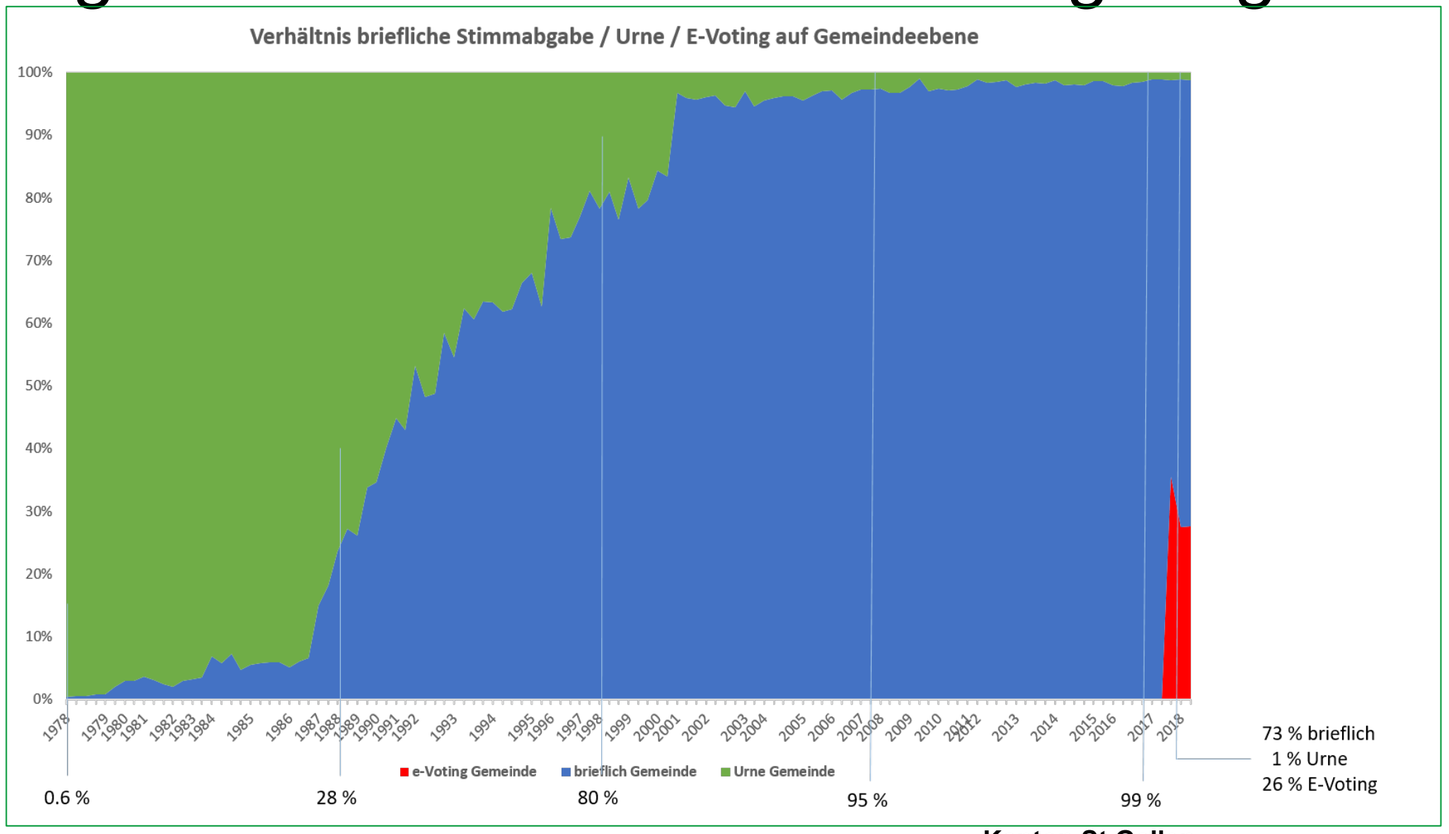


Quelle: Erhebung Nationale E-Government-Studie 2019, Zielgruppe Bevölkerung, DemoSCOPE.

Legende: Basis sind alle Befragten, die das Internet nutzen (n = 2549).

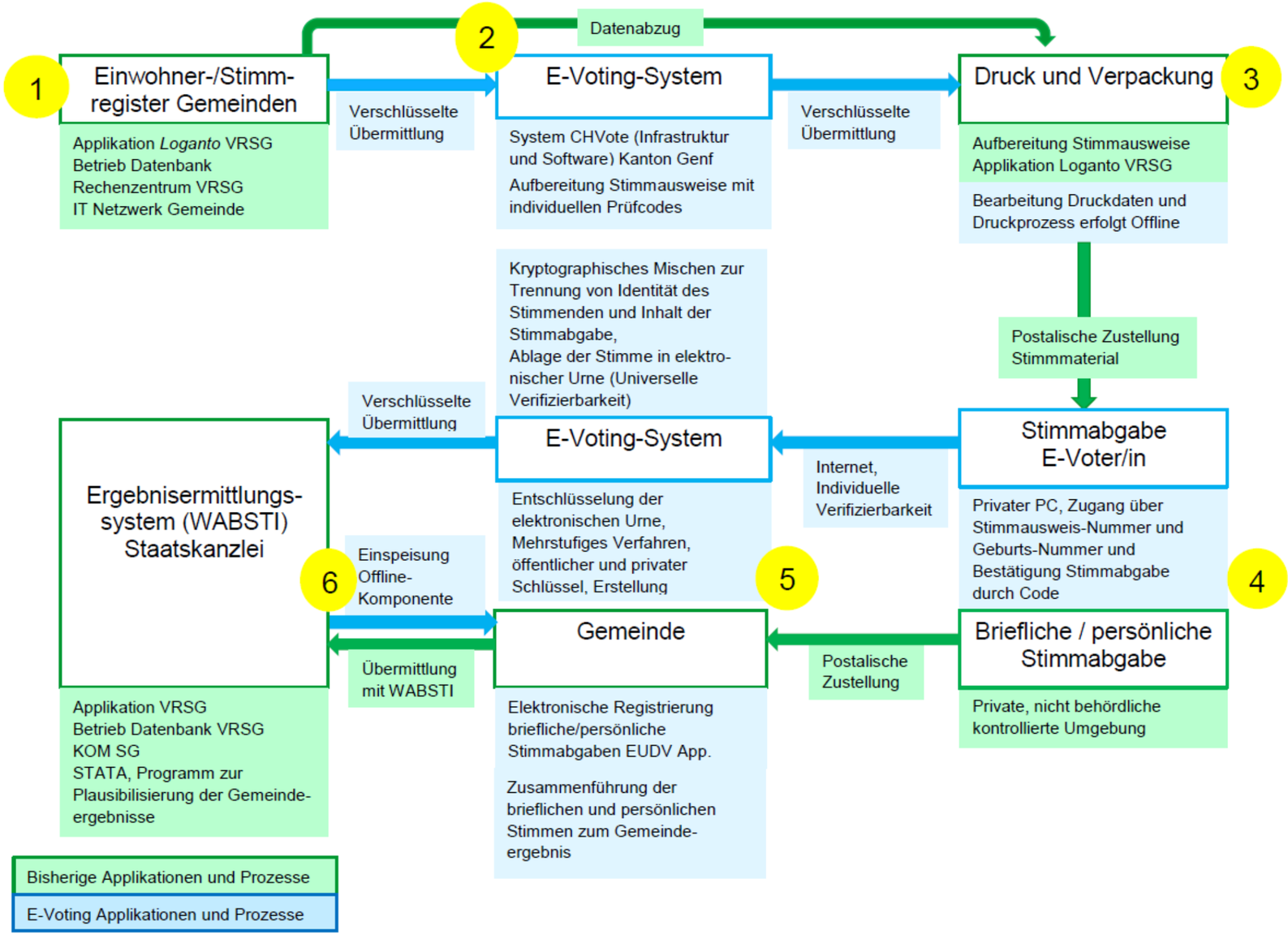
Gründe für E-Voting

- E-Voting wird von den Stimmberechtigten genutzt



Gründe für E-Voting

Wahlen und Abstimmungen finden auch ohne E-Voting in einem digitalen Umfeld statt:



Gründe für E-Voting

Der Staat steht auch ohne E-Voting vor der Herausforderung sichere und vertrauenswürdige Wahlen und Abstimmung in einem digitalen Umfeld durchzuführen.

- E-Voting ist ein Hauptreiber für die Verbesserung der Sicherheit und Nachvollziehbarkeit sämtlicher Prozessschritte bei Wahlen und Abstimmungen.

- Der Kanton St.Gallen bearbeitet aufgrund der Erfahrungen und der Notwendigkeit einer Zertifizierung kantonaler Prozesse im Rahmen von E-Voting folgende Themen:
  - Umfassende Prozessanalyse sämtlicher Prozessschritte
  - Entwicklung eines VotingCardTools zur Erstellung von Stimmrechtsausweisen
  - Prozessunterstützung für das Durchführen von Wahlen und Abstimmungen
  - Datenverschlüsselung und sichere Übermittlung von Daten
  - Neuausschreibung Ergebnisermittlungssoftware

Stand der Dinge: E-Voting läuft seit dem Jahr 2004 erfolgreich

- Seit 2004 über 300 E-Voting-Einsätze in insgesamt 14 Kantonen

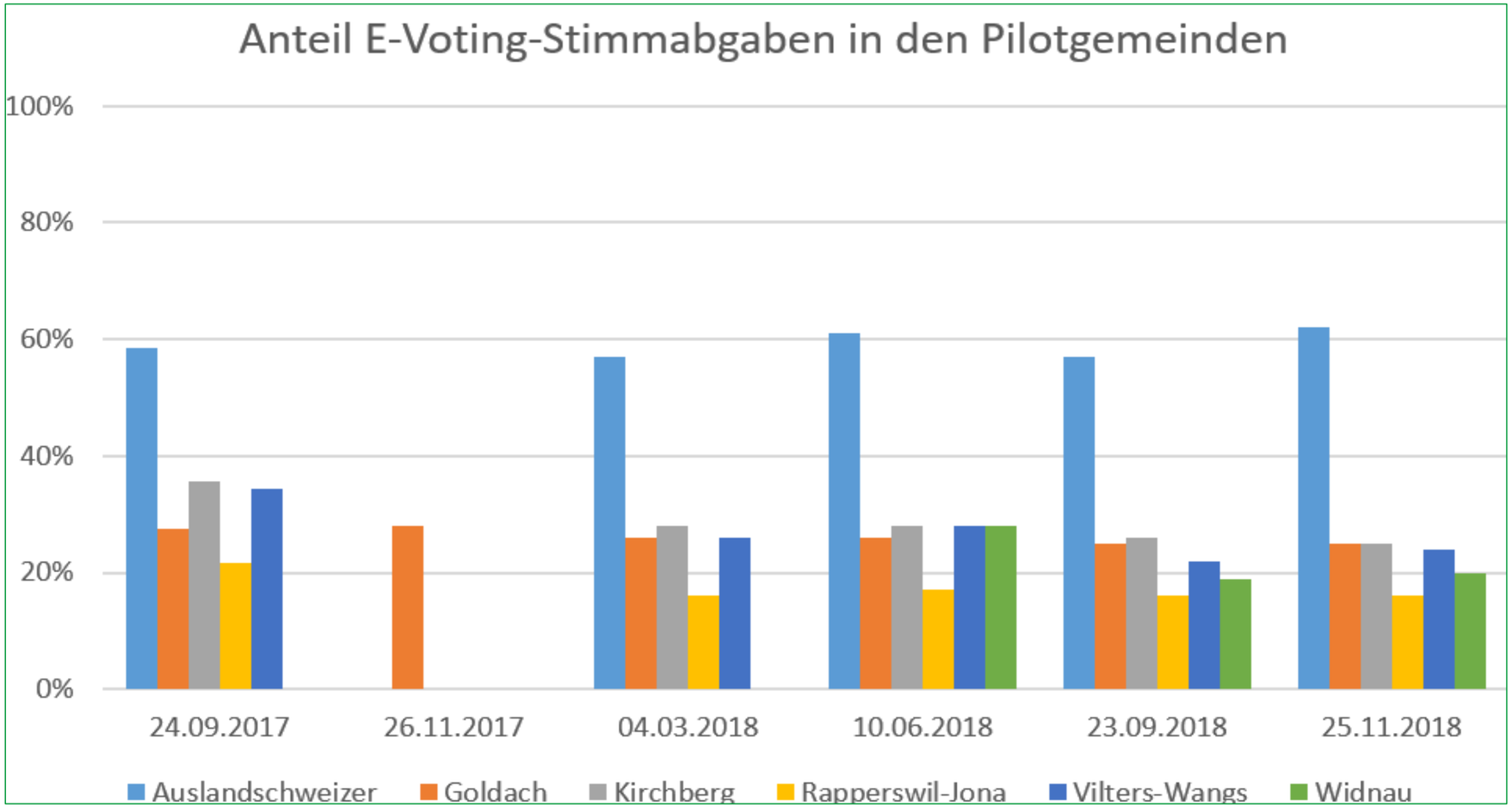
- Aktuell sind zwei E-Voting-Systeme im Einsatz:
  1. E-Voting-System des Kantons Genf (noch bis 2020)
     (Genf, Bern, Luzern und Aargau)

  2. E-Voting-System der Schweizerischen Post (Neuenburg, Fribourg, Kantone Thurgau, *Basel-Stadt*, *Glarus und St.Gallen*)

E-Voting in den Ostschweizer Kantonen

- 2009 Gründung des Consortiums Vote électronique (u.a. Kantone Graubünden, Schaffhausen und Thurgau; ab 2014: Zürich und Glarus): 17 Abstimmungen und 1 Wahl mit E-Voting für Auslandschweizer Gemeinde
- 2015 Auflösung des Consortiums Vote électronique
- *Kanton St.Gallen*
  - 2016 Öffentliche Ausschreibung und Zuschlag an den Kanton Genf
  - Juni 2017 Grundbewilligung durch den Bundesrat für Auslandschweizer Gemeinde sowie 5 Pilotgemeinden
  - 24. September 2017 Erster Einsatz von E-Voting für St.Galler Pilotgemeinden
  - 19. September 2018 Verabschiedung gesetzlicher Grundlagen für ordentlichen Betrieb
  - 30. Juni 2019 Erster Einsatz des E-Voting-Systems der Post (Vorbehalt Parlamentsentscheid)
- *Kanton Thurgau*
  - 2017 Öffentliche Ausschreibung und Zuschlag an die Schweizerische Post
  - 23. September 2018: Erfolgreicher Einsatz des neuen Systems
- *Kanton Glarus*
  - 2017 Gesetzliche Grundlage für Ausweitung von E-Voting verabschiedet. Öffentliche Ausschreibung und Zuschlag an die Schweizerische Post
  - Projekt zur Zeit sistiert.
- *Kanton Graubünden*
  - 2018 Gesetzliche Grundlagen zur Einführung von E-Voting als ordentlicher dritter Stimmkanal verabschiedet
  - Zuschlag an E-Voting System der Post erteilt

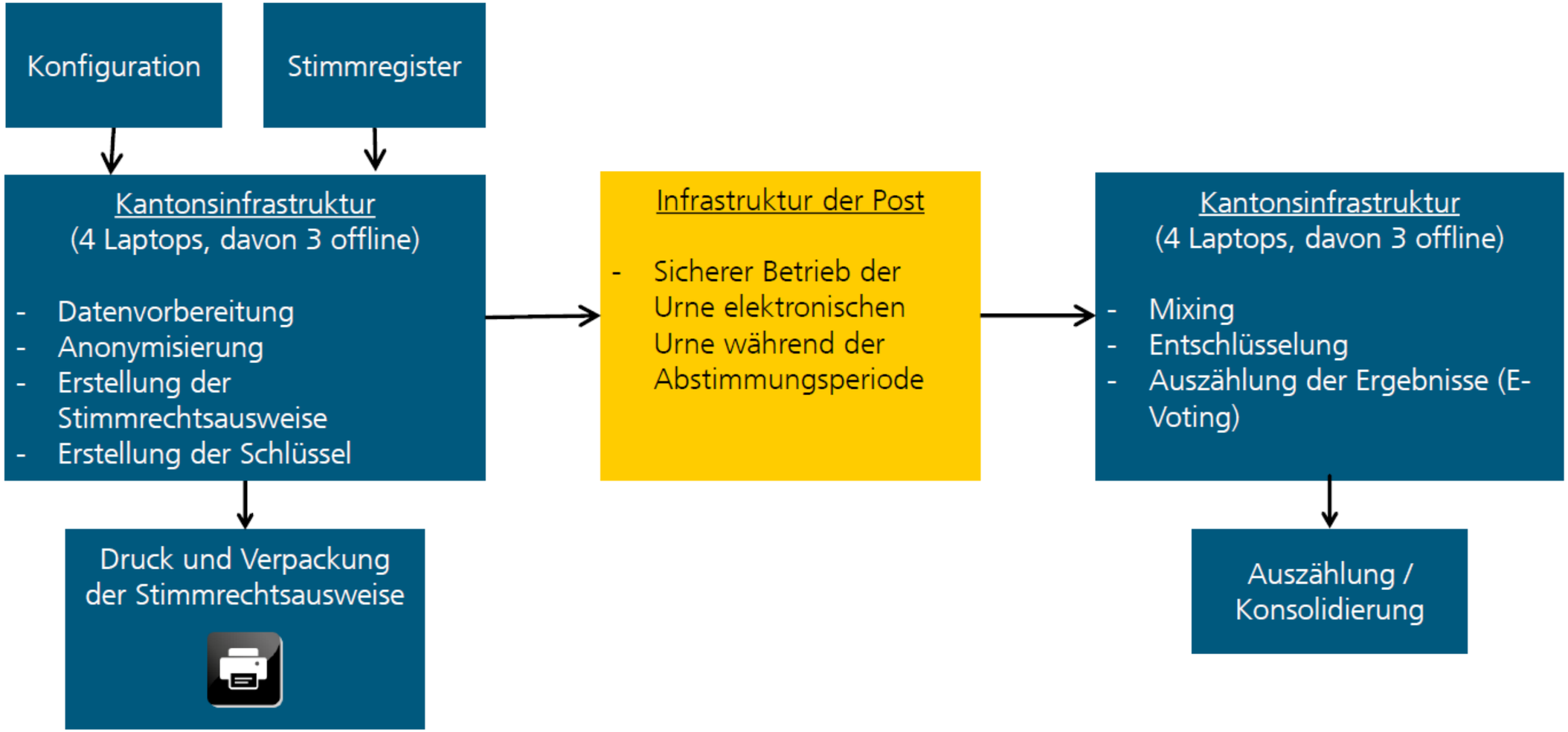
E-Voting im Kanton St.Gallen



E-Voting und Datenschutz: «Privacy by Design»

- Die Post gewährleistet die sichere Übermittlung der abgegebenen Stimmen in der digitalen Welt.
- Die EV-Lösung deckt die Anforderungen der Bundeskanzlei für die Übermittlung der abgegebenen Stimmen bei Urnengängen (Abstimmungen und Wahlen) auf Bundes-, Kantons- und Gemeindeebene ab.
- Der Kanton allein hat die Entscheidgewalt über den Abstimmungsprozess.
- Die Post als Betreiberin der EV-Lösung verfügt zu keinem Zeitpunkt über personenbezogene Daten der Stimm- und Wahlberechtigten. Das Stimmgeheimnis bleibt jederzeit gewahrt.
- Die Anonymisierung des Stimmregisters obliegt dem Kanton und wird mit der Infrastruktur des Kantons durchgeführt.
- Alle sensiblen Daten, insbesondere die abgegebenen Stimmen, werden gemäss den Anforderungen der Bundeskanzlei lückenlos verschlüsselt.
- Nur die Verantwortlichen des Kantons (Wahlbüro bzw. Beauftragte des Regierungsrats für Wahlen und Abstimmungen) kennen die geheimen Ver- und Entschlüsselungscodes für die Urne.
- Der Kanton ist immer für den 1st-Level-Helpdesk gegenüber den Stimmberechtigten zuständig.

E-Voting und Datenschutz: Aufgabenteilung Kanton und Post



E-Voting und Datenschutz: End-To-End Verschlüsselung

End-to-End-Verschlüsselung stellt sicher, dass

- die Stimme **beim Gerät** des Wählers (zusätzlich zum SSL-Kanal) verschlüsselt ist
- die Stimme **nur von der Wahlkommission** entschlüsselt werden kann
- die Stimme **nie** von einer anderen Organisation/Person entschlüsselt werden kann

E-Voting und Datenschutz: Daten bei der Post

In der Infrastruktur der Post sind während des Urnenganges folgende Daten gespeichert:

- Identifikator der Stimmrechtsausweise (offen), und sein Status
- Hashcode des Geburtsdatums oder -jahrs (für Authentifikationszwecke)
- Hashcode des Initialisierungscodes
- Verschlüsselte Stimme (kann nur von der versammelten Wahlkommission entschlüsselt werden)

Die Infrastruktur ist dediziert und es gibt keine Verbindung mit anderen von der Post betriebenen Datenbanken.

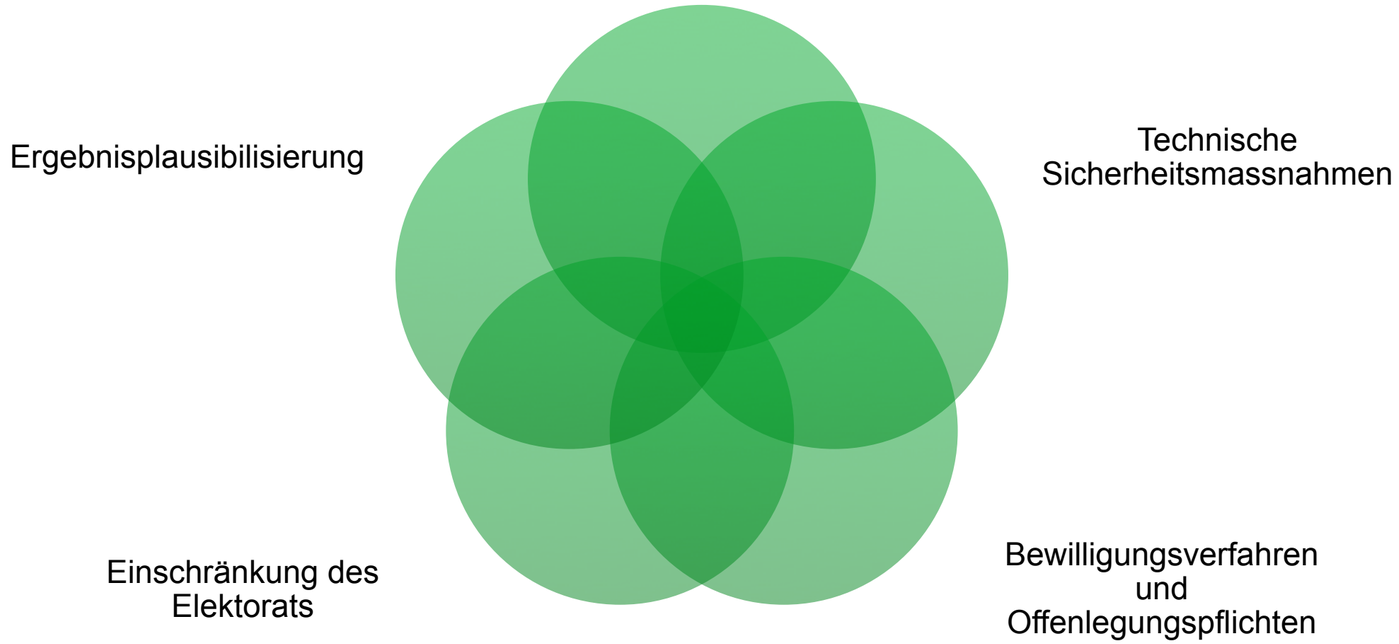
Wie weiter mit E-Voting

- Verlauf 2020: Einführung System mit universeller Verifizierbarkeit
- Jahr 2021: Einführung Anmeldeverfahren in sämtlichen Gemeinden (einbezogenes Elektorat bleibt unter 30 Prozent)
- Jahr 2021/2022: Grundsatzentscheid von Regierung und Kantonsrat über das weitere Vorgehen

Vielen Dank für Ihre Aufmerksamkeit.

Wie sicher ist E-Voting?

Die Sicherheit von E-Voting stützt sich auf vier Sicherheitsbereiche:



Technische Sicherheitsmassnahmen

Sicherheitsmassnahmen:

- Technische und organisatorische
- Individuelle Verifizierbarkeit
- Universelle Verifizierbarkeit

Sicherheit vor Tempo

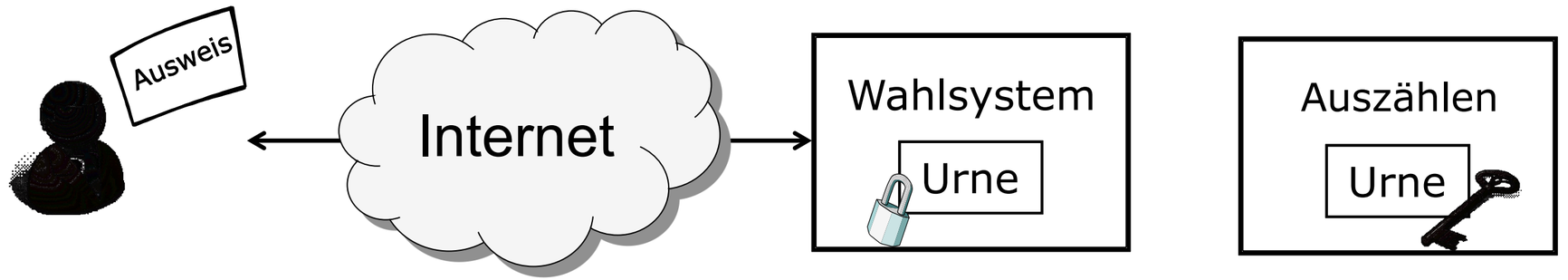
Je nach Ausbau der Sicherheit, werden E-Voting-Systeme für einen grösseren Teil des Elektorats zugelassen

- \- Technische und organisatorische Massnahmen 30%
- \+ Individuelle Verifizierbarkeit 50%
- \+ Universelle Verifizierbarkeit 100%

Beispiele (tech. Massnahmen)

Die Stimmen werden verschlüsselt abgelegt

- Der Schlüssel zur Entschlüsselung existiert nur in einem isolierten System beim Kanton
- Während der Abstimmung ist dieses System unter Verschluss
- Bei der Auszählung wird die Urne in das isolierte System kopiert und entschlüsselt



Beispiele (tech. Massnahmen)

Zugriffskontrolle

- Logischer Zugriff auf die Maschinen ist strikt geregelt
- Physischer Zugang zu den Servern ebenfalls
- Das E-Voting-System ist im internen Netzwerk von anderen Systemen abgeschottet

Logging

- Ereignisse werden protokolliert

Beispiele (org. Massnahmen)

Rollenverteilung

- Rollen und Kompetenzen werden genau geregelt
- 4 Augen Prinzip: manche Zugriffe sind nur zu zweit möglich
- Rollentrennung: manche Rollen sind nicht kumulierbar

Prüfungen

- Es werden Sicherheitsaudits durchgeführt
- Es werden Teststimmen vor und während dem Wahlgang abgegeben und ausgezählt

Beispiele (org. Massnahmen)

- Zulassung des Systems
  - 30%: Durch Begleitgruppe des Bundes und der Kantone
  - 50% und 100%: Zertifizierung durch eine vom Bund akkreditierte Stelle (SAS), Prüfung durch die Bundeskanzlei
- Offenlegung des Quellcodes
- Öffentlicher Intrusionstest
- Vernetzung mit Fachkreisen
- Krisenvereinbarungen und Krisenzellen

Individuelle Verifizierbarkeit

Die Stimmberechtigten können selber prüfen, ob ihre Stimme korrekt abgegeben worden ist

Dies verhindert eine unerkannte Manipulation der Stimmen

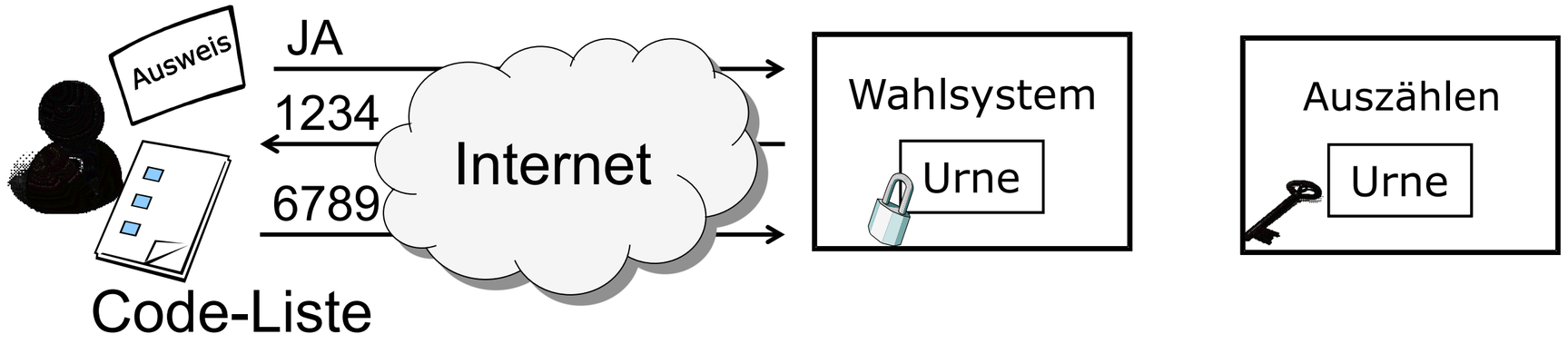
- auf der Plattform der Stimmberechtigten (Virus)
- beim Transfer durch das Internet

Individuelle Verifizierbarkeit

Das Stimmmaterial enthält persönliche Code-Listen, z.B. «ja» : 1234

Das System bestätigt den korrekten Erhalt der Stimme indem es die Codes anzeigt (1234 für «ja»)

Die Stimmberechtigten bestätigen ihre Wahl mit einem Bestätigungscode (z.B. 6789)



Individuelle Verifizierbarkeit

Ein Virus auf dem PC des Wählers oder im Internet kann die Stimmen nicht unerkannt manipulieren, da er die entsprechenden Codes nicht kennt

- Die Codes existieren nur auf dem Papier (Stimmmaterial)

Wenn der Wähler die richtigen Codes sieht, weiss er, dass seine Stimme korrekt übermittelt worden ist

Wenn das System den richtigen Bestätigungscode erhält, weiss es, dass die Stimme definitiv abgegeben wurde

Universelle Verifizierbarkeit

- Mathematische Beweise belegen, dass die abgegebenen Stimmen unverändert ausgezählt worden sind
- Unabhängige Prüfung der Beweise

- Wahrung des Stimmgeheimnisses
  - Die Stimmen werden von den Stimmberechtigten verschlüsselt (end-to-end Verschlüsselung, das online System sieht nie unverschlüsselte Stimmen)
  - Bevor sie entschlüsselt werden, werden sie offline anonymisiert (kryptografisches Mischen)
    - Für jeden Schritt wird ein mathematischer Beweis generiert

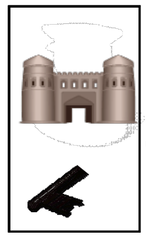
Universelle Verifizierbarkeit

Mathematische Beweise:

- Jede eingehende Stimme wurde
  - mit einem gültigen Stimmausweis generiert,
  - die Verifizierungscodes wurden richtig berechnet
  - der korrekte Bestätigungscode wurde erhalten
- Die verschlüsselten Stimmen wurden anonymisiert und gemischt, ohne dass deren Inhalt verändert wurde
- Die Stimmen wurden korrekt entschlüsselt

Universelle Verifizierbarkeit

Es werden vier *Kontroll-Komponenten* eingesetzt



Sie führen ein Register aller Beweise

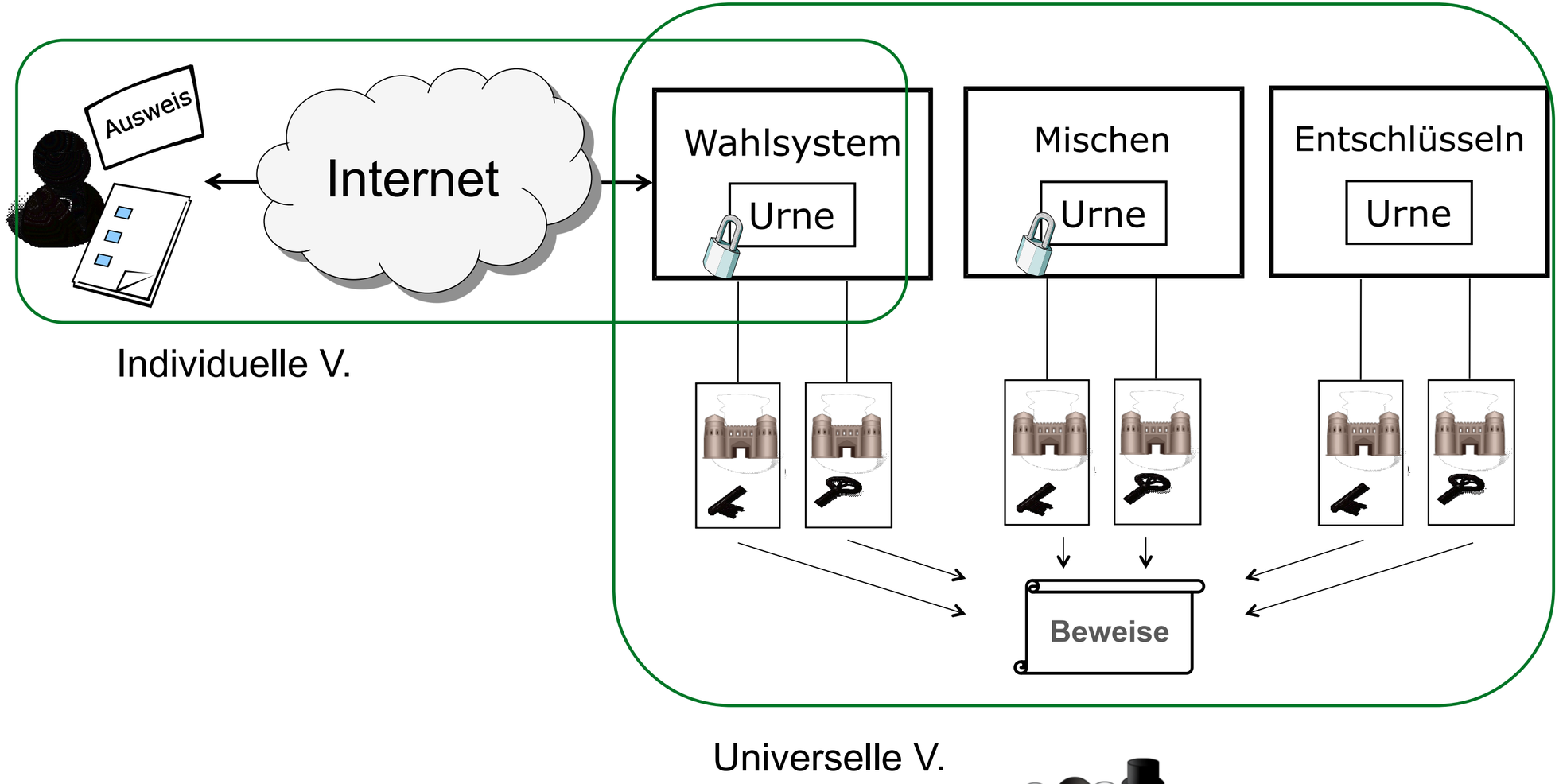
- Es können keine Stimmen gelöscht werden

Sie enthalten je einen Teil des Schlüssels zur Entschlüsselung

- Stimmen können nicht vor dem Mischen entschlüsselt werden

Wenn nur *eine von vier* Kontroll-Komponenten richtig rechnet, ist jegliche unerkannte Manipulation unmöglich

Gesamtbild


Ausweis
Internet
Wahlsystem
Urne
Mischen
Urne
Entschlüsseln
Urne
Beweise
Individuelle V.
Universelle V.

Zusammenfassung

Technische und organisatorische Massnahmen ergeben ein sehr hohes Sicherheitsniveau

Individuelle Verifizierbarkeit verhindert unerkannte Manipulationen auf der Plattform der Wählenden oder im Internet

Universelle Verifizierbarkeit verhindert unerkannte Manipulationen innerhalb des E-Voting-Systems

Bewilligungsverfahren und Offenlegungspflicht

- Art. 84 Abs. 2 BPR verlangt für Wahl- und Abstimmungsverfahren mit technischen Mitteln eine *Genehmigung* des Bundesrates.

- Werden mehr als 30 Prozent des Elektorats bei einem E-Voting-Urnengang miteinbezogen, müssen gemäss Art. 7 Abs. 2 VEleS das System und sein Betrieb hinsichtlich mehrerer Kriterien von einer unabhängigen Stelle überprüft werden (*Zertifizierung*).

- Vorgesehen ist zudem, dass der *Quellcode* der Software des E-Voting-Systems offengelegt werden muss, sobald im System die vollständige Verifizierbarkeit (individuelle Verifizierbarkeit und universelle Verifizierbarkeit) umgesetzt ist.

- Darüber hinaus finden öffentliche Intrusionstests statt.

Einschränkung des Elektorats

- Das vom Kanton St.Gallen eingesetzte E-Voting-System ist für 30 Prozent des Elektorats zugelassen.
- Im Rahmen der laufenden Pilotphase im Kanton St.Gallen wird rund 8'000 Auslandschweizerinnen und Auslandschweizern sowie rund 37'000 Stimmberechtigten in den Pilotgemeinden die Möglichkeit zur elektronischen Stimmabgabe gewährt. Das entspricht rund 14 Prozent des Elektorats.
- In den bisherigen Abstimmungen sind zwischen **drei und vier Prozent sämtlicher Stimmen** (rund 6’000 zu rund 178’000) elektronisch eingegangen.
- Der Anwendungsbereich von E-Voting bleibt in der Pilotphase damit stark eingeschränkt.

Schritte der Plausibilisierung

- Grundsatz
  - Systematische Manipulationen von Ergebnissen sind in einem E-Voting-System mit universeller Verifizierbarkeit bereits vor einer Plausibilisierung erkennbar.

- Plausibilisierung in zwei Schritten
  - Teilergebnisse der E-Voter (elektronisch Stimmenden) einer Gemeinde X werden mit den Teilergebnissen der E-Voter einer Gemeinde Y verglichen.

  - Die Gemeindeergebnisse der E-Voting Gemeinden, d.h. das gesamte Gemeindeergebnis, bestehend aus Urnen-, brieflichen und elektronischen Stimmen, wird mit Ergebnissen der anderen Gemeinden verglichen.

Beispiel und Fazit

- Beispiel
  - Wenn das Verhältnis von Ja- und Nein-Stimmen bei den E-Votern bei 80% zu 20% und bei den beiden anderen Stimmkanälen bei 55% zu 45% liegen würde, wäre dies nicht plausibel.

- Fazit
  - Neben den rein technischen Hürden des E-Voting-Systems führen die stark dezentralisierten Strukturen im Bereich Wahlen und Abstimmungen zu einer zusätzlichen Hürde für eine Manipulation eines Ergebnisses. Es bedarf vertiefter politikwissenschaftlicher und statistischer Kenntnisse sowie erhebliche technische Kenntnisse zur Programmierung entsprechender Algorithmen für eine plausible Ergebnisbeeinflussung.