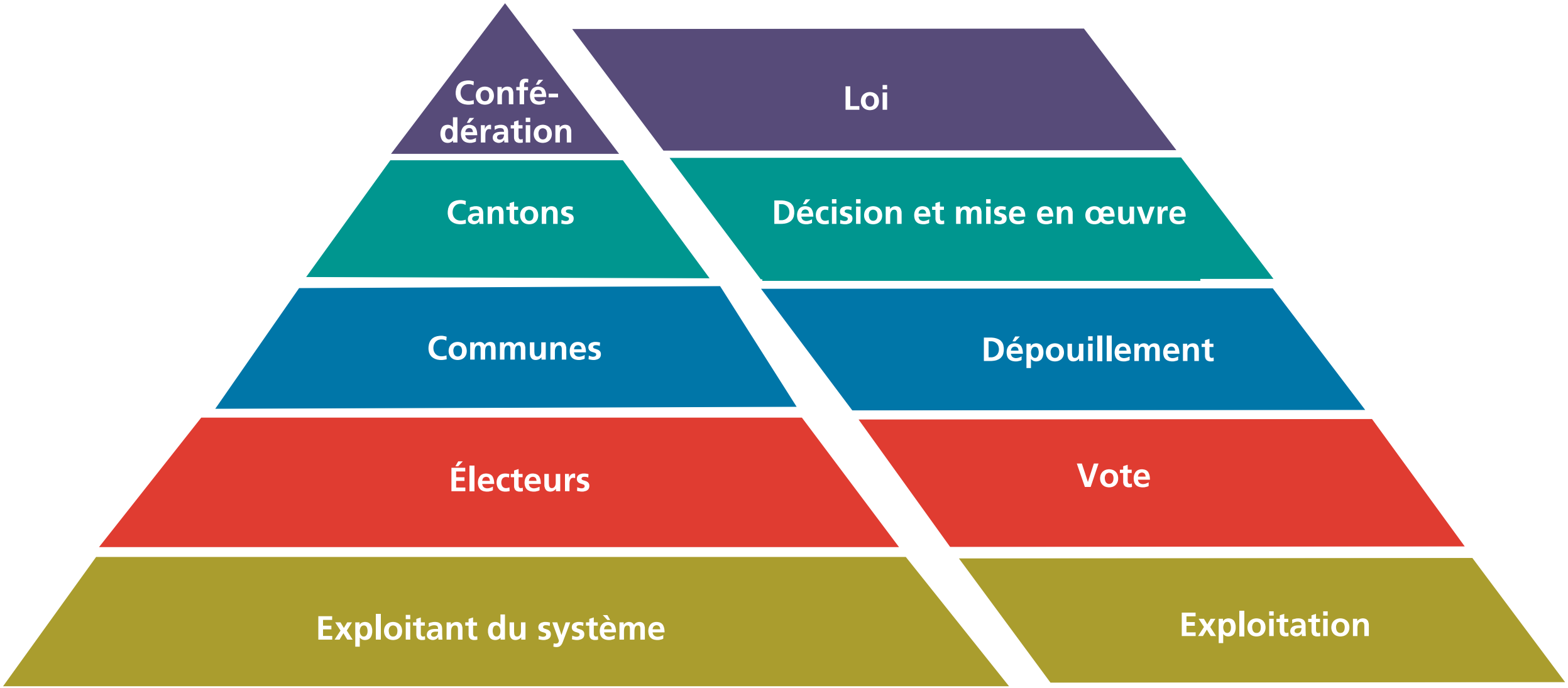
SYSTÈME DE VOTE ÉLECTRONIQUE DE LA POSTE – EXPÉRIENCES ET REVERS SUR LE CHEMIN VERS UN SYSTÈME COMPLÈTEMENT VÉRIFIABLE

14.05.2019, 19E SÉMINAIRE D'INFORMATIQUE JURIDIQUE DE MACOLIN, DENIS MOREL, RESPONSABLE DIGITAL PUBLIC SERVICES

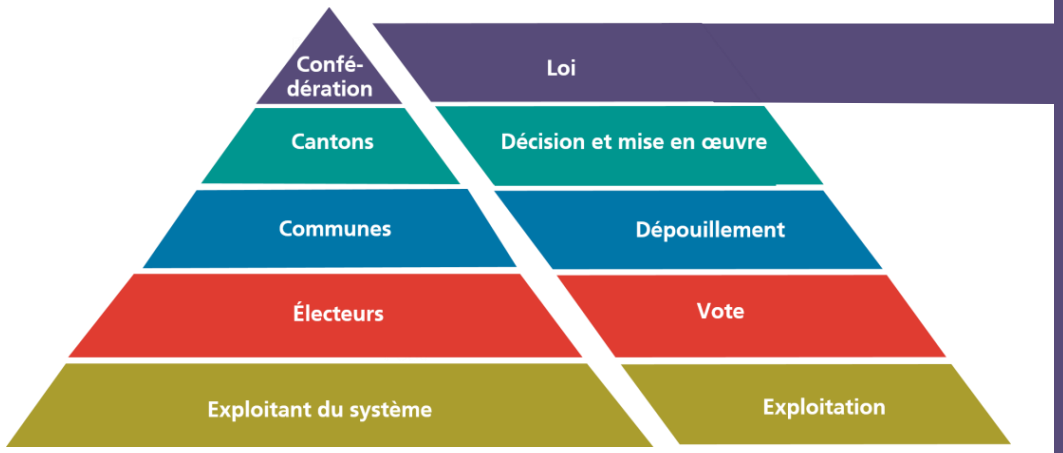
LA POSTE

INTRODUCTION
RÔLES DES ACTEURS DU VOTE ÉLECTRONIQUE

VOTE ÉLECTRONIQUE - RÉPARTITION DES RÔLES

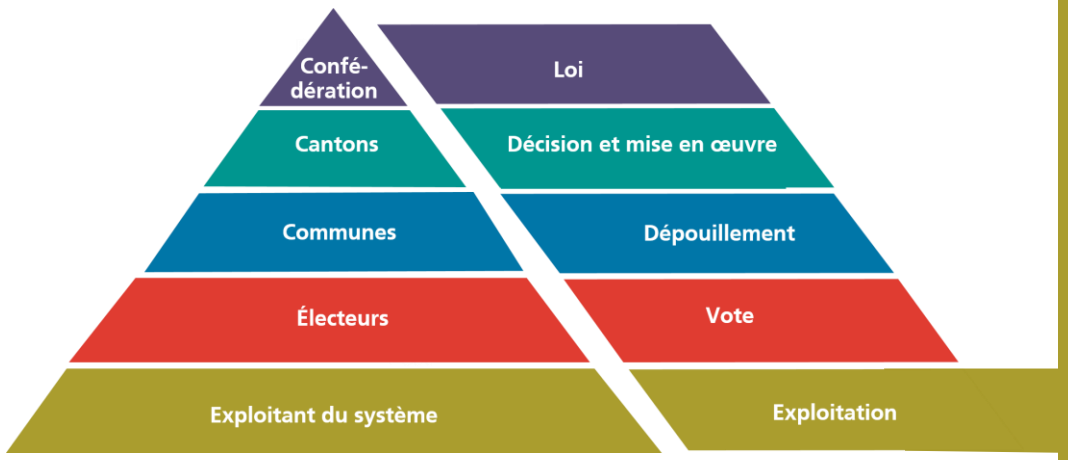


VOTE ÉLECTRONIQUE - RÉPARTITION DES RÔLES
ACTEUR CONFÉDÉRATION



- Définit les **conditions-cadres légales** (loi et ordonnance) pour les élections fédérales et les votations
- Prévoit par la loi la possibilité (optionnelle) pour les cantons d'introduire le **vote électronique**
- Définit de manière uniforme pour tous les cantons les **exigences de sécurité** vis-à-vis du système et de l'exploitation
- Délivre aux cantons **l'autorisation d'exploitation** et contrôle que toutes les conditions requises soient remplies
- **Surveille** l'exploitation dans les cantons

VOTE ÉLECTRONIQUE - RÉPARTITION DES RÔLES
ACTEUR FOURNISSEUR DU SYSTÈME

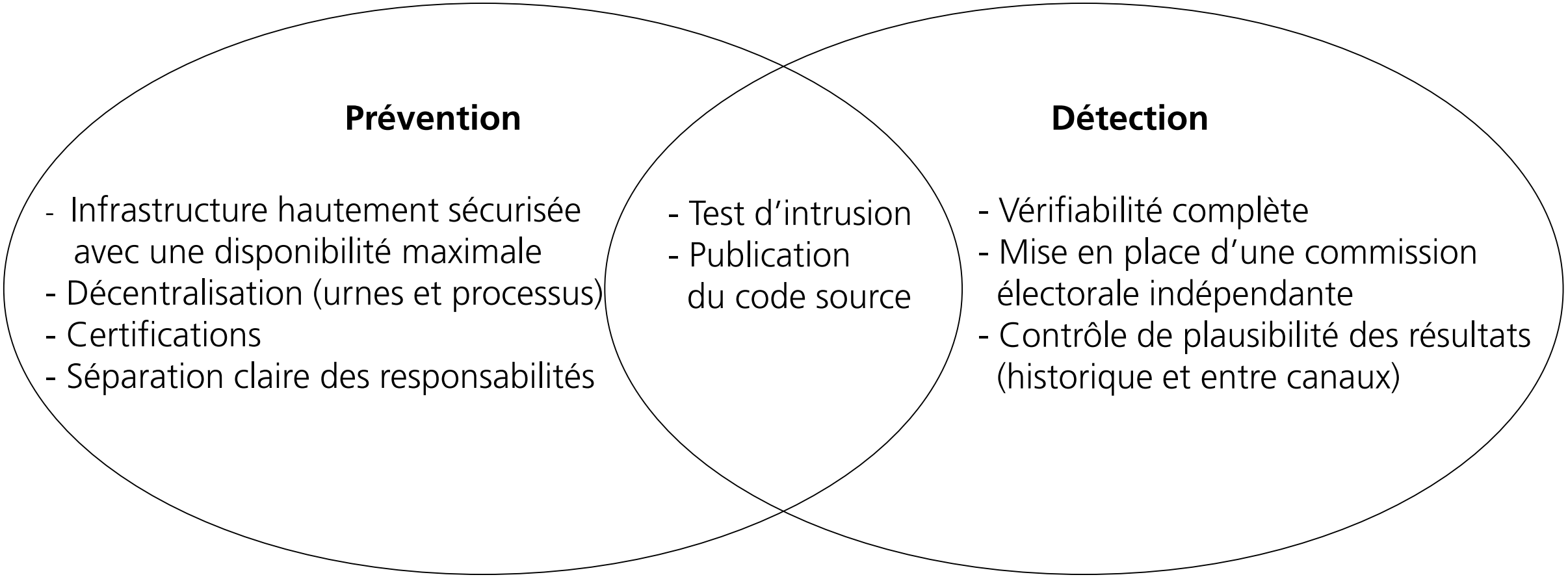


- **Développe le système** et **l'exploitation** conformément aux exigences de la Confédération
- Est responsable de **l'exploitation** de **l'urne électronique**
- **Met l'urne à disposition** du canton pour que le canton puisse exécuter ses processus en toute autonomie
- Publie le **code source** du système conformément aux exigences du droit fédéral
- Garantit le **stockage des données** conforme à la loi en Suisse

EXIGENCES DE SÉCURITÉ
APERÇU DES PRINCIPAUX ÉLÉMENTS DE SÉCURITÉ

ÉLÉMENTS DE SÉCURITÉ

VÉRIFIABILITÉ COMPLÈTE – COMPOSANTE CENTRALE DU MIX DE SÉCURITÉ

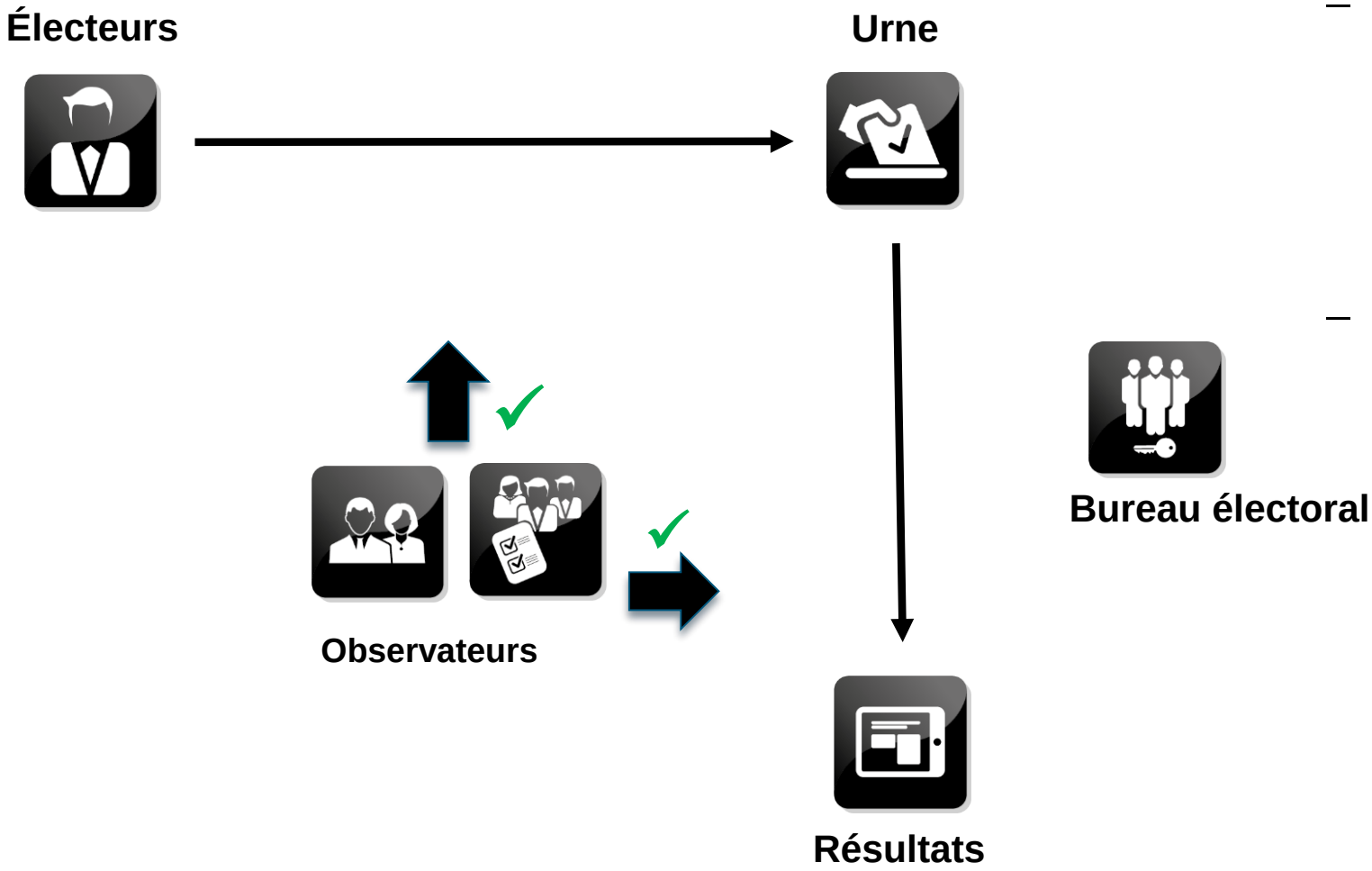


EXIGENCES DE SÉCURITÉ

VÉRIFIABILITÉ INDIVIDUELLE +
VÉRIFIABILITÉ UNIVERSELLE
= VÉRIFIABILITÉ COMPLÈTE

EXIGENCES DE SÉCURITÉ

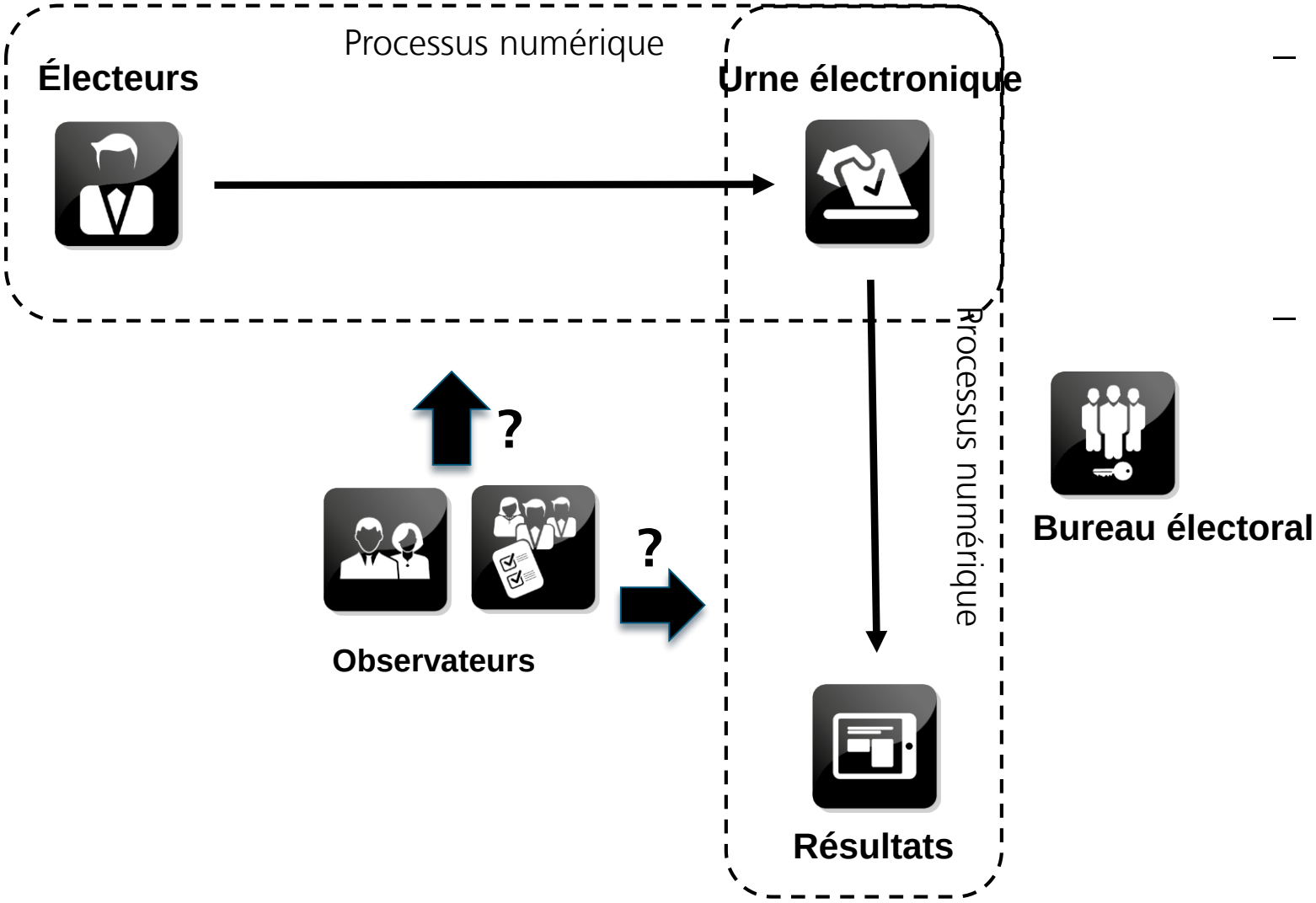
DANS LE CADRE DE VOTATIONS «PHYSIQUES», TOUT EST FACILEMENT OBSERVABLE ….



- Voix et processus (p. ex. dépouillement) reposent exclusivement sur des **éléments physiques**
- Les processus peuvent être observés par le bureau électoral, **uniquement par des moyens humains**

VÉRIFIABILITÉ COMPLÈTE

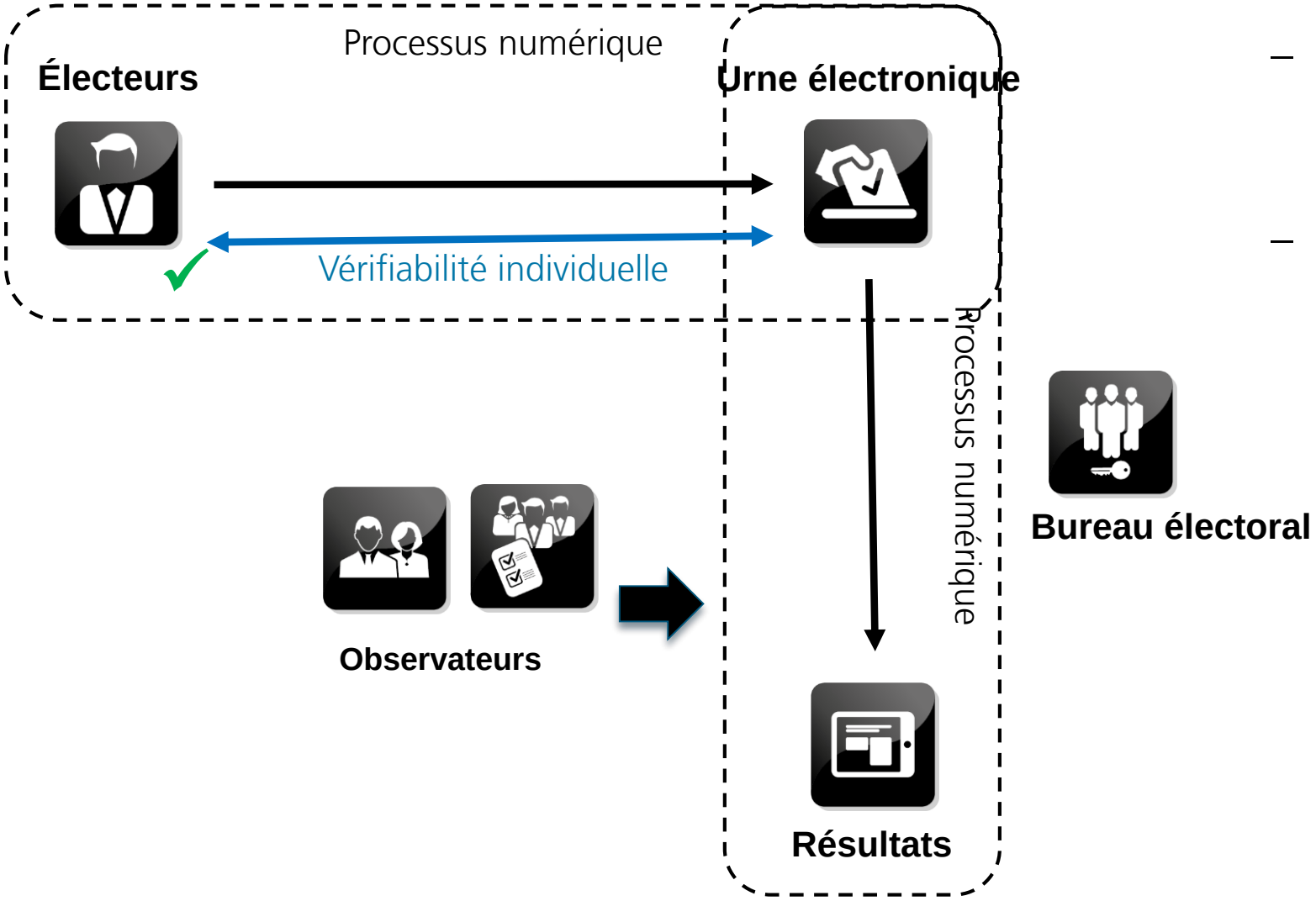
DANS LE CADRE DE VOTATIONS ÉLECTRONIQUES, L'OBSERVATION EST PLUS DIFFICILE



- Les processus (p. ex. dépouillement) reposent sur des **éléments numériques** (données/logiciel)
- Les processus ne peuvent **pas être observés par des humains**

https://youtu.be/Hzd7ViuFAcQ

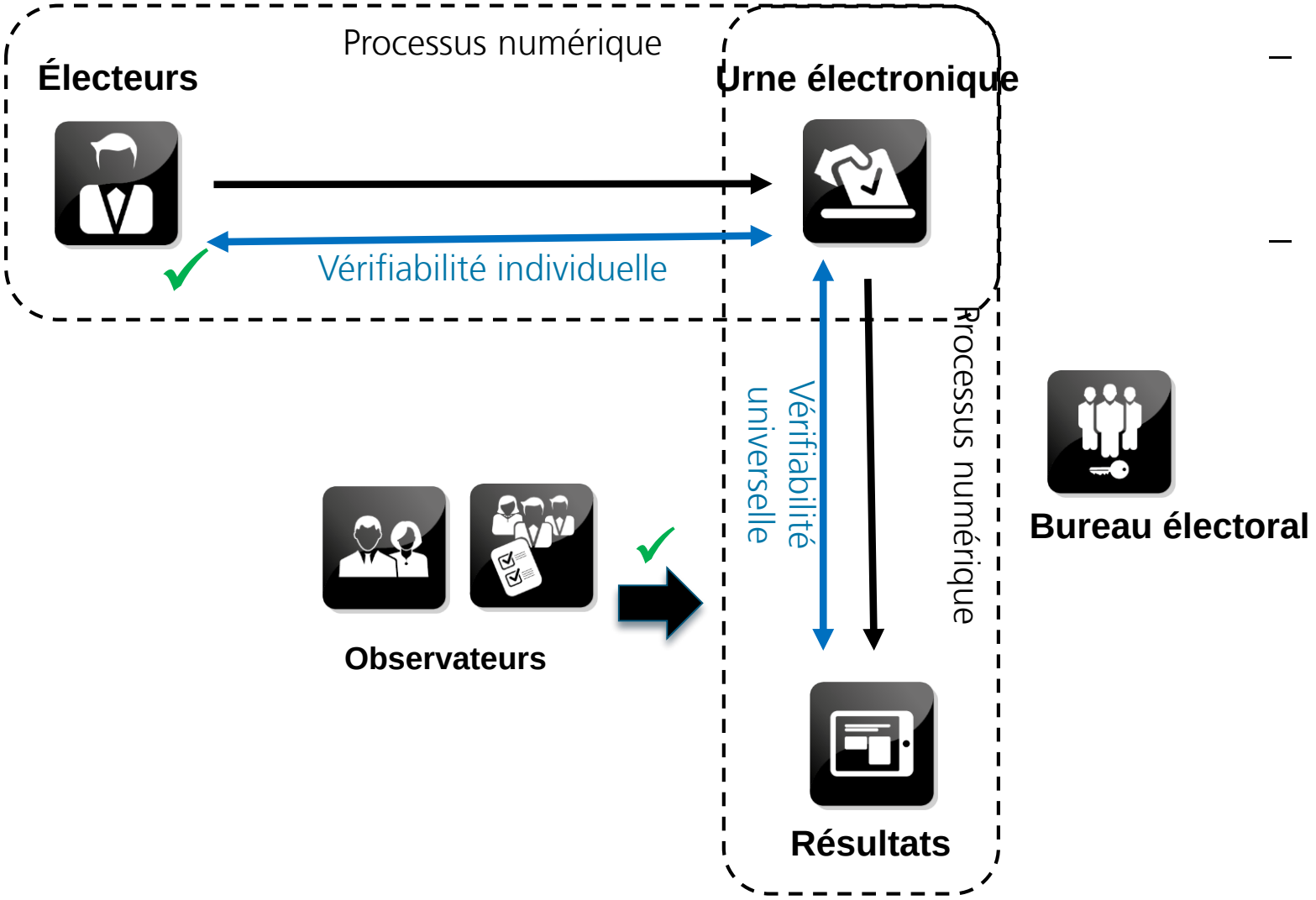
VÉRIFIABILITÉ COMPLÈTE
EN TANT QUE MOYEN POUR L'OBSERVATION DU PROCESSUS NUMÉRIQUE



- L'électeur peut vérifier que sa voix a été déposée dans l'urne **comme souhaité** (vérifiabilité individuelle)
- Traçabilité **«cast as intended»**

https://youtu.be/2UI3VsszqPE

VÉRIFIABILITÉ COMPLÈTE
EN TANT QUE MOYEN POUR L'OBSERVATION DU PROCESSUS NUMÉRIQUE



- L'électeur peut vérifier que sa voix a été déposée dans l'urne **comme souhaité** (vérifiabilité individuelle)
- Le bureau électoral peut vérifier que l'urne **n'a pas été falsifiée** et que **toutes les voix ont été correctement comptabilisées** (vérifiabilité universelle)

EXIGENCES DIFFÉRENTIÉES CONCERNANT LA SÉCURITÉ
50% OU 100% DE L'ÉLECTORAT

Pour 50% de l'électorat

- **Certification** conformément à la norme industrielle
- **Vérifiabilité individuelle**

Pour 100% de l'électorat

- **Certification** conformément à la norme industrielle
- **Vérifiabilité individuelle**

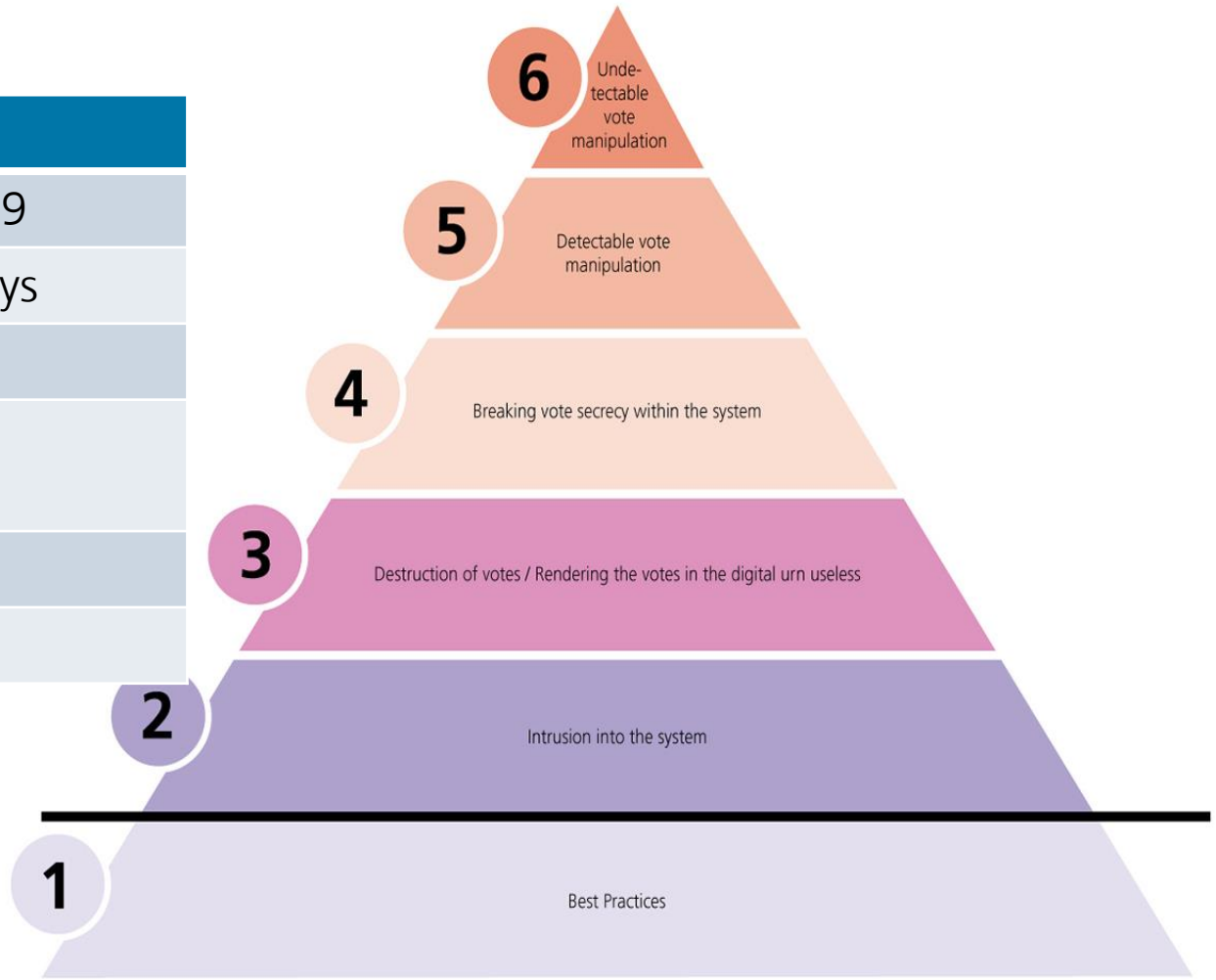
Et également:
- **Vérifiabilité universelle**
- Publication du **code source**
- **Test d'intrusion public** (aucune exigence légale mais exigence de la part des cantons et de la Chancellerie fédérale)

CERTIFICATION CONFORMÉMENT À LA NORME INDUSTRIELLE

- Certification d'après la régulation de l'OVotE (50% et 100%)
- Certification ISO 27001
- Vérification de la conformité du système (infrastructure, fonctionnement, processus de gestion, gestion des risques, gouvernance, sécurité de l'information, fonctionnalités logicielles, processus de test, etc.)
- Les thèmes spécialisés ne sont pas complètement audités. L'audit est réalisé sur la base d'échantillons de test basé sur les risques. Des recommandations d'amélioration sont mises en œuvre en continu.
- Accréditation de l'organisme de certification par SECO-SAS
- Cycle de 3 ans (audit principal, deux audits de renouvellement, audit de recertification)
- Le processus d'amélioration continue est un élément important de l'audit
- Les non-conformités sont classifiées: légères, importantes, critiques

RÉSULTATS DU PIT (PUBLIC INTRUSION TEST)
À VRAI DIRE UN SUCCÈS

Élément	Résultat
Durée	du 25.02.2019 au 24.03.2019
Researcher	3186 personnes dans 137 pays
Submitted Findings	173
Accepted Findings	16 dans la catégorie 1 (Best Practices)
Compensation max.	CHF 150 000
Compensation versée	CHF 2000



il n'a pas été possible de manipuler l'urne notariée ni de gêner le scrutin.

ENJEUX DU CODE SOURCE

- Trois failles, dont l'une concerne le système actuellement utilisé
- Les failles se situent au niveau cryptographique
- Même si les failles sont très difficiles à exploiter dans la réalité, ce sont des non-conformités
- Les failles n'ont pas été décelées lors des certifications

Contradiction entre les objectifs des mesures transparentes et les attentes politiques

Objectifs des mesures transparentes

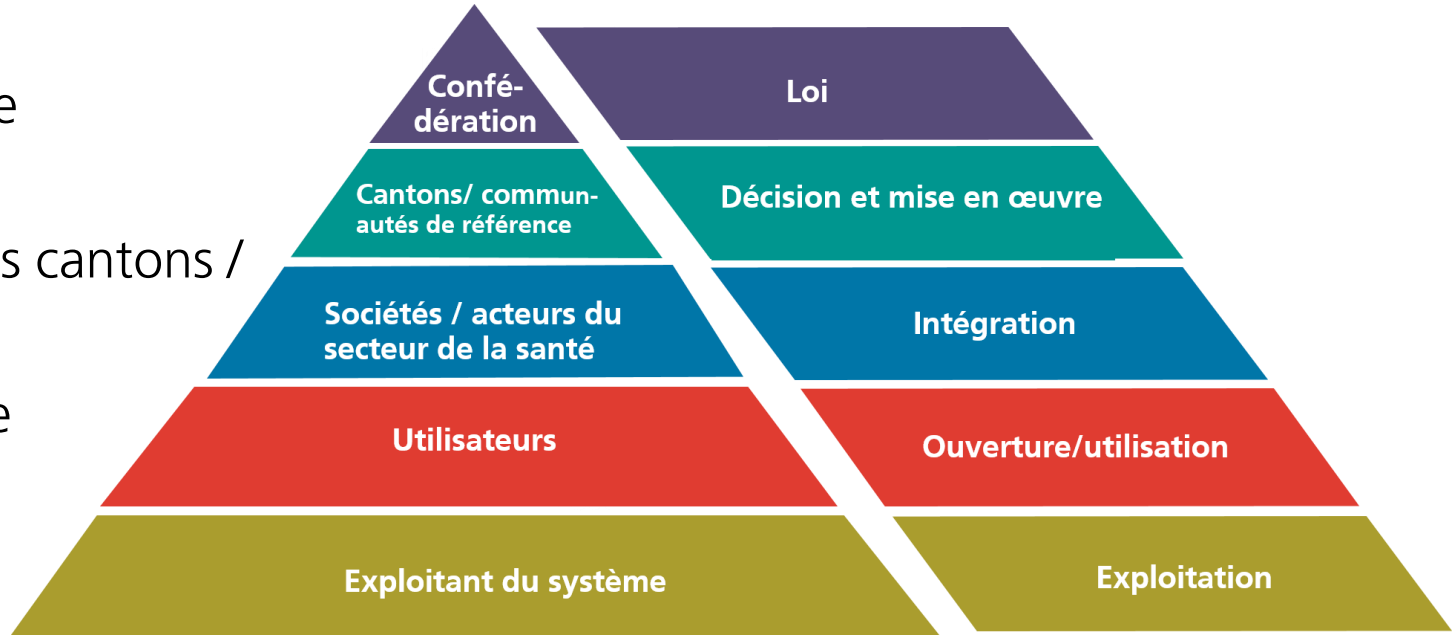
- Améliorer le système
- Trouver des erreurs qui n'ont pas été remarquées
- Couverture par une large communauté / grande expertise
- Culture de l'erreur nécessaire

Attentes politiques

- Culture zéro erreur
- Perfection exigée

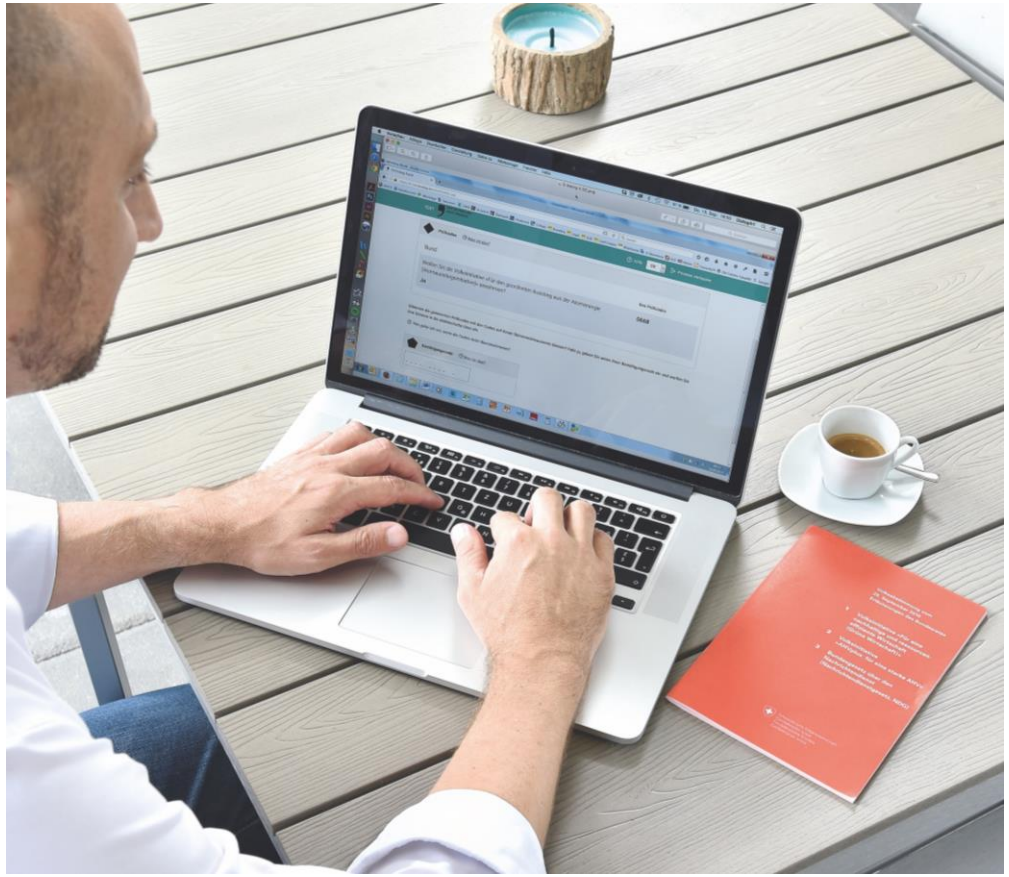
COMPARAISON AVEC D'AUTRES LOIS
PAR EXEMPLE: E-ID, DEP/DOSSIER ÉLECTRONIQUE DU PATIENT

- Des offres sont actuellement lancées sur le marché (marché libre, pas de commande de l'État)
- La Confédération définit les conditions-cadres. Une procédure de certification a été définie sur la base de ces directives
- Après la certification, le produit peut être proposé sur le marché
- L'introduction est de la responsabilité des cantons / communautés de référence
- Les thèmes ont une importance politique élevée



OÙ EN EST LE VOTE ÉLECTRONIQUE?

- Les failles de la publication du code source ont été corrigées
- La poste a pris des mesures pour optimiser ses processus
- Les cantons veulent que le système puisse être remis en service pour les élections au Conseil national. Tous les acteurs poursuivent cet objectif
- La Chancellerie fédérale fait un état des lieux pour la future autorisation des systèmes



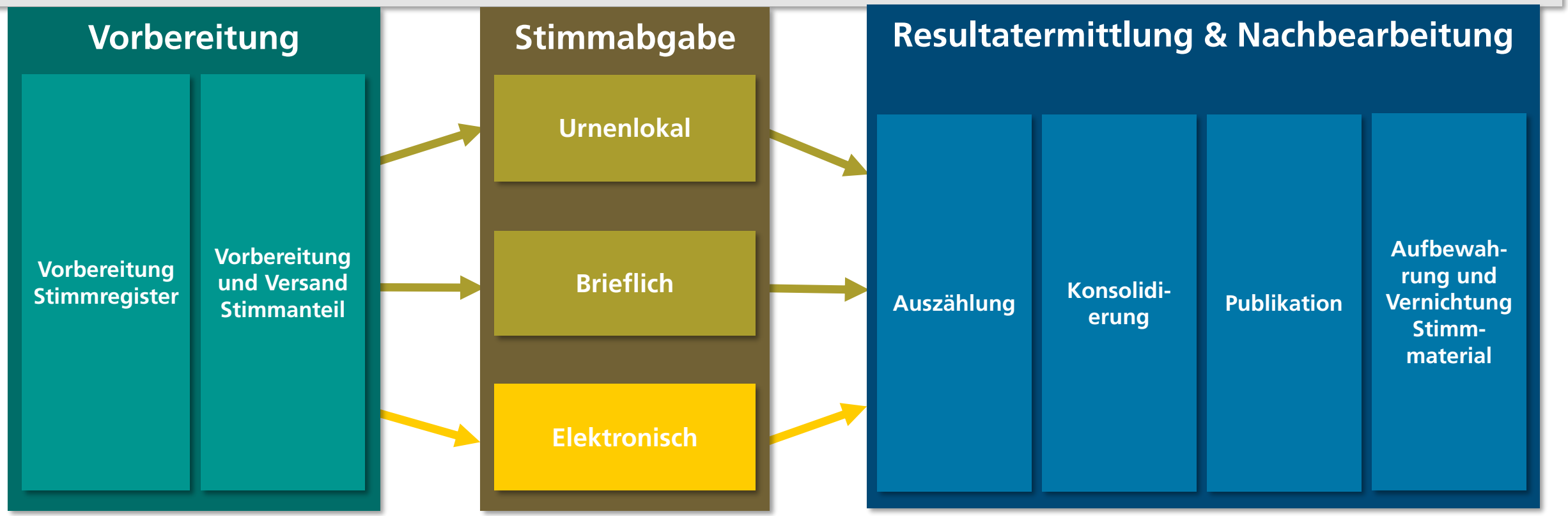
QUESTIONS

- La certification (norme industrielle) est-elle le bon instrument?
- Nécessaire pour toutes les parties de l'examen?
- La certification doit-elle être étendue par d'autres vérifications?
- Était-ce une bonne chose de publier le code source après la certification?
- Comment faut-il gérer les attentes contradictoires (bon marché, exigence de perfection, culture de l'erreur, coûts élevés, réalité du développement de logiciels, ….)?
- Comment les acteurs sont-ils à même de gérer les fausses informations qui circulent?

LA POSTE
MERCI

BACKUP

E-VOTING ALS TEIL DES ABSTIMMUNGSPROZESSES



E-VOTING - DIGITALISIERUNG DER BRIEFLICHEN ABSTIMMUNG

E-VOTING IN DER SCHWEIZ BEDEUTET ONLINE-VOTING

- Die Schweiz hat E-Voting (Online-Voting) zusätzlich zur brieflichen Abstimmung eingeführt
- In der Schweiz ist es üblich, an einem anderen Ort als dem Wahllokal abzustimmen (z.B. brieflich, zu Hause)
- Dank der brieflichen Abstimmung sind gewisse Fragestellungen nicht relevant (z.B. sozialer Druck innerhalb Familie)

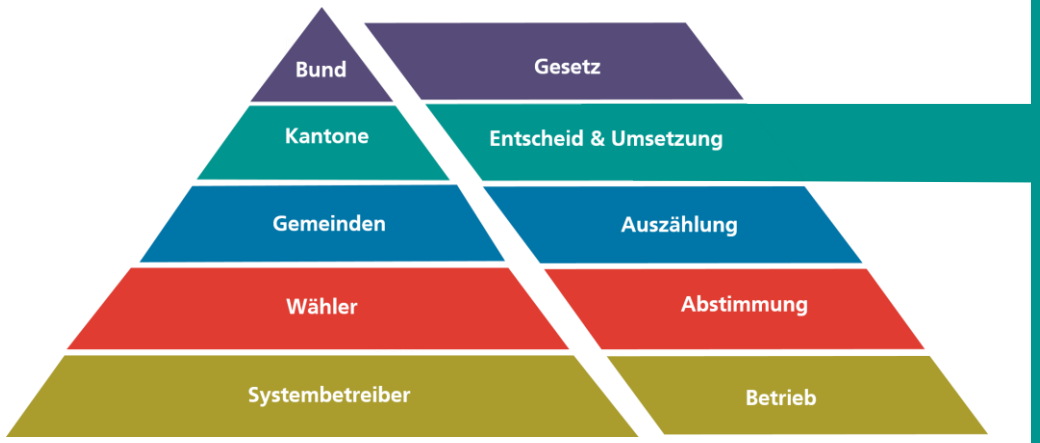
ROLLENVERTEILUNG E-VOTING
AKTEUR GEMEINDE

- **Auszählen** gemäss kantonaler Regelung
- **Konsolidierung** der Ergebnisse auf Gemeinde-ebene

ROLLENVERTEILUNG E-VOTING
AKTEUR WÄHLER

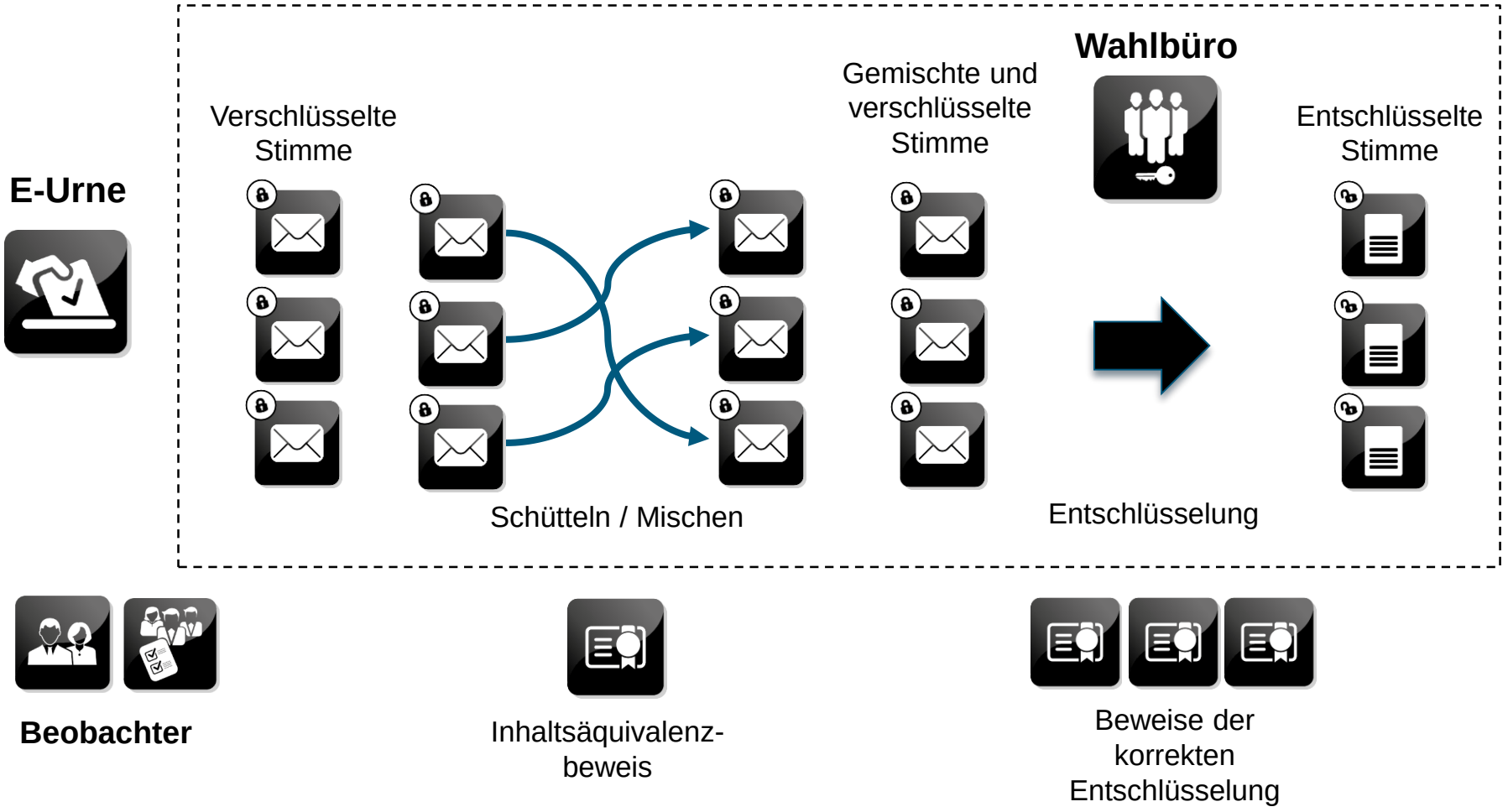
- **Entscheidet** über welchen **Kanal** er/sie wählt/stimmt (physisch, brieflich, elektronisch)
- Vollzieht die **Abstimmung** und die **Wahlen**

ROLLENVERTEILUNG E-VOTING
AKTEUR KANTON



- **Entscheidet** frei über die Einführung von E-Voting und erstellt die nötige Rechtsgrundlage
- **Entscheidet frei über das System** und den Systembetreiber
- Stellt die **Finanzierung** sicher
- Lässt die für E-Voting relevanten kantonseigenen **Prozesse zertifizieren**
- Beantragt beim Bund eine **Bewilligung** für das gewählte System
- Erstellt **Risikoanalysen** über den Betrieb von E-Voting
- Der Kanton behält jederzeit die vollständige **Kontrolle und Verantwortung** bei der Durchführung von Wahlen und Abstimmungen
- Der Kanton bereitet die Daten vor, die **Sicherheits-verschlüsselung** und entschlüsselt die Urne

UNIVERSELLE VERIFIZIERBARKEIT
GENERIERUNG DER BEWEISE



- **Inhaltsäquivalenzbeweis:** Beweist, dass die Stimmen nicht durch den Mixing-Prozess manipuliert wurden
- **Beweise der korrekten Entschlüsselung:** Beweist, dass die Stimmen während des Entschlüsselungsprozesses nicht manipuliert wurden

VOTE ÉLECTRONIQUE - RÉPARTITION DES RÔLES