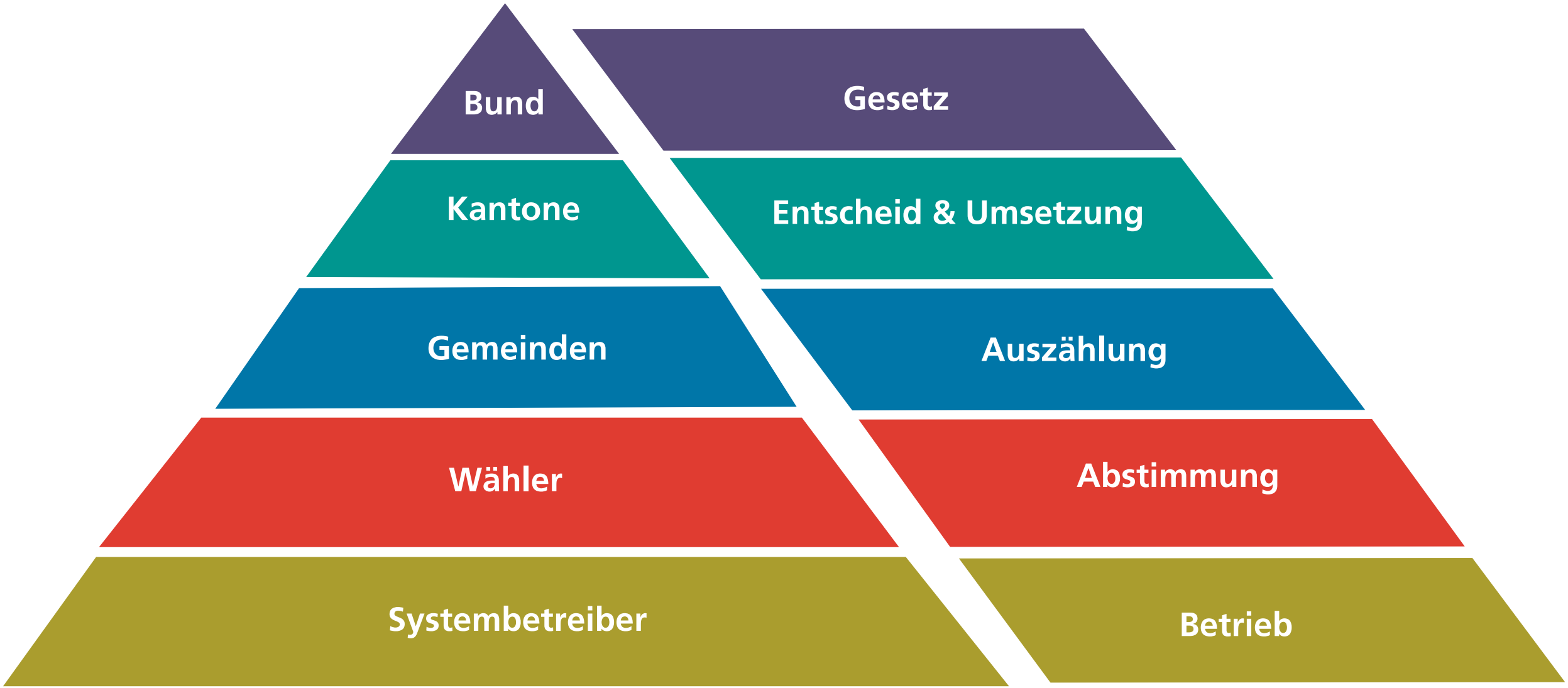
DAS E-VOTING-SYSTEM DER POST – ERFAHRUNGEN UND RÜCKSCHLÄGE AUF DEM WEG ZUM VOLLSTÄNDIG VERIFIZIERBAREN SYSTEM

14.05.2019, 19. MAGGLINGER RECHTS-INFORMATIKSEMINAR, DENIS MOREL, LEITER DIGITAL PUBLIC SERVICES

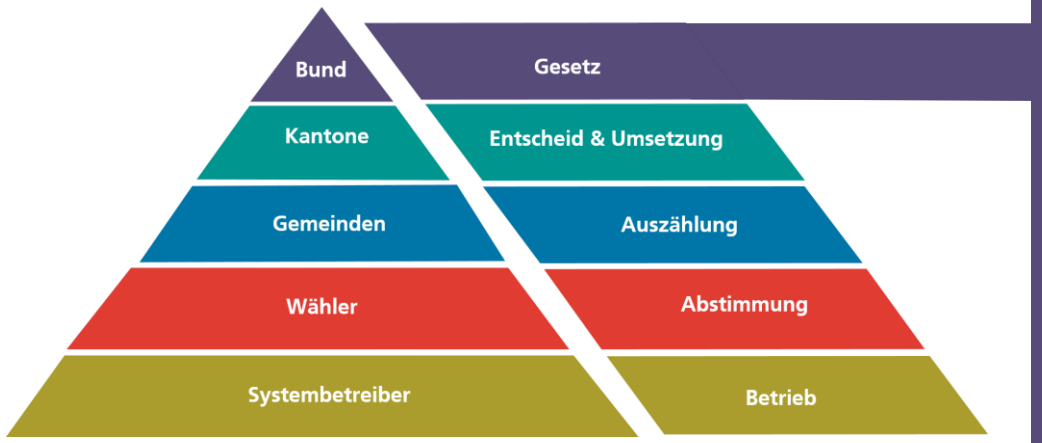
DIE POST

EINLEITUNG
ROLLEN DER AKTEURE BEI E-VOTING

ROLLENVERTEILUNG E-VOTING

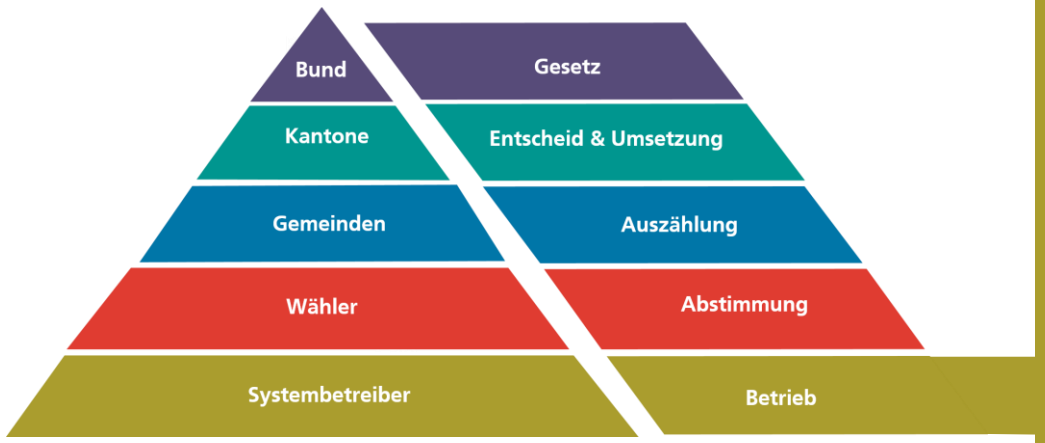


ROLLENVERTEILUNG E-VOTING
AKTEUR BUND



- Bestimmt die **gesetzlichen Rahmenbedingungen** (Gesetz und Verordnung) für Bundeswahlen und Abstimmungen
- Sieht gesetzlich die Möglichkeit vor, dass die Kantone freiwillig **E-Voting einführen** können
- Definiert für alle Kantone einheitlich die **Sicherheits-anforderungen** an das System und den Betrieb
- Erteilt den Kantonen die **Bewilligung zum Betrieb** und prüft das Vorliegen aller Voraussetzungen
- **Überwacht** den Betrieb in den Kantonen

ROLLENVERTEILUNG E-VOTING
AKTEUR SYSTEMANBIETER

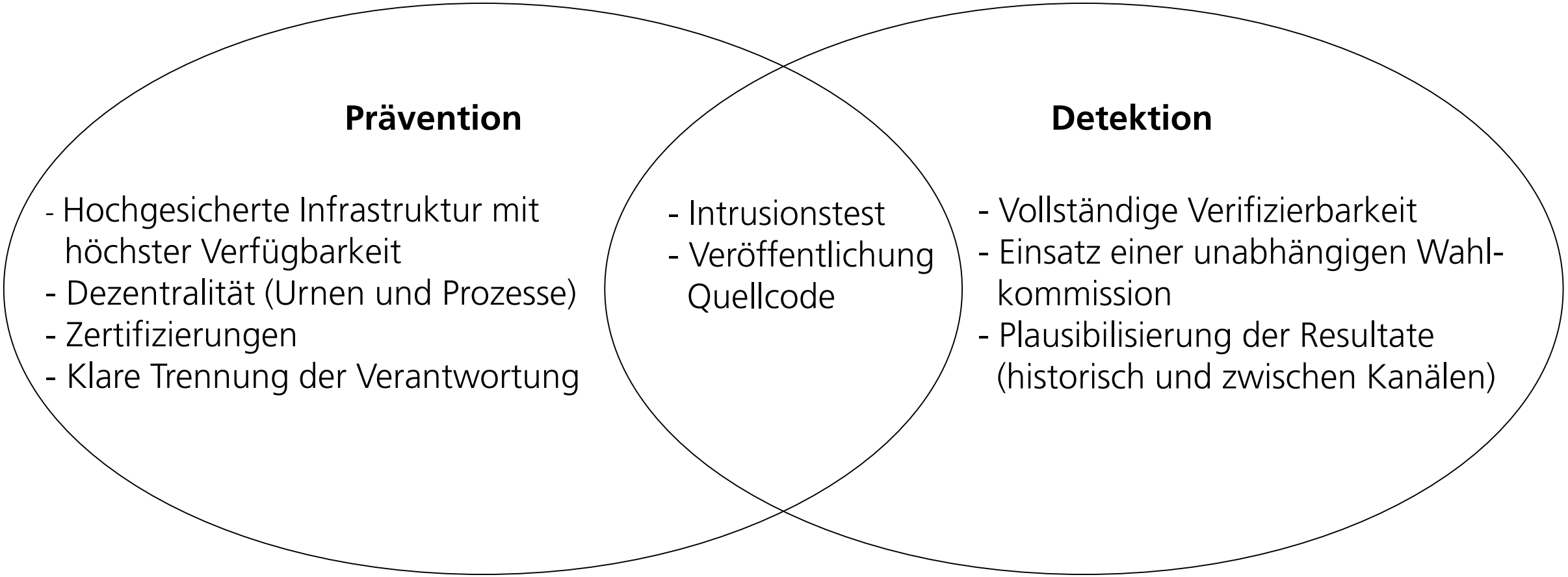


- **Entwickelt System** und **Betrieb** gemäss den Anforderungen des Bundes
- Ist verantwortlich für den **Betrieb** der **elektronischen Urne**
- **Stellt die Urne** dem Kanton **zur Verfügung**, damit der Kanton seine Prozesse unabhängig durchführen kann
- Publiziert den **Quellcode** des Systems gemäss den bundesrechtlichen Anforderungen
- Stellt die gesetzeskonforme **Datenhaltung** in der Schweiz sicher

SICHERHEITSANFORDERUNGEN
ÜBERSICHT ÜBER DIE WICHTIGSTEN SICHERHEITSELEMENTE

SICHERHEITSELEMENTE

VOLLSTÄNDIGE VERIFIZIERBARKEIT – ZENTRALER TEIL DES SICHERHEITSMIXES

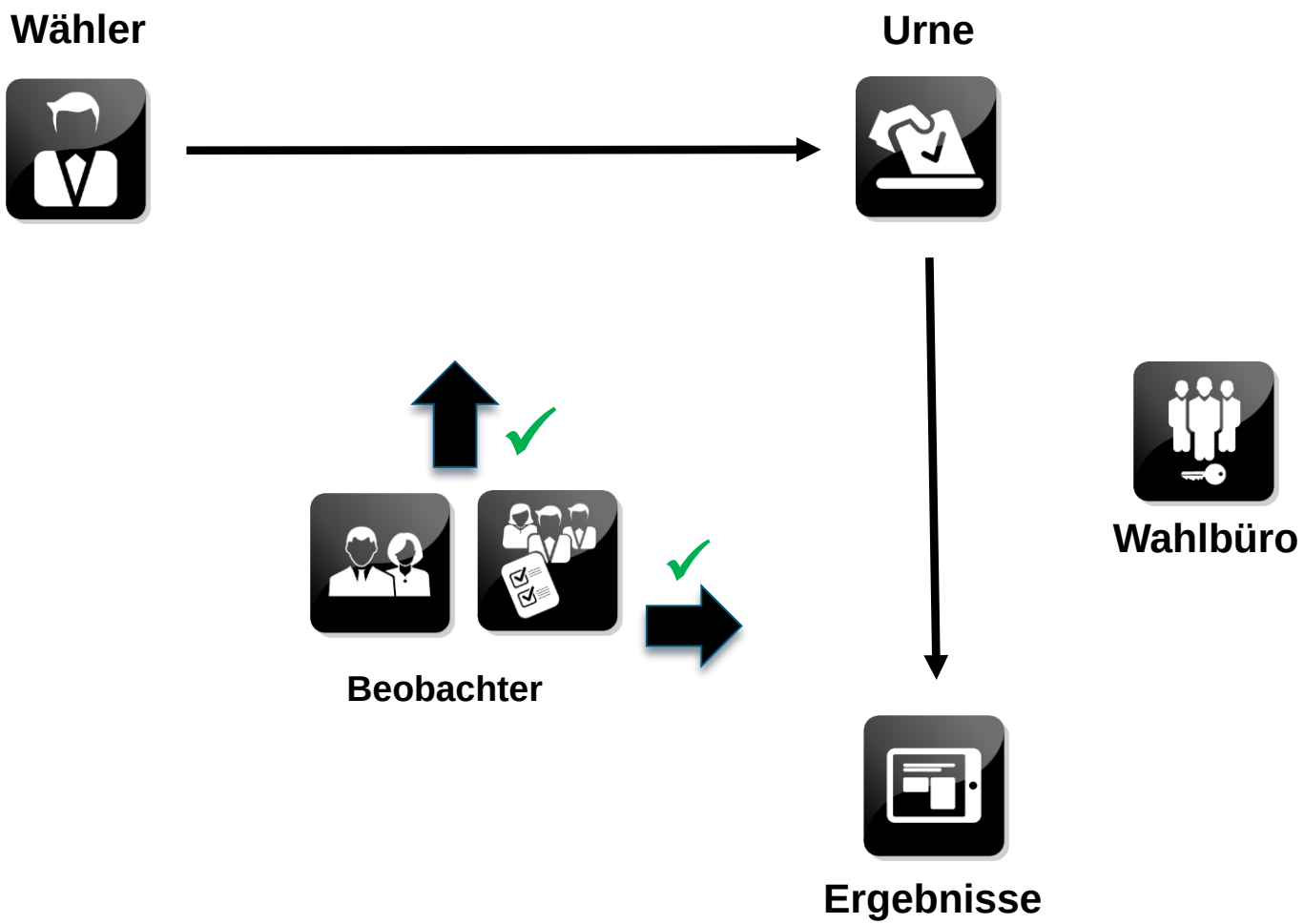


SICHERHEITSANFORDERUNGEN

INDIVIDUELLE VERIFIZIERBARKEIT +
UNIVERSELLE VERIFIZIERBARKEIT
= VOLLSTÄNDIGE VERIFIZIERBARKEIT

SICHERHEITSANFORDERUNGEN

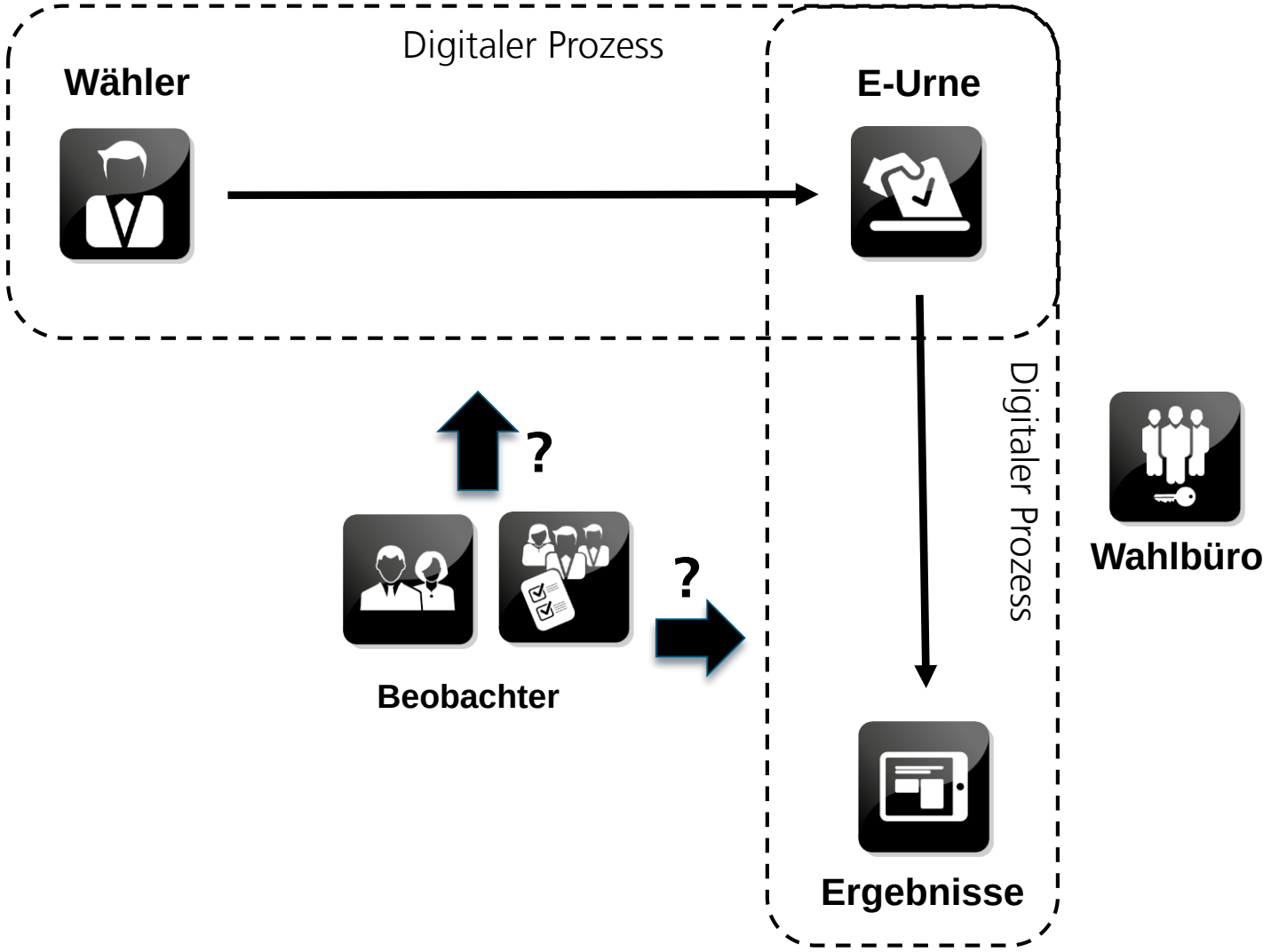
BEI DEN «PHYSISCHEN» ABSTIMMUNGEN IST ALLES EINFACH BEOBACHTBAR ….



- Stimme und Prozesse (z.B. Auszählung) basieren ausschliesslich auf **physischen Elementen**
- Prozesse können vom Wahlbüro, **nur mit menschlichen Mitteln** beobachtet werden

VOLLSTÄNDIGE VERIFIZIERBARKEIT

BEI ELEKTRONISCHEN ABSTIMMUNGEN IST DIE BEOBACHTUNG SCHWIERIGER

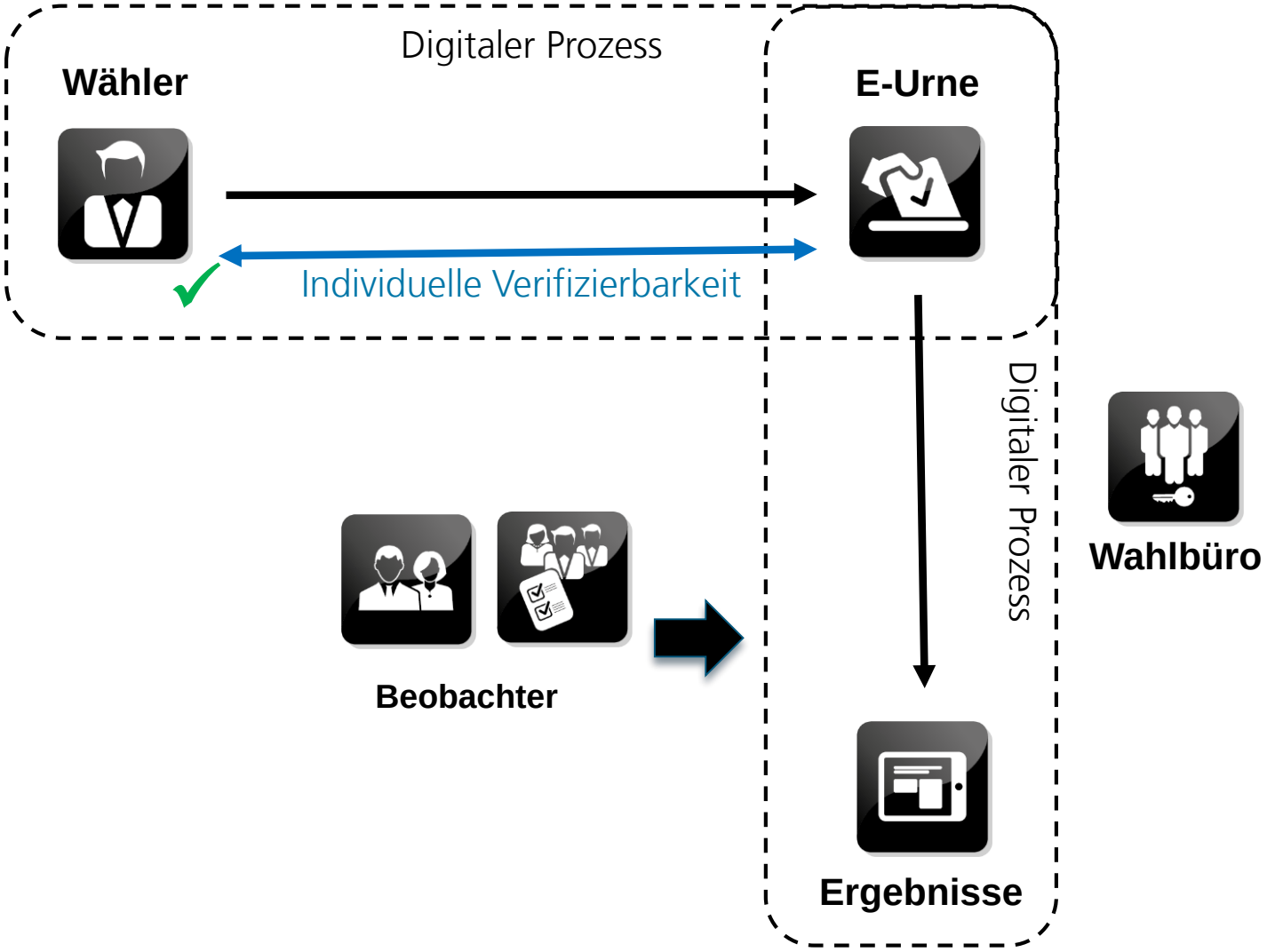


- Prozesse (z.B. Auszählung) basieren auf **digitalen Elementen** (Daten/Software)
- Prozesse können **nicht durch Personen** beobachtet werden

https://youtu.be/Hzd7ViuFAcQ

VOLLSTÄNDIGE VERIFIZIERBARKEIT

ALS MITTEL FÜR DIE BEOBACHTUNG DES DIGITALEN PROZESSES

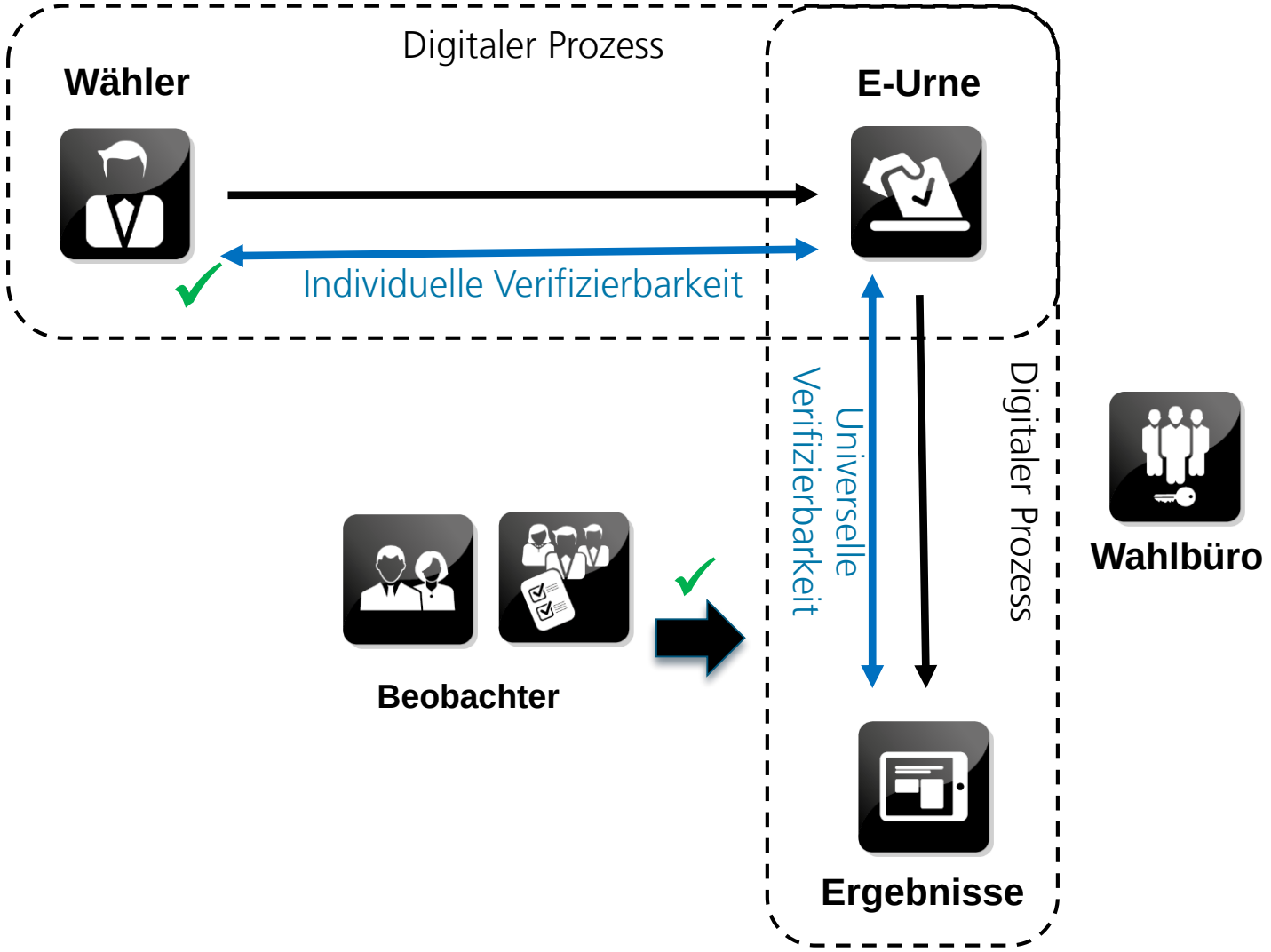


- Der Wähler kann verifizieren, dass seine Stimme in der Urne **wie gewünscht** abgelegt wurde (individuelle Verifizierbarkeit)
- Nachvollziehbarkeit **«cast as intended»**

https://youtu.be/2UI3VsszqPE

VOLLSTÄNDIGE VERIFIZIERBARKEIT

ALS MITTEL FÜR DIE BEOBACHTUNG DES DIGITALEN PROZESSES



- Der Wähler kann verifizieren, dass seine Stimme in der Urne **wie gewünscht** abgelegt wurde (individuelle Verifizierbarkeit)
- Das Wahlbüro kann verifizieren, dass die Urne **nicht verfälscht** wurde und dass **alle Stimmen korrekt gezählt** wurden (universelle Verifizierbarkeit)

UNTERSCHIEDLICHE ANFORDERUNGEN AN DIE SICHERHEIT
50% VS 100% DES ELEKTORATS

Für 50% des Elektorats

- **Zertifizierung**, gemäss Industriestandard
- **Individuelle Verifizierbarkeit**

Für 100% des Elektorats

- **Zertifizierung**, gemäss Industriestandard
- **Individuelle Verifizierbarkeit**

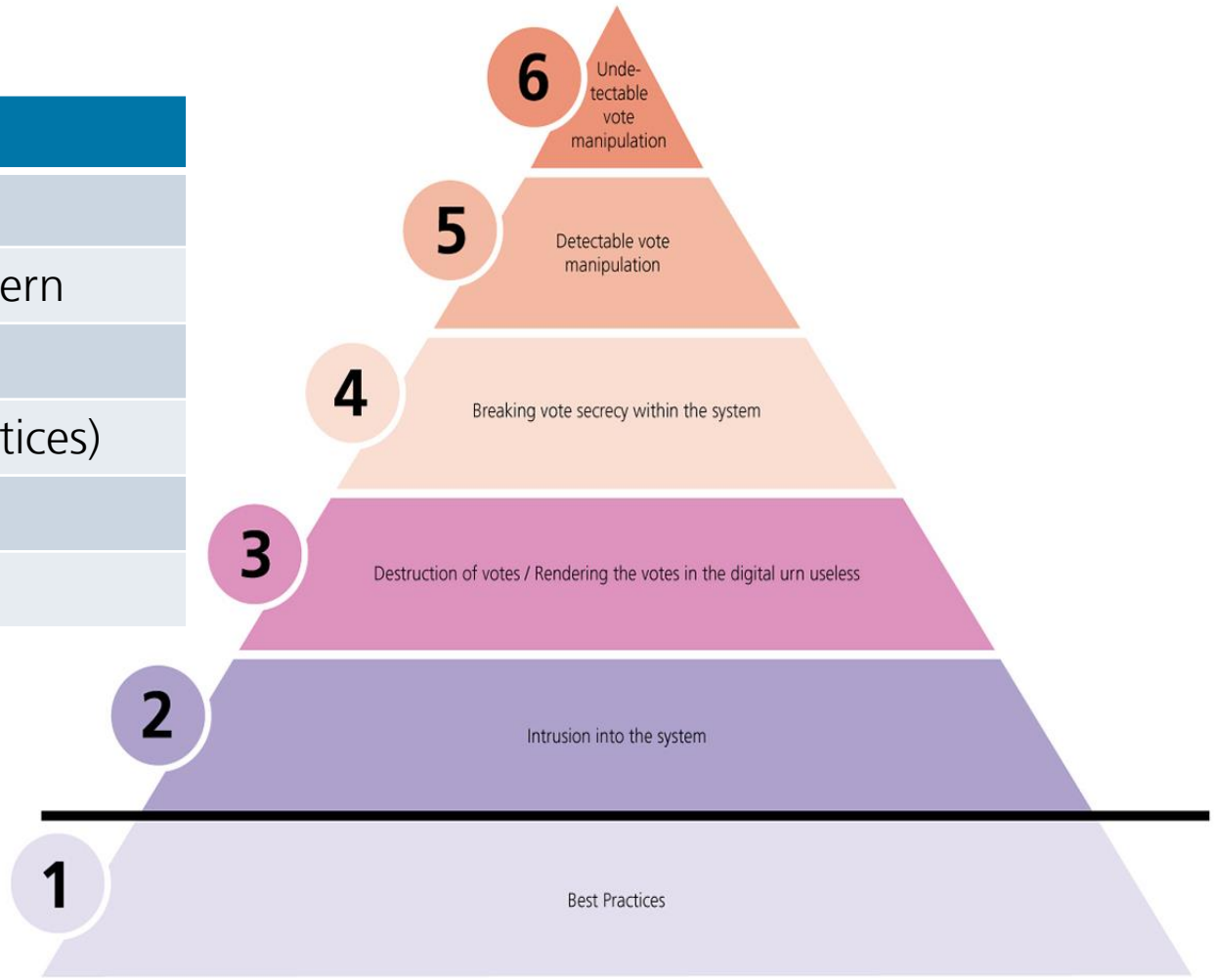
plus zusätzlich:
- **Universelle Verifizierbarkeit**
- Veröffentlichung des **Quellcodes**
- **Public Intrusionstest** (keine gesetzliche Anforderung, sondern Anforderung von Kantonen und Bundeskanzlei)

ZERTIFIZIERUNG GEMÄSS INDUSTRIESTANDARD

- Zertifizierung nach der Regulation VEleS (50% und 100%)
- Zertifizierung nach ISO 27001
- Prüfung der Compliance des Systems (Infrastruktur, Betrieb, Managementprozesse, Risikomanagement, Governance, Informationssicherheit, Softwarefunktionalitäten, Testprozesse, usw.)
- Fachthemen werden nicht vollumfänglich auditiert. Das Audit wird auf Basis von Prüfstichproben risikobasiert ausgeführt. Massnahmenempfehlungen werden kontinuierlich umgesetzt.
- Akkreditierung der Zertifizierungsstelle durch SECO-SAS
- 3-Jahres-Zyklus (Main-Audit, 2 Wiederholungs-Audits, Re-Zertifizierungs-Audit)
- Kontinuierlicher Verbesserungsprozess ist ein wichtiges Element des Audits
- Die Nicht-Konformitäten werden klassifiziert: leicht, schwer, kritisch

ERGEBNISSE PIT (PUBLIC INTRUSION TEST)
EIGENTLICH EIN ERFOLG

Element	Ergebnis
Dauer	25.02.2019 bis 24.03.2019
Researcher	3186 Personen aus 137 Ländern
Submitted Findings	173
Accepted Findings	16 der Kategorie 1 (Best Practices)
Max. Kompensation	CHF 150’000.-
Ausbezahlte Kompensation	CHF 2’000



Die notariell beglaubigte Urne konnte weder manipuliert noch der Urnengang gestört werden.

HERAUSFORDERUNGEN IM QUELLCODE

- Drei Findings, eines davon betrifft das im Einsatz stehende System
- Die Findings sind auf kryptographischer Ebene
- Obwohl die Findings in der Realität sehr schwer zu nutzen wären, sind es Nicht-Konformitäten
- Die Findings wurden bei der Zertifizierungen nicht entdeckt

Widerspruch zwischen Zielen der Transparentmassnahmen und der Erwartungshaltung der Politik

Ziele der Transparentmassnahmen

- System verbessern
- Fehler finden, die übersehen wurden
- Abdeckung durch eine breite Gemeinschaft / viel Expertenwissen
- Notwendige Fehlerkultur

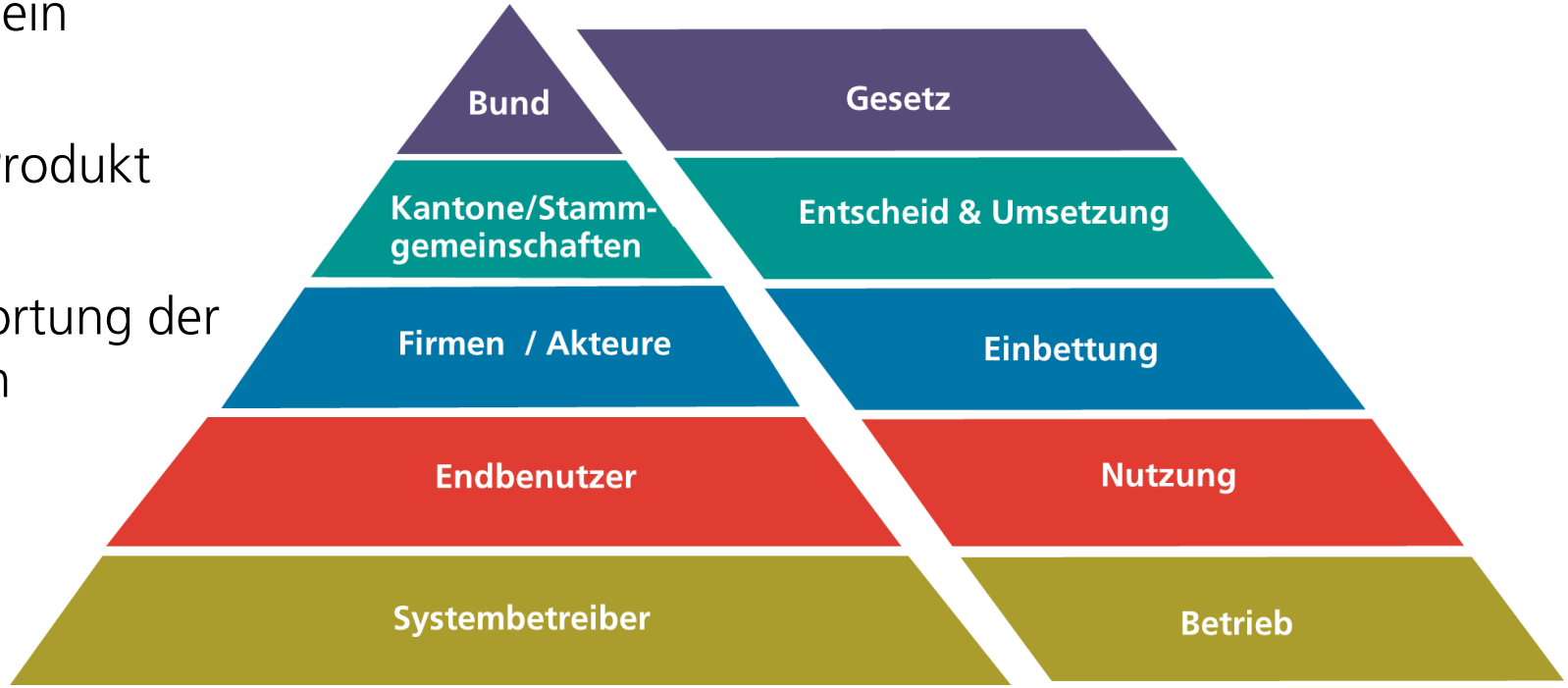
Erwartungshaltung der Politik

- Null-Fehler-Kultur
- Geforderte Perfektion

VERGLEICH ZU ANDEREN GESETZEN

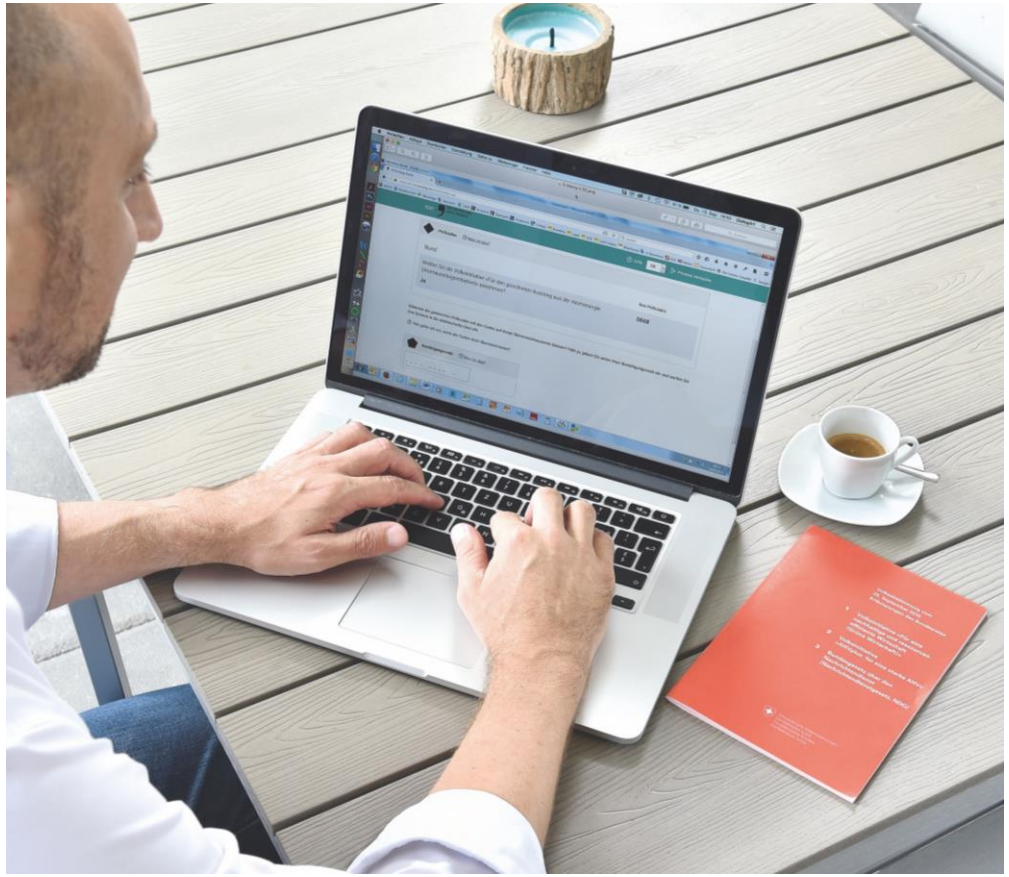
Z.B. E-ID ODER EPD/ELEKTRONISCHES PATIENTENDOSSIER

- Angebote werden zur Zeit im Markt eingeführt (freier Markt, kein Staatsauftrag)
- Der Bund definiert die Rahmenbedingungen. Aufgrund dieser Vorgaben wurde ein Zertifizierungsverfahren definiert
- Nach der Zertifizierung kann das Produkt am Markt angeboten werden
- Die Einführung ist in der Verantwortung der Kantonen / Stammgemeinschaften
- Die Themen haben eine hohe politische Relevanz



WIE GEHT ES WEITER MIT E-VOTING?

- Findings aus der Offenlegung des Quellcodes wurden behoben
- Die Post hat Massnahmen getroffen, um ihre Prozesse zu optimieren
- Die Kantone wollen, dass das System wieder für die Nationalratswahlen eingesetzt werden kann. Alle Akteure streben nach diesem Ziel
- Die Bundeskanzlei macht eine Auslegeordnung für die zukünftige Bewilligung von Systemen



FRAGE, DIE SIE SICH STELLEN

- Ist die Zertifizierung (Industriestandard) das richtige Instrument?
- Für alle Teile der Prüfung notwendig?
- Soll die Zertifizierung mit anderen Prüfungen erweitert werden?
- War es richtig, den Quellcode nach der Zertifizierung zu veröffentlichen?
- Wie soll mit den widersprüchlichen Erwartungshaltungen umgegangen werden (kostengünstig, geforderte Perfektion, Fehlerkultur, hohe Kosten, Realität der SW-Entwicklung usw.) ?
- Wie können die Akteure mit zirkulierenden Falschinformationen umgehen?

DIE POST
VIELEN DANK