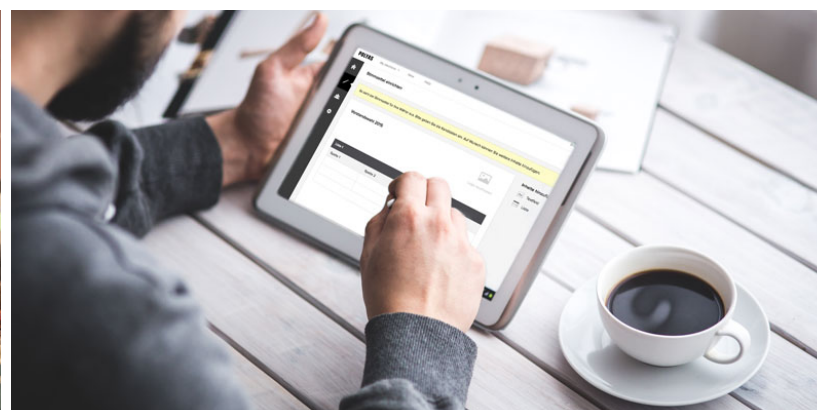
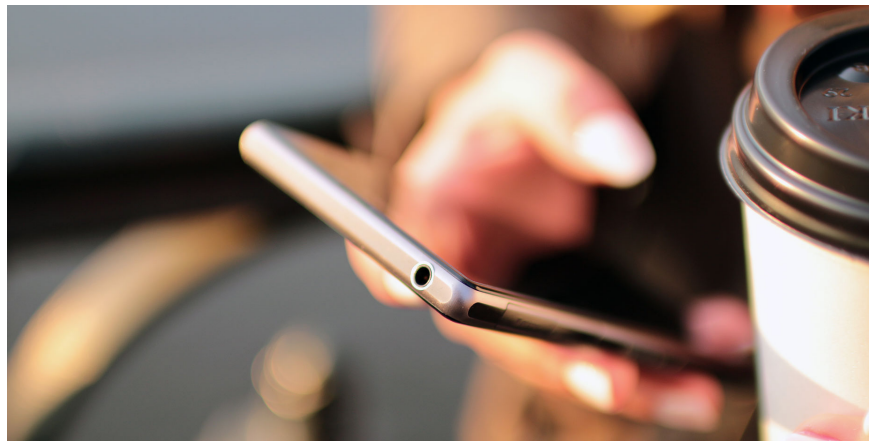


Die Online-Wahl im 21. Jahrhundert



Inhalt

- 1 Polyas Online-Wahlen
- 2 Rahmenbedingungen, Erfahrungen, Herausforderungen
- 3 Technische Hintergründe

Polyas Management Team



Ralf Müller (48), CEO

Internationalisierung, Strategie, Finanzen, Personal

Diplom-Kaufmann, Tübingen

Ehemals Holtzbrinck, Gründer Smartsteuer.de mit Exit in 2012 an Haufe Lexware Gruppe



Tomasz Truderung (45), Head of Research

Produktentwicklung & Forschung

PhD in Computer Science, University of Wrocław

Ehemals Universität Trier, INRIA-LORIA-Lorraine (Nancy, France), Christian-Albrechts-Universität zu Kiel



Anna-Maria Palzkill (32), Head of Marketing & Sales

Marketing Global, Sales & Operations DACH

Diplom-Kommunikationswissenschaft, Universität Hohenheim

Ehemals Festo AG, Fraunhofer Institut (IPA), Wilford Schupp Architekten Stuttgart / London



Patrick Busch (32), Head of SaaS Development

IT & Systems

Dipl. Wirt.-Informatik, Hochschule Karlsruhe

Ehemals Teamleiter bei 1&1, Senior Developer Micromata

Polyas Meilensteine



1996

Erste Wahlen durch die Micromata GmbH (mittelständisches Softwarehaus in Kassel verantwortlich u.a. für DHL-Tracking Portal, Online-Frankierung etc.)



2013

Kirche von Kurhessen-Waldeck: Kombiniertes Wahlverfahren aus Online-Wahl, Briefwahl und Urnenwahl für 800.000 Wahlberechtigte



2015

Über 100 Kunden mit mehr als 3 Millionen Wählern
End-to-End Betreuung kombinierter Wahlverfahren



2016

Common Criteria Zertifizierung

Januar

POLYAS erfüllt als weltweit erster Wahlanbieter die Common Criterias für Online Wahlen



Februar

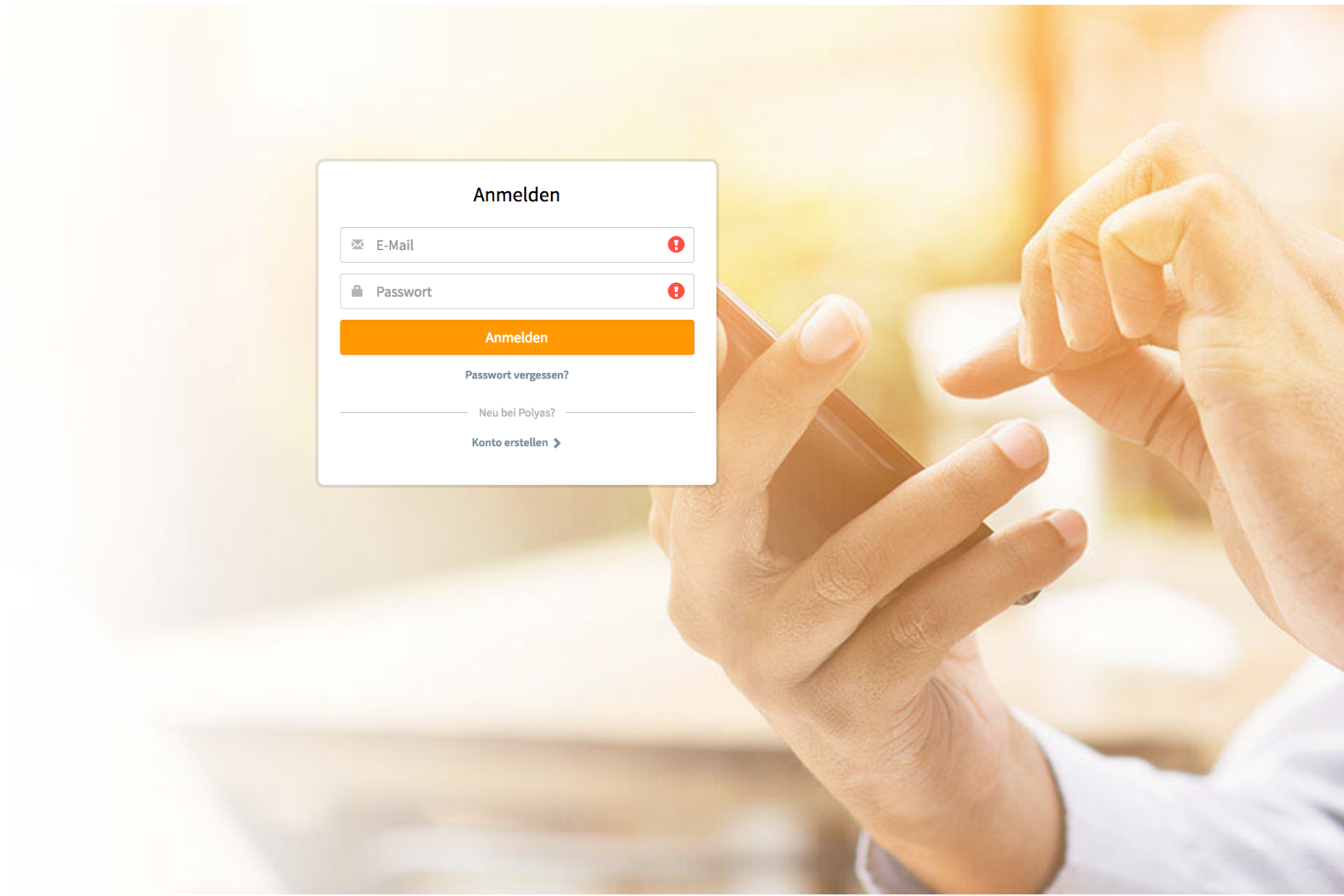
Die GEMA beauftragt als erste Verwertungsgesellschaft die POLYAS mit der Durchführung der Mitgliederversammlung 2017



Juni

Internationalisierung

Polyas: Das erste Online-Wahlsystem as a Service



The background image shows a person's hands holding a smartphone. Overlaid on the screen is a white login form titled 'Anmelden'. The form contains two input fields: 'E-Mail' with an envelope icon and 'Passwort' with a lock icon. Both fields have a red exclamation mark icon to their right, indicating an error. Below the fields is an orange 'Anmelden' button. Underneath the button are links for 'Passwort vergessen?', 'Neu bei Polyas?', and 'Konto erstellen >'.

Anmelden

✉ E-Mail !

🔒 Passwort !

Anmelden

[Passwort vergessen?](#)

Neu bei Polyas?

[Konto erstellen >](#)

Online-Wahlen mit Polyas sind einfach zu veranstalten

1



Online Stimmzettel erstellen

2



Wählerverzeichnis hochladen

3

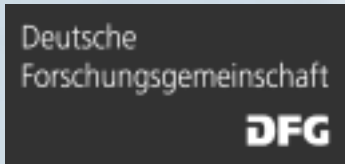


Wahlzeitraum festlegen

Sämtliche Wahlverfahren sind einfach zu kombinieren



Referenzen – Auswahl unserer Kunden



hochschule macromedia
university of applied sciences

Beiersdorf

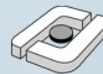
SwissLife



Brandenburgische
Architektenkammer
Körperschaft des öffentlichen Rechts



Architekten schaffen Räume.



Hochschule Osnabrück
University of Applied Sciences

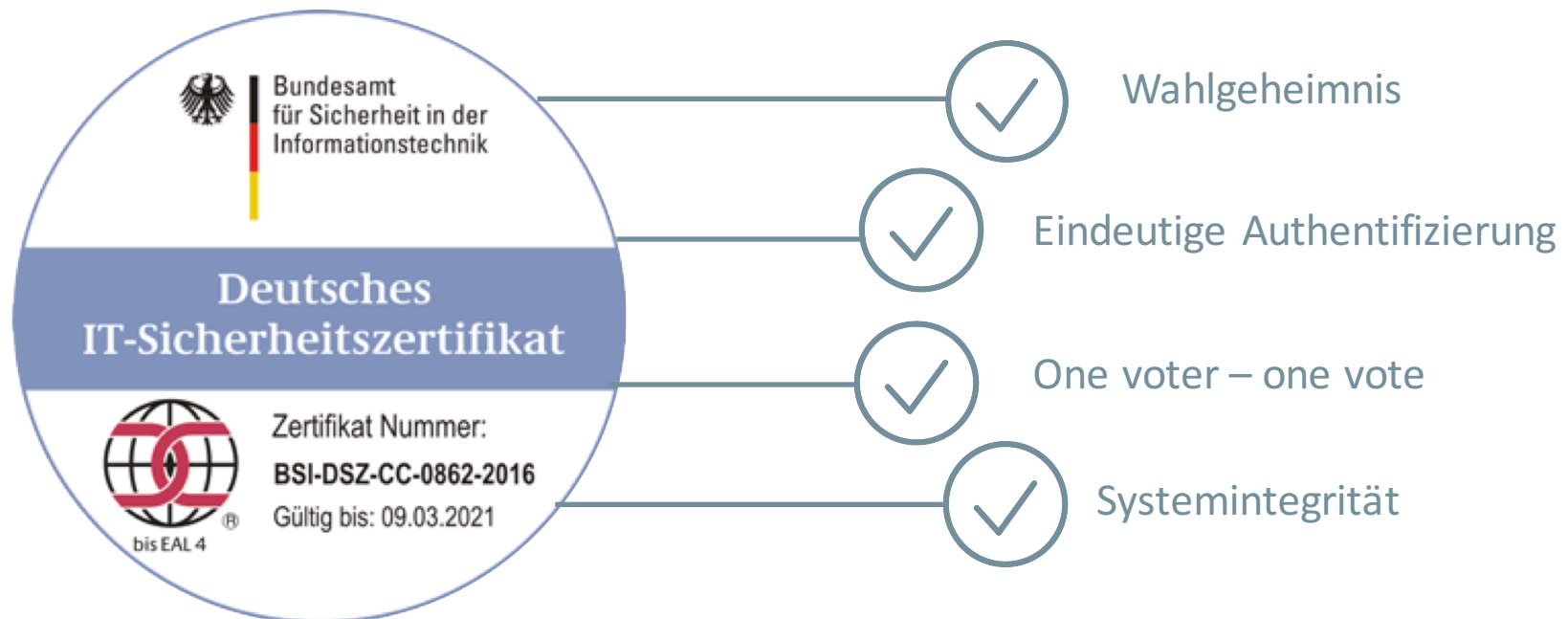


Polyas CORE 2.2.3 erhält weltweit erste und einzige Zertifizierung

Common Criteria: internationale Sicherheits-Standards für Funktionalität und Vertrauenswürdigkeit von IT-Produkten

Bundesamt für Sicherheit in der Informationstechnik erteilt Zertifizierung

Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI) führt Systemprüfung und Vor-Ort-Abnahme durch



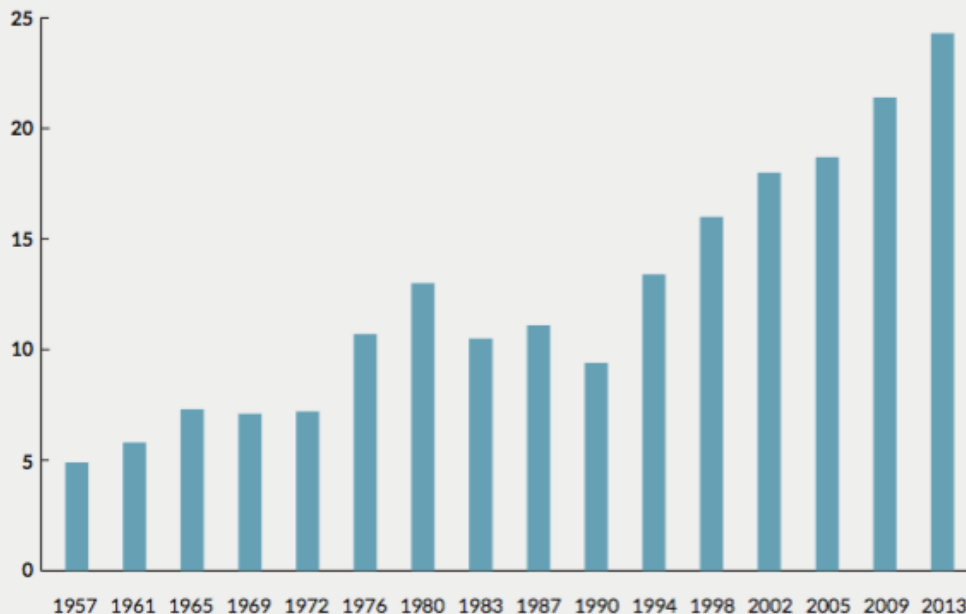
Inhalt

- 1 Polyas Online-Wahlen
- 2 Rahmenbedingungen, Erfahrungen, Herausforderungen
- 3 Technische Hintergründe

Anteil der Fernwähler steigt

ABBILDUNG 1 Anteil der Briefwähler bei Bundestagswahlen seit 1957

in Prozent



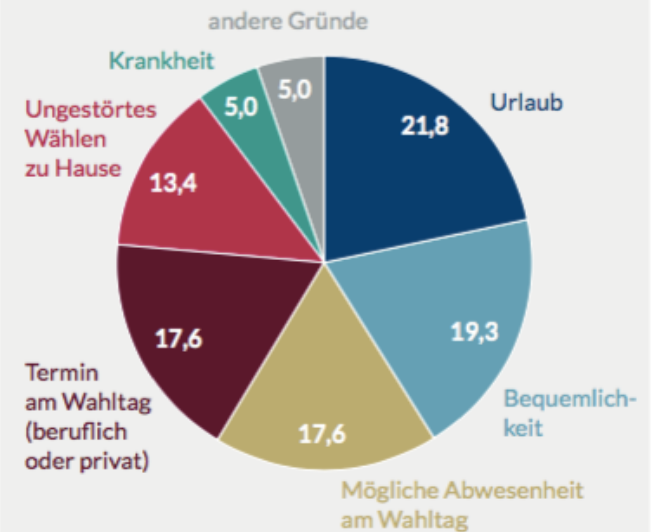
Quelle: Bundeswahlleiter, eigene Darstellung.

| BertelsmannStiftung

ABBILDUNG 4 Gründe für die Briefwahl bei der Bundestagswahl 2013

in Prozent

Frage: „Warum haben Sie bei der Bundestagswahl per Brief gewählt?“



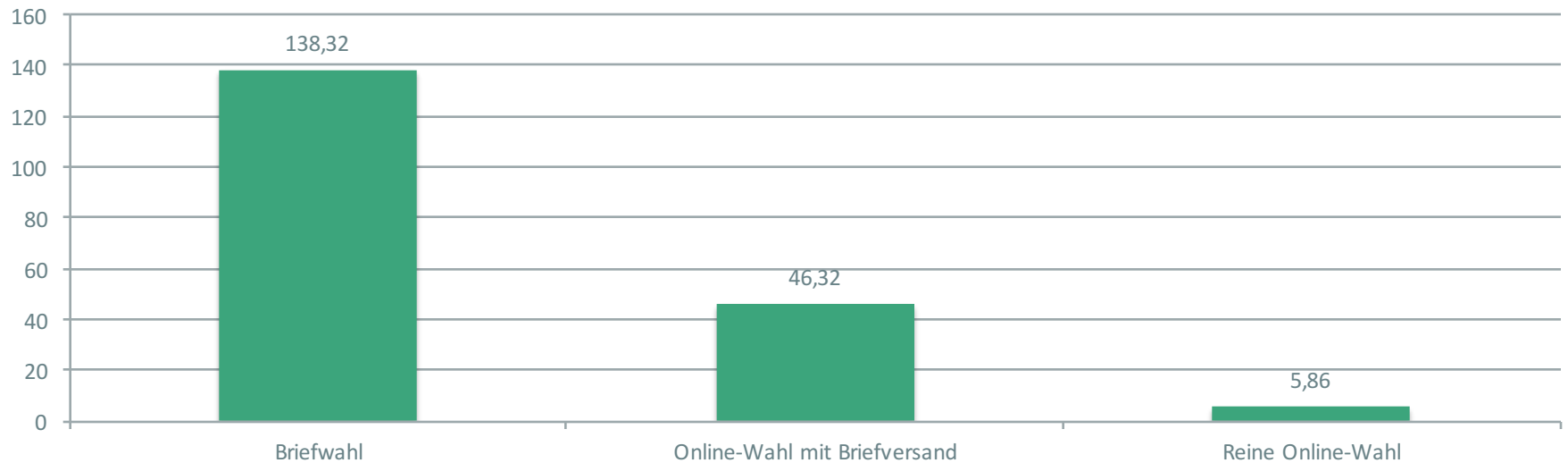
n=2.850 wahlberechtigte Befragte; Mehrfachnennung war möglich; zusammengefasste Antworten: private und berufliche Termine (Termin am Wahltag), Gebrechlichkeit und Krankheit (Krankheit).

Quelle: infratest dimap 2015.

| BertelsmannStiftung

Die Online-Wahl bietet erhebliches Einsparpotential

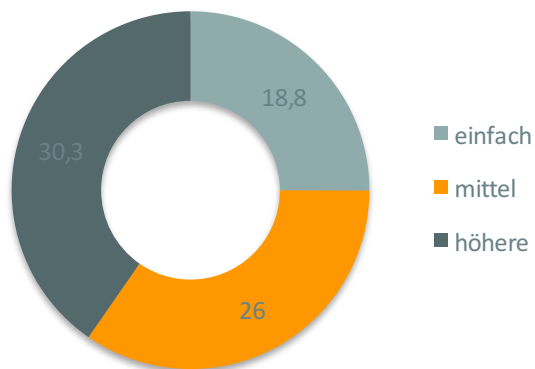
CO₂-Emissionen nach Wahlverfahren
(in Gramm pro Wähler)



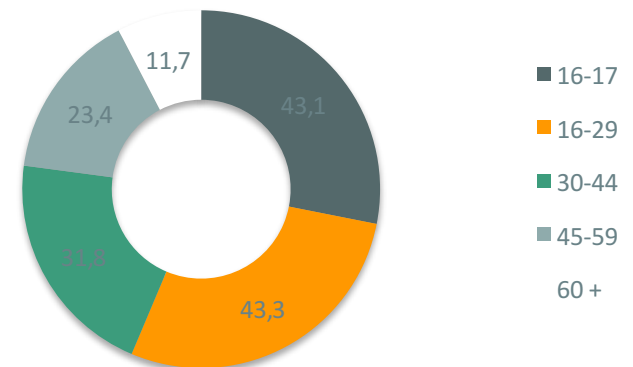
Zustimmung zu Online-Wahlen

„Würden Ihnen Online-Wahlen persönlich das Wählen erleichtern?“ Zustimmung in Prozent

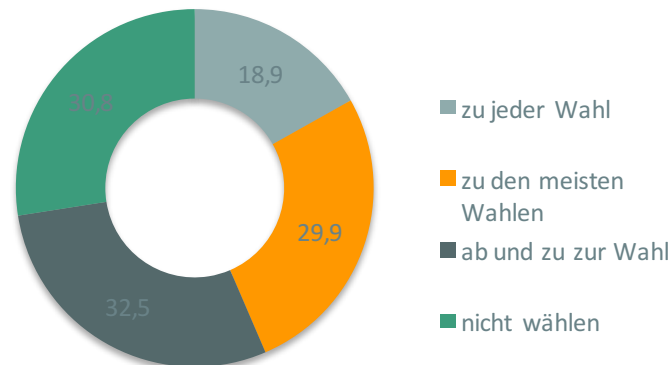
Schulbildung



Altersgruppen



Wahlbeteiligung



Polyas Erfahrung zur Wahlbeteiligung und Wahlverfahren



Wahl der universitären und studentischen Gremien mit bis zu 100 Stimmzettelkombinationen

Vormals Präsenzwahl und Briefwahl auf Anfrage,
Jetzt Online-Wahl mit Briefwahl auf Anfrage

Steigerung der Wahlbeteiligung

- Gremienwahlen der FSU Jena von 8% (2014) auf 13% (2016)
Anteil Briefwähler: < 1%
- Senatswahlen der JLU Gießen von 12,28% (2015) auf: 21,82% (2016)
Anteil Briefwähler: < 1%

Rechtslage positiv:

Konkrete Vorgaben aus dem Online-Wahl-Urteil von 2013

- OVG Weimar Urteil vom 30.5.2013 erlaubt Online-Wahl an einer Körperschaft des Öffentlichen Rechts (FSU Jena)
- Urteil gibt Hinweise zur Ausgestaltung der Wahlordnung
 - Mindestsicherheitsstandard der Software (BSI-Standard)
 - Verpflichtung des Wählers zum Ausspähschutz (Antivirensoftware)
 - Übereilungsschutz (Überprüfung der Stimmabgabe auf Korrektheit)
 - Umgang mit technischen Störungen während der Wahl
- Die Rechtsaufsicht stimmt zu

Daten: Datenschutz und Datensicherheit



Systemsicherheit

- ✓ Jährliche Penetration-Tests und Security Audits durch Physikalisch-Technische Bundesanstalt
- ✓ Gewährleistung von 99% Verfügbarkeit sowie persönliche Ansprechpartner bei unerwartetem Systemverhalten

Datensicherheit

- ✓ Hochqualifizierte und regelmäßig überprüfte Sicherungsmaßnahmen der Datenverarbeitungsprozesse
- ✓ Verträge zur Auftragsdatenverarbeitung mit allen betroffenen Mitarbeitern und Unterauftragnehmern
- ✓ ISO 27001 zertifizierte Serverstandorte in Deutschland: 1&1 und Hetzner

Polyas CORE 2.2.3 erhält weltweit erste und einzige Zertifizierung



Zertifikat für Online-Wahlen BSI-DSZ-CC-0862-2016

- **Common Criteria:** internationale Sicherheits-Standards für Funktionalität und Vertrauenswürdigkeit von IT-Produkten
- **Bundesamt für Sicherheit in der Informationstechnik** erteilt Zertifizierung in Deutschland
- **Deutsches Forschungszentrum für Künstliche Intelligenz** nimmt Prüfung von Polyas vor

Folgende Bedingungen werden u.a. erfüllt:

- Eindeutige Identifikation und Authentifizierung der Wahlberechtigten für die Stimmabgabe durch Wähler-ID und einmalgültiges Passwort, optionale Steigerung durch Zweifaktor-Authentifizierung.
- Von der abgegebenen Stimme ist kein Rückschluss auf die Identität des Wählers herstellbar durch die Anonymisierung über einen Token.
- Ständige Integritätsprüfung durch Prüfsummen erlaubt keine nachträgliche Änderung, Löschung oder Ergänzung von Stimmen.

Zertifizierung: Interpretation des Zertifikats

Formulierungen lassen an einigen Stellen mehrere Möglichkeiten für eine BSI-konforme Wahl zu

→ „Übertragung der Zugangsdaten auf sicherem Übertragungsweg“

Was ist ein sicherer Übertragungsweg?

- Postversand?
- Postversand nur mit PostIdent?
- Postversand nur mit Einschreiben?
- Email?
- Email nur verschlüsselt? PGP oder SMIME?
- SMS?
- Bei Postversand: Wie kommen die Zugangsdaten zum Druckdienstleister?

→ Interpretationsspielraum

Zertifizierung: Interpretation des Zertifikats

Zertifizierung ist ein Prozess über mehrere Jahre, in der IT sind das mehrere Generationen

→ Heutige Selbstverständlichkeiten im Betrieb nicht anwendbar

Virtualisierung weder explizit erlaubt noch untersagt

- Virtual Machines?
- Docker?

→ Sichere BSI-Konformität nur bei echten physikalischen Servern

Zertifizierung: Interpretation des Zertifikats

Vergleich zur Briefwahl

- Wer erhält den Brief?
- Wer öffnet den Brief?
- Wer garantiert, dass die Person die die Unterlagen ausfüllt unbeeinflusst ist?

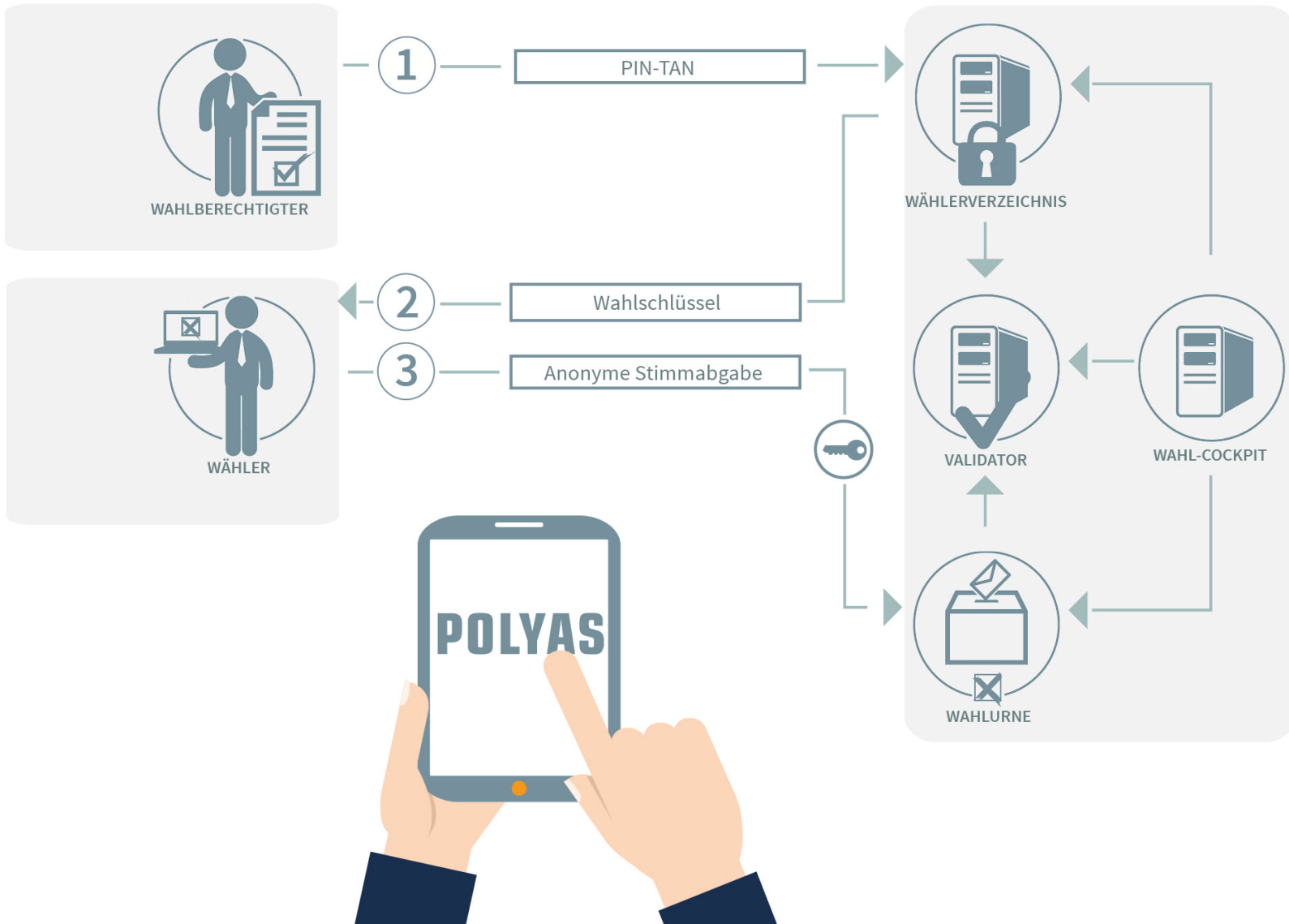
→ Online-Wahl ist nicht inhärent sicherer oder unsicherer

→ ABER: Ansprüche an Sicherheit sind von Gesetzgeberseite trotzdem höher

Inhalt

- 1 Polyas Online-Wahlen
- 2 Rahmenbedingungen, Erfahrungen, Herausforderungen
- 3 Technische Hintergründe

Technischer Ablauf der Online-Stimmabgabe



Online-Wahl: Schritt 1 – Anmeldung über ID und Passwort

The screenshot shows a web browser window with the address bar displaying 'POLYAS GmbH'. The page has two tabs: 'Stimmzettel' and 'Kandidatenwahl'. The main content area features the 'POLYAS' logo and a version identifier '2.2.3-(master)-r@403d8868360f6b31'. Below this, the title 'Wahl des Betriebsrats' is followed by the instruction 'Schritt 1 von 5: Anmelden am Wahlsystem'. A sub-instruction reads 'Bitte geben Sie Ihre ID und das Passwort ein.' The 'Anmeldung:' section contains two input fields: an 'ID:' field with the value '22749' and a 'Passwort:' field with masked characters. An orange button labeled 'Am Wahlsystem anmelden >' is positioned at the bottom right of the form.

POLYAS
2.2.3-(master)-r@403d8868360f6b31

Wahl des Betriebsrats

Schritt 1 von 5: Anmelden am Wahlsystem

Bitte geben Sie Ihre ID und das Passwort ein.

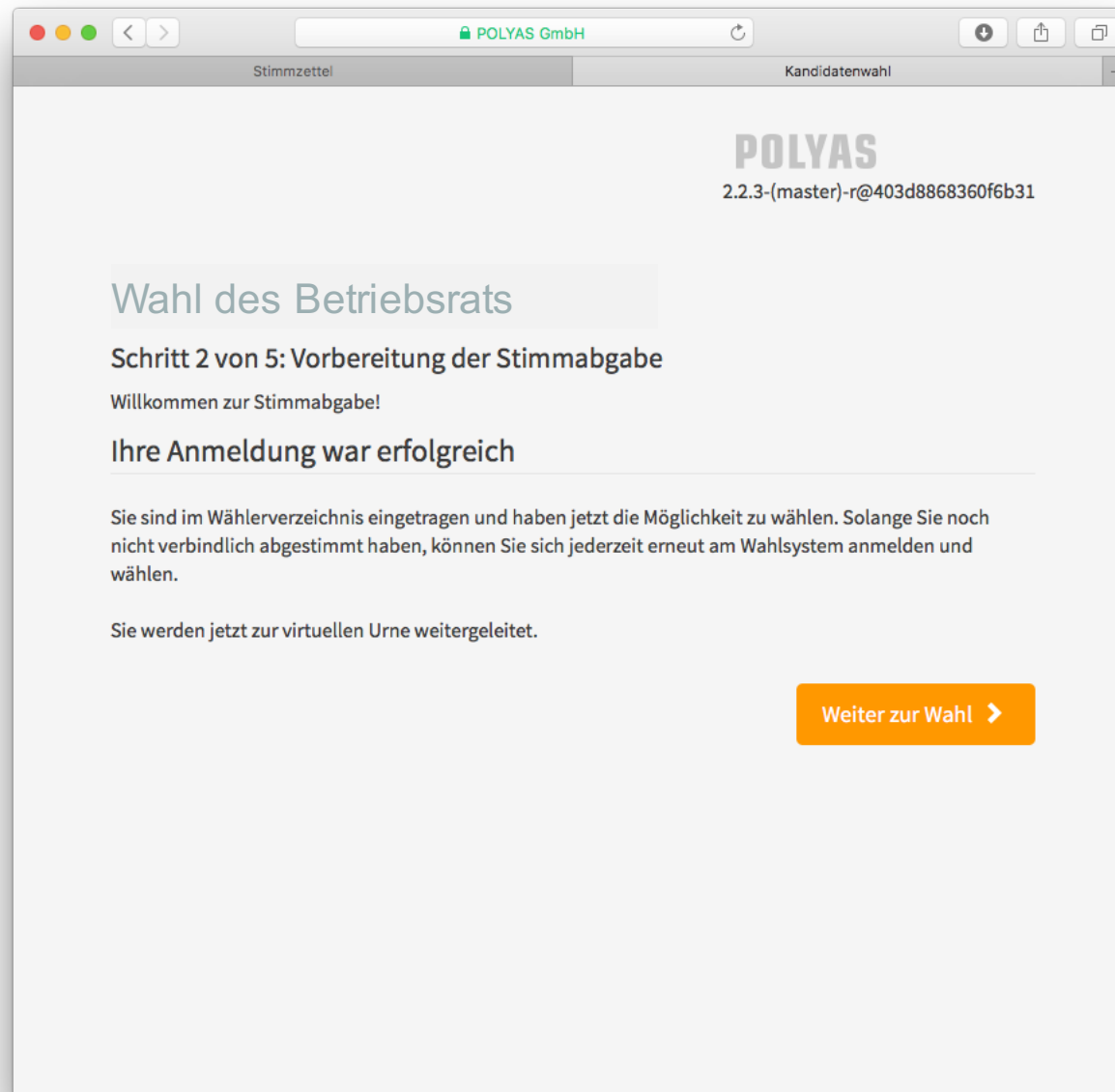
Anmeldung:

ID:
22749

Passwort:

Am Wahlsystem anmelden >

Online-Wahl: Schritt 2 – Vorbereitung Stimmabgabe



Online-Wahl: Schritt 3 – Stimmabgabe

The screenshot shows a web browser window with the address bar displaying "POLYAS GmbH". The page has two tabs: "Stimmzettel" (selected) and "Kandidatenwahl". The main content area features the POLYAS logo and a unique identifier "2.2.3-(master)-r@403d8868360f6b31". The title "Wahl des Betriebsrats" is followed by the instruction "Schritt 3 von 5: Stimme für die Wahl abgeben". A yellow box states "Sie haben jetzt die Möglichkeit zu wählen." Below this, a white box contains a table with the heading "Sie haben 1 Stimme zur Verfügung." The table lists three options: Eric Mustermann, Erika Musterfrau, and an option to vote invalid. At the bottom, there are two buttons: "Wahl unterbrechen" and "Stimmabgabe prüfen".

POLYAS
2.2.3-(master)-r@403d8868360f6b31

Wahl des Betriebsrats

Schritt 3 von 5: Stimme für die Wahl abgeben

Sie haben jetzt die Möglichkeit zu wählen.

Sie haben 1 Stimme zur Verfügung.

	Vorname	Nachname
☐	Eric	Mustermann
☐	Erika	Musterfrau
☐	Ungültig wählen	

Wahl unterbrechen

Stimmabgabe prüfen

Online-Wahl: Schritt 4 (1/2) – Stimmabgabe bestätigen

The screenshot shows a web browser window with the address bar displaying "POLYAS GmbH". The page has two tabs: "Stimmzettel" (active) and "Kandidatenwahl". The main content area displays the "POLYAS" logo and a unique identifier "2.2.3-(master)-r@403d8868360f6b31". The title "Wahl des Betriebsrats" is followed by "Schritt 4 von 5: Bestätigung der Stimmabgabe". A message states: "Ihre Stimmabgabe wird Ihnen im nächsten Schritt zur Bestätigung angezeigt. Sie können Ihre Wahl anschließend korrigieren oder Ihre Stimme wird wie folgt gezählt:". A red warning box contains the text: "Sie haben keine Stimme vergeben. Ihr Stimmzettel wird als ungültig gezählt." Below this, a box indicates "Sie haben 1 Stimme zur Verfügung." and contains a table with three rows: "Eric Mustermann", "Erika Musterfrau", and "Ungültig wählen". At the bottom, there are three buttons: "Auswahl korrigieren", "Wahl unterbrechen", and "verbindliche Stimmabgabe".

POLYAS
2.2.3-(master)-r@403d8868360f6b31

Wahl des Betriebsrats

Schritt 4 von 5: Bestätigung der Stimmabgabe

Ihre Stimmabgabe wird Ihnen im nächsten Schritt zur Bestätigung angezeigt. Sie können Ihre Wahl anschließend korrigieren oder Ihre Stimme wird wie folgt gezählt:

Sie haben keine Stimme vergeben. Ihr Stimmzettel wird als ungültig gezählt.

Sie haben 1 Stimme zur Verfügung.

	Vorname	Nachname
☐	Eric	Mustermann
☐	Erika	Musterfrau
☐	Ungültig wählen	

Auswahl korrigieren Wahl unterbrechen **verbindliche Stimmabgabe**

Online-Wahl: Schritt 4 (2/2) – Stimmabgabe bestätigen

The screenshot shows a web browser window with the address bar displaying "POLYAS GmbH". The page has two tabs: "Stimmzettel" (selected) and "Kandidatenwahl". The main content area displays the POLYAS logo and a unique identifier "2.2.3-(master)-r@403d8868360f6b31". Below this, the title "Wahl des Betriebsrats" is shown. The current step is "Schritt 4 von 5: Bestätigung der Stimmabgabe". A message states: "Ihre Stimmabgabe wird Ihnen im nächsten Schritt zur Bestätigung angezeigt. Sie können Ihre Wahl anschließend korrigieren oder Ihre Stimme wird wie folgt gezählt:". A table lists the voting options, with the first option, "Eric Mustermann", selected. At the bottom, there are three buttons: "Auswahl korrigieren", "Wahl unterbrechen", and "verbindliche Stimmabgabe".

POLYAS
2.2.3-(master)-r@403d8868360f6b31

Wahl des Betriebsrats

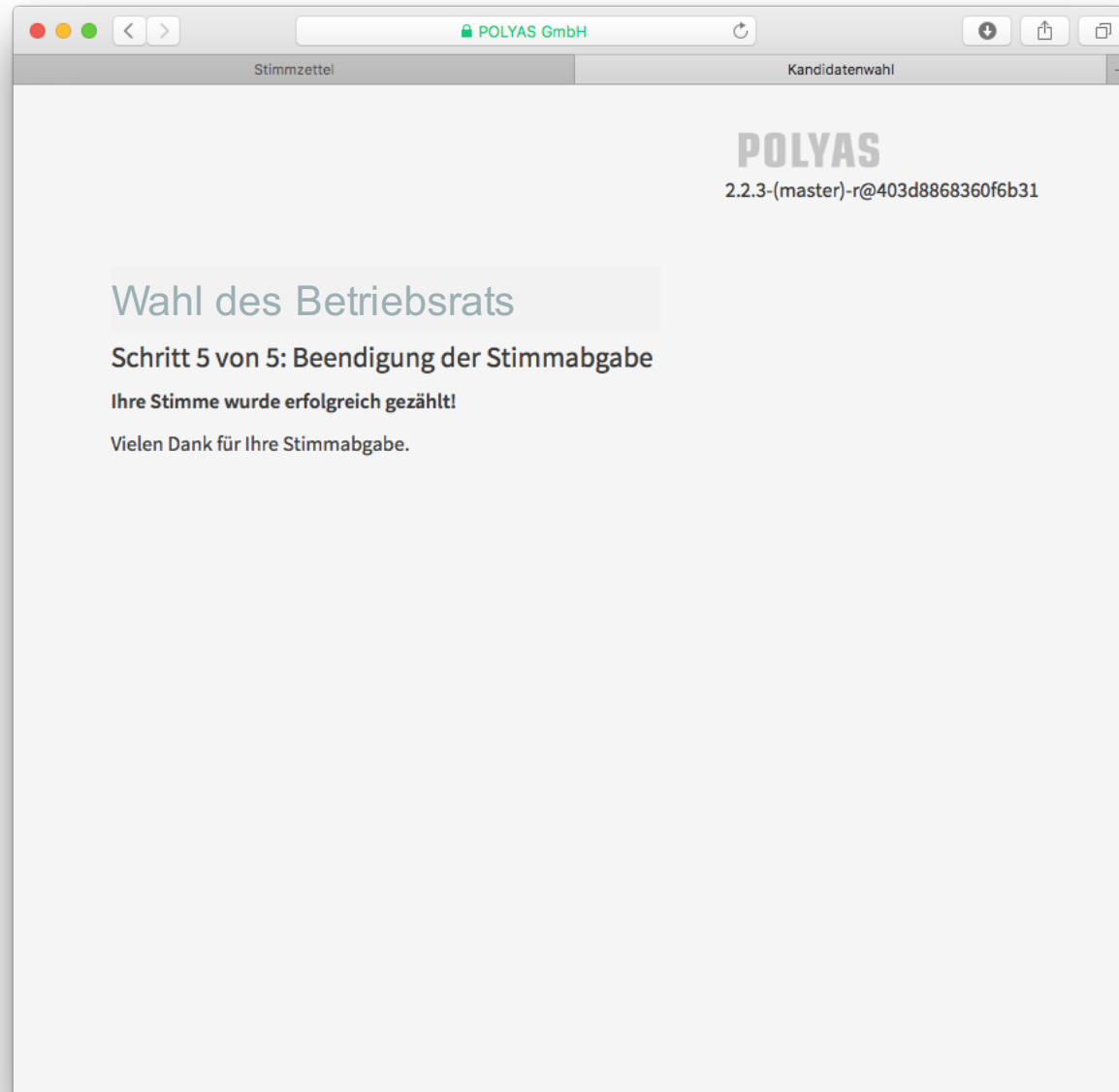
Schritt 4 von 5: Bestätigung der Stimmabgabe

Ihre Stimmabgabe wird Ihnen im nächsten Schritt zur Bestätigung angezeigt. Sie können Ihre Wahl anschließend korrigieren oder Ihre Stimme wird wie folgt gezählt:

Sie haben 1 Stimme zur Verfügung.		
	Vorname	Nachname
☒	Eric	Mustermann
☐	Erika	Musterfrau
☐	Ungültig wählen	

Auswahl korrigieren Wahl unterbrechen **verbindliche Stimmabgabe**

Online-Wahl: Schritt 5 – Stimmabgabe beendet



SaaS-Lösung: Grundvoraussetzungen

- Grundsätzlich gut funktionierende und sichere Lösung
- Einrichtungsaufwände minimieren durch Automatisierung
- Skalierbarkeit darf weder Sicherheit noch Verfügbarkeit beeinträchtigen
- Volle Transparenz muss beibehalten werden
- Weiterhin physikalische Trennung der Teilsysteme

Infrastruktur: Grundüberlegungen

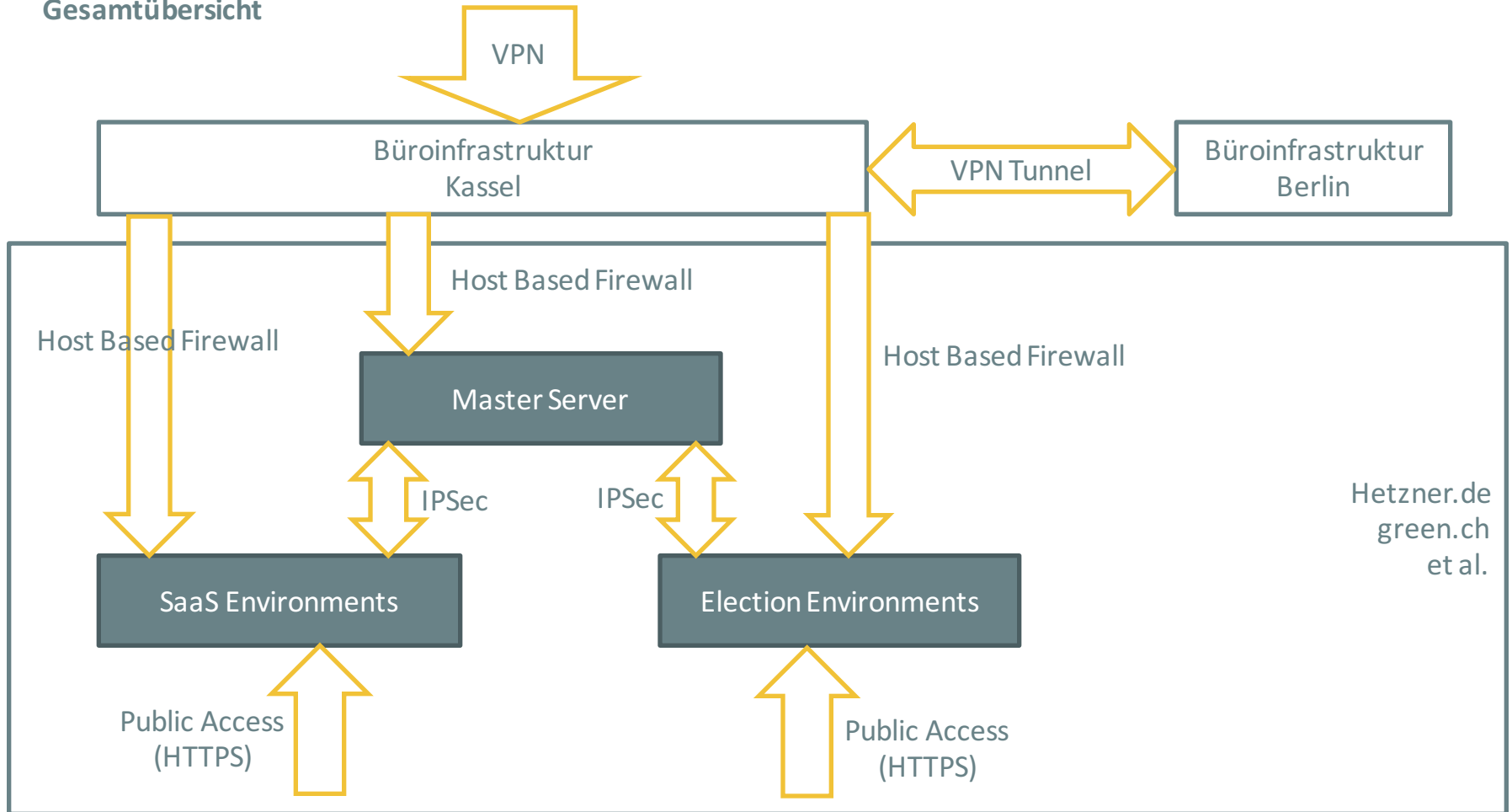
- Keine Cloud von Drittanbietern
 - Kein AWS, kein GCE
- Keine DDOS-Mitigation über Drittanbieter
 - Z.B. Cloudflare
- Für Office: Nutzung von Services in DE nach DE-Recht
 - Kein GoogleMail
 - Keine MS Office Cloud
 - Keine Dropbox

→ Nur selbst aufgesetzte Server und Services in DE-Rechenzentren (min. ISO27001)

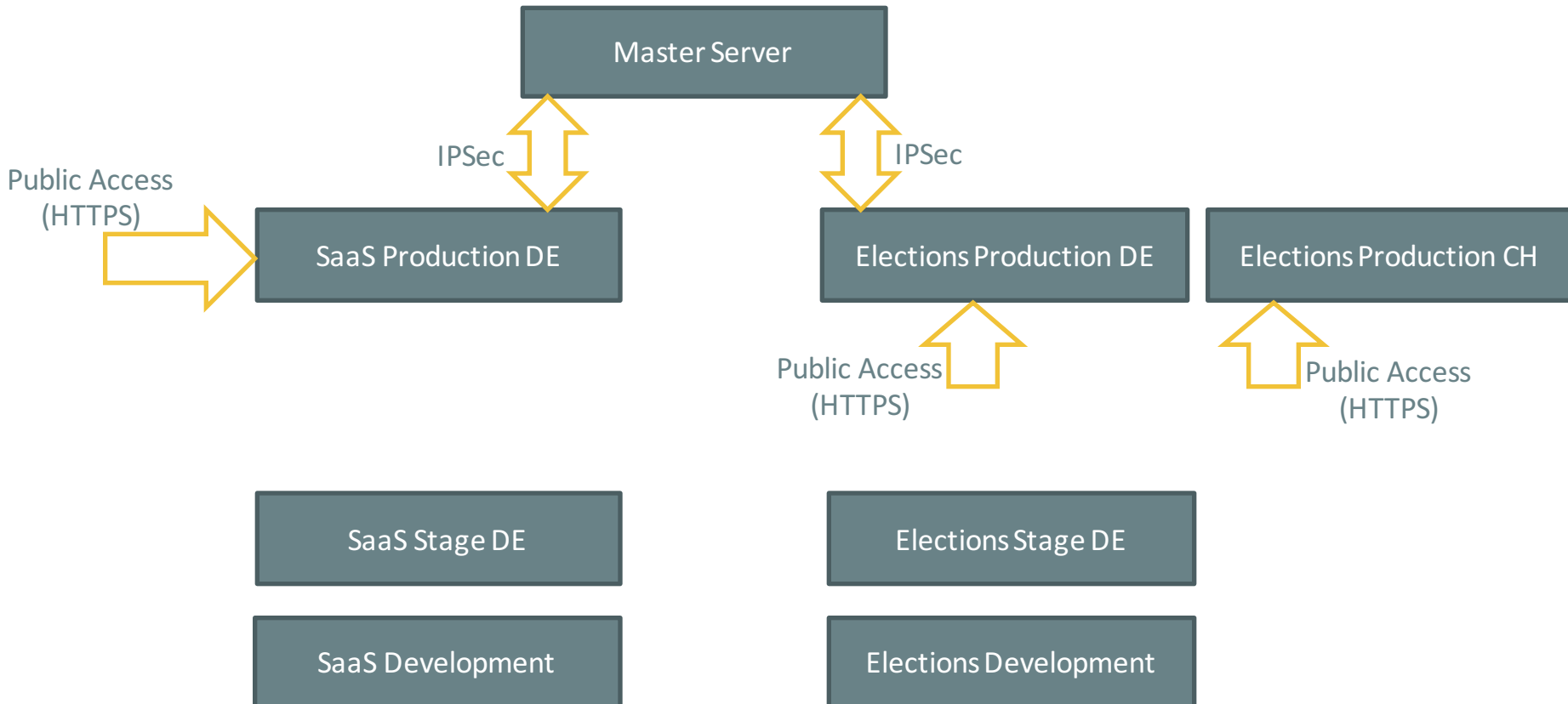
Infrastruktur: **Verwendete Technologien**

- Server: **Debian**
 - Virtualisierung: **Docker**
 - Orchestrierung: **Rancher**
- Ermöglicht die komplette Trennung verschiedener Wahlen
- Aufbau einer service-orientierten Architektur möglich
- Hohe Flexibilität
- Nachteil: Junge Technologien mit Kinderkrankheiten

Gesamtübersicht

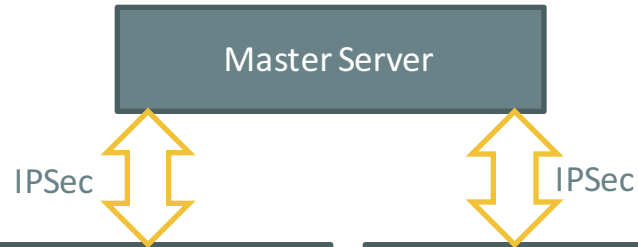


Detailansicht Environments



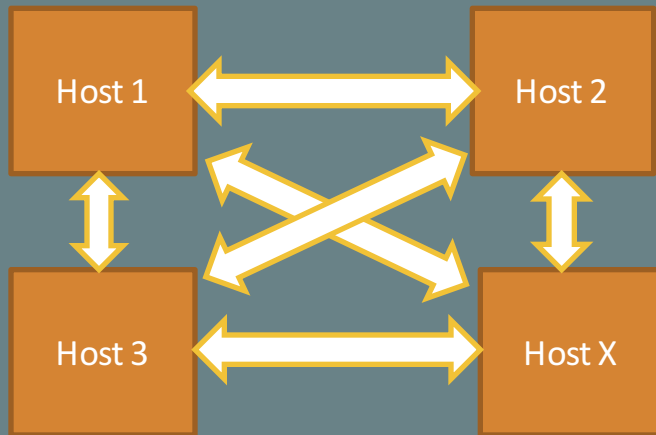
Detailansicht Production DE

Applications:
Container via Docker

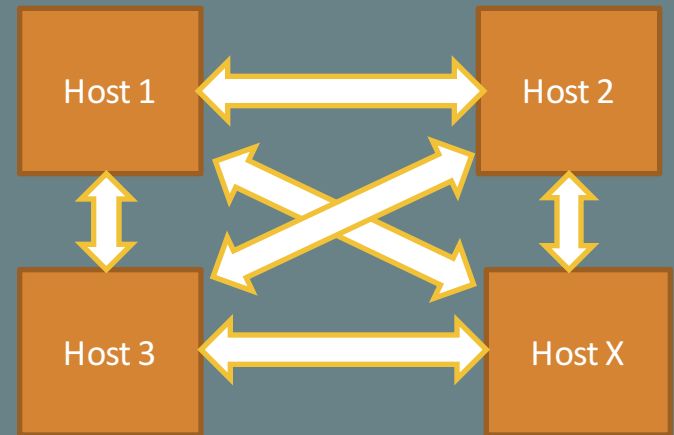


All Hosts in Environment:
IPSec & Host Based Firewalls

SaaS Production DE



Elections Production DE



SaaS-Lösung: Erreichte Milestones

- Getrennte Environments für Wahlen, Self Service, Office-Infrastruktur
- Länderspezifische Environments (aktuell: DE, CH)
- Staging-Environment 1:1 wie Produktion
- Development-Environment für Tests an Infrastruktur-Changes
- Hohe Komplexität verwaltbar durch kleines Team

Polyas NG: Individuelle und universelle Verifizierbarkeit

- Jeder Schritt einzeln nachvollziehbar
- Die Gesamtheit der durchgeführten Schritte ist nachvollziehbar

→ Zero Knowledge Proof

- Mathematisches Verfahren, um die Korrektheit einer kryptographischen Operation nachzuweisen
- Verwendete Geheimnisse/Verfahren (z.B. Verschlüsselungsschlüssel, Methodenaufbau) werden hierbei nicht preisgegeben
- Standardverfahren moderner Kryptographie, z. B. Mischen und Entschlüsseln

→ Anstreben eines neuen Zertifikats

- Klare Aussage zu Virtualisierung
- Prinzipien statt in Stein gemeißelte Details
- Flexibilität für Weiterentwicklung aufrechterhalten

Polyas NG: Kern-Charakteristika

Bulletin Boards

- Unveränderlich (Nur schreib- und lesbar)
- Öffentlich

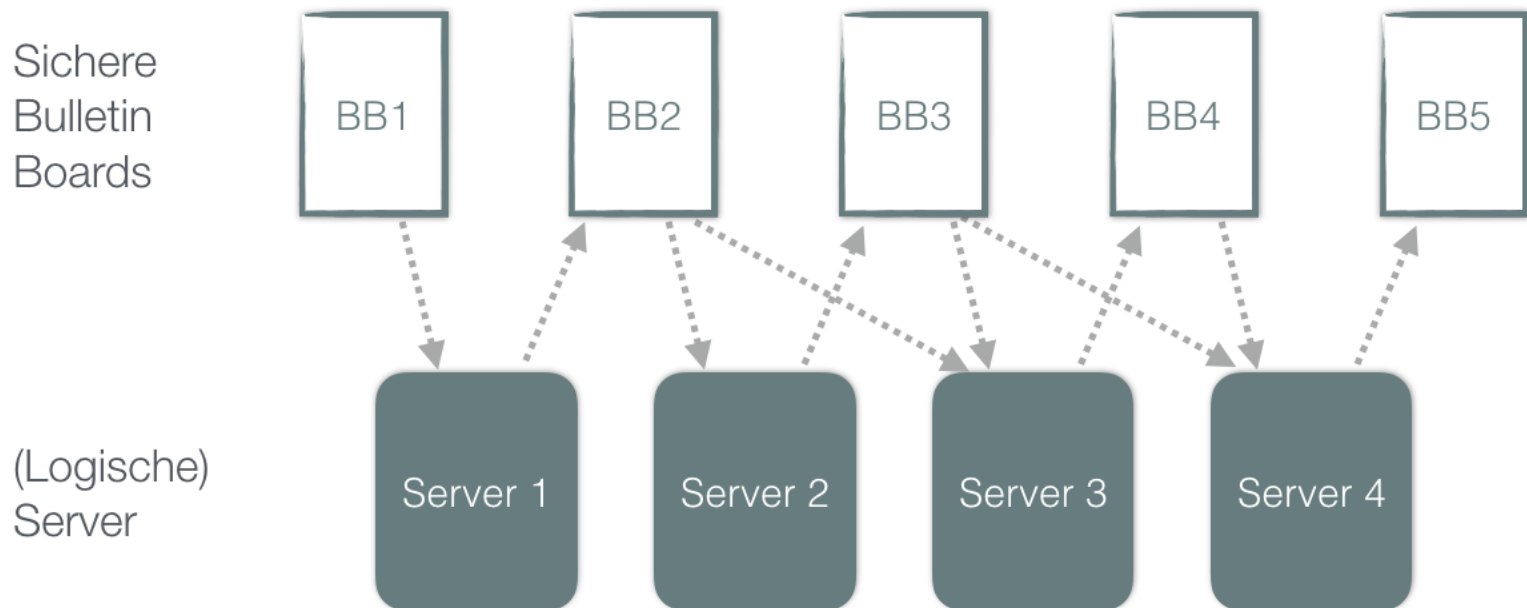
Logische Server

- Lesen aus einem oder mehreren Boards und schreiben in andere Boards
- Jeder Server führt eine vorab genau festgelegte Funktion aus
- Modular und wiederverwendbar (z.B. Verschlüsselungsalgorithmen...)

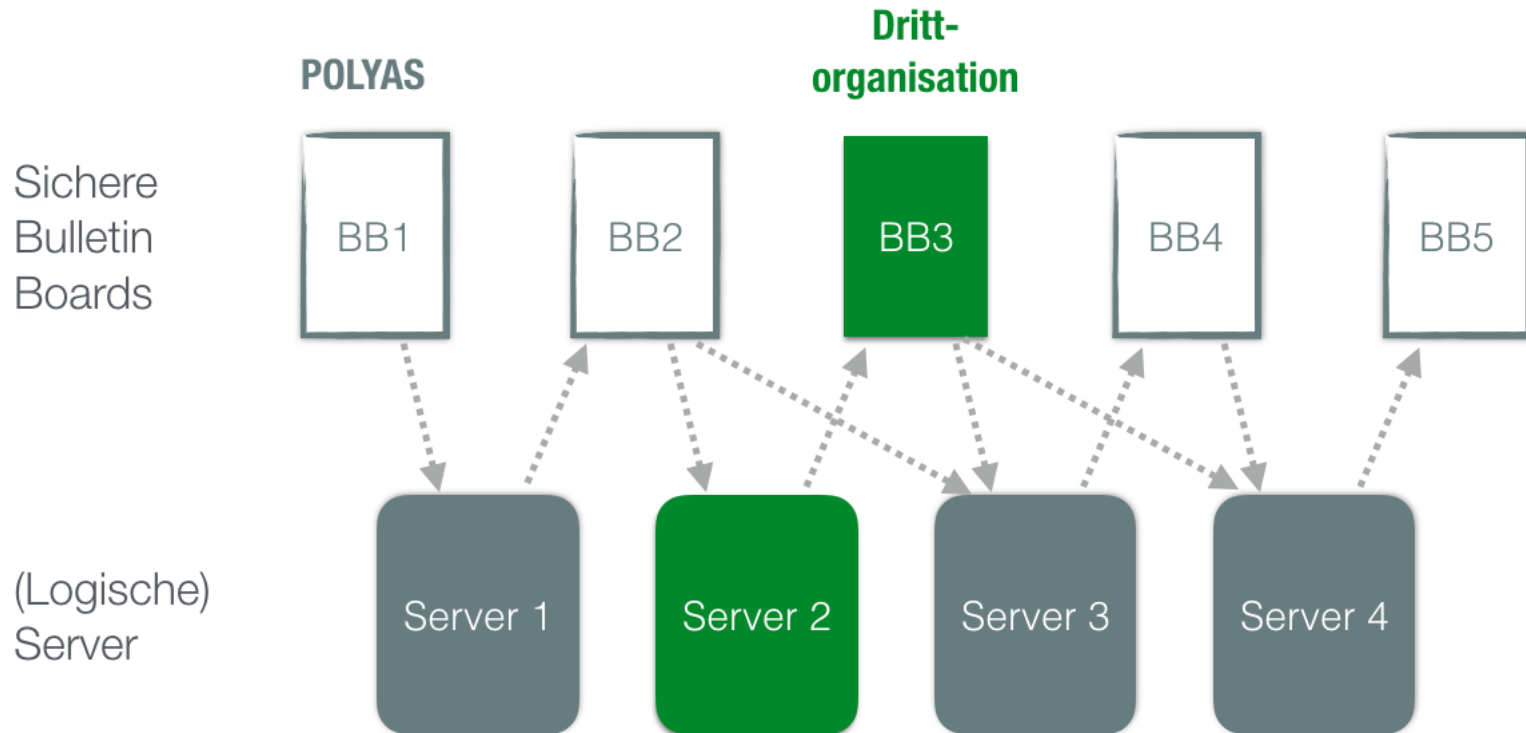
Polyas Next Generation

Polyas NG als generalisiertes Framework, das konfigurierbar unterschiedliche Anforderungen an E-Voting-Systeme abbildet

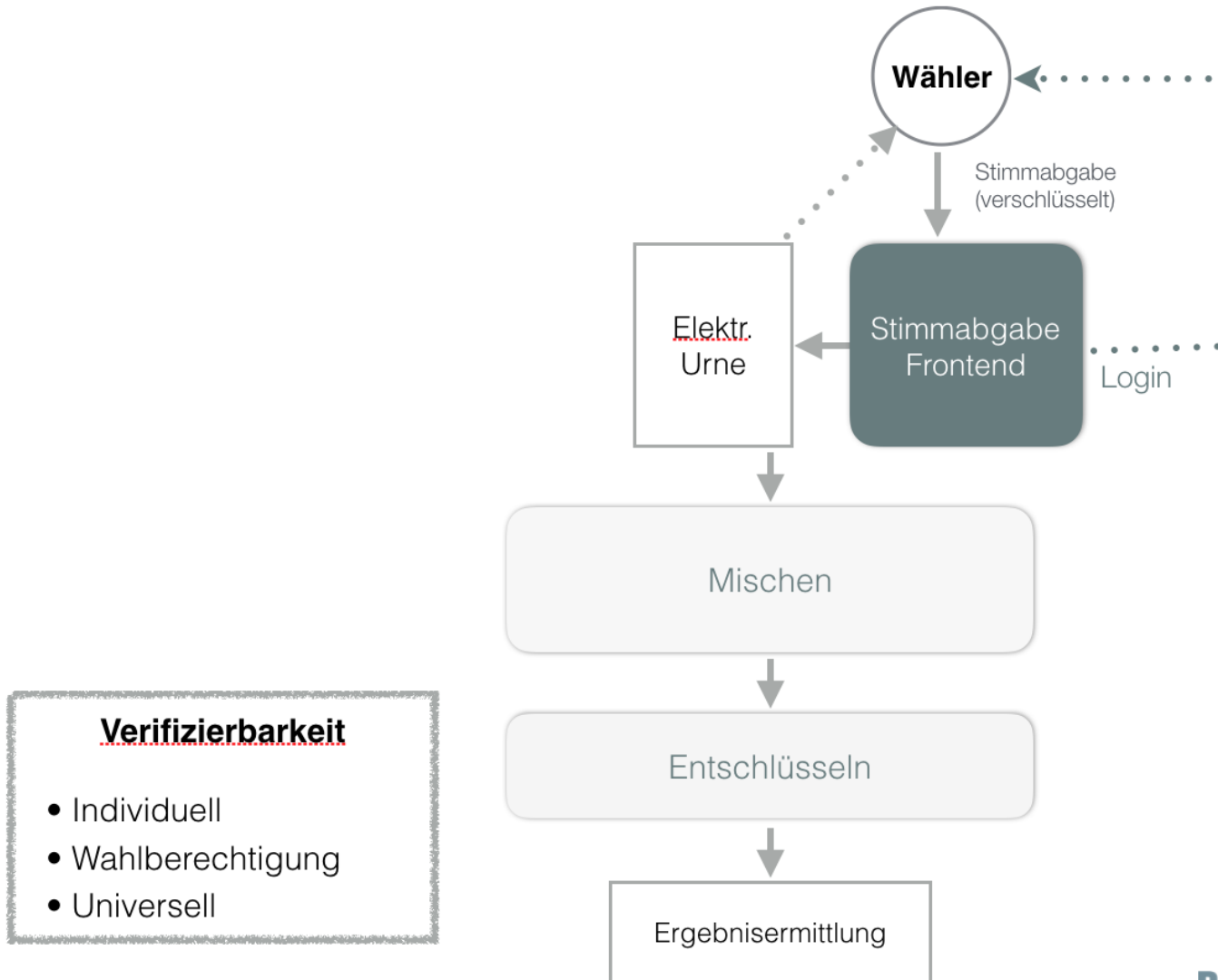
Polyas NG: Bulletin Boards



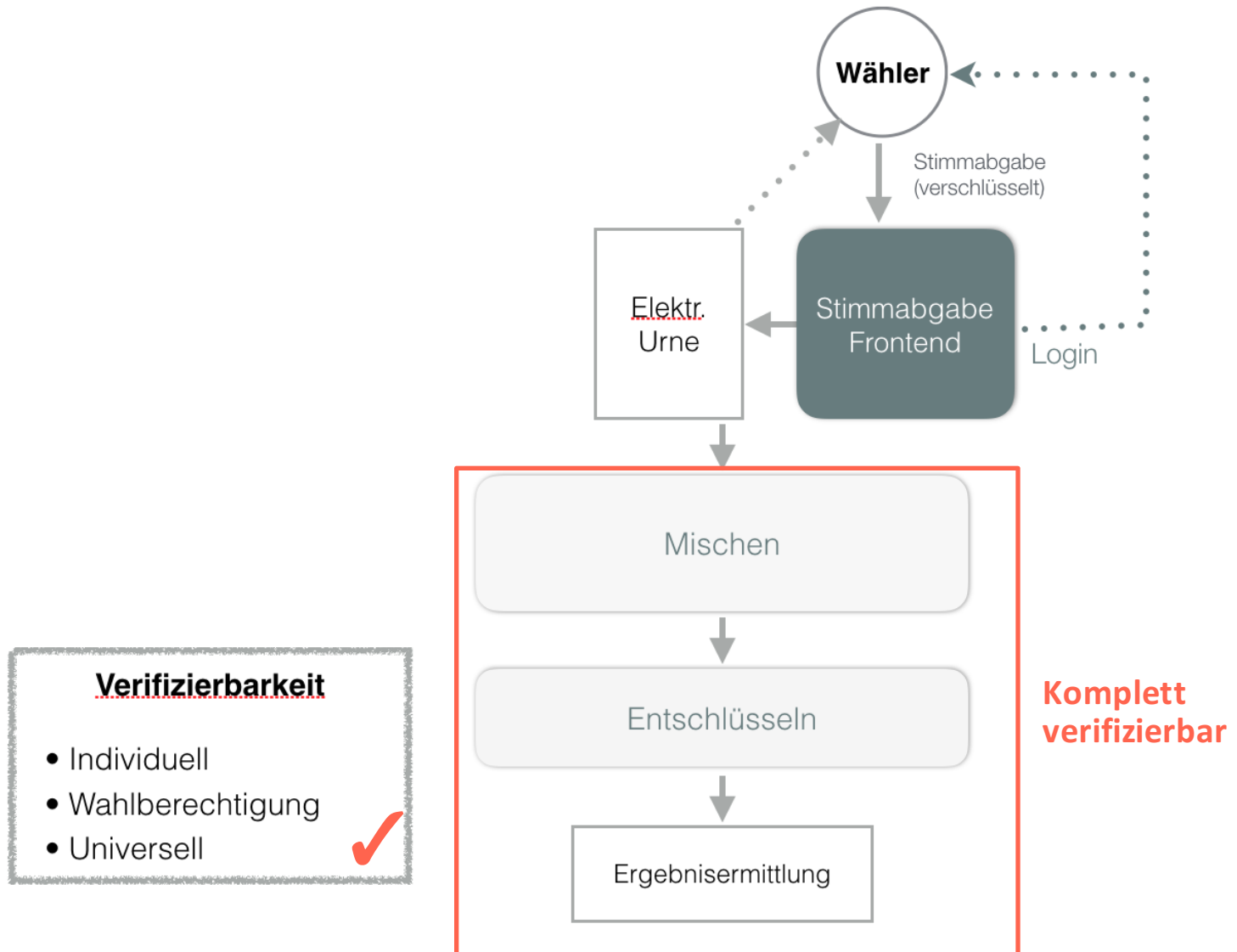
Polyas NG: Öffentliche Bulletin Boards



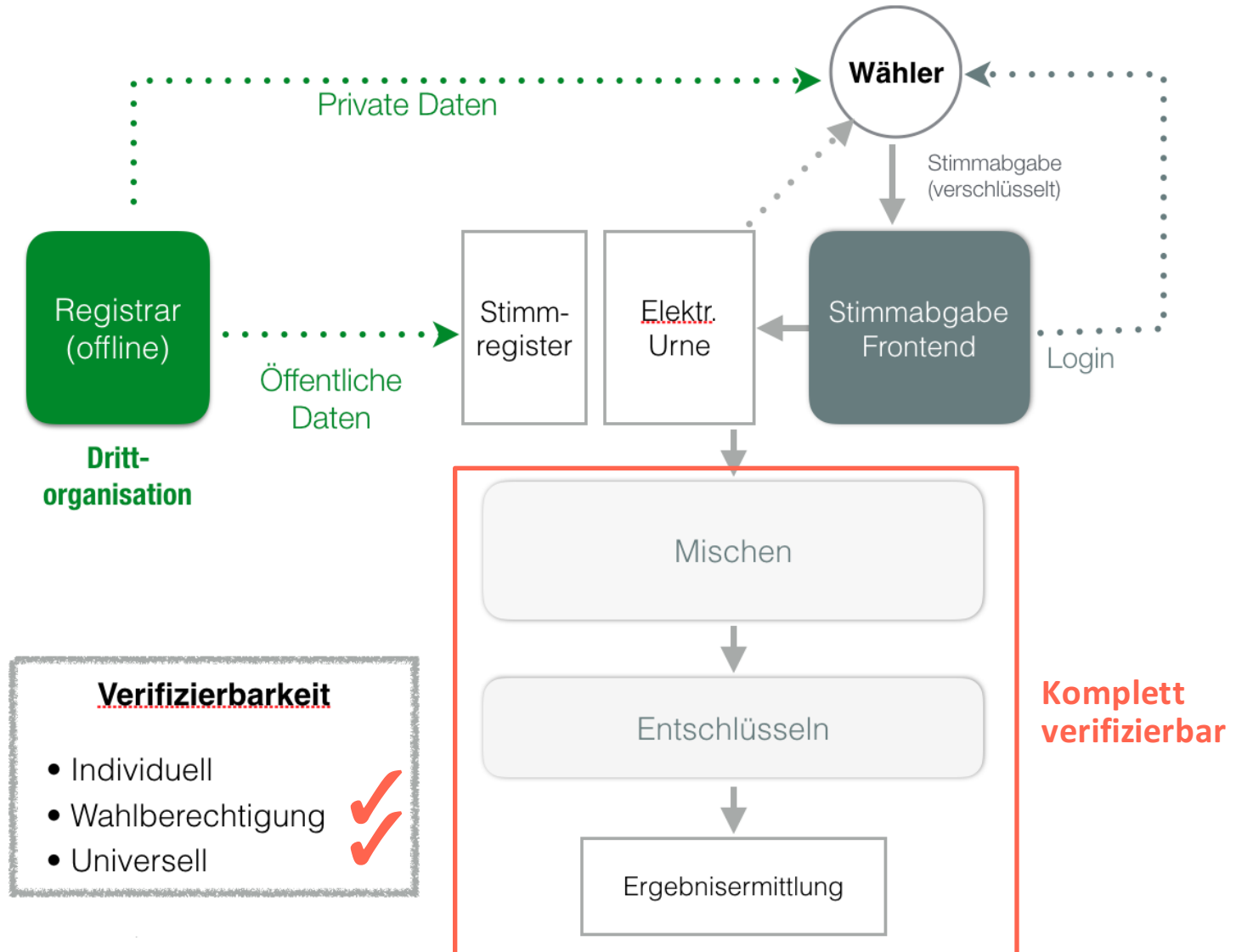
Polyas NG: Ablauf Verifizierbarkeit



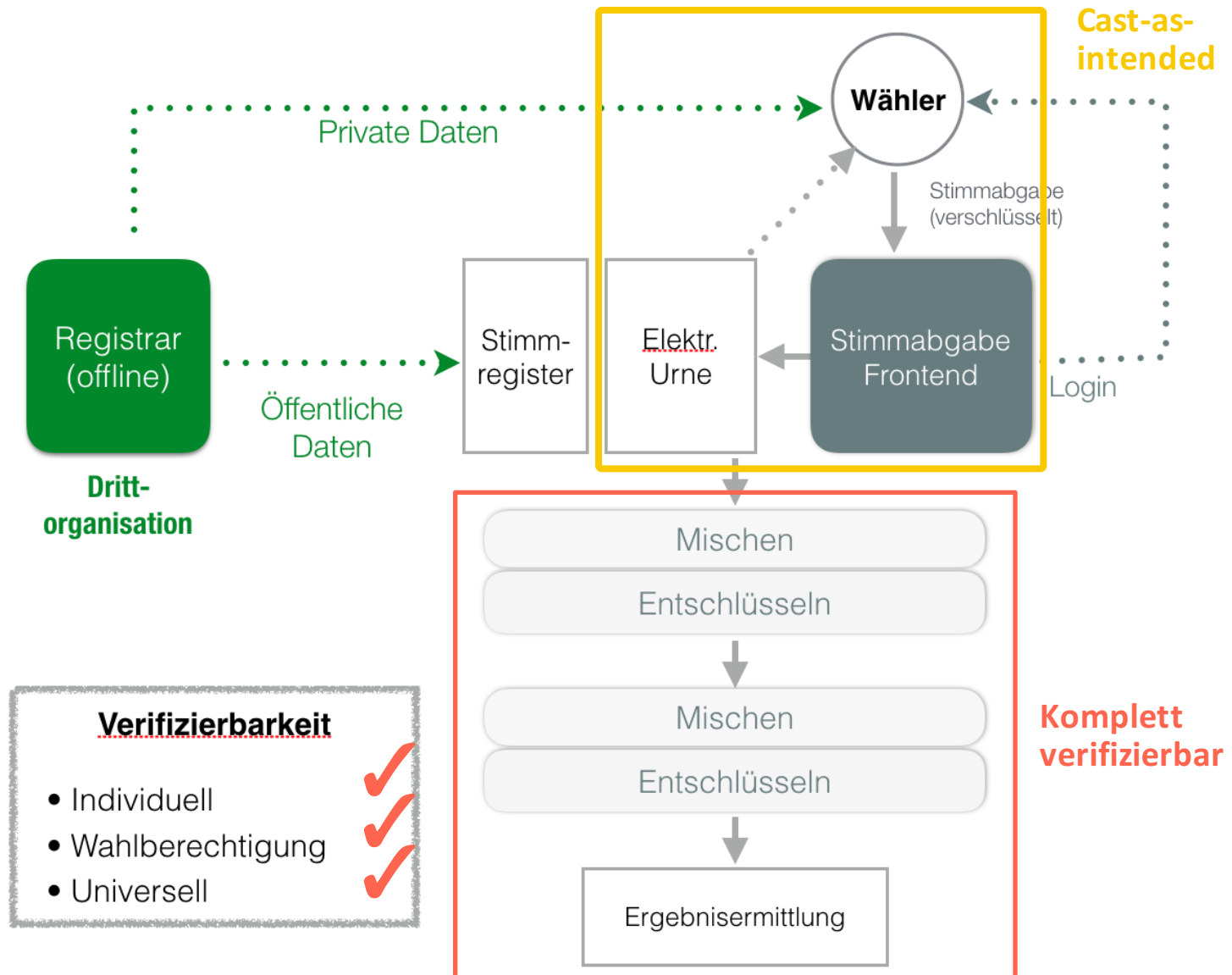
Polyas NG: Ablauf Verifizierbarkeit



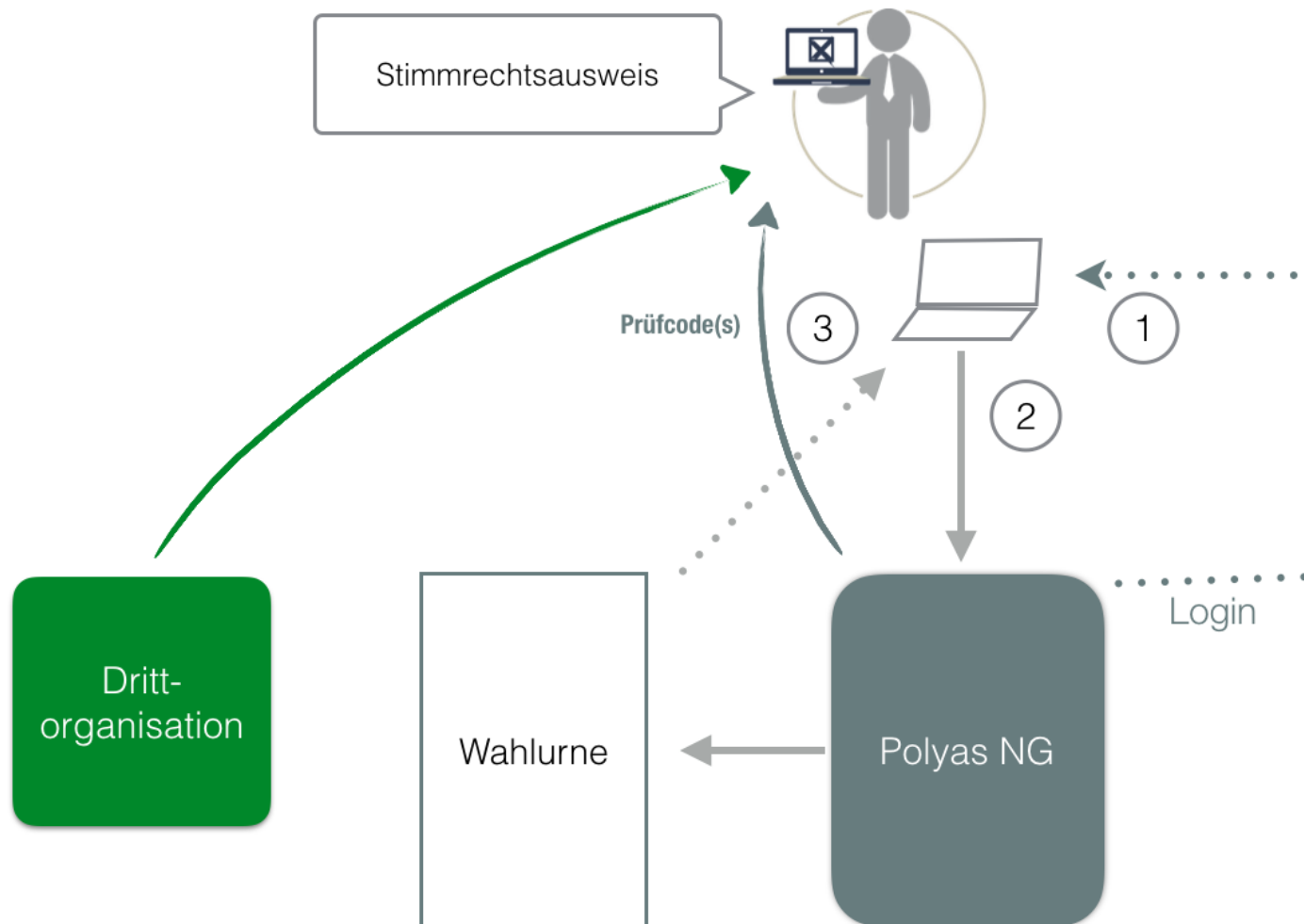
Polyas NG: Ablauf Verifizierbarkeit



Polyas NG: Ablauf Verifizierbarkeit



Technischer Ablauf der Stimmabgabe: **Konfiguration Code Voting**





POLYAS

Polyas GmbH

Alte Jakobstraße 88

10179 Berlin

www.polyas.de

Tel.: +49 30 – 880 6010 - 00