# Infrastrukturen des Vertrauens: Eine umfassende Analyse technischer, juristischer und strategischer Rahmenbedingungen für die sortitionsbasierte digitale Demokratie

## Exekutivzusammenfassung

Die Modernisierung der demokratischen Infrastruktur erfordert eine Konvergenz von kryptographischem Vertrauen, verfassungsrechtlicher Legitimation und robuster algorithmischer Governance. Dieser Bericht liefert eine erschöpfende Untersuchung der Komponenten, die notwendig sind, um ein sicheres, legitimes und resilientes System für geloste Bürgerräte (*Citizens' Assemblies*) innerhalb der Bundesrepublik Deutschland zu operationalisieren. Die Analyse adressiert die spezifische Anforderung, eine Brücke zwischen der etablierten repräsentativen Demokratie und innovativen deliberativen Modellen zu schlagen, wobei ein besonderer Fokus auf der technischen Integrität und der juristischen Machbarkeit liegt.
Die Untersuchung gliedert sich in fünf kritische Domänen:

1. **Kryptographische Verifikation für Bürger:** Eine detaillierte technische Pädagogik, die Laienmitglieder von Bürgerräten befähigt, die X-Road Security Server-Logs zu auditieren und die Zufälligkeit ihrer eigenen Auswahl via *drand*-Beacon zu verifizieren. Hierbei wird strikt zwischen Rohdaten (ASiC-Container) und interpretierten Berichten unterschieden.
2. **Algorithmische Risikoanalyse:** Ein Sicherheitsaudit der Deliberationsplattform Pol.is unter dem Aspekt des Social Engineering, der Cluster-Manipulation durch Sybil-Angriffe und der Framing-Effekte in der PCA-basierten Konsensfindung.
3. **Verfassungsrechtliche Legitimation:** Ein juristisches Gutachten zur Vereinbarkeit geloster Gremien mit Art. 20 Abs. 2 GG, unter besonderer Berücksichtigung der ununterbrochenen Legitimationskette und der Rolle von Experimentierklauseln in den Gemeindeordnungen.
4. **Grenzüberschreitende Interoperabilität:** Ein technisches Blaupausen-Konzept zur Anbindung des estnischen X-Road-Datenaustauschmodells an deutsche Melderegister unter Nutzung der eIDAS-Verordnung und SAML/OIDC-Protokolle.
5. **Strategische Spieltheorie:** Eine formale Simulation der Interaktion zwischen gewähltem Stadtrat und gelostem Bürgerrat unter Bedingungen der Haushaltsnot (Fiskalkrise), mit einer Analyse von *Blame-Shifting*-Gleichgewichten und Selbstbindungsmechanismen.

# Teil I: Technische Souveränität für den Bürger-Auditor

## 1.1 Der X-Road Security Server: Ein Verifikations-Tutorial für Laien

Die fundamentale Prämisse digitaler Verwaltungstransparenz ist, dass der Bürger dem Wort des

Staates nicht blind vertrauen muss, sondern befähigt wird, die Daten des Staates zu verifizieren. Im Kontext eines Bürgerrats können Mitglieder Zugang zu Rohdatenprotokollen verlangen, um sicherzustellen, dass die ihnen präsentierten Informationen nicht manipuliert wurden. Die X-Road-Architektur, das Rückgrat der estnischen digitalen Gesellschaft und zunehmend Standard für den paneuropäischen Datenaustausch, bietet hierfür einen Mechanismus über das **Security Server Message Log**.
Dieses Tutorial ist für den *Bürger-Auditor* konzipiert – einen Laien ohne kryptographische Vorbildung, der die Integrität von Datenaustauschen prüfen muss.

### 1.1.1 Konzeptioneller Rahmen: Der digitale Umschlag (ASiC)

Bevor der Bürger mit der Software interagiert, muss er die Unterscheidung zwischen **Rohdaten** und **Berichten** verinnerlichen. Ein Bericht (PDF/Excel) ist eine menschenlesbare Zusammenfassung, analog zu einer Fotokopie, und anfällig für redaktionelle Manipulation. Die Rohdaten hingegen sind der "versiegelte Umschlag". Im X-Road-Ökosystem wird jede Nachricht, die zwischen Behörden gesendet wird, in einen digitalen Container verpackt, den sogenannten **Associated Signature Container (ASiC)**.
Dieser Container beinhaltet drei essentielle Komponenten:

1. **Der Nachrichteninhalt (Message Content):** Die eigentlichen Daten (z.B. eine XML-Datei mit Haushaltszahlen oder Meldedaten).
2. **Die digitale Signatur (Digital Signature):** Der kryptographische Beweis der Herkunft, erstellt durch das Signaturzertifikat des Security Servers der sendenden Behörde.
3. **Der Zeitstempel (Timestamp):** Ein von einer vertrauenswürdigen Time-Stamping Authority (TSA) ausgestelltes Zertifikat, das die Existenz der Daten zu einem exakten Zeitpunkt beweist.

**Zielsetzung:** Das Ziel des Bürger-Auditors ist es nicht, den XML-Code zu parsen, sondern zu verifizieren, dass das *Siegel* (Signatur) ungebrochen und der *Poststempel* (Zeitstempel) valide ist.

### 1.1.2 Schritt-für-Schritt-Verifikationsanleitung

**Phase 1: Akquise des Beweismittels** Der Administrator des Security Servers darf dem Bürgerrat keine Textdatei übergeben; er muss den **ASiC-Container** aushändigen.

1. **Anforderung:** Bitten Sie das technische Sekretariat um den "Signierten Dokumentencontainer" (Dateiendung .asice oder .bdoc), der zu der Transaktions-ID (QueryID) gehört, die im Sitzungsprotokoll referenziert wird.
2. **Metadaten-Check:** Stellen Sie sicher, dass der Dateiname oder die internen Metadaten der queryId entsprechen.

**Phase 2: Das Verifikationswerkzeug (DigiDoc4)** Während technische Administratoren Kommandozeilen-Tools wie asicverifier nutzen, sollte der Laie den **RIA DigiDoc4 Client** verwenden. Dies ist eine benutzerfreundliche GUI-Anwendung, die von der estnischen Informationssystembehörde entwickelt wurde, aber vollständig kompatibel mit den europäischen eIDAS-Standards ist und ASiC-E-Container verarbeiten kann.
*Schritt 1: Installation*

- Laden Sie den DigiDoc4 Client aus dem offiziellen Repository (z.B. id.ee oder App Stores) herunter.
- Installieren Sie die Software. **Wichtig:** Zur bloßen *Verifikation* eines Containers benötigen Sie keinen eigenen Kartenleser oder eine eigene eID-Karte. Die Verifikationsfunktion ist

offen zugänglich.

*Schritt 2: Laden des Containers*

- Starten Sie DigiDoc4.
- Ziehen Sie die .asice-Datei per Drag-and-Drop in das Hauptfenster.
- **Visuelles Feedback:** Die Oberfläche analysiert sofort die kryptographische Struktur. Sie sehen eine Liste der enthaltenen Dateien (z.B. message.xml) und eine Seitenleiste, die den Status der "Unterschriften" anzeigt.

*Schritt 3: Interpretation der Indikatoren* Dies ist die kritische Analyse der "Rohdaten".

- **Grüner Haken ("Signature Valid" / "Allkirjad kehtivad"):** Dies ist der Goldstandard. Er bedeutet:
  - **Integrität:** Die Daten in message.xml wurden seit dem Versand um kein einziges Bit verändert.
  - **Identität:** Das Zertifikat, mit dem unterschrieben wurde, gehört zweifelsfrei der angegebenen Behörde (z.B. "Stadtverwaltung Köln via Governikus").
  - **Zeit:** Der Zeitstempel ist kryptographisch korrekt mit den Daten verkettet und von einer gelisteten TSA validiert.
- **Rote Warnung ("Signature Unknown" / "Invalid"):** Der Container ist verdächtig. Dies kann auf eine fehlende Trust Service List (TSL) Konfiguration hinweisen oder auf eine tatsächliche Manipulation der Daten. In diesem Fall darf der Inhalt nicht als Entscheidungsgrundlage akzeptiert werden.

**Phase 4: Erweiterte Verifikation (Der Hash-Abgleich)** Für den skeptischen Auditor, der hinterfragt, ob der gedruckte "Bericht" tatsächlich aus den "Rohdaten" stammt:

1. Öffnen Sie die Datei innerhalb des Containers (z.B. message.xml) über DigiDoc4 oder extrahieren Sie sie.
2. Generieren Sie den **SHA-256 Hash** dieser Datei (DigiDoc4 zeigt diesen oft in den Dateieigenschaften an, oder nutzen Sie ein Online-Tool).
3. Vergleichen Sie diesen Hash-Wert (eine Zeichenfolge wie 8f4b...) mit dem Hash, der im offiziellen PDF-Bericht des Bürgerrats abgedruckt ist.
4. Stimmen die Hashes überein, ist mathematisch bewiesen, dass der Bericht eine exakte Repräsentation der Rohdaten ist.

### 1.1.3 Die Architektur der Zeitstempel (Timestamping)

Für das Verständnis ist entscheidend, dass X-Road ein **Batch-Timestamping** verwendet, um Skalierbarkeit zu gewährleisten. Der Security Server sammelt Signaturen und sendet diese periodisch gebündelt an die TSA.

- **Implikation für Bürger:** Wenn ein ASiC-Container unmittelbar nach einer Transaktion heruntergeladen wird, fehlt möglicherweise noch der finale Zeitstempel der TSA. Der Auditor sollte daher stets einen "archivierten" Container anfordern, bei dem die Zeitstempelkette (Hash Chain) abgeschlossen ist.

## 1.2 Verifizierung des Orakels: Eine Anleitung für drand

In einer auf dem Losverfahren basierenden Demokratie ruht die Legitimität des Gremiums vollständig auf der Fairness des Auswahlprozesses. Wenn die Zufallsziehung vorhersagbar oder manipulierbar ist, ist der Bürgerrat "gekapert". Das **drand-Protokoll** der *League of Entropy* bietet hierfür "publicly verifiable randomness" (öffentlich verifizierbare Zufälligkeit).

### 1.2.1 Das Konzept: Warum dem Beacon vertrauen?

Traditionelle Zufallsgeneratoren (wie Würfel eines Beamten oder die random()-Funktion eines Computers) erfordern Vertrauen in den Bediener. *drand* (Distributed Randomness Beacon) wird von einem Konsortium unabhängiger Organisationen (Cloudflare, EPFL, University of Chile, etc.) generiert. Keine einzelne Entität besitzt den "Schlüssel" zur Zufälligkeit. Jede Organisation hält nur Fragmente (Shards), die über *Threshold Cryptography* (Schwellwertkryptographie) kombiniert werden müssen, um den Zufallswert zu erzeugen. Ein Angreifer müsste mehr als die Hälfte dieser global verteilten Institutionen gleichzeitig kompromittieren, um den Wert zu manipulieren.

### 1.2.2 Das Verifikationsprotokoll für Bürger

Ziel ist der Nachweis, dass die "Zufallszahl" zur Auswahl der Bürger nicht vom Stadtrat gewählt wurde, sondern zu einem fixierten Zeitpunkt vom Universum (via drand-Netzwerk) generiert wurde.

**Schritt 1: Identifikation der Auswahl-Runde (Pre-Commitment)** Die Auswahllogik des Bürgerrats muss sich *im Vorfeld* auf eine zukünftige **Rundennummer** festlegen.

- *Beispiel:* "Wir nutzen den Zufallswert, der vom drand 'Mainnet' Beacon in Runde #100.000 generiert wird. Diese Runde findet am 15. Januar um 12:00:00 UTC statt."
- **Bürger-Check:** Prüfen Sie, ob diese Festlegung (das "Pre-Commitment") öffentlich publiziert wurde, *bevor* der Zeitpunkt der Generierung erreicht war.

**Schritt 2: Zugriff auf den Explorer** Der Bürger-Auditor muss keinen eigenen Node betreiben. Er nutzt einen visuellen Block-Explorer.

- **URL:** Navigieren Sie zu drand.love oder einem Drittanbieter-Explorer wie beaconcha.in (falls integriert).
- **Suche:** Geben Sie die Rundennummer (z.B. 100000) in das Suchfeld ein.

**Schritt 3: Visuelle Verifikation des "Puls"** Der Explorer zeigt folgende Daten an:

- **Round:** 100000
- **Randomness (Output):** Eine lange hexadezimale Zeichenkette (z.B. 8d7f3...). Dies ist der Seed für den Auswahlalgorithmus.
- **Signature:** Der kryptographische Beweis (BLS-Signatur).
- **Time:** Die sekundengenaue Zeit der Generierung.

**Schritt 4: Die Beweiskette (Chain of Custody)** Verifizieren Sie die Verbindung zur Vergangenheit. Die Zufälligkeit von Runde 100.000 ist im "Chained Mode" kryptographisch von der Signatur der Runde 99.999 abgeleitet.

- **Aktion:** Klicken Sie auf "Previous Round".
- **Konzept:** Dies erzeugt eine unbrechbare Kette ("Hash Chain"). Um Runde 100.000 zu fälschen, müsste man die gesamte Historie des Beacons bis zum "Genesis Block" neu berechnen, was rechnerisch unmöglich ist.

**Schritt 5: Unabhängige Berechnung (Optional für Fortgeschrittene)** Für den "Super-Auditor", der der Webseite nicht traut:

1. Laden Sie das drand CLI-Tool herunter.
2. Führen Sie den Befehl aus: drand get public --round 100000.
3. Vergleichen Sie den ausgegebenen String mit dem auf der Webseite. Stimmen sie überein, zeigt die Webseite die Wahrheit an.

# Teil II: Algorithmische Demokratie und Risikoanalyse

## 2.1 Pol.is: Risikoanalyse zu Social Engineering

Pol.is nutzt maschinelles Lernen (spezifisch Principal Component Analysis, PCA), um Teilnehmer basierend auf ihren Abstimmungen (Zustimmen/Ablehnen/Passen) zu clustern. Im Gegensatz zu Foren erlaubt es keine direkten Antworten ("No Replies Hierarchy"), um "Flame Wars" zu verhindern und stattdessen eine "visuelle Karte" des Konsenses zu erstellen. Dennoch ist das System nicht immun gegen Manipulation.

### 2.1.1 Angriffsvektor 1: Die Sybil-Attacke und Cluster-Verzerrung

Das primäre Risiko in Pol.is ist nicht das Hacken des Servers, sondern das **Social Engineering der Meinungsmatrix**.

- **Mechanismus:** Ein Angreifer erstellt zahlreiche gefälschte Identitäten (Sybils).
- **Auswirkung auf PCA:** Pol.is clustert Nutzer basierend auf der Ähnlichkeit ihrer Votings. Wenn 1.000 Sybils identisch abstimmen (z.B. "Zustimmen" zu einer radikalen These), identifiziert der PCA-Algorithmus eine massive, kohärente "Gruppe". Dies verzerrt die Visualisierung und lässt eine Randmeinung als Hauptströmung erscheinen.
- **Algorithmische Schwäche:** PCA ist empfindlich gegenüber Ausreißern und Dichte. Eine künstlich hohe Dichte an identischen Vektoren zieht die Hauptkomponenten (Achsen der Karte) in Richtung der manipulierten Meinung.

### 2.1.2 Angriffsvektor 2: Der "Seed" Framing-Effekt (Agenda Setting)

- **Mechanismus:** Die ersten Kommentare definieren die Dimensionen des Diskurses. Wenn eine koordinierte Gruppe das System in der ersten Stunde mit Aussagen zu einem Nischenthema flutet (z.B. "Die Finanzkrise liegt nur an den Radwegen"), bilden sich die ersten Cluster entlang dieser Achse.
- **Psychologischer Effekt:** Spätere Teilnehmer agieren innerhalb dieses etablierten semantischen Rahmens. Dies ist eine Form des algorithmisch verstärkten Agenda Settings. Die PCA "lernt", dass dies das wichtigste Unterscheidungsmerkmal der Gruppe ist.

### 2.1.3 Angriffsvektor 3: Koordiniertes "Brigading" gegen den Konsens

- **Mechanismus:** Pol.is hebt "Konsens-Statements" hervor (hohe Zustimmung über alle Cluster hinweg). Eine Angreifergruppe kann strategisch "Zustimmen" bei banalen Aussagen votieren, um als "normale Bürger" zu erscheinen, aber gleichzeitig gezielt "Passen" oder "Ablehnen" bei gegnerischen konstruktiven Vorschlägen, um deren Sichtbarkeit zu reduzieren.
- **Resultat:** Der vom System gemeldete "Common Ground" wird zugunsten des Narrativs der Angreifer verschoben.

### 2.1.4 Designphilosophie und informelle Hierarchien

Pol.is entfernt explizit den "Antworten"-Button, um die "informellen Hierarchien" traditioneller Foren zu demontieren, in denen Macht denjenigen zuwächst, die am lautesten schreien oder die meiste Zeit haben.

- **Theoretische Basis:** Durch die Behandlung jedes Votums als Datenpunkt in einer Matrix versucht Pol.is, "stille" Teilnehmer gleichwertig zu behandeln.
- **Neue Verwundbarkeit:** Die Hierarchie verschiebt sich von *rhetorischem Geschick* zu *Koordinationsfähigkeit*. Der Nutzer, der 50 Leute organisieren kann, um in einem spezifischen Muster abzustimmen, wird zum neuen "Power User", der für den Laien unsichtbar bleibt, aber die Mathematik dominiert.

### 2.1.5 Mitigierungsstrategien für Bürgerräte

1. **Striktes Gatekeeping:** Integration von Pol.is in die X-Road/eID-Infrastruktur (siehe Teil IV), um das Prinzip "Eine Person, eine Stimme" durchzusetzen und Sybils technisch zu unterbinden.
2. **Moderation von Seed-Kommentaren:** Die Einstellung "Strict Moderation" muss auf die initiale Phase angewendet werden, um sicherzustellen, dass die Dimensionen (Achsen) des Diskurses divers und repräsentativ gesetzt werden, bevor die breite Masse beitritt.
3. **Cluster-Dichte-Analyse:** Datenwissenschaftler müssen die *Dichte* der Cluster auditieren. Ein hyper-dichtes Cluster (wo 100% der Mitglieder zu 100% identisch abstimmen) ist ein Signaturmerkmal eines Botnetzes oder einer strikten Instruktionsliste ("Brigading"), kein organisches menschliches Verhalten.

# Teil III: Juristisches Gutachten (Rechtsgutachten)

## Betreff: Verfassungsrechtliche Legitimation geloster Bürgerräte nach Art. 20 Abs. 2 GG

**An:** Verfassungsausschuss **Datum:** 14. Januar 2026

## 3.1 Der verfassungsrechtliche Kern: Die Legitimationskette

Artikel 20 Absatz 2 des Grundgesetzes (GG) statuiert: *"Alle Staatsgewalt geht vom Volke aus. Sie wird vom Volke in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt"*.
Das Bundesverfassungsgericht (BVerfG) leitet hieraus das Erfordernis einer **ununterbrochenen Legitimationskette** ab. Jedes staatliche Handeln muss auf den Willen des Volkes zurückführbar sein, der sich primär in **Wahlen** manifestiert. Diese Kette verläuft vom Wähler zum Parlament, vom Parlament zur Regierung und von dort in die Verwaltung.

## 3.2 Das Problem des Losverfahrens (Sortition)

Geloste Bürgerräte repräsentieren die Bevölkerung deskriptiv (als Spiegelbild der Demographie), aber nicht präskriptiv (durch den Wahlakt). Ihnen fehlen zwei wesentliche Legitimationsformen:

1. **Personelle demokratische Legitimation:** Die Mitglieder sind nicht gewählt. Sie können nicht abgewählt oder zur Verantwortung gezogen werden.

2. **Sachlich-inhaltliche Legitimation:** Sie sind nicht an den durch Parteiprogramme und Wahlkampf vermittelten Willen der Wählerschaft gebunden.

Daraus folgt zwingend: Die Übertragung von **verbindlichen Entscheidungsbefugnissen** (*Entscheidungsrechten*) an einen Bürgerrat würde gegen Art. 20 Abs. 2 GG verstoßen. Es würde Staatsgewalt an ein Gremium übertragen, das weder ein gewähltes Parlament noch eine parlamentarisch kontrollierte Verwaltung ist. Das "Volk" übt Gewalt durch *Wahlen* aus, nicht durch statistische Stichproben.

## 3.3 Die Rolle als konsultatives Organ

Das Grundgesetz verbietet jedoch nicht die *konsultative* Einbindung. Der Staat ist frei, sich sachkundig zu machen.

- **Beratende Funktion:** Ein Bürgerrat, der Empfehlungen erarbeitet, fungiert als qualifiziertes Instrument der Meinungsbildung. Er stärkt die "Input-Legitimation" der gewählten Repräsentanten, indem er ihnen tiefere Einblicke in eine informierte öffentliche Meinung verschafft, die über bloße Umfragen hinausgeht.
- **"Aus der Mitte des Bundestages":** Gemäß Art. 76 GG müssen Gesetzesvorlagen von der Bundesregierung, dem Bundesrat oder aus der "Mitte des Bundestages" eingebracht werden. Ein Bürgerrat kann kein Initiativrecht haben. Eine parlamentarische Fraktion kann jedoch die Empfehlungen des Rates "adoptieren" und formell als eigenen Entwurf einbringen. Dies wahrt die formale Legitimationskette.

## 3.4 Der "Selbstbindungsbeschluss" als Brücke

Um die Lücke zwischen "machtloser Beratung" und "verfassungswidriger Macht" zu schließen, nutzen Kommunen (z.B. Aachen, Köln) das Instrument des **politischen Selbstbindungsbeschlusses**.

- **Mechanismus:** Der Stadtrat verabschiedet eine Resolution: *"Wir verpflichten uns, die Empfehlungen des Bürgerrats umzusetzen, sofern sie rechtlich zulässig und budgetneutral sind"*.
- **Rechtsnatur:** Diese Bindung ist *politisch*, nicht *juristisch*. Der Rat behält rechtlich das letzte Wort (Art. 38 Abs. 1 GG schützt das freie Mandat: "an Aufträge und Weisungen nicht gebunden"). Ein Beschluss, der eine automatische Inkraftsetzung der Bürgerratsvoten ohne Ratsabstimmung vorsähe, wäre nichtig, da der Rat sich nicht seiner Verantwortung entledigen kann ("Verbot der Flucht aus der Verantwortung").
- **Faktische Wirkung:** Die hohen politischen Kosten eines Wortbruchs ("Wählerbestrafung") erzeugen jedoch eine *faktische* Bindungswirkung, die dem Bürgerrat Gewicht verleiht.

## 3.5 Experimentierklauseln im Kommunalrecht

Landesgesetze wie die *Gemeindeordnung NRW* (§ 26) enthalten Experimentierklauseln, die neue Formen der Bürgerbeteiligung ermöglichen. Zwar autorisieren diese explizit oft nur Bürgerbegehren, sie bieten jedoch den administrativen Spielraum ("Organisationshoheit"), um Bürgerräte als Teil der Verwaltungsstruktur zu finanzieren und zu organisieren. Sie erlauben es, den Bürgerrat als "vorbereitenden Ausschuss" sui generis zu behandeln.

## 3.6 Gutachterliches Fazit

Ein Bürgerrat mit verbindlicher legislativer oder exekutiver Gewalt ist unvereinbar mit der repräsentativen Demokratie des Art. 20 Abs. 2 GG. Ein Bürgerrat jedoch, der als **konsultatives Organ** integriert ist und dessen Empfehlungen durch einen **politischen Selbstbindungsbeschluss** des gewählten Rates gewürdigt werden, ist verfassungsrechtlich unbedenklich und sogar förderlich. Er reichert die parlamentarische Entscheidung mit deliberativer Qualität an, ohne die Kette der Legitimation zu durchtrennen.

# Teil IV: Die technische Brücke – Integration des "Estnischen Modells" in deutsche Meldeämter

Die föderale Struktur Deutschlands macht die Datenintegration im Vergleich zum zentralisierten estnischen Register komplex. Die Anbindung eines X-Road-basierten Auswahlsystems für Bürgerräte an deutsche **Meldeämter** erfordert die Navigation durch das eIDAS-Framework und die spezifischen deutschen Middleware-Lösungen.

## 4.1 Die Architektur der Interoperabilität

Ziel ist es, dass eine Plattform für Bürgerräte (die auf X-Road läuft) das deutsche Melderegister abfragen kann, um die Eignung eines gelosten Bürgers zu verifizieren (z.B. "Wohnhaft in München seit >3 Monaten?").

**Die Komponenten:**

1. **X-Road Security Server (Estnische Seite/Plattformseite):** Agiert als Konsument des Identitätsdienstes.
2. **eIDAS Node (Die Brücke):** Der europäische Standard für grenzüberschreitende Identitäten.
    - *Connector:* Befindet sich auf der Seite der anfragenden Plattform (X-Road).
    - *Proxy Service:* Befindet sich auf der deutschen Seite (Identitätsquelle).
3. **Deutsche eIDAS-Middleware:** Die spezifische Softwarekomponente (bereitgestellt durch BSI/Governikus), die die Kommunikation mit dem *Personalausweis* (nPA) und den Meldeämtern handhabt.

## 4.2 Das Integrationsprotokoll: SAML & OIDC

X-Road nutzt nativ SOAP oder REST mit gegenseitigem TLS (mTLS). eIDAS nutzt hingegen **SAML 2.0** (Security Assertion Markup Language) für Identitäts-Assertions.

**Der Datenfluss:**

1. **Request:** Der X-Road Security Server sendet eine REST-Anfrage an den **X-Road eIDAS Adapter**.
2. **Übersetzung:** Der Adapter übersetzt die Anfrage in einen **SAML Authentication Request**.
3. **Routing:** Der SAML-Request wird an die **Deutsche eIDAS-Middleware** (Proxy Service) geleitet.
4. **Authentifizierung:** Der deutsche Bürger nutzt seinen *Personalausweis* (nPA) und die *AusweisApp2*, um sich gegenüber der Middleware zu authentifizieren.
5. **Attribut-Abfrage:** Die Middleware verifiziert die Identität gegen die Attribute des

**Melderegisters** (XMeld-Standard: Name, Anschrift, Alter).
6. **Assertion:** Die Middleware signiert die Attribute und sendet eine **SAML Response** zurück.
7. **Delivery:** Der Adapter entpackt das SAML-Paket, validiert die deutsche Signatur und übergibt die verifizierten Daten an den X-Road Security Server.

## 4.3 Technische Herausforderungen & Lösungen

- **Attribut-Mapping:** Deutsche Meldeämter nutzen das OSCI-XMeld-Schema. Dieses muss auf das **eIDAS Minimum Data Set (MDS)** gemappt werden. Ein spezifisches Problemfeld war das Attribut "Geschlecht", das in eIDAS-Nodes Updates erforderte, um diverse Identitäten (in Deutschland "divers") korrekt abzubilden.
- **Vertrauensanker (Trust Anchors):** Die X-Road-Instanz muss dem Signaturzertifikat des deutschen eIDAS-Nodes vertrauen. Dies erfordert, dass die deutsche Certificate Authority (CA) in den Trust Store des X-Road Central Servers importiert wird.
- **Rechtsgrundlage:** Der Zugriff auf *Melderegisterdaten* erfordert eine Rechtsgrundlage nach DSGVO und Bundesmeldegesetz (BMG). Der "Selbstbindungsbeschluss" oder eine spezifische kommunale Satzung, die den Bürgerrat einsetzt, muss als öffentliches Interesse definiert werden, um diesen Zugriff zu legitimieren.

# Teil V: Spieltheoretische Simulation

## 5.1 Szenario: Die Haushaltskrise (Budget Crisis)

**Kontext:** Eine Stadt steht vor einem massiven Haushaltsdefizit ($10 Mio.). **Spieler:**
1. **Stadtrat (Council - C):** Gewählte Politiker. Motiviert durch **Wiederwahl (R)** und **Allgemeinwohl (W)**.
2. **Bürgerrat (Assembly - A):** Gelost. Motiviert rein durch **Allgemeinwohl (W)** (da keine Wiederwahl notwendig ist).

**Mögliche Züge (Strategien):**
- **Kürzungen (Cut):** Hoher Nutzen für das Wohl (W_{high}) durch fiskalische Stabilität, aber negativer Nutzen für die Wiederwahl (R_{loss}) durch Unpopularität.
- **Steuererhöhung (Tax):** Hoher Nutzen für W, negativer Nutzen für R.
- **Verschiebung (Delay / "Kick the Can"):** Negativer Nutzen für W (Schulden wachsen), aber positiver Nutzen für R (kurzfristige Ruhe).

## 5.2 Das Signalspiel (Signaling Game)

Die Interaktion wird als **Signalspiel** mit unvollständiger Information modelliert. Die Wähler kennen den "Typ" des Stadtrats nicht (Kompetent/Verantwortungsvoll vs. Inkompetent/Populistisch).

**Ablauf:**
1. **Stage 1:** Der Rat erkennt das Defizit. Er wählt: *Alleine entscheiden* oder *Delegieren*.
2. **Stage 2:** Falls delegiert, berät der Bürgerrat und gibt eine Empfehlung (z.B. "Kürzungen").
3. **Stage 3:** Der Rat stimmt über die **Annahme** oder **Ablehnung** der Empfehlung ab.
4. **Stage 4:** Wähler beobachten das Ergebnis und wählen in der nächsten Periode.

## 5.3 Auszahlungsmatrix und Gleichgewichtsanalyse

| Strategieprofil | Auszahlung Rat (U_C) | Auszahlung Assembly (U_A) | Ergebnis |
|---|---|---|---|
| **Rat handelt allein (Delay)** | R_{high} - W_{loss} | -W_{loss} | Krise vertieft sich; Rat wird wiedergewählt (kurzfristig). |
| **Rat handelt allein (Cut)** | R_{low} + W_{gain} | W_{gain} | Budget saniert; Rat verliert Wahl (Blame). |
| **Delegation -> Annahme (Cut)** | R_{med} + W_{gain} | W_{gain} | **Blame Shifting Equilibrium**. |

**Insight: Blame Shifting als Feature** Die Simulation enthüllt ein **"Blame Shifting Equilibrium"**.

- Trifft der Rat eine schmerzhafte Entscheidung (Cut) allein, bestrafen die Wähler ihn hart (R_{low}).
- Folgt der Rat der Empfehlung des Bürgerrats, kann er signalisieren: "Wir vollstrecken nur den Willen des Volkes."
- Dies erzeugt einen "Schutzschild". Die Wähler bestrafen den Rat *weniger* für denselben schmerzhaften Schnitt, wenn er von ihren Peers (dem Bürgerrat) empfohlen wurde (R_{med}).
- **Resultat:** Die Existenz des Bürgerrats erlaubt es dem Stadtrat, fiskalisch verantwortungsvolle Politik zu betreiben (Maximierung von W), die er sich aus Angst vor Abwahl sonst nicht trauen würde.

## 5.4 Die Variable der "Selbstbindung" (Commitment Device)

Wenn der Rat *ex ante* einen **Selbstbindungsbeschluss** fasst (siehe Teil 3.4):

- Dies entfernt die Option "Ablehnen" in Stage 3.
- Es löst das **Zeitinkonsistenz-Problem**. Politiker wissen, dass sie kurz vor der Wahl versucht sein werden, das Problem zu verschleppen ("Delay"). Indem sie sich *jetzt* an den Bürgerrat binden, verpflichten sie sich auf den optimalen Langzeitpfad (W_{gain}) und akzeptieren ein moderates Wiederwahlrisiko, um die populistische Falle zu vermeiden. Der Bürgerrat fungiert hier als *Ulysses-Pakt* für die Politik.

# Fazit

Die Legitimation einer sortitionsbasierten Demokratie ruht auf einem Trias aus **Verifikation**, **Sicherheit** und **Integration**. Technisch müssen Bürger mit Werkzeugen wie **X-Road** **ASiC-Containern** und **drand**-Explorern ausgestattet werden, um die "Black Box" staatlicher Auswahl und Daten zu auditieren. Sicherheitstechnisch erfordern Plattformen wie **Pol.is** eine strikte Identitätsintegration (eID), um eine algorithmische Kaperung durch koordinierte Angreifer ("Brigading") zu verhindern. Rechtlich verlangt das **Grundgesetz** eine ununterbrochene Legitimationskette, die verhindert, dass diese Räte zu Souveränen werden; sie müssen "konsultative Organe mit Zähnen" bleiben – Zähne, die durch **politische Selbstbindungsbeschlüsse** statt durch verfassungsrechtliche Autorität verliehen werden. Schließlich zeigt die Spieltheorie, dass diese Räte keine Bedrohung für gewählte Politiker sind, sondern strategische Assets ("Commitment Devices"), die es Demokratien ermöglichen,

langfristige Probleme zu lösen, indem sie den Zyklus kurzfristiger Wahlanreize durchbrechen.

## Zitierte Quellen

### Quellenangaben

1. X-Road: Message Log Data Model, https://docs.x-road.global/DataModels/dm-ml_x-road_message_log_data_model.html 2. Security Server User guide - X-Road: 7.7.0, https://x-tee.ee/docs/live/xroad/ug-ss_x-road_6_security_server_user_guide.html 3. How Is the Time-Stamping Service Used in X-Road?, https://nordic-institute.atlassian.net/wiki/spaces/XRDKB/pages/859209748/How+Is+the+Time-Stamping+Service+Used+in+X-Road 4. X-Road: Security Server Architecture, https://docs.x-road.global/Architecture/arc-ss_x-road_security_server_architecture.html 5. Are you sure you want digitally signed notice?, https://www.ra.ee/vau/index.php/en/help/default/sview?code=ddoc_confirm 6. End user applications of eID - ria.ee, https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/end-user-applications-eid 7. Digital signing - Smart-ID, https://www.smart-id.com/digital-signing/ 8. Manual installation of Trust Service Status Lists of certificates in DigiDoc4 application - ID.ee, https://www.id.ee/en/article/manual-installation-of-trust-service-status-lists-of-certificates-in-digidoc-client-2/ 9. Drand: Home, https://www.drand.love/ 10. League of Entropy - Wikipedia, https://en.wikipedia.org/wiki/League_of_Entropy 11. drand/drand: A Distributed Randomness Beacon Daemon - Go implementation - GitHub, https://github.com/drand/drand 12. Distributed Randomness Beacon - Cloudflare, https://www.cloudflare.com/leagueofentropy/ 13. Protocol Specification | drand, https://docs.drand.love/docs/specification/ 14. Drand | Filecoin Docs, https://docs.filecoin.io/basics/the-blockchain/drand 15. Polis - The Computational Democracy Project | The Computational ..., https://compdemocracy.org/polis/ 16. Enhancing Security in Social Networks through Machine Learning: Detecting and Mitigating Sybil Attacks with SybilSocNet - Semantic Scholar, https://pdfs.semanticscholar.org/94e7/20b2e09b9167e5b783a9a441d4bd6f85e7c8.pdf 17. View of Manufacturing rage: The Russian Internet Research Agency's political astroturfing on social media | First Monday, https://firstmonday.org/ojs/index.php/fm/article/view/10801/9723 18. Online astroturfing: A problem beyond disinformation - ResearchGate, https://www.researchgate.net/publication/361389437_Online_astroturfing_A_problem_beyond_disinformation 19. Algorithmic Amplification for Collective Intelligence - | Knight First Amendment Institute, https://knightcolumbia.org/content/algorithmic-amplification-for-collective-intelligence 20. A STUDY OF COMMUNITY DETECTION ALGORITHMS, POLARIZATION METRICS AND APPLICATION - UPCommons, https://upcommons.upc.edu/server/api/core/bitstreams/4df4da1f-548f-4d48-9935-a6cde44c3f29/content 21. The Algorithmic Ecology: An Abolitionist Tool for Organizing Against Algorithms - stoplapdspying, https://stoplapdspying.medium.com/the-algorithmic-ecology-an-abolitionist-tool-for-organizing-against-algorithms-14fcbd0e64d0 22. Moderation Schemes - The Computational Democracy Project, https://compdemocracy.org/moderation/ 23. Restricting clustering to 2-5 groups impacts group aware/informed consensus and comment routing · Issue #1289 · compdemocracy/polis -

GitHub, https://github.com/compdemocracy/polis/issues/1289 24. Art 20 GG - Einzelnorm - Gesetze im Internet, https://www.gesetze-im-internet.de/gg/art_20.html 25. Demokratische Legitimation (Art. 20 Abs. 2 GG) und Wissenschaftsförderung (Art. 91b GG) - Universität Greifswald,
https://epub.ub.uni-greifswald.de/files/13728/Dissertation_Oster_Veroeffentlichung.pdf 26. Bürgerräte und Gesetzgebungsverfahren Sachstand - Deutscher Bundestag,
https://www.bundestag.de/resource/blob/894386/9a7bd24fbc77fb379b22dc6e45982905/WD-3-022-22-pdf-data.pdf 27. Bürger versus Bürgermeister? Demokratie und Partizipation in Stadt und Land - Universität Osnabrück,
https://www.uni-osnabrueck.de/fileadmin/fb10/inst-isvwr/Tagungen/BIG/31._BIG_Working_Paper.pdf 28. Neue Formen demokratischer Beteiligung von Bürgern Ausarbeitung - Deutscher Bundestag,
https://www.bundestag.de/resource/blob/550340/1cfa9b21f88835679b09f0eec7bf60c0/wd-3-037-18-pdf-data.pdf 29. Citizens' Assemblies in Germany — IACL-IADC Blog,
https://blog-iacl-aidc.org/2024-posts/2024/11/28/citizens-assemblies-in-germany 30. Bindungswirkung von Beschlüssen, erneuter Beschluss,
https://ratsinfo.elbtalaue.de/buergerinfo/vo0050.asp?__kvonr=16661 31. Bürgerrat per Bürgerantrag, https://www.buergerrat.de/aktuelles/buergerrat-per-buergerantrag/ 32. Experimentierklauseln im Kommunalrecht, https://d-nb.info/969187041/34 33. SGV § 26 (Fn 23) Bürgerbegehren und Bürgerentscheid | RECHT.NRW.DE,
https://recht.nrw.de/lmi/owa/br_bes_detail?sg=2&menu=1&bes_id=6784&anw_nr=2&aufgehoben=N&det_id=701431 34. eIDAS SAML Attribute Profile,
https://docs.swedenconnect.se/technical-framework/mirror/eidas/eIDAS_SAML_Attribute_Profile_v1.2-FINAL.pdf 35. eIDAS-Node version 2.5 - European Commission,
https://ec.europa.eu/digital-building-blocks/sites/spaces/DIGITAL/pages/467109344/eIDAS-Node+version+2.5?src=contextnavpagetreemode 36. Three Steps to integrate the German eIDAS-Middleware,
https://ec.europa.eu/digital-building-blocks/sites/download/attachments/467109300/2021_04_30_German%20eID_MW-Integration_v1_1.pdf?version=1&modificationDate=1678712607281&api=v2 37. MyAcademicID Blueprint Architecture - Projects,
https://projects.uni-foundation.eu/myacademic-id/wp-content/uploads/sites/9/2021/03/MyAID_Blueprint_Architecture_FinalV2.pdf 38. D2.1. HEALTHeID Functional Specification - SPMS,
https://spms.min-saude.pt/wp-content/uploads/2019/08/D2.1_HealtheID_functionalSpecs_20190523_rev.pdf 39. X-Road® Architecture, https://x-road.global/architecture 40. Applications of Game Theory to Topics in Political Economy - The University of North Carolina at Chapel Hill,
https://cdr.lib.unc.edu/downloads/d504rm608?locale=en 41. Electoral decisions: The role of the government in power, the opposition and the voters an approach from the perspective of game theory - American Institute of Mathematical Sciences,
https://www.aimsciences.org/article/doi/10.3934/jdg.2024009 42. Political Game Theory Nolan McCarty Adam Meirowitz - Princeton University,
https://www.princeton.edu/~nmccarty/Political_Game_Theory%20.pdf 43. Mitigating the Political Cost of Financial Crisis with Blame Avoidance Discourse: The Case of Turkey - ResearchGate,
https://www.researchgate.net/publication/370064666_Mitigating_the_Political_Cost_of_Financial_Crisis_with_Blame_Avoidance_Discourse_The_Case_of_Turkey 44. STOP US BEFORE WE SPEND AGAIN: INSTITUTIONAL CONSTRAINTS ON GOVERNMENT SPENDING,
http://www.sas.rochester.edu/psc/primo/primobudget.pdf 45. PROBABILISTIC VOTING MODEL,
https://didattica.unibocconi.it/mypage/dwload.php?nomefile=APE12_TIMEINCONSISTENCY20

101103182038.PDF 46. Discipline and Selection: Explication of the Models in Principled Agents, https://andy.egge.rs/papers/besley_explication.pdf