Die folgenden Statements von POLYAS beziehen sich auf das Wahlsystem POLYAS CORE 2.2.3 und sind für die Diskussionen der KIF verwertbar.

| 1. Inwieweit erfüllt das elektronische Wahlsystem der Firma Polyas in der für den Einsatz bei Hochschulwahlen z.B. an der Universität Duisburg-Essen sowie der Johannes Gutenberg Universität Mainz geplanten Variante diese Grundsätze? |
|---|
| Das Online-Wahlsystem POLYAS CORE 2.2.3 erfüllt u.a. folgende Anforderungen:<br>• Von der abgegebenen Stimme ist keinerlei Rückschluss auf die Identität des Wählers herstellbar.<br>• Es ist dem Wähler nicht möglich, seine Wahlentscheidung gegenüber Dritten zu beweisen.<br>• Die Wahlberechtigten werden für die Stimmabgabe eindeutig und zuverlässig identifiziert und authentifiziert, sodass nur registrierte Personen aus dem Wählerverzeichnis wählen können.<br>• Die Wähler dürfen jeweils nur einmal eine Stimme abgeben.<br>• Stimmen dürfen nicht während der Übertragung im Netzwerk verändert, gelöscht oder ergänzt werden.<br>• Stimmen in der Wahlurne dürfen nicht nachträglich verändert, gelöscht oder ergänzt werden.<br>• Zwischenergebnisse dürfen nicht berechnet werden.<br><br>Damit ist die Online-Stimmabgabe bei POLYAS konform mit den Wahlgrundsätzen einer freien, gleichen, geheimen, allgemeinen und unmittelbaren Wahl. |

| 2. Wie ist die Erfüllung der Grundsätze graduell zwischen den in Deutschland für allgemeine Wahlen zugelassenen Systemen der Urnenwahl und der Briefwahl einzuordnen? |
|---|
| Wir sind keine Juristen und können leider aus diesem Grund hierüber keine rechtsverbindliche Einschätzung abgeben.<br><br>Grundsätzlich erfüllen *alle* für allgemeine Wahlen zugelassenen Systeme die geltenden Wahlgrundsätze. Wie die Briefwahl wird die Online-Wahl konkret zu den *Fernwahlverfahren* hinzugerechnet.<br><br>Da die Fernwahl eine barriereärmere Form der Stimmabgabe darstellt, erfolgt damit eine Stärkung des Grundsatzes der Allgemeinheit. |

3. Die Resolution sieht folgende zusätzlichen Anforderungen, die sich aus den Wahlgrundsätzen ergeben, wenn für eine Wahl oder Teile einer Wahlhandlung ein elektronisches System eingesetzt werden:

- Der Quellcode, das Kompilat und die Hardware des verwendeten Systems können jederzeit durch die Öffentlichkeit eingesehen und überprüft werden
- Alle Schritte einer Wahl müssen der öffentlichen Überprüfbarkeit unterliegen, soweit nicht andere verfassungsrechtliche Belange eine Ausnahme rechtfertigen
- Beim Einsatz elektronischer Wahlgeräte müssen die Schritte der Wahlhandlung und der Ergebnisermittlung von den Wahlberechtigten zuverlässig und ohne besondere Sachkenntnis überprüft werden können

Inwieweit erfüllen Ihre Systeme diese Anforderungen (hier sind technische Details von Interesse und nicht nur ggf. vorhandene Zertifizierungen)?

Uns ist die zentrale Bedeutung von Integrität einer Online-Wahlsoftware deutlich bewusst. Aus diesem Grund setzen wir bei POLYAS in der Kommunikation auf höchste Transparenz und in der Entwicklung auf verifizierbare Prozesse und nachhaltige Verschlüsselung. Unsere Wahlsysteme halten die geltenden Wahlgrundsätze (frei, gleich, geheim, allgemein, unmittelbar) nachweislich ein.

Für den POLYAS CORE 2.2.3, dem zentralen Bestandteil der Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach Common Criteria Standards, liegen umfangreiche Dokumentationen und Handreichungen für Wahlleiter und Wahlberechtigte vor, die wir Kunden jederzeit zur Verfügung stellen. Mit unserem Verifikationstool können Wahlergebnisse universell überprüft werden - auch ohne technische Vorkenntnisse.

Sollten wir politische Wahlen durchführen, was wir aktuell nicht tun, werden wir zu diesem Zeitpunkt in Erwägung ziehen, den Quellcode des dafür eingesetzten Systems zu veröffentlichen.

Sollten Sie an diesem Punkt konkret weiterführenden Gesprächsbedarf sehen, schlage ich vor, dass wir es gesondert vertiefen.

4. Welche besonderen Kenntnisse sind im Umgang mit den Systemen sowie zur Überprüfung von Ergebnissen notwendig?

Die Online-Stimmabgabe und sogar das Erstellen einer Online-Wahl ist ohne besondere Kenntnisse möglich.

Hierzu empfehle ich einen kurzen Überblick in unseren Support: www.polyas.de/support
Dort sind auch Schritt-für-Schritt-Anleitungen verlinkt, die mit Screenshots einen plastischen Überblick über die einzelnen Schritte geben.

Die Überprüfung der Wahlergebnisse anhand des Verifikationstools ist ebenso möglich, ohne besondere Kenntnisse. Die dazugehörige Anleitung beschreibt die notwendigen Schritte. Mehr dazu: https://www.polyas.de/sicherheit/wahlergebnisse-ueberpruefen

Zudem werden Wahlergebnisse vom System nicht nur in summierter Form und im maschinenlesbaren XML-Format ausgegeben, sondern die einzelnen abgegebenen anonymen Stimmzettel können auch im Excelformat eingesehen werden.

5. Des weiteren wird gefordert, dass die elektronische Stimmabgabe durch eine nicht-elektronische Stimmabgabe (z.B. Urnenwahl) überschrieben werden kann. Ist das mit den für den für den Einsatz bei Hochschulwahlen vermarkteten Systemen möglich?

In unserem aktuellen System POLYAS CORE 2.2.3 können wir die Inhalte einer Wahlurne nicht überschreiben oder entnehmen. Dies entspricht den uns bekannten Wahlordnungen, wonach in der Wahlurne eingegangene Stimmzettel nicht mehr verändert, ergänzt oder gelöscht werden dürfen. An diesen Grundsatz halten wir uns strikt. Wird also in Ergänzung zur Online-Wahl eine Urnenwahl durchgeführt, greifen organisatorische-administrative Methoden zur Sicherstellung, dass keine Wahlberechtigten in beiden Verfahren ihre Stimme abgeben können.

**Weitere relevante Punkte zur Einordnung Ihrer Antworten wären folgende:**

6. Entstehen den Universitäten durch Mechanismen, die die Überprüfbarkeit und Fehlertoleranz erhöhen, zusätzliche Kosten (im Vergleich zu den initial angebotenen Systemen)?

Das derzeit angebotene Tool zur universellen Verifikation wird den Kunden von POLYAS kostenfrei überlassen. Zudem haben wir eine Anleitung erstellt, ein Verifikationstool selbst zu programmieren und übergeben diese Anleitung ebenso kostenfrei.

Werden darüber hinaus Dienstleistungen gewünscht, müssen wir diese nach Aufwand bepreisen.

7. Welche externen Überprüfungen haben stattgefunden?

Neben der Überprüfung durch das Deutsche Forschungszentrum für künstliche Intelligenz (DFKI) und dem Bundesministerium für Sicherheit in der Informationstechnik (BSI) im Rahmen der Zertifizierung nach Common Criteria führen wir regelmäßig Penetrationtests mit externen Prüfpartnern durch.

Weitere Informationen zu den Penetrationtests finden Sie hier:
https://www.polyas.de/sicherheit/systemsicherheit

| 8. Inwieweit werden persönliche Daten von Hochschulangehörigen für die Durchführung der Wahl an die Firma Polyas weitergeben? |
|---|
| Mit Hochschulen tauschen wir keine personenbezogenen Daten von Wahlberechtigten aus.<br><br>Es gibt grundsätzlich drei Varianten für die Authentifizierung bei Hochschulwahlen:<br><br>1. Die Hochschule implementiert eine Anmeldeplattform mit Schnittstelle an ihr LDAP-Adressverzeichnis und führt in ihrem System eine Pseudonymisierung der Benutzerkennungen durch. POLYAS erhält so nur die pseudonymisierten Nutzerkennungen.<br>2. Die Hochschule implementiert einen SecureLink im Intranet und ordnet jeder Benutzerkennung eine eindeutige Kennung zu, führt also eine Pseudonymisierung durch. POLYAS erhält nur die pseudonymisierten Nutzerkennungen.<br>3. Die Hochschule übermittelt den Wahlberechtigten Zugangsdaten zur Online-Wahl im Format PIN/TAN. Diese sind frei wählbar und können komplett ohne personenbezogene Daten (anonym) erstellt werden. POLYAS erhält nur anonyme Nutzerkennungen.<br><br>Bitte informieren Sie sich bei der Wahlleitung Ihrer Hochschule, welches Verfahren in dem konkreten Fall eingesetzt wird.<br><br>Weitere Informationen zum Datenschutz bei Hochschulwahlen können Sie hier nachlesen: https://www.polyas.de/hochschulen/hochschulwahlen/datenschutz |

| 9. Inwieweit können Mitarbeiter*innen der Firma Polyas oder Hochschulangehörige die Wahlentscheidungen einzelner Personen einsehen? |
|---|
| Da die Stimmzettel ohne personenbezogene Daten erfasst und gespeichert werden, haben weder MitarbeiterInnen von POLYAS noch Mitglieder des beauftragenden Wahlvorstands Kenntnis von Wahlentscheidungen einzelner Wähler. |

| 10. Inwieweit kann auf die Entscheidung von Untergruppen von Wahlberechtigten geschlossen werden? |
|---|
| Das Wahlgeheimnis gilt für alle Segmentierungen von Wählern im Wählerverzeichnis uneingeschränkt. Wir empfehlen zur faktischen Wahrung des Wahlgeheimnisses die Wähler(unter-)Gruppen nicht zu klein zu fassen. |

**11. Welche Vorteile bieten die vermarkteten Systeme gegenüber einer Urnenwahl? Gegenüber einer Briefwahl?**

Grundsätzlich bieten Fernwahlverfahren gegenüber eine Präsenzwahl den Vorteil der ortsunabhängigen Stimmabgabe und damit die Antwort auf geänderte Lebensbedingungen in Bezug auf die Megatrends Mobilität und Digitalisierung. Somit tragen Fernwahlverfahren zur Steigerung der Wahlbeteiligung bei, wobei die Online-Wahl gegenüber der Briefwahl deutlich niedrigere Kosten und Aufwände aufweist und zudem eine Manipulationsfreiheit nachweisbar ist.

Mehr zum Vergleich der Online-Wahl mit der Briefwahl finden Sie in diesem Artikel: https://www.polyas.de/blog/de/online-wahlen/sicherheit/online-wahlen-die-briefwahl-des-21-jahrhunderts

und hier: https://www.polyas.de/blog/de/allgemein-de/fokus-sicherheit-briefwahl

**12. Welche Nachteile gibt es?**

Bitte entschuldigen Sie, dass wir aus der Natur der Sache heraus vor allem die Vorteile in der Online-Wahl sehen.

An dieser Stelle möchten wir jedoch betonen, dass wir nicht das Ziel haben, die Urnenwahl abzulösen. Dieses Ritual der Stimmabgabe, das von einigen Menschen aktiv und feierlich gelebt wird und eine hohe Bedeutung hat, sollte unserer Meinung nach weiterhin Bestand behalten. Wir wollen lediglich eine bedarfsorientierte und kosteneffiziente Möglichkeit der Fernwahl mit unserem Online-Wahlsystem als zusätzlichen Weg der Stimmabgabe etablieren.

**13. Das unter [0] verlinkte Zertifikat des Bundesamts für Sicherheit in der Informationstechnik bescheinigt eine Einsetzbarkeit der von Ihnen entwickelten Systeme für Gremienwahlen sowie nicht-politische Wahlen mit geringem Angriffspotenzial. Inwiefern halten sie Hochschulwahlen an einer Universität (z.B. für Studierendenparlamente und Universitätsversammlungen, in denen z.B. Haushalte von etlichen Millionen verabschiedet werden) für unpolitisch und uninteressant für Manipulationsversuche?**

Hochschulwahlen sind aus unserer Sicht ein wichtiger Baustein der demokratischen Gesellschaft und daher sollten Online-Wahlsysteme auch für diese Wahlen eine umfassende Rechtssicherheit bieten.

Im Gegensatz zu anderen Rechtsformen haben Hochschulen und Universitäten als Körperschaften des öffentlichen Rechts Satzungsautonomie und können sich (bis auf wenige Ausnahmen, wie Bayern) eine eigene Wahlordnung geben.

Wir teilen nicht die Ansicht, dass aus der Stellungnahme des BSI abzuleiten wäre, dass Hochschulwahlen "unpolitisch" oder "uninteressant für Manipulationsversuche" wären

14. Inwieweit ist ihr System gegen Manipulationsversuche abgesichert?

**A) Datenschutz und Datensicherheit**

POLYAS hostet seit 2018 alle Online-Wahlen auf den mehrfach zertifizierten Servern der Open Telekom Cloud. Dabei stehen die Kernwerte Datensicherheit, Verfügbarkeit und Skalierbarkeit im Vordergrund. Die mehrfach zertifizierte Open Telekom Cloud arbeitet mit einer Anti-DDos-Funktion zum Schutz öffentlicher IP-Adressen.

Ebenso ist der Zutritt zu den Servern, auf denen Ihre Daten gespeichert werden, gemäß ISO27001 nur befugten Personen möglich. So kann POLYAS zum einen die Einhaltung der EUDSGVO gewährleisten und zum anderen verhindern, dass unbefugte Dritte Manipulationen direkt an den Servern vornehmen können.

Durch diesen Hostingpartner kann POLYAS höchste Sicherheitsstandards im Datenschutz und Qualitätsmanagement gewährleisten.
Mehr zum Hosting: https://www.polyas.de/sicherheit/open-telekom-cloud

Darüber hinaus finden regelmäßige Penetration- und Hackertests beziehungsweise Sicherheitsaudits durch unabhängige Prüfpartner statt, um potenzielle Sicherheitslücken frühzeitig zu erkennen und schnellstmöglich zu schließen. Zusätzlich werden regelmäßig automatisierte Selbsttests des Systems durchgeführt, um die Performanz und Stabilität der Online-Wahlsoftware zu kontrollieren.

**B) Verschlüsselungen und Prüfsummen**

Die Stimmabgabe der Wähler erfolgt ausschließlich über eine verschlüsselte Verbindung via SSL-Server-Zertifikat der D-Trust GmbH, einem Unternehmen der Bundesdruckerei.

Im POLYAS CORE 2.2.3 werden Passwörter per SHA-256 Algorithmen gehasht.

Um Manipulationen der Stimmzettel in der virtuellen Wahlurne vorzubeugen und diese zu erkennen, kommen im POLYAS CORE 2.2.3 Blockprüfsummen zum Einsatz. Dazu wird nach jeweils 30 eingegangen Stimmen ein Block gebildet. Die 30 Stimmen werden nun zufällig angeordnet, so dass nicht mehr zurückverfolgt werden kann, wann welche Stimme eingegangen ist. Über den Block wird eine SHA-256-Prüfsumme gebildet. Die Prüfsumme wird nach jedem Block in das Wählerverzeichnis geschrieben. Ab dem zweiten Block wird die vorherige Prüfsumme mit einbezogen. Wird also eine Stimme manipuliert, stimmen die Prüfsumme des Blockes und alle nachfolgenden Prüfsummen nicht mehr mit denen der Urne überein. So wird eine Manipulation bei einer nochmaligen Überprüfung des Wahlergebnisses aufgedeckt.

Auch wird jede Stimme wird im Rahmen der Stimmabgabe mit einem zufälligen AES128 Schlüssel verschlüsselt und dieser mit dem öffentlichen Schlüssel der Wahlurne verschlüsselt. Erst bei der Auszählung wird der private Schlüssel der Wahlurne genutzt um die zufälligen AES Schlüssel wiederherzustellen und damit die Stimmen zu entschlüsseln. Als asymmetrisches Verschlüsselungsverfahren kommt hierbei RSA zum Einsatz,

ECB/CBC/GCM wird hierbei nicht verwendet, da der AES-Schlüssel innerhalb eines RSA-Ciphertexts verschlüsselt werden kann.

**C) Prävention unerlaubter Zugriffe**

Brute Force Angriffe werden bei POLYAS unterbunden, indem die Anzahl der Zugriffsversuche pro Zeiteinheit und IP-Adresse streng limitiert wird.

Um Manipulationen durch korrupte Parteien während der Wahlorganisation zu vermeiden, wird für Hochschulwahlen häufig das Wahlvorstandsinterface eingesetzt, welches das Prinzip einer Separation-of-Duty umsetzt und alle Vorgänge während der Wahldurchführung sichtbar macht. Ebenso bedarf es der Autorisierung mehrerer befugter Personen, um Aktionen (Wahl starten, Wahl stoppen, Auszählung starten) durchführen zu können. Des Weiteren besteht im Wahlvorstandsinterface jederzeit die Möglichkeit, Systemselbsttests durchzuführen, sodass sichergestellt werden kann, dass alle Komponenten des Online-Wahlsystems korrekt arbeiten.

Um zu erfahren, ob bei der Online-Wahl an Ihrer Hochschule ein Wahlvorstandsinterface zur Administration der Online-Wahl zum Einsatz kommt, wenden Sie sich bitte an ihren Wahlvorstand.

15. Das Bundesverfassungsgericht hat sich in seinem Urteil vom 03. März 2009 gegen den Einsatz von rechnergesteuerten Wahlgeräten (sogenannten Wahlcomputern) ausgesprochen [1]. Inwieweit können die Systeme der Firma Polyas die Nachvollziehbarkeit garantieren, die bei Wahlcomputern nicht ausreichend gegeben war? Inwiefern können weitere Bedenken des Bundesverfassungsgerichts ausgeräumt werden?

Wahlcomputer und Online-Wahlen sind zwei komplett unterschiedliche Systeme. Hierzu empfehle ich diesen Artikel: https://www.polyas.de/blog/de/online-wahlen/sicherheit/warum-sind-wahlcomputer-nicht-erlaubt

Im Gegensatz zum Wahlcomputer sind Online-Wahlen überprüfbar. Wir arbeiten bei POLYAS sogar an Verifikationsmethoden, die das vom Bundesverfassungsgericht geforderte Öffentlichkeitsprinzip erfüllen werden.
Mehr dazu unter: https://www.polyas.de/ueber-polyas/forschung

Bislang bereits eingesetzt wird die universelle Überprüfung des Wahlergebnisses, d.h. das Wahlergebnis kann erneut ausgezählt werden und eine Systemintegrität (Manipulationsfreiheit) kann nachgewiesen werden. Dies war bereits Gegenstand im Verwaltungsgericht Gera im Verfahren 2K 541/15 Ge vom 24. Mai 2017 zur Online-Hochschulwahl an der Universität Jena: „der Grundsatz der Öffentlichkeit (für eine Onlinewahl) sei als ausreichend gewahrt anzusehen, insbesondere sei es möglich das Wahlergebnis nachzuvollziehen“.

Eine typische Eigenschaft von IT-Systemen ist es, dass aus technischen Gründen einige Personen (die Administrator*innen) für Deployment, Betrieb und Wartung massiv zusätzliche Rechte haben. Diese erlauben zum Beispiel das Auslesen und Editieren von Datenbanken, das Umleiten von Anfragen usw. Hinzu kommt, dass ihre Aktionen oftmals aus technischen Gründen nicht von den üblichen Log-Systemen erfasst werden (oder die Rechte auch die Änderung dieser Logs erlauben)

Immer wieder werden Fälle bekannt, in denen Administrator*innen (z.B. aus persönlichen Interessen, gegen das Angebot von Vorteilen oder als Rache für eine Kündigung) die von ihnen verwalteten Systeme stören, verändern oder darin gespeicherte Informationen weitergeben oder veröffentlichen.

| 16. Wie ist das System gegen Manipulationen von Innen, also durch Administrator*innen in Ihrer Firma geschützt? |
|---|
| Grundsätzlich sind auch Angriffe von innen im Common Criteria Protection Profile für Online-Wahlen definiert und die jeweiligen Präventionsmaßnahmen im POLYAS CORE 2.2.3 im Zertifizierungsreport aufgelistet.<br><br>Wir haben Sicherungen im POLYAS CORE 2.2.3 u.a. für folgende Szenarien:<br>• Stimmen löschen / hinzufügen: Es erfolgt ein Abgleich zwischen der im Wählerverzeichnis angegebenen Anzahl abgegebener Stimmen und der Anzahl der in der Urne befindlichen Stimmzettel. Da dies getrennte Systeme sind, die bei einer laufenden / abgeschlossenen Wahl nicht geändert werden können – auch nicht von Entwicklern mit Administratorenrechten – ist dieser Abgleich ein effektiver Schutzmechanismus.<br>• Stimmen verändern: Die Bildung von Blockprüfsummen ist ein wirksamer Schutz gegen die Veränderung abgegebener Stimmzettel. Genauere Erläuterung zum Prinzip finden Sie unter Ziffer 14 B und 17.<br>• Stimmen auslesen: Das „Brechen des Wahlgeheimnisses“ ist unterbunden durch das sog. Tokenprinzip: Jedem Wähler wird nach erfolgter Authentifizierung (Schritt 1 im Online-Wahlsystem) ein Token zugewiesen, anhand dessen die Stimmabgabe erfolgt. Nach der verbindlichen Stimmabgabe wird das Token unwiderruflich gelöscht. So werden keine personenbezogenen Daten während der Stimmabgabe weitergegeben und eine Zuordnung zu einer Identität ist nicht möglich. Auch POLYAS ist zu keinem Zeitpunkt in der Lage, nachzuvollziehen, welche Personen wie abgestimmt haben. Weder ein Administrator noch ein Election Manager. |

| 17. Kann technisch verhindert werden, dass Administrator*innen Stimmabgaben manipulieren? Wie? |
|---|
| Hierfür kommen verschiedene Sicherheitsmechanismen zum Tragen, u.a. wie schon in Ziffer 14 B erwähnt, Blockprüfsummen in der digitalen Wahlurne: Eine Prüfsumme wird hierbei über einen Block von Stimmen in der Urne gebildet. Diese Prüfsumme wird stets (iterativ) neu berechnet, sobald sich eine festdefinierte Anzahl weiterer Stimmen in der Urne befindet und bezieht dabei die zuvor auf dieselbe Weise berechnete Prüfsumme über die bisherigen Stimmenblöcke ein. Eine eben abgegebene Stimme wird einem |

Stimmblock zugeordnet. Sobald dieser Stimmblock 30 Einträge enthält, wird automatisch eine Blockprüfsumme berechnet.
Die Selbsttests im System (einsehbar z.B. für den Kunden im Wahlvorstandsinterface) nutzen die Blockprüfsummen für die Datenintegritätsprüfungen.

Von außen ist die Erstellung der Blockprüfsumme nicht beeinflussbar, bzw. eine versuchte Einflussnahme würde aufgedeckt werden bei der Datenintegritätsprüfung.

18. Kann technisch verhindert werden, dass Administrator*innen die Zuordnung von Personen/Accounts und abgegebener Stimme auslesen? Wie?

Da bereits rein technisch die Daten getrennt werden und Stimmzettel zu keinem Zeitpunkt mit personenbezogenen Daten verknüpft werden, können auch Administratoren keinen Zusammenhang herstellen.

19. Werden weitere Maßnahmen ergriffen, um unberechtigte Zugriffe durch administrativ-technisches Personal Ihrer Firma aber auch aller anderen beteiligten Institutionen zu verhindern?

Wir befinden uns im Zertifizierungsprozess nach ISO 27001 und müssen daher organisatorische Normen und Managementpraktiken zur Informationssicherheit unter Berücksichtigung unserer spezifischen Sicherheitsrisiken in den Blick nehmen.
Beispielhaft nennen kann ich Ihnen einige TOMs:

- Zutrittskontrolle via Transponder
- Zugangskontrolle via Protokollierung
- Abkapselung von sensiblen Systemen durch getrennte Netzbereiche
- Dokumentierte Berechtigungskonzepte
- Verschlüsselte Speicherung von personenbezogenen Daten
- Release- und Patchmanagement
- Übermittlung von Daten über verschlüsselte Datennetze oder VPN
- ...

Alle POLYAS Mitarbeiter haben sich auf die „IT-Nutzungs- und Sicherheitsrichtlinien für Mitarbeiter der POLYAS GmbH“ vertraglich verpflichtet, bei deren Zuwiderhandlung gesetzliche Konsequenzen folgen.

Spannend für Sie ist sicher ebenso dieser Ausblick:

In einem Entwicklungsprojekt arbeiten wir gemeinsam mit der Gesellschaft für Informatik e.V. an der Online-Wahlsoftware POLYAS CORE 3.0.
Der CORE 3.0 ist eine komplett andere Plattform mit einer ganz anderen Systemarchitektur als der CORE 2.2.3 und setzt andere kryptografische Maßnahmen ein.
Eine Zertifizierung hierfür ist ebenfalls in Planung.

In der Variante „VERIFIABLE“ beinhaltet der CORE 3.0 Möglichkeiten der individuellen Verifikation, eine Möglichkeit zur kundenseitigen Erzeugung der Passwörter zum Schutz vor "Ballot Stuffing" und weitere Ausbaustufen zur Umsetzung des Prinzips der "Separation of Duty".

Mehr zum Status des CORE 3.0 VERIFIABLE: https://www.polyas.de/ueber-polyas/forschung