# Technische Dokumentation:
## *Digitales Losverfahren zur Auflösung von Gleichständen*

POLYAS

Dieses Dokument beschreibt das Protokoll, das von POLYAS verwendet wird, um Gleichstände bei Wahlen auf eine überprüfbare, pseudo-zufällige Weise aufzulösen. Ein Gleichstand tritt auf, wenn zwei oder mehr Kandidaten oder Optionen die gleiche Anzahl an Stimmen in einem Wahl- oder Abstimmungsverfahren erhalten. In solchen Fällen kann ein Mechanismus zur zufälligen Bestimmung der Reihenfolge dieser Entitäten erforderlich sein. Das Hauptziel des beschriebenen Protokolls besteht darin sicherzustellen, dass die Reihenfolge der Auslosung tatsächlich folgende Kriterien erfüllt:

- **pseudo-zufällig**: das Ergebnis ist unvorhersehbar und gleichverteilt,
- **fair**: weder das POLYAS-System noch der Wahlausschuss können das Ergebnis manipulieren, um bestimmte Kandidaten zu bevorzugen,
- **überprüfbar**: es kann überprüft werden, um die obigen Bedingungen sicherzustellen.

Um dies zu erreichen, kombiniert der Prozess zwei Zufallsquellen — eine vom POLYAS-System erzeugte und eine vom Wahlausschuss bereitgestellte —, um die Reihenfolge der Auflösung zu bestimmen. Um Fairness zu gewährleisten, verpflichtet sich das POLYAS-System, wie unten ausführlich beschrieben, zu seinem Zufallswert, bevor der Benutzer, der den Wahlausschuss vertritt, seine Zufälligkeit einbringt.

### Übersicht über das Protokoll

Wenn ein oder mehrere Gleichstände auftreten und der Benutzer, der den Wahlausschuss vertritt, beschließt, das von POLYAS angebotene digitale Losverfahren zu verwenden, werden die folgenden Protokollschritte ausgeführt.

1. Das POLYAS-System generiert einen zufälligen Wert, den System-Startwert (sSeed), und berechnet hieraus einen Prüfwert, indem eine Hash-Funktion angewendet wird. Der resultierende Prüfwert wird dem Benutzer angezeigt, der ihn zum späteren Abgleich speichern sollte.

   Das System generiert sSeed, ohne den Wert des Benutzer-Startwerts zu kennen, der erst im nächsten Schritt bereitgestellt wird. Da das System den Benutzer-Startwert nicht vorhersagen kann, ist es nicht in der Lage, die endgültige Auslosung zu beeinflussen, die von beiden Startwerten abhängt.

Sie haben eine Frage?
Kontaktieren Sie uns gerne:
**support@polyas.de**

**POLYAS GmbH**
Marie-Calm-Str. 1-5
34131 Kassel

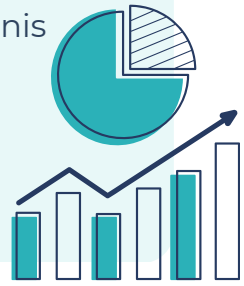
Durch die Anzeige des Prüfwerts ist das System an seinen gewählten Startwert gebunden. Das bedeutet, dass es später nicht in der Lage sein wird, einen anderen Wert zu verwenden, da dieser nicht mit dem angezeigten Prüfwert übereinstimmen würde (dank der Kollisionsresistenz der verwendeten Hash-Funktion).
Technische Anmerkung: Um den Prüfwert für einen gegebenen Wert zu berechnen, wenden wir die SHA-256-Funktion auf die Byte-Darstellung dieses Wertes an (unter der Annahme der UTF-8-Kodierung). SHA-256 ist eine moderne Hashing-Methode, die sowohl Kollisionsresistenz als auch Preimage-Resistenz bietet, die beiden Sicherheitseigenschaften, die für die Zuverlässigkeit unserer Methode erforderlich sind.

2. Der Benutzer wird aufgefordert, seinen zufälligen Startwert, den Benutzer-Startwert (uSeed), bereitzustellen. Beachten Sie, dass der Benutzer zu diesem Zeitpunkt noch keine Kenntnis über den Startwert des Systems hat, obwohl das System bereits durch die Anzeige des Prüfwerts daran gebunden ist. Daher kann der Benutzer das Ergebnis der Auslosung nicht beeinflussen, indem er einen speziell angefertigten Benutzer-Startwert wählt.

3. Die Auslosung wird durch die Startwerte bestimmt. Der System-Startwert (sSeed) und der Benutzer-Startwert (uSeed) werden dann kombiniert, um die Platzierungen für jeden Gleichstandsfall zu bestimmen.

4. Prüfdaten: Der Prüfwert, der System-Startwert (sSeed) und der Benutzer-Startwert (uSeed) sind in der endgültigen Ergebnisdokumentation enthalten, zusammen mit dem Ergebnis der Auslosung. Sie finden Sie in der Auswertungsdatei mit dem Namen “resolved_evaluation” am Ende bzw. auf den letzten Seiten unter “Information für Auditoren”.
Der Benutzer sollte nun seinen gespeicherten Prüfwert mit dem in der Dokumentation enthaltenen Prüfwert vergleichen. Die Einbeziehung dieser Prüfdaten in die Dokumentation ermöglicht eine unabhängige Überprüfung der Korrektheit des Prozesses. Insbesondere kann der Prüfer das Ergebnis neu berechnen, indem er die bereitgestellten Startwerte und den Algorithmus verwendet und durch den Vergleich des neu berechneten Ergebnisses mit dem dokumentierten Ergebnis bestätigen, dass der Prozess korrekt durchgeführt wurde.

[Den Algorithmus des digitalen Losverfahrens finden Sie auch veröffentlicht auf GitHub >]



Sie haben eine Frage?
Kontaktieren Sie uns gerne:
**support@polyas.de**

**POLYAS GmbH**
Marie-Calm-Str. 1-5
34131 Kassel