Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Sektion Politische Rechte

Beschlussprotokoll

15. Sitzung
UAG Neuausrichtung und Wiederaufnahme der Versuche

Datum	Donnerstag, 1. Oktober 2020
Zeit	09:45 – 17:00 Uhr
Ort	Rathaus Bern
Anwesende Mitglieder	- Mirjam Hostettler, BK (Vorsitz) - Oliver Spycher, BK - Aurore Borer, BK - Evelyn Mayer, BK (Protokoll) - Nicolas Fellay, FR - Didier Steiner, FR - Marius Kobi, TG - Barbara Erni, TG - Emilia Nunes, SG - Moritz Zaugg, BE
Anwesende Gäste	- Philippe Oechslin, Objectif sécurité, i.A. der BK - Denis Morel, Post - [redacted] Post - [redacted] Post
Entschuldigt	- Yvonne Schaffner, BS - Philipp Egger, SG - Pascal Fontana, NE - Rico Mazzoleni, GR - Thomas Hardegger, GR - Thomas Wehrli, AG

1. Begrüssung und Einleitung

1.1 Traktanden und Zielsetzung

Die Traktanden und Zielsetzung werden wie vorgeschlagen verabschiedet.

1.2 Verabschiedung Protokoll vom 16./17. September 2020

Die Kantone werden ihre Anpassungsvorschläge für das Protokoll vom 16./17.09.2020 schriftlich einreichen. Die Verabschiedung erfolgt am 20.10.2020.

1.3 Parlamentarische Geschäfte

Behandlung im Ständerat vom 24.09.2020:

- pa. Iv. Müller 18.427: keine Folge gegeben > erledigt
- pa. Iv. Zanetti/Grüter 18.468: keine Folge gegeben > erledigt

- Standesinitiative Genf 19.312: keine Folge gegeben > Nationalrat

Behandlung im Ständerat vom 17.09.2020:

- Mo. Sommaruga 20.3908 > SPK-S

2. Besprechung Massnahmen

Die UAG diskutiert die folgenden Massnahmen:

1.3 Herstellerunabhängige Komponenten

1.4 Vertrauensannahmen Parametergenerierung und Druckprozess

1.6 Einführung zusätzliche Verifizierbarkeit

2.15 Kantonale Verifizierungsprozesse

BK und die Kantone präsentieren ihre Vorarbeiten und Einschätzungen zu den Massnahmen, anschliessende Plenumsdiskussion. Die Resultate der Diskussionen sind in der Tabelle ab S. 4 festgehalten.

3. Wrap-up Massnahmenkatalog

Die UAGNW diskutiert den aktuellen Stand des Massnahmenkatalogs. Insbesondere die folgenden Massnahmen werden diskutiert:

Offenlegung Quellcode

Die UAGNW beschliesst, zur Offenlegung unter Open Source Lizenz keine separate Massnahme im Massnahmenkatalog zu führen. Die Differenz zwischen BK und Kantonen wird unter der Massnahme C.2 (Offenlegung des Quellcodes) aufgeführt.

Bug-Bounty-Programm

Die Kantone und die Post halten fest, dass die Kategorien und Höhe der Entschädigungen von der Post und nicht von der BK festgelegt werden sollen. Falls die BK die Anforderungen festlegt, soll die BK die Finanzierung übernehmen. Die UAGNW beschliesst, dass die Massnahme so angepasst wird, dass die BK die Anforderungen in Absprache mit den Kantonen und Systemanbieter festlegt sowie dass eine Mitfinanzierung des Bundes geprüft wird. Die Post wird der UAGNW eine Kostenschätzung zustellen.

4. Weiteres Vorgehen

Zwischenstand Schlussbericht

Die BK wird den Kantonen am Montag, 05.10.2020 einen aktualisierten Entwurf des Schlussberichts zustellen. Dieser Entwurf umfasst die finalisierten Einleitungskapitel sowie die ausführliche Beschreibung der Massnahmen (mit einigen Ausnahmen) im Kapitel 3. Die Kantone werden gebeten, der BK bis am 09.10.2020 eine Rückmeldung zu diesem Entwurf zukommen zu lassen.

Den Entwurf der Beschreibungen der ausstehenden Massnahmen sowie die Kapitel 4 und 5 wird die BK den Kantonen so rasch als möglich zustellen.

Adressierung der Finanzierungsthematik im Schlussbericht

Die finanziellen Auswirkungen der Massnahmen werden im Schlussbericht pro Massnahme dargelegt. Zusätzlich wird das Thema der Finanzierung dieser Massnahmen sowie der mittel- bis langfristigen Sicherstellung der Finanzierung in einem separaten Kapitel ausführlich behandelt. Dabei soll insbesondere die Problematik der Finanzierung aus Sicht der Kantone dargestellt sowie Möglichkeiten zur Finanzierung aufgezeigt werden. Dem SA VE sind entsprechende Anträge zu stellen.

Grobplanung Neuausrichtung und Wiederaufnahme der Versuche

Die BK hat einen ersten Entwurf für eine Planung der Umsetzung der Massnahmen erstellt (s. Beilage). Die BK geht bei dieser Planung von verschiedenen Annahmen aus (z.B. unabhängige Überprüfung ohne WTO-Ausschreibung, keine Entdeckung erheblicher Mängel im System, Expertinnen und Experten sind im gewünschten Zeitraum verfügbar). Die UAG nimmt zur Kenntnis, dass nach Einschätzung der BK eine Wiederaufnahme der Versuche im November 2021 nicht realistisch ist. Eine Wiederaufnahme im Februar 2022 ist nur möglich, wenn die unterbreitete Zeitplanung mit den getroffenen Annahmen und ohne Verzögerungen umgesetzt werden kann. Die Kantone werden gebeten, der BK eine Rückmeldung zur unterbreiteten Planung zu geben. Die Darstellung der zeitlichen Planung im Schlussbericht bzw. in einem separaten Dokument für den SA VE wird noch geprüft.

5. Zusammenfassung

Nächste Sitzung der UAG

- 20.10., 09:45-17:00 Uhr (ISB, Bern)

Besprechung Massnahmen, Stand vom 01.10.2020

Nr.	Massnahme (gemäss Entwurf BK, 01.10.2020)	Beschreibung (gemäss Entwurf BK, 01.10.2020)	Zeitpunkt Umsetzung	Stand der Diskussionen in der UAGNW
1.	**Weiterentwicklung der Systeme**			
1.3	Einsatz von herstellerunabhängigen Komponenten (Verifier / Kontrollkomponenten)	Die Anforderungen der BK werden so angepasst, dass vollständig verifizierbare Systeme über einen Verifier und eine oder zwei von vier Kontrollkomponenten mit herstellerunabhängiger Software verfügen. Priorität hat eine herstellerunabhängige Kontrollkomponente, die bei der Erzeugung von Prüfcodes zum Einsatz kommt und die Stimmen bis zur Auszählung aufbewahrt. Die Erarbeitung des Pflichtenhefts und allfälliger Grundlagen im Rahmen eines Vorprojekts soll beginnen, sobald die im Sinn von Massnahme A.5/1.4 angepasste Systemspezifikation vorliegt. Ziel ist ein Ersteinsatz der neuen Kontrollkomponente spätestens 3-4 Jahre nach dem Wiedereinsatz.	Unabhängige Online-Kontrollkomponente: 3-4 Jahre nach Wiedereinsatz	Grundsätzlich sind die Kantone der Ansicht, dass in den Bereichen der Massnahmen 1.3, 1.4 und 1.6 zuerst vertiefte Abklärungen zu möglichen Varianten der Umsetzung, den betrieblichen Auswirkungen und den Kosten durchgeführt sowie die Finanzierung sichergestellt werden müssen, bevor über die Umsetzung entschieden werden kann. Insbesondere bei der Massnahme 1.3 (Einsatz unabhängiger Komponenten gehen die Kantone davon aus, dass die Komplexität im Betrieb stark ansteigen würde. Bei der Massnahme 1.4 (Abschwächung Vertrauensannahmen) anerkennen sie den Handlungsbedarf, jedoch ist eine Vertiefung vor dem Entscheid zur Umsetzung notwendig. Bei der Massnahme 1.6 (Public Bulletin Board) sind die Kantone mit der vorgesehenen Vertiefung einverstanden. Die BK teilt die Auffassung wonach die Komplexität infolge Massnahmen 1.3 und 1.4 steigt. Gleichzeitig wurde die Thematik bereits so weit vertieft, dass die Umsetzbarkeit, unter dem Vorbehalt sehr unerwarteter neuer Erkenntnisse, als gegeben erachtet werden darf. Ein Entscheid, diese Massnahmen umsetzen zu wollen, kann und muss jetzt gefällt werden, ein Aufschub wäre unglaubwürdig. Finanzierungsquellen müssen jetzt sichergestellt werden. Auch als Signal nach aussen ist ein solcher Entscheid wichtig. Nicht zuletzt haben die Experten anlässlich des Dialogs klar festgehalten, dass Diversität und Unabhängigkeit als Grundvoraussetzung für vertrauenswürdiges E-Voting gelten müssen. Die Umsetzung von Massnahmen 1.3 und 1.4 sind dazu entscheidend. Demgegenüber ist die BK einverstanden, dass in Bezug auf Massnahme 1.6 elementare Fragen noch offen sind, die es zunächst zu vertiefen gilt.
1.4	Abschwächung der zulässigen Vertrauensannahmen in die Software, die kryptografische Parameter generiert, und den Druckprozess	Es soll mit herstellerunabhängiger Software festgestellt werden können, dass kryptografische Parameter und insbesondere die Prüfcodes zufällig erzeugt wurden. Zur Erreichung der gewünschten Entropie müssen für die Erzeugung privater Werte mindestens vier Kontrollkomponenten zum Einsatz kommen. Stichprobeweise sollen zufällig aus-	Anpassung Software und Prozess: 2 Jahre nach Wiedereinsatz	Die Post hält fest, dass sie für die Umsetzung der Massnahme 1.4 keinen verbindlichen Zeithorizont ankündigen kann. Als erster Meilenstein muss die Post das Krypto-Protokoll anpassen. Dafür würde sie rund 1 Jahr benötigen.

Nr.	Massnahme (gemäss Entwurf BK, 01.10.2020)	Beschreibung (gemäss Entwurf BK, 01.10.2020)	Zeitpunkt Umsetzung	Stand der Diskussionen in der UAGNW
		gewählte Stimmrechtsausweise dahingehend geprüft werden, ob die Werte korrekt im Sinn der überprüften Werte gedruckt wurden. Der angepasste Prozess und die angepasste Software sollen spätestens 2 Jahre nach dem Wiedereinsatz zum Einsatz gebracht werden.	Einsatz unabhängige Software zur Überprüfung der korrekten Parametergenerierung: 2 Jahre nach Wiedereinsatz	Diese Massnahmen haben hohe finanzielle Auswirkungen. Die Kantone halten fest, dass die finanziellen Ressourcen der Kantone beschränkt sind und sie die Kosten der Umsetzung dieser Massnahmen nicht tragen können. Die UAGNW wird im Schlussbericht darlegen, dass die Finanzierung dieser Massnahmen nicht gesichert ist und dass neue Finanzierungsmöglichkeiten geprüft werden müssen. Die UAGNW einigt sich darauf, dass bei allen drei Massnahmen eine Vertiefung als erste Etappe angegeben wird. Diese Vertiefungen sollen die konkrete Umsetzung, die betrieblichen Abläufe, Zuständigkeiten, eine genauere Kostenschätzung und die konkrete zeitliche Planung umfassen. Für die Vertiefungen wird jeweils ein Zeithorizont angegeben, von dem für den Einsatz der Instrumente ausgegangen werden soll. Nach Abschluss der Vertiefungen werden dem SA VE Anträge für das weitere Vorgehen unterbreitet. Die Differenz besteht darin, dass die BK einen Grundsatzentscheid des SA VE, Massnahmen 1.3 und 1.4 umsetzen zu wollen, für nötig hält und Finanzierungsquellen bereits jetzt gesucht werden müssen. Nach Ansicht der BK müsste die Federführung für Massnahmen 1.3 und 1.4 bei den Kantonen liegen, da primär operationelle Fragen der Kantone und der Post sowie Fragen der Zusammenarbeit zwischen den verschiedenen Akteuren mit Relevanz für den Betrieb geklärt werden müssen. Die BK ist einverstanden, dass die Federführung für die Vertiefung der Fragen im Zusammenhang mit Massnahme 1.6 bei der BK liegen müsste. Unter Verweis auf Ressourcenknappheit befürworten die Kantone eine Federführung der BK auch bei den übrigen Massnahmen. Die Federführung für die Vertiefungen zu Massnahmen 1.3 und 1.4 muss weiter diskutiert werden. BK macht einen Anpassungsvorschlag für die Massnahmen.
1.6	Einführung eines zusätzlichen Mechanismus für die Verifizierbarkeit, dessen Wirksamkeit nicht auf den heute geltenden Vertrauensannahmen basiert	Das Ziel besteht darin, den Stimmberechtigten eine Alternative zu den vom Hersteller zur Verfügung gestellten Mitteln für die Überprüfung zu geben. Dazu sollen die Stimmberechtigten mithilfe eines Zweitgeräts (z.B. eines Mobiltelefons) feststellen können, dass ihre Stimme korrekt bei einer oder mehreren vom Hersteller unabhängigen Instanzen angekommen ist. Damit soll die Wirksamkeit der individuellen Verifizierbarkeit nicht von der Vertrauenswürdigkeit der Druckerei oder der Kontrollkomponenten abhängen. Im Rahmen der Überprüfung im Sinn der universellen Verifizierbarkeit soll festgestellt werden können, dass alle bei den unabhängigen Instanzen eingegangenen Stimmen bei der Auszählung mitberücksichtigt wurden. Eine Studie soll Fragen rund um die technische Umsetzung sowie unter Einbezug von Stimmberechtigten Fragen zur Vertrauensbildung und Akzeptanz behandeln: Gestützt auf die Ergebnisse der Studie erarbeiten Bund und Kantone gemeinsam einen Vorschlag für die Modalitäten einer möglichen Umsetzung (technische Umsetzung, Kommunikation, wissenschaftliche Begleitung, Umgang und Verantwortlichkeiten im Zusammenhang mit vermuteten Manipulationen oder mit sonstigen Problemen bei der Überprüfung), einen möglichen Zeitplan für die Einführung sowie eine Kostenschätzung und unterbreitet den Vorschlag der Steuerungsebene zum Entscheid für die Umsetzung.	Abschluss Studie: 1 Jahr nach Wiedereinsatz Antrag auf Umsetzung oder Verzicht: bis 2 Jahre nach Wiedereinsatz	

Nr.	Massnahme (gemäss Entwurf BK, 01.10.2020)	Beschreibung (gemäss Entwurf BK, 01.10.2020)	Zeitpunkt Umsetzung	Stand der Diskussionen in der UAGNW
2.	**Wirksame Kontrolle und Aufsicht**			
2.15	Präzisierung der Anforderungen an die kantonalen Prozesse in Bezug auf die universelle Verifizierbarkeit	Die Anforderungen an die kantonalen Prozesse in Bezug auf die universelle Verifizierbarkeit sind in Ziff. 2 und 4.4 des Anhangs der VEleS geregelt. Diese Anforderungen sollen präzisiert und dabei die folgenden Aspekte berücksichtigt werden: - Wirksamer Einsatz von Prüferinnen und Prüfern - Einbezug der Prüferinnen und Prüfer in den Prozess zur Auszählung der elektronischen Urne - Bereitstellen oder Integration technischer Instrumente, welche von den Prüferinnen und Prüfern bestimmt werden - Behandlung der allfälligen Unregelmässigkeiten, die von den Prüferinnen und Prüfern festgestellt werden - Transparenz gegenüber der Öffentlichkeit in Bezug auf die Verifizierung	Wiedereinsatz	Die BK führt aus, dass die bestehenden Anforderungen, deren Struktur und Aufbau im Anhang der VEleS für die kantonalen Prozesse beim Betrieb von vollständig verifizierbaren Systemen überarbeitet werden müssen. Implizit genannte Anforderungen sollen dabei präziser formuliert werden. Mit dem Inputpapier wird aufgezeigt, wie diese Überarbeitung aussehen soll. Die Kantone möchten auf die Diskussion nicht eintreten. Aus ihrer Sicht steht bei der Wiederaufnahme die erstmalige Umsetzung der kantonalen Prozesse für die vollständige Verifizierbarkeit im Vordergrund. Es besteht daher kein Bedarf für eine Massnahme in diesem Bereich. Die UAGNW kommt zum Schluss, dass für die Überarbeitung keine Massnahme im Massnahmenkatalog aufgeführt werden soll. Die Massnahme wird gestrichen und die BK unterbreitet im Rahmen der VEleS-Revision einen Vorschlag für die Überarbeitung. Die Kantone betonen, dass dabei berücksichtigt werden muss, dass die Verantwortung für die kantonalen Prozesse bei den Kantonen liegt und sie eine Erhöhung der Anforderungen zum jetzigen Zeitpunkt ablehnen. Die BK wird sich beim Entwurf der VEleS-Revision an den heute bestehenden Anforderungen orientieren, welche die Grundsätze regeln und den Kantonen die Ausgestaltung und Umsetzung überlassen.