Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK
Sektion Politische Rechte

Beschlussprotokoll

13. Sitzung
UAG Neuausrichtung und Wiederaufnahme der Versuche

Datum	Mittwoch, 16. September 2020
Zeit	09:45 – 17:00 Uhr
Ort	Informatiksteuerungsorgan des Bundes ISB, Schwarztorstrasse 59, 3003 Bern
Anwesende Mitglieder	- Mirjam Hostettler, BK (Vorsitz) - Oliver Spycher, BK - Aurore Borer, BK - Evelyn Mayer, BK (Protokoll) - Nicolas Fellay, FR - Didier Steiner, FR - Pascal Fontana, NE - Marius Kobi, TG - Barbara Erni, TG - Emilia Nunes, SG - Moritz Zaugg, BE - Rico Mazzoleni, GR - Yvonne Schaffner, BS
Anwesende Gäste	- Philippe Oechslin, Objectif sécurité, i.A. der BK - Christian Folini, i.A. der BK - Denis Morel, Post - [redacted] Post - [redacted] Post
Entschuldigt	- Philipp Egger, SG - 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 02. September 2020

Das Protokoll vom 02.09.2020 wird ohne Änderungen verabschiedet.

1.3 Mitteilungen aus den Kantonen

Der Kanton AG wird nicht mehr an den Sitzungen der UAG teilnehmen können. Der Einbezug des Kantons AG erfolgt zukünftig über die Informationen und den Austausch im PA VE.

1.4 Berichterstattung Sitzung des SA VE vom 14. September 2020

Berichterstattung zur Sitzung des SA VE vom 14.09.2020 durch die BK:

- Der Zwischenbericht der UAG und das Management Summary des Dialogs mit der Wissenschaft wurden zur Kenntnis genommen und verdankt.
- Der SA VE hat im Hinblick auf den Schlussbericht folgende Aspekte festgehalten:
  - Die Ergebnisse aus dem Dialog mit der Wissenschaft müssen in die Arbeiten der UAG einfliessen und im Schlussbericht ausgewiesen werden.
  - Der SA VE nimmt zur Kenntnis, dass der Schlussbericht einige Massnahmen enthalten wird, welche erst nach Verabschiedung des Schlussberichts konkretisiert und ausgearbeitet werden.
  - Im Schlussbericht muss eine zeitliche Planung der Umsetzung der Massnahmen aufgezeigt werden; eine Priorisierung der Massnahmen wäre wünschenswert.
- Zu einzelnen Themen hat sich der SA VE vertieft ausgetauscht. Die wichtigsten Aspekte:
  - Plausibilisierung: Der SA VE befürwortet, dass für den Wiedereinsatz keine Pflicht zur Anwendung einer einheitlichen Methode vorgesehen ist. Sollte in Zukunft eine einheitliche Methode vorhanden sein, ist in diesem Bereich Transparenz anzustreben.
  - Die Limitierung des Elektorats für vollständig verifizierbare Systeme wird als wichtige Massnahme betrachtet. Die Limitierung von 30% des kantonalen und von 10% des nationalen Elektorats soll weiterverfolgt werden.
  - Offenlegung Quellcode: Qualität des Quellcodes muss vor einer erneuten Offenlegung sichergestellt werden.
  - Bug Bounty-Programm: Die Rollen der Akteure im Bug Bounty-Programm sollen geprüft werden, das NCSC könnte sich eine Beteiligung vorstellen.
  - Das Thema der Kommunikation ist wichtig. Der Lead liegt beim Kanton FR.
- Revision VEleS: Bevor die Konsultation der Kantone, Post und Wissenschaft eröffnet wird, möchte der SA VE einen Entwurf der Vorlage diskutieren. Die BK klärt ab, ob und wann dazu eine zusätzliche Sitzung des SA VE vereinbart wird.

1.5 Kommunikation

Die UAG diskutiert, ob vor der Verabschiedung des Schlussberichts weitere Informationen zum Dialog mit der Wissenschaft (namentlich die ausführliche Zusammenfassung und das Management Summary) publiziert werden sollen. Die BK klärt das weitere Vorgehen BK-intern ab und informiert die UAG.

2. Besprechung Massnahmen

Die UAG diskutiert die folgenden Massnahmen:

1.1 Qualität Quellcode / 1.2 Qualitätssicherung Entwicklung / 1.8 Methode Bereitstellung des Systems / 3.2 Transparenz Prüfergebnisse / 3.3 Offenlegung Quellcode / 3.4 Vermehrter Einbezug Öffentlichkeit

BK und die Kantone präsentieren ihre Vorarbeiten und Einschätzungen zu den Massnahmen, anschliessende Plenumsdiskussion. Die Resultate der Diskussionen sind in der Tabelle ab S. 5 festgehalten.

Die Massnahme 3.6 Führung Bug-Bounty-Programm wird auf die Sitzung vom 17.09.2020 verschoben.

3. Zusammenfassung

<u>Nächste Sitzungen der UAG</u>

- 17.09., 10:00-17:00 Uhr (Frauenfeld)
- 01.10., 09:45-17:00 Uhr (Staatskanzlei Bern)
- 20.10., 09:45-17:00 Uhr (ISB, Bern)

Beschlussprotokoll

14. Sitzung
UAG Neuausrichtung und Wiederaufnahme der Versuche

Datum	Donnerstag, 17. September 2020
Zeit	10:00 – 17:00 Uhr
Ort	Grosses Sitzungszimmer, Schlossmühlestrasse 15, 8510 Frauenfeld
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 - Philipp Egger, SG - Rico Mazzoleni, GR
Anwesende Gäste	- Philippe Oechslin, Objectif sécurité, i.A. der BK - Denis Morel, Post - [redacted] Post - [redacted] Post
Entschuldigt	- Moritz Zaugg, BE - Yvonne Schaffner, BS - Thomas Wehrli, AG - Emilia Nunes, SG - Thomas Hardegger, GR - Pascal Fontana, NE

1. Begrüssung und Einleitung

1.1 Traktanden und Zielsetzung

Die Traktanden und Zielsetzung werden wie vorgeschlagen verabschiedet.

2. Besprechung Massnahmen

Die UAG diskutiert die folgenden Massnahmen:

2.2 Kompetenzordnung Konformitätsprüfung

2.3 Konzept Konformitätsprüfung

2.14 Prozess Umgang mit Nicht-Konformitäten

BK und die Kantone präsentieren ihre Vorarbeiten und Einschätzungen zu den Massnahmen, anschliessende Plenumsdiskussion. Die Resultate der Diskussionen sind in der Tabelle ab S. 5 festgehalten.

3. Wrap-up Qualität Quellcode und Entwicklung, Transparenzmassnahmen, unabhängige Überprüfung

Die BK und die Kantone präsentieren ihre Vorarbeiten und Einschätzungen zur Massnahme 3.6 Bug-Bounty-Programm. Plenumsdiskussion der Massnahme 3.6 und Abschlussdiskussion zu allen Massnahmen zur Qualität Quellcode und Entwicklung, Transparenzmassnahmen, unabhängige Überprüfung. Die Resultate dieser Diskussionen sind in der Tabelle ab S. 5 festgehalten.

4. Stand Massnahmenkatalog

Update zu den Zusatzaufträgen

Die BK gibt einen kurzen Überblick zu den ausstehenden Zusatzaufträgen:

- Plausibilisierung: Uwe Serdült erarbeitet ein Papier (Frist Ende Woche).
- Print Office: Das Papier der Post zeigt, dass die mögliche Anforderung umgesetzt werden kann. Das Papier wurde mit Kryptoexperten diskutiert.
- Public Bulletin Board: Vanessa Teague und Olivier Pereira haben ein Papier mit Umsetzungsmöglichkeiten eines Public Bulletin Boards erarbeitet. Anpassungen und abschliessende Rückmeldungen stehen noch aus.

Diskussion der Ergebnisse in der UAG am 01.10.2020.

Massnahmenkatalog

Die BK wird den Massnahmenkatalog für die Sitzung vom 01.10.2020 überarbeiten und bereits diskutierte Umformulierungen unterbreiten. Ausserdem wird die Spalte mit den Kostenschätzungen so weit als möglich ausgefüllt. Zusätzlich zu den bereits geplanten Themen werden an der Sitzung vom 01.10.2020 die folgenden Massnahmen für eine abschliessende Diskussion traktandiert:

- Massnahme 1.7 (Handlungsbedarf: Konkretisierung Analyse System zur Beurteilung der forensic readiness)
- Massnahme 3.6 (Handlungsbedarf: Vorschlag für Internet Test; Rolle der Akteure, insbesondere NCSC)
- Massnahme 2.10 (Diskussion Papier Serdült und allenfalls Anpassung der Massnahme)
- Massnahme 2.11 (Massnahmen in Bewilligungsverfahren abbilden, v.a. unabhängige Überprüfung)

5. Zusammenfassung und weiteres Vorgehen, nächste UAG-Sitzungen

Planung Schlussbericht

Die BK hat der UAG einen aktualisierten Entwurf der Einleitungskapitel zugestellt und bittet um Rückmeldung. Der Schlussbericht wird fortlaufend ergänzt und der UAG für Rückmeldungen zugestellt. Zur zeitlichen Planung vgl. Folien 15/16.

Nächste Sitzungen der UAG

- 01.10., 09:45-17:00 Uhr (Staatskanzlei Bern)
- 20.10., 09:45-17:00 Uhr (ISB, Bern)

Besprechung Massnahmen, Stand vom 16./17.09.2020

Nr.	Massnahme (gemäss Entwurf BK, 16.09.2020)	Beschreibung (gemäss Entwurf BK, 16.09.2020)	Zeitpunkt Umsetzung	Stand der Diskussionen in der UAGNW
1.	**Weiterentwicklung der Systeme**			
1.1	Definieren von Kriterien zur Beurteilung der Qualität des Quellcodes und der entsprechenden Dokumentation	Die Anforderungen in der VEleS in Bezug auf den Quellcode und die entsprechende Dokumentation sollen überarbeitet werden. Dazu werden Kriterien für die Qualität erarbeitet. Mit diesen Kriterien sollen die folgenden Ziele erreicht werden: – Prüfarbeiten und Entdeckung von Mängeln ermöglichen – Prüfung der sicherheitsrelevanten Eigenschaften der Software ermöglichen – Prüfung der Korrektheit und Nachvollziehbarkeit des Quellcodes und der Dokumentation ermöglichen Der Qualitätssicherungsprozess bei der Softwareentwicklung soll sich auf diese Kriterien abstützen. Die Erfüllung dieser Kriterien wird im Bewilligungsverfahren geprüft.	Wiedereinsatz	Die UAG diskutiert die möglichen Kriterien. Aus Sicht der Kantone ist die Beschreibung der Massnahme zu abstrakt gehalten, die effektiven Kriterien sind noch nicht ersichtlich. Die Kantone halten fest, dass diese Kriterien so rasch als möglich vorliegen müssen, damit die Kantone und die Post Klarheit über die Anforderungen und Arbeiten für den Wiedereinsatz haben. Die BK wird die Kriterien für die VEleS-Revision ausarbeiten. Die BK wird der UAG einen Zeitplan für die weiteren Arbeiten unterbreiten. Die Formulierung der Massnahme soll darlegen, dass es sich um eine Präzisierung der bestehenden Anforderungen handelt. Die BK prüft eine Umformulierung der Massnahme.
1.2	Stärkung der Qualitätssicherung im Entwicklungsprozess von E-Voting-Systemen	Die Anforderungen der VEleS im Bereich der Qualitätssicherung im Entwicklungsprozess von E-Voting-Systemen werden überarbeitet. Es sind Prozesse für die Qualitätssicherung zu definieren und anzuwenden, dabei sollen folgende Ziele erreicht werden: – Nachvollziehbarkeit und Kontrolle von Anpassungen – Laufende Nachvollziehbarkeit zwischen den einzelnen Elementen der Dokumentation (Protokoll, Spezifikation, Architektur, etc.) und dem Quellcode – Ergebnisse von Prüfprozessen in die Entwicklung einfliessen lassen – Die Konformität der verschiedenen Systembestandteile und Prozesse mit den entsprechenden Anforderungen gewährleisten Die Umsetzung dieser Prozesse wird im Rahmen des Bewilligungsverfahren geprüft.	Wiedereinsatz	Die UAG ist mit dieser Massnahme mit folgenden Umformulierungen einverstanden: - Nachvollziehbarkeit zwischen der Dokumentation und dem Quellcode muss in beide Richtungen gegeben sein. - Letzten Satz streichen. - Die Formulierung der Massnahme soll darlegen, dass es sich um eine Präzisierung der bestehenden Anforderungen handelt. Die BK macht einen Vorschlag für die Umformulierung der Massnahme.
1.8	Anwendung einer bewährten und nachvollziehbaren Deployment-Methode	Zielsetzungen: – Die Methode zur Bereitstellung des Systems aus dem Quellcode (Deployment) erlaubt es, sicherzustellen, dass die eingesetzte Software mit der publizierten, geprüften und zugelassenen Version übereinstimmt.	Wiedereinsatz	Die UAG ist sich bei der Zielsetzung dieser Massnahme einig und diskutiert den Stand der Arbeiten bei der Post. Es ist davon auszugehen, dass die mit dieser Massnahme vorgesehenen Anforderungen für den Wiedereinsatz erfüllt werden können. Die Formulierung in Bezug auf die Schwachstellen wird so angepasst, dass sich die Aussage auf Schwachstellen bezieht, welche das System

Nr.	Massnahme (gemäss Entwurf BK, 16.09.2020)	Beschreibung (gemäss Entwurf BK, 16.09.2020)	Zeitpunkt Umsetzung	Stand der Diskussionen in der UAGNW
		– Zusätzlich zu dieser Nachvollziehbarkeit soll die Deployment-Methode Manipulationen der Systembestandteile so weit als möglich verhindern. – Es muss verhindert werden, dass mit den eingesetzten Entwicklungsinstrumenten und Bibliotheken Schwachstellen eingeführt werden. Die BK stellt entsprechende Anforderungen an den Systemanbieter.		angreifbar machen. Ausserdem wird auf den Prozess zum Umgang mit Nicht-Konformitäten verwiesen. Die BK macht einen Vorschlag.
2.	**Wirksame Kontrolle und Aufsicht**			
2.2	Anpassung der Zuständigkeiten bei den Konformitätsprüfungen des Systems und der zugrundeliegenden Prozessen	Die bisherigen Anforderungen an die Zertifizierung haben nachweislich nicht gegriffen. Mit der Überarbeitung der Zuständigkeiten bei der Prüfung der Systeme soll die Wirksamkeit und Glaubwürdigkeit der Prüfung sichergestellt werden. Die Unabhängigkeit zwischen der Prüfstelle und der geprüften Stelle spielt hierbei eine wichtige Rolle. Die Aufgabenteilung zwischen Bund und Kantonen soll so angepasst werden, dass der Bund mehr Verantwortung und eine direktere Rolle bei der Prüfung der Systeme übernimmt: – Der Systemanbieter soll für Prüfungen in Bezug auf den Betrieb des Systems in seinen Rechenzentren zuständig sein (Zertifikation ISO 27001 gemäss Ziff. 5.3 Anhang der VEleS) – Der Bund soll für Prüfungen der Erfüllung der Anforderungen in Bezug auf das System und die zugrundeliegenden Prozesse zuständig sein (gemäss Ziff. 5.1, 5.2, 5.3 in Teilen, 5.4, 5.5 und 5.6 Anhang der VEleS) Für die Überprüfungen sind unabhängige Expertinnen und Experten zu mandatieren.	Wiedereinsatz	Die UAG ist sich einig, dass die unabhängigen Überprüfungen in Zukunft von der BK in Auftrag gegeben werden sollen (mit Ausnahme von ISO 27001 gemäss Ziff. 5.3 Anhang der VEleS). Der UAG ist wichtig, dass die Auswirkungen der neuen Zuständigkeiten auf den Ablauf des Bewilligungsverfahrens diskutiert werden. Die unabhängige Überprüfung soll vor dem Bewilligungsverfahren stattfinden. Die Kantone betonen, dass es wichtig ist, dass sich die BK frühzeitig und verbindlich dazu äussert, ob das System den gesetzlichen Anforderungen entspricht. Die Verantwortung für die unabhängige Überprüfung liegt bei der BK. Sobald diese über die Ergebnisse der Überprüfung verfügt, soll sie sich dazu äussern, denn zu diesem Zeitpunkt sind sämtliche für die Einschätzung der BK erforderlichen Informationen vorhanden. Diese Einschätzung kann aus Sicht der Kantone nicht erst mit dem Entscheid über die Grundbewilligung erfolgen. Aus Sicht der Kantone ist es unter dem geltenden Recht möglich, die Beurteilung dieses Aspekts der Bewilligung vorzuziehen. Diese Beurteilung ist nicht von den Gegebenheiten in den Kantonen abhängig und für alle Kantone gleich. Es würde sich um eine Art Vorentscheid der BK handeln. Den Regierungen der Kantone muss zum Zeitpunkt ihrer Entscheide über die Einreichung eines Gesuchs die Einschätzung der BK über das System vorliegen. Die BK hält fest, dass sie dem Grundbewilligungsentscheid des Bundesrates nicht vorgreifen kann. Allfällige Mängel könnten womöglich erst im Gesamtkontext, d.h. in Kenntnis der im Rahmen des Gesuchs eingereichten Risikobeurteilung beurteilt werden, Die BK schlägt vor, dass sie sich während den Prüfungen laufend mit den Kantonen austauschen und die Prüfberichte zustellen wird. Die BK wird ihre ersten Einschätzungen zu den Prüfergebnissen mit den Kantonen teilen.

Nr.	Massnahme (gemäss Entwurf BK, 16.09.2020)	Beschreibung (gemäss Entwurf BK, 16.09.2020)	Zeitpunkt Umsetzung	Stand der Diskussionen in der UAGNW
				Die BK präzisiert auf Nachfrage die folgenden Aspekte: - Die BK nimmt eine unabhängige Prüfung vor, wenn ein Kanton eine Absichtserklärung zum Einsatz dieses Systems einreicht. - Eine erste Prüfung des Post-Systems erfolgt für den Wiedereinsatz; erneute Prüfungen werden durch wesentliche Änderungen des Systems ausgelöst. - Ist das System bereits geprüft, können weitere Kantone dieselbe Version einsetzen, ohne dass eine erneute Prüfung notwendig ist. - Im Bewilligungsverfahren werden die weiteren Unterlagen der Kantone (Risikobeurteilungen, rechtliche Grundlagen, Budget, etc.) geprüft. Die BK erstellt ein Schema, um diese Prozesse darzustellen.
2.3	Erarbeitung eines Prüfkonzepts für die Beurteilung der Konformität des Systems und der zugrundeliegenden Prozesse	Basierend auf den angepassten Zuständigkeiten bei der Überprüfung des Systems und der Prozesse gemäss Massnahme 2.2 wird ein Prüfkonzept erstellt. Das Prüfkonzept wird so ausgestaltet, dass eine umfassende Prüfung der Sicherheitsanforderungen gewährleistet wird. Die Zuständigkeit liegt bei der BK, um die Kohärenz sicherzustellen und Schwierigkeiten bei der Auslegung zu vermeiden. Die BK kann dazu externe Expertinnen und Experten beiziehen. Das Konzept soll u.a. die folgenden Aspekte vorsehen: – Klare Definition der Prüftiefe der verschiedenen Bereiche in Bezug auf deren Geltungsbereich und Gültigkeitsdauer – Durchlässigkeit zwischen den verschiedenen Prüfbereichen, um ungeprüfte Stellen zu vermeiden – Einbezug von qualifizierten und unabhängigen Expertinnen und Experten – Publikation der Prüfberichte	Wiedereinsatz	Die UAG ist mit dem Inhalt der Massnahme einverstanden. Die BK wird eine zeitliche Planung für die Umsetzung dieser Massnahme unterbreiten.
2.14	Erarbeitung und Umsetzung eines Prozesses zum Umgang mit Nicht-Konformitäten	Die BK erarbeitet einen Prozess zum Umgang mit Nicht-Konformitäten in Bezug auf die Anforderungen. Dieser Prozess soll auch bei vermuteten Nicht-Konformitäten umgesetzt werden. Ziel ist es, im Umgang mit Nicht-Konformitäten Unklarheiten so weit als möglich zu vermeiden und einen Einsatz von E-Voting sicherzustellen, bei dem die Anforderungen der VEleS erfüllt werden. In diesem Prozess werden folgende Aspekte definiert: - Definition von Nicht-Konformitäten	Wiedereinsatz	Die UAG ist sich zu dieser Massnahme einig.

Nr.	Massnahme (gemäss Entwurf BK, 16.09.2020)	Beschreibung (gemäss Entwurf BK, 16.09.2020)	Zeitpunkt Umsetzung	Stand der Diskussionen in der UAGNW
		- Festlegen von Kriterien, die im Umgang mit Nicht-Konformitäten angewendet werden - Regelung der Akteure und deren Rollen		
3.	**Stärkung der Transparenz und des Vertrauens**			
3.2	Publikation bewilligungsrelevanter Prüfberichte	Bund, Kantone und Systemanbieter sollen gegenüber der Öffentlichkeit Transparenz in Bezug auf Prüfergebnisse schaffen. Berichte, Belege und Zertifikate, die im Rahmen der Prüfungen gemäss Ziffer 5 des Anhangs der VEleS erstellt werden, sind zu publizieren. Weitere Unterlagen, die für deren Nachvollziehbarkeit sowie den Bewilligungsentscheid notwendig sind, sind ebenfalls zu publizieren. Es ist zu prüfen, ob auch Repliken publiziert werden sollen, welche die geprüfte Organisation in Bezug auf die publizierten Prüfberichte erstellt.	Wiedereinsatz	Die UAG ist sich einig, dass in Bezug auf bewilligungsrelevante Prüfberichte mehr Transparenz geschaffen werden soll. Zielpublikum der Publikationen sind primär Fachkreise; die breite Öffentlichkeit ist mittelbares Zielpublikum. Diskussion des Geltungsbereichs: - Es sollen alle Prüfberichte publiziert werden, auch wenn sie keine oder nur unerhebliche Findings enthalten. - Für den Wiedereinsatz wird vorgesehen, dass nur bewilligungsrelevante Prüfberichte publiziert werden. Eine Ausweitung auf weitere Unterlagen kann zu einem späteren Zeitpunkt wieder thematisiert werden. - Die Prüfberichte müssen nachvollziehbar sein. Wird in den Prüfberichten auf weitere Unterlagen verwiesen, müssen diese öffentlich zugänglich sein, ausser es besteht ein Grund zur Ausnahme. Eine kurze Beschreibung der Punkte aus den Unterlagen, die nicht veröffentlicht werden können, aber im Prüfbericht berücksichtigt sind, hilft, die Nachvollziehbarkeit zu erhalten. - Von der Publikation soll in begründeten Fällen abgesehen werden können (z.B. aufgrund Erhöhung eines Risikos, Datenschutz, interne Sicherheitsrichtlinien, Geschäftsgeheimnisse, etc.). Die Ausnahmen werden in die Massnahme aufgenommen. Die Publikation der Prüfberichte ist im ganzen Prozess zur Mandatierung zu berücksichtigen. Die Publikation ist bereits zum Zeitpunkt der Mandatsvergabe mit den Mandatsträgern zu thematisieren. Vor der Publikation eines Schlussberichts können sich die Mandatsträger und die geprüfte Stelle austauschen. Repliken auf publizierte Prüfberichte sollen publiziert werden.
3.3	Präzisierung der Anforderungen der Bundeskanzlei an die Offenlegung des Quellcodes	Die Erfahrungen mit der Offenlegung des Quellcodes des Post-Systems haben gezeigt, dass eine Präzisierung der Anforderungen der BK notwendig ist. Die Anforderungen an die zu publizierenden Unterlagen sollen insbesondere folgende Aspekte umfassen:	Wiedereinsatz	Die Frage, ob der Quellcode eines E-Voting-Systems unter eine Open-Source-Lizenz (OSL) gestellt werden muss, wird in der UAGNW vertieft und kontrovers diskutiert.

Nr.	Massnahme (gemäss Entwurf BK, 16.09.2020)	Beschreibung (gemäss Entwurf BK, 16.09.2020)	Zeitpunkt Umsetzung	Stand der Diskussionen in der UAGNW
		- Quellcode, Dokumentation der gesamten Software, Dateien mit relevanten Inputparametern sind offenzulegen. - Hilfestellungen und ergänzende Dokumentationen sind zu publizieren, so dass Dritte das System in der eigenen Infrastruktur effizient kompilieren, in Betrieb nehmen und analysieren können. - Dokumentationen zur Infrastruktur, Drittsoftware und Betriebsprozesse sind so weit als möglich zu publizieren. Zumindest die wesentlichen Elemente sind zusammenfassend zu beschreiben. - Die Darstellung der offengelegten Unterlagen entspricht der gängigen Praxis Es gelten folgende Anforderungen in Bezug auf die Nutzungsbedingungen: - Der Zugang zum Quellcode wird unentgeltlich und anonym gewährt. Es wird darauf verzichtet, Personen, die auf die offengelegten Informationen zugreifen möchten, zur Preisgabe ihrer Identität aufzufordern. - Der Quellcode darf für ideelle und namentlich wissenschaftliche Zwecke genutzt werden. Dazu gehört der Austausch bei der Fehlersuche sowie das Recht zu publizieren. Dieses Recht wird explizit eingeräumt. - Rechtliche Ahndung von Zuwiderhandlungen erfolgt höchstens bei kommerzieller Verwendung und allenfalls bei der Durchführung grösserer Urnengänge. Die Ahndung von Zuwiderhandlung in anderen Bereichen wird explizit ausgeschlossen. - In den Lizenzbestimmungen ist auf die Nutzungsbedingungen hinzuweisen, auf Willenserklärungen der Nutzenden ist wenn möglich zu verzichten. Zu diskutieren: Open Source oder Massnahmen, die einem allfälligen Verzicht auf eine Open Source Lizenz kompensieren könnten.		<u>Dialog mit der Wissenschaft:</u> Die Expertinnen und Experten erachten eine Offenlegung des Quellcodes unter einer OSL als erfolgsversprechender als eine Publikation unter proprietärer Lizenz. Mit einer OSL können die Ziele von Transparenz, öffentlicher Überprüfung, Vertrauen der Öffentlichkeit und Aufbau einer Community von Fachpersonen wirksamer erreicht werden. Eine Offenlegung unter einer proprietären Lizenz kann auch zur Erreichung dieser Ziele führen, jedoch nicht in demselben Ausmass. Die Expertinnen und Experten empfehlen eine Open-Source-Publikation auch deshalb, weil damit v.a. die kryptografischen Elemente in anderen Anwendungen eingesetzt und weiterentwickelt werden können. Von einer solchen Weiterverwendung könnten die Entwicklung und die Sicherheit von E-Voting-Systemen profitieren. <u>Einschätzung der Kantone:</u> Die Kantone lehnen es ab, für E-Voting eine OSL zu verlangen. Die Post kann und will ihr E-Voting-System nicht unter eine OSL stellen. Wird eine OSL verlangt, zieht sich die Post zurück. Damit gäbe es kein E-Voting-System mehr. Hätten die Kantone heute die Wahl zwischen einem System mit OSL und einem System ohne OSL, dürften sie das System mit OSL wählen. Allerdings ist diese Fragestellung hypothetisch, weil es kein System mit OSL gibt. OSL könnte nur dann einen Zusatznutzen schaffen, wenn sich eine Community heranbildet, die sich aktiv an der Weiterentwicklung des Codes beteiligt. Die Kantone bezweifeln sowohl, dass OSL einen erheblichen Zusatznutzen schafft, als auch, dass sich eine Community bilden wird. Eine OSL bietet nicht per se mehr Sicherheit: Beim Genfer System (CHVote) hat sich keine Community gebildet, und beim OSL-Projekt openSSL blieb eine Sicherheitslücke zwei Jahre unentdeckt (Heartbleed). Es fehlt eine Rechtsgrundlage dafür, OSL für E-Voting vorzuschreiben. Eine solche Verpflichtung stellte zudem eine hohe Markteintrittshürde dar und wäre aus regulatorischer Sicht problematisch. <u>Einschätzung der Post:</u> Das E-Voting-System der Post ist proprietär. Die Post erteilt dafür zurzeit keine OSL. Sie beabsichtigt auch nicht, dies in absehbarer Zeit zu tun, da ihr dies aus rechtlichen, tatsächlichen und ökonomischen Gründen nicht möglich ist. Die Post müsste für OSL entschädigt werden. Die Kosten wären sehr hoch.

Nr.	Massnahme (gemäss Entwurf BK, 16.09.2020)	Beschreibung (gemäss Entwurf BK, 16.09.2020)	Zeitpunkt Umsetzung	Stand der Diskussionen in der UAGNW
				<u>Einschätzung der BK:</u> Die BK erkennt die Vorteile aber keine materiellen Punkte, die gegen Open-Source sprechen. Aus materieller Sicht müsste die Software unter eine OSL gestellt werden. Wenn die Software oder Teile davon in anderen Projekten zum Einsatz kommen würde, beispielsweise bei Wahlen in einem anderen Land, profitiert die Schweiz von den Überprüfungen, die dort gemacht werden. Dies steht im Einklang mit der Empfehlung aus dem Dialog mit der Wissenschaft, dass kryptographische Bausteine standardisiert werden sollen, Dabei könnte schrittweise vorgegangen werden. Dahingehende Verbindlichkeiten sind aber zu schaffen. Die Offenlegung allein des Verifiers unter OSL dürfte ungeeignet sein, um Erfahrungen zu sammeln, da die wiederverwendbaren Schlüsselelemente, wie beispielsweise das Mixnet im Verifier nicht enthalten sind. Wie allfällige Verpflichtungen der Post gegenüber Scytl sowie kommerzielle Interessen zu gewichten sind, muss der Steuerungsebene überlassen werden. Die UAG einigt sich darauf, dass es sich bei diesem Thema im Fall des Post-Systems letztlich um einen politischen Entscheid handelt. Die UAG soll im Schlussbericht die Differenzen z.H. des SA VE ausweisen. Die BK wird ausserdem eine Umformulierung und Kürzung der Massnahme vorschlagen. Dabei wird insbesondere die Formulierung der «grösseren Urnengänge» angepasst (Urnengänge zu Testzwecken sind erlaubt).
3.4	Vermehrter Einbezug der Öffentlichkeit	Bund, Kantone und Systemanbieter erstellen ein Konzept, um einen vermehrten Einbezug der Öffentlichkeit sicherzustellen. Dabei soll nebst Politik, Fachkreisen und Interessensverbänden auch ein Fokus auf die breite Öffentlichkeit gelegt werden. In diesem Konzept sind Vorhaben zur aktiven Kommunikation vorzusehen. Dazu können beispielsweise folgende Aktivitäten vorgesehen werden: - Durchführung und Beteiligung an Informations- und Diskussionsveranstaltungen (Konferenz für Politik, Parteien, Verbände und die Wissenschaft; E-VoteID-Konferenz in Bregenz) - Ideenwettbewerbe (bspw. für Social-Engineering-Attacken) und Hackathons - Betreiben einer Informationsplattform	Konzept: Wiedereinsatz	Die UAG ist mit dem Inhalt dieser Massnahme einverstanden. Die Beschreibung wird gekürzt (Beispiele im Schlussbericht aufführen). Bis zum Wiedereinsatz soll ein Konzept vorliegen, ausserdem ist die Umsetzung erster Aktivitäten zu prüfen.

Nr.	Massnahme (gemäss Entwurf BK, 16.09.2020)	Beschreibung (gemäss Entwurf BK, 16.09.2020)	Zeitpunkt Umsetzung	Stand der Diskussionen in der UAGNW
3.6	Führung eines ständigen Bug-Bounty-Programms	Zum Einbezug von unabhängigen Personen wird zum offengelegten Quellcode und der Dokumentation von E-Voting-Systemen ein ständiges Bug-Bounty-Programm geführt. Dieses soll u.a. folgende Anforderungen erfüllen: - Das Bug-Bounty-Programm läuft grundsätzlich ununterbrochen und die Offenlegung von Mängeln ist in Abhängigkeit von der Kritikalität finanziell zu entschädigen. - Es reicht, Fehler anhand des Quellcodes aufzuzeigen. Für eine Entschädigung muss kein erfolgreicher Angriff aufgezeigt werden (Teilnehmende können den Quellcode in der eigenen Infrastruktur anhand des laufenden Systems analysieren; vgl. Massnahme 3.3). - Angriffe auf die Infrastruktur des Anbieters müssen erlaubt sein. Die Zielsetzung dieses Tests besteht im Eindringen in die Infrastruktur. DOS- und Social-Engineering-Angriffe müssen ebenfalls behandelt werden. Dies kann unabhängig vom Bug-Bounty-Programm erfolgen, im Fall von DOS-Angriffen auch im geschlossenen Rahmen). Zuständigkeiten und Umgang mit Meldungen: - Der Systemanbieter ist für das Programm zuständig. Er ermöglicht dessen Durchführung und nimmt Meldungen entgegen. Er kategorisiert die Meldungen und informiert die betroffenen Teilnehmenden über seine begründeten Entscheidungen. Er publiziert sämtliche Meldungen mit einem bestätigten Befund. - Der Systemanbieter reagiert auf die Meldungen und trifft Massnahmen. - Der BK obliegt die Oberaufsicht. Sie legt die Anforderungen fest und gibt die Kriterien für die Kategorisierung der Meldungen vor. Sind Teilnehmende mit der Entscheidung des Systemanbieters nicht einverstanden, können sie sich an die BK wenden. - Bund und Kantone erhalten uneingeschränkten Zugriff auf die Meldungen und Antworten des Systemanbieters. Im Rahmen der Bewilligungsverfahren ist eine Zusammenfassung der Meldungen und der geplanten / getroffenen Massnahmen einzureichen.	Wiedereinsatz	Die UAG ist sich einig, dass ein Programm zur Fehlersuche grosse Vorteile bietet (Aufbau Community, Weiterentwicklung System). Das vorgeschlagene Bug-Bounty-Programm soll drei Bereiche umfassen (s. Folie Post): Internet Test, dynamische Fehlersuche und statische Fehlersuche. Die UAG ist sich einig, dass zu den Bereichen der dynamischen und statischen Fehlersuche ein öffentliches und ständiges Programm geführt werden soll. Im Bereich des Internet Tests ist man sich einig, dass es sich dabei um eine gute Transparenzmassnahme gegenüber der Öffentlichkeit handelt. Obwohl die Entdeckung gravierender Sicherheitslücken im Rahmen dieses Internet Tests nicht wahrscheinlich ist, ist die Durchführung eines solchen Internet Tests wichtig. Es muss noch diskutiert werden, ob in diesem Bereich ein ständiges Programm notwendig ist oder wiederkehrende Tests sinnvoller wären. Allenfalls könnten isolierte Events kommunikativ besser aufbereitet werden und würden weniger Kosten verursachen. Aus Sicht der BK ist eine finanzielle Entschädigung notwendig, um einen breiten Einbezug externer Fachkreise sicherzustellen. Die Kantone und die Post bringen an, dass die finanziellen Auswirkungen eines solchen Programms kaum abschätzbar sind. Die BK hält fest, dass wertvolle Meldungen honoriert werden sollen, dass aber zum Beispiel kleine Findings ausgeschlossen werden könnten. Nach grossen Findings ist ein Abbruch des Bug-Bounty-Programms ohnehin wahrscheinlich, sodass auch die Kosten im kontrollierbaren Rahmen bleiben. Ausserdem könnte sich die Höhe der Entschädigungen an anderen Programmen orientieren (wie z.B. PIT). Die BK wird auch noch mit dem Nationalen Zentrum für Cybersicherheit NCSC dessen Rolle im Bug-Bounty-Programm klären. Die Post klärt ab, wie hoch die zusätzlichen Kosten für die Post wären. Sie bringt auch die Idee ein, dass nicht die Meldung von Fehlern, sondern Findings mit konkreten Vorschlägen für die Behebung von Fehlern entschädigt werden könnte. In der Massnahme soll präzisiert werden, dass DDOS- und Social Engineering-Angriffe ausgeschlossen sind. Die BK passt die Formulierung der Massnahme an und unterbreitet eine gekürzte Fassung der Beschreibung.

Nr.	Massnahme (gemäss Entwurf BK, 16.09.2020)	Beschreibung (gemäss Entwurf BK, 16.09.2020)	Zeitpunkt Umsetzung	Stand der Diskussionen in der UAGNW
		Die Nutzungsbedingungen sind wie folgt auszugestalten: - Eine Teilnahme ist anonym möglich. - Publikationen zu Mängeln sind erlaubt. - Es gelten Regeln im Sinn einer «responsible disclosure». Namentlich können die Teilnehmenden aufgefordert werden, Mängel umgehend zu melden, eine maximale Sperrfirst für Publikationen einzuhalten und mit Informationen zu vermuteten Mängeln verantwortungsvoll umzugehen.		