



## Beschlussprotokoll

### 9. Sitzung

### UAG Neuausrichtung und Wiederaufnahme der Versuche

<b>Datum</b>	Donnerstag, 18. Juni 2020
<b>Zeit</b>	08:30 – 11:30 Uhr
<b>Ort</b>	Videokonferenz
<b>Anwesende Mitglieder</b>	<ul style="list-style-type: none"><li>- Mirjam Hostettler, BK (Vorsitz)</li><li>- Oliver Spycher, BK</li><li>- Aurore Borer, BK</li><li>- Evelyn Mayer, BK (Protokoll)</li><li>- Nicolas Fellay, FR</li><li>- Didier Steiner, FR</li><li>- Pascal Fontana, NE</li><li>- Marius Kobi, TG</li><li>- Barbara Erni, TG</li><li>- Emilia Nunes, SG</li><li>- Moritz Zaugg, BE</li><li>- Rico Mazzoleni, GR</li><li>- Yvonne Schaffner, BS</li></ul>
<b>Anwesende Gäste</b>	<ul style="list-style-type: none"><li>- Christian Folini, netnea AG, i.A. der BK</li><li>- Philippe Oechslin, Objectif sécurité, i.A. der BK</li><li>- Denis Morel, Post</li><li>- [REDACTED] Post</li><li>- [REDACTED] Post</li></ul>
<b>Entschuldigt</b>	<ul style="list-style-type: none"><li>- Philipp Egger, SG</li><li>- Thomas Wehrli, AG</li></ul>

#### 1. Begrüssung und Einleitung

##### 1.1 Traktanden und Zielsetzung

Die Traktanden und Zielsetzung werden wie vorgeschlagen verabschiedet.

##### 1.2 Verabschiedung Protokoll vom 20. Mai 2020

Das Protokoll vom 20. Mai 2020 wird ohne Änderungen verabschiedet.

#### 2. Präsentation aktueller Stand Dialog mit der Wissenschaft

Die BK und Christian Folini präsentieren den aktuellen Stand des Dialogs mit der Wissenschaft. Auf der Plattform sind die Diskussionsblöcke 1-5 aufgeschaltet; die Diskussionsblöcke 6-12 werden in nächster Zeit lanciert. Einige Expertinnen und Experten beteiligen sich sehr aktiv, andere eher punktuell. Pro Woche werden momentan rund 50 Kommentare erfasst, die in vielen Fällen gut vorbereitet und von hoher Qualität sind. Die Diskussionen sind zeitintensiv und der Dialog wird in den nächsten Wochen noch intensiver

geführt werden müssen, damit alle Themen abgeschlossen werden können. Der Dialog auf der Plattform läuft noch bis zum 10. Juli 2020, anschliessend wird eine Zusammenfassung erarbeitet.

Die BK hat an der letzten Sitzung die Diskussionsblöcke 1 «Wirksamkeit der Kryptografie» und 2 «Herstellerunabhängige Komponenten» vorgestellt. Die BK präsentiert die laufenden Diskussionsblöcke 3-5:

#### Diskussionsblock 3 «Druckerei / Parametergenerierung»

Der Diskussionsblock 3 basiert auf Massnahme 1.4 des Massnahmenkatalogs. Diese hat zum Ziel, dass in Zukunft den Druckereien weniger vertraut werden muss. Dies kann beispielsweise mit einer verifizierbaren und verteilten Parametergenerierung erreicht werden. Einige Lösungsvorschläge wie zum Beispiel das Drucken auf verschiedenen Druckmaschinen sind in der Umsetzung komplex und hätten grosse Auswirkungen auf die Prozesse und Kosten.

Die BK hat deshalb den Expertinnen und Experten auf der Plattform zwei Lösungsvorschläge für eine künftige Regulierung unterbreitet, wobei der eine höchstens als Überbrückungsmassnahme gelten könnte.

Die Expertinnen und Experten sehen in der verifizierbaren und verteilten Parametergenerierung eine Notwendigkeit. Die Überbrückungsmassnahme wurde nicht kommentiert; es gibt dabei wohl zu wenig Mehrwert im Bereich Sicherheit. Den eigentlichen Lösungsvorschlag der BK haben die Expertinnen und Experten kaum bewertet. Es scheint, als würden die Expertinnen und Experten noch weiter gehen wollen mit den Anforderungen, indem sie den Druckprozess auf mehrere Druckmaschinen verteilen würden (Lösungsansätze Ford und Perrig), was mit den vorhandenen finanziellen Mitteln kaum umsetzbar wäre. Die Antworten auf den Lösungsvorschlag der BK müssen noch vertieft werden. Die BFH und die Post haben den Auftrag erhalten, eine Lösung zu skizzieren, die mit dem besprochenen Vorschlag für die Regulierung im Einklang steht. Weitere Experten haben den Auftrag erhalten, die Lösungen bis August zu prüfen und zu kommentieren.

#### Diskussionsblock 4 «Public Bulletin Board»

Das Public Bulletin Board würde eine vom Systemanbieter unabhängige Verifizierung bieten. Zusätzlich zu den heutigen Prüfcodes könnte der Stimmberechtigte z.B. mit dem Mobiltelefon einen QR-Code scannen und damit eine unabhängige Bestätigung der korrekt erfassten Stimme abholen. Die Software für diese Bestätigung muss vom Systemanbieter unabhängig sein (Entwicklung und Support). Der Stimmberechtigte müsste damit keiner Komponente des Systemanbieters mehr vertrauen und stattdessen beliebige Software verwenden.

Insgesamt haben sich die Expertinnen und Experten positiv geäussert und bestätigen, dass ein Public Bulletin Board zum Vertrauen der Bevölkerung beitragen könnte. Allerdings sagen die Experten klar: Die Lösung muss gut umgesetzt werden. Einige Experten haben angegeben, dass Public Bulletin Boards im Ausland bereits eingesetzt werden (z.B. Australien, Norwegen). Für die Schweiz müsste eine individuelle Lösung gefunden werden, wie die BK festhält. Einige problematische Bereiche wie die Wahrung des Stimmgeheimnisses, Einfluss zukünftiger Entwicklungen (wie z.B. Quantencomputer) und die öffentliche Sichtbarkeit der Anzahl abgegebenen Stimmen müssen bei der Lösungsfindung berücksichtigt werden. Die Einführung eines Public Bulletin Boards müsste auch auf kommunikativer Ebene begleitet werden. Die Stimmberechtigten müssten in der Benutzung instruiert und über die Wirksamkeit und Wichtigkeit der bisherigen und der zusätzlichen Möglichkeit zur Verifizierung informiert werden.

Die BK hat Pereira / Teague beauftragt, ein Papier zu Umsetzungsmöglichkeiten mit ihren Vor- und Nachteilen und Kostenschätzungen zu erstellen. Die BFH und Basin / Capkun, ev. weitere Experten, werden Pereira / Teague unterstützen; zur Vertiefung der Themen Benutzerfreundlichkeit, Kommunikation, Vertrauen und Wahrnehmung in der Öffentlichkeit wird sich Serdült und ev. weitere Experten beteiligen. Diese Arbeiten sollen der UAG eine genügende Grundlage für einen Entscheid in diesem Bereich bieten. Der weitere Dialog in der UAG zum Thema Public Bulletin Board wird gemäss BK ergebnisoffen sein.

#### Diskussionsblock 5 «Unabhängige Überprüfung»

Die BK gibt einen kurzen Überblick zu den Fragestellungen bei den unabhängigen Prüfungen. Insbesondere wird diskutiert, wer unabhängige Überprüfungen in Auftrag geben soll und welche Bereiche in welcher Tiefe geprüft werden sollen. Die BK führt aus, dass die Expertinnen und Experten darauf hinweisen, dass der Bund die Prüfungen in Auftrag geben soll und dass dabei nicht nur die kryptografischen Elemente,



sondern insbesondere auch auf deren Umsetzung ein besonders starker Akzent gelegt werden muss. Eine Vertiefung der Diskussionen ist v.a. im Bereich der Akzeptanz von Non-Konformitäten notwendig.

### 3. Berichterstattung UAG und Fahrplan

#### Zwischenbericht für SA VE

Die BK stellt den Aufbau des Zwischenberichts vor und verdankt die Rückmeldungen der Kantone. Weiteres Vorgehen:

- Finale Rückmeldungen der Kantone bis am 18.06., nachmittags.
- Versand an SA VE, sobald die definitive Fassung vorliegt.
- Übersetzung auf Französisch wird Anfang der Woche vom 22.06. verschickt.

Die Aussage der BK im Zwischenbericht, dass die BK den Stand der Arbeiten bei der Post nicht kennt, wird diskutiert. Die BK hält fest, dass sie im Rahmen der Präsentationen der Post in der UAG über die Arbeiten informiert wurde. Die wesentlichen Punkte sind jedoch unbekannt und können deshalb nicht beurteilt werden. Die Kernfragen zu Verbesserungsmassnahmen, deren Umsetzung im Quellcode, in der Spezifikation und in den Prozessen können nur aufgrund der Einsichtnahme in die entsprechenden Unterlagen beurteilt werden. Solche liegen der BK nicht vor. Die Kantone betonen, dass die Post Vertragspartnerin der Kantone ist. Die Kantone sind verantwortlich dafür, dass die BK die notwendigen Informationen erhält.

#### Planung der anstehenden UAG-Arbeiten und Berichterstattung

Die BK präsentiert den Zeitplan für die anstehenden Arbeiten (vgl. Folien 13-14). Weitere UAG-Sitzungen sind für den Zeitraum Juli-Oktober 2020 geplant. Eine entsprechende Doodle-Umfrage wurde verschickt. Es sind ganztägige Workshops in Bern geplant (1 x August, 3 x September, 2 x Oktober). Sobald die Sitzungstermine festliegen, wird die Planung der zu behandelnden Themen konkretisiert und laufend angepasst. Für die Sitzung des SA VE vom 14. September wird ein weiterer Zwischenbericht erarbeitet, der Schlussbericht soll an der Sitzung vom 06. November vorgelegt werden. Die UAG hält fest, dass die Arbeiten in der UAG weiterhin und so weit als möglich parallelisiert werden.

### 4. Kommunikation

Die BK informiert über die Medienmitteilung, die am 22. oder 23.06.2020 mit der Liste der Expertinnen und Experten und dem Fragebogen publiziert wird. Die Medienmitteilung wurde der UAG zur Information zugestellt, sie wird auch dem SA VE zugestellt. Die Kantone bringen das Anliegen ein, dass sie stärker in die Kommunikationsmassnahmen einbezogen werden. Die BK hält fest, dass das Thema der Kommunikation im Juni unter den Staatsschreiberinnen und -schreibern thematisiert wird, die Rollen von Bund und Kantonen jedoch unterschiedlich sind und dies auch in der Kommunikation zu berücksichtigen ist.

### 5. Weiteres Vorgehen und Varia

#### Parlamentarische Geschäfte

Die BK gibt einen kurzen Überblick zum Stand der parlamentarischen Geschäfte auf Stufe Bund:

- Ip. Grüter 20.3475 «Abhängigkeiten und Ungereimtheiten beim E-Voting-System der Post»: eingereicht am 02.06.2020. Beantwortung durch den BR bis zur Herbstsession (Federführung beim GS-UVEK)
- Mo. Zanetti (E-Versand): Beratung im SR am 18.06.2020; einstimmig abgelehnt.
- pa. Iv. Müller, pa. Iv. Zanetti und Standesinitiative GE: Anhörung der SSK in der SPK-S am 18.08.2020

#### Termine nächste Sitzungen der UAG:

Doodle-Umfrage wurde verschickt.