CH++

Olga Baranova, Geschäftsleiterin CH++
Hannes Gassert, Präsident CH++
hello@chplusplus.org

Kommission für Rechtsfragen Nationalrat RK-N
Bern, 18. Januar 2024

Sehr geehrte Nationalrätinnen und Nationalräte,

CH++ ist eine zivilgesellschaftliche Organisation, die sich für mehr und schnellere Handlungsfähigkeit in der Schweizer Politik und Verwaltung durch Technologie und Wissenschaft einsetzt. Wir wollen eine fortschrittliche Schweiz, die Entscheide mit der Wissenschaft fällt und sie solide und wirksam mit zukunftsträchtiger Technologie umsetzt. Aus diesem Grund stehen wir hier heute für folgende Grundsätze ein: "Privacy by Design", Datensparsamkeit, dezentrale Datenspeicherung und Offenheit der eingesetzten Technologien und Standards.

In den laufenden E-ID Prozess ist CH++ seit der Neulancierung 2021 involviert und hat sich verschiedentlich eingebracht, zuletzt diese Woche zur Wahl eines Technologie-Szenarios. CH++ begrüsst die aktuelle Vorlage und sieht sie als grossen Fortschritt an auf dem Weg zu einer einfach nutzbaren, vertrauenswürdigen und breit akzeptierten E-ID als staatliche Infrastruktur für möglichst alle Menschen in der Schweiz.

Um den Erfolg des Vorhabens zu unterstützen und die flexible Handlungsfähigkeit des Bundes auf diesem Gebiet sicherzustellen, schlagen wir Ihnen im Folgenden eine Reihe von Anpassungen des aktuellen Entwurfs vor. Diese sind das Resultat unserer Beratungen mit Expertinnen und Experten aus Forschung, Entwicklung und Industrie.

Art. 1 Absatz 2 Nummer 1

Datenschutz durch Technik (Privacy by Design) und datenschutzfreundliche Voreinstellungen

Begründung: “Privacy by Design” ist ein wichtiger Fachbegriff und die deutsche Übersetzung wiedergibt seinen Sinn nur zum Teil. Da es sich seit der Motion für die Neulancierung um eine Kernanforderung an die E-ID handelt, sind wir der Auffassung, dass auf den englischen Fachbegriff nicht verzichtet werden kann.

Art. 1 Absatz 2 Nummer 5 und 6 neu

5. Nachvollziehbarkeit und Wiederverwendbarkeit

Begründung: Dieser Grundsatz bildet die Basis für die Veröffentlichung des Quellcodes, wie sie im Weiteren ausformuliert wird. Wir sind der festen Überzeugung, dass es im Sinne unseres Landes ist, hier auf eine umfassende Publikation mit weitgehenden Nutzungsrechten zu setzen. Dies nicht nur im Einklang mit mit dem Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG), sondern auch aufgrund der positiven Erfahrungen mit den COVID-19 Contact Tracing Apps, wo die Schweiz eine globale Vorreiterrolle für dezentrale, datensparsame und wirksame Anwendungen hat einnehmen können. Nicht zuletzt erhöht eine Geheimhaltung der Software oder die Unterbindung weiterer Verwendung des Quellcodes die Sicherheit nicht — ganz im Gegenteil “security by obscurity” ist Gift dafür.

6. Infrastruktur jederzeit unter vollständiger staatlicher Kontrolle

Begründung: Dieser Grundsatz stellt sicher, dass im Betrieb der E-ID keinerlei Cloud-Komponenten oder andere Infrastruktur Dritter beigezogen wird. Dies stärkt die Sicherheit, das Vertrauen und die Unabhängigkeit — und damit die strategische Handlungsfähigkeit. Die Vergangenheit, beispielsweise der Einsatz von Cloud-Komponenten in der COVID-19 Contact Tracing App und die Debatte um die Hyperscaler-Beschaffung hat gezeigt, dass hier ein entsprechender Grundsatz nötig ist.

Art. 9 Absatz 1

Beim Vorweisen eines elektronischen Nachweises muss die Inhaberin oder der Inhaber nachweislich einfach und ohne Fachkenntnisse bestimmen können, welche Bestandteile davon und welche davon abgeleiteten Informationen an die Verifikatorin übermittelt werden.

Begründung: Die Einfachheit muss für die Benutzerinnen und Benutzer gewährleistet sein, damit sie ihre Rechte effektiv wahrnehmen können. Entsprechend muss nachgewiesen und gemessen werden, dass dies tatsächlich der Fall ist. Andernfalls

CH++

Olga Baranova, Geschäftsleiterin CH++
Hannes Gassert, Präsident CH++
hello@chplusplus.org

werden viele der technischen und organisatorischen Massnahmen gegen die Überidentifikation ad absurdum geführt.

Art. 10

Die Ausstellerinnen und Verifikatorinnen melden dem Bundesamt für Cybersicherheit jeden Cyberangriff auf ihre Systeme mit möglicherweise wesentlichen Konsequenzen.

Begründung: Die Meldepflicht muss ressourcenschonend ausgestaltet sein. Deswegen sind wir der Meinung, dass die zu meldenden Cyberangriffe entsprechend präzisiert werden müssen. Die Meldung erfolgt an das Bundesamt für Cybersicherheit BACS.

Art. 11 Absatz 1

veröffentlicht den Quellcode zum Zweck der Nachvollziehbarkeit und Wiederverwendbarkeit

Begründung: Für die Durchführung der Veröffentlichung ist es relevant, mit welchem Zwecke dies geschieht. Da es für die Sicherheit des Systems hilfreich ist, wenn möglichst viele auf dessen Basis weitere Entwicklungen vornehmen, ist auch dieser Zweck klar zu benennen. Ohne eine solche Offenheit hätte eine internationale Erfolgsstory wie die Contact Tracing App und die Integration Schweizer Technologie in führende Smartphone-Betriebssysteme nie stattfinden können. Eine solche Chance geben wir damit auch der Schweizer E-ID.

Art. 11 Absatz 2

Streichen.

Begründung: Ausnahmen vom Transparenzgebot sind nur äusserst spärlich, transparent begründet und extrem gut abgestützt zu fällen. Solche Sicherheitsgründe wären zudem nicht vom BIT, sondern primär vom BACS geltend zu machen und zu vertreten. Nun sieht das EMBAG bereits vor, dass aus Sicherheitsgründen eine Open Source Veröffentlichung unterbunden werden kann. Entsprechend gilt es diesen Absatz zu streichen.

Art. 16

Wir empfehlen, die Online-Identitätsprüfung beizubehalten und gleichzeitig die Offline-Identitätsprüfung so attraktiv wie möglich zu gestalten (z.B. über die Möglichkeit, bei einer Identitätskarten- oder Reisepasserneuerung die e-ID mitzubeantragen). Bei allen Bedenken wäre eine Abkehr von der Online-Ausstellung, wie dies mitunter gefordert wird, das Ende der E-ID.

Art. 18 Buchstabe f neu

Wenn ihre Sicherheit nicht gewährleistet werden kann.

Begründung: Die Möglichkeit des Widerrufs sollte auch dann vorhanden sein, falls die Sicherheit des ganzen Systems oder einer Teilmenge der Identitäten kompromittiert ist (z.B., wenn Schwachstellen in der unterliegenden Verschlüsselungstechnik ans Licht kommen). Die Erfahrungen aus der Industrie zeigen, dass schnelle, skalierbare Widerrufsmöglichkeiten in so einem Falle entscheidend sind, um Missbrauch zu verhindern.

Art. 22 Absatz 1 Buchstabe b

die Zuverlässigkeit der Transaktion zwingend davon abhängt

Begründung: Wir sind überzeugt, dass nur Identitätsmerkmale abgefragt werden dürfen, die tatsächlich und alternativlos benötigt werden. Das Kriterium der Zuverlässigkeit ist relativ weit gefasst, entsprechend ist es angezeigt, eine Qualifizierung vorzunehmen und nur zwingend benötigte Merkmale zuzulassen.

Art. 22 Absatz 2

Wir legen nahe, den Prozess auf Verordnungsebene zu klären, insbesondere in Hinsicht auf die Kommunikation (z.B. Warnung der Nutzerinnen und Nutzer bei Ausschluss einer Verifikatorin) und die Rekursmöglichkeiten. Ebenso ist der Einbezug des BACS zu regeln.