CH++

Olga Baranova, secrétaire générale CH++
Hannes Gassert, président CH++
hello@chplusplus.org

Commissions des affaires juridiques CAJ
Berne, 18 janvier 2024

Chères Conseillères nationales,
Chers Conseillers nationaux,

CH++ est une organisation de la société civile qui s'engage pour une plus grande capacité d'action dans la politique et l'administration suisses grâce à la technologie et à la science. Notre objectif est une Suisse progressiste, prenant des décisions basées sur la science et les mettant en œuvre de manière solide et efficace avec des technologies prometteuses. C'est pourquoi nous défendons les principes suivants : "Privacy by Design", économie de données, stockage décentralisé des données et ouverture des technologies et standards.

Depuis la relance de la E-ID en 2021, CH++ est impliquée dans le processus et a contribué de différentes manières, notamment cette semaine avec le choix d'un scénario technologique. CH++ accueille favorablement la proposition actuelle et la considère comme un grand progrès vers une E-ID facile à utiliser, fiable et largement acceptée en tant qu'infrastructure étatique pour le plus grand nombre de personnes en Suisse.

Pour renforcer davantage le succès de ce projet et garantir la flexibilité ainsi que la capacité d'action de la Confédération, nous vous suggérons ci-dessous une série d'amendements. Ces derniers résultent de nos consultations avec des spécialistes des domaines de la recherche, du développement et de l'industrie.

Art. 1 al. 2 let. a ch. 1

la protection des données dès la conception (Privacy by Design) et par défaut

Justification : « Privacy by Design » est un terme technique important et sa traduction en français ne restitue que partiellement son sens. Puisqu'il s'agit d'une exigence centrale pour l'E-ID depuis les motions pour sa relance, nous sommes d'avis qu'il ne peut être fait abstraction du terme technique anglais.

Art. 1 al. 2 let. a ch. 5 et 6 *nouveau*

5. la traçabilité et la réutilisabilité

Justification : Ce principe constitue la base de la publication du code source, comme il sera développé par la suite. Nous sommes convaincus qu'il est dans l'intérêt de notre pays de miser sur une publication exhaustive avec des droits d'utilisation étendus. Ceci, non seulement en accord avec la Loi fédérale sur l'utilisation des moyens électroniques pour l'accomplissement des tâches des autorités (LMETA), mais aussi en raison des expériences positives avec les applications de traçage des contacts COVID-19, où la Suisse a pu jouer un rôle de précurseur pour des applications décentralisées, économes en données et efficaces. Enfin, la non-divulgation du logiciel ou l'interdiction de l'utilisation ultérieure du code source ne renforce pas la sécurité — bien au contraire, la « sécurité par l'obscurité » est un poison pour celle-ci.

6. le contrôle étatique complet de l'infrastructure à tout moment

Justification : Ce principe garantit qu'aucun composant de cloud ou autre infrastructure tierce ne sera utilisé dans l'exploitation de l'E-ID. Cela renforce la sécurité, la confiance et l'indépendance - et donc la capacité d'action stratégique. Le passé, par exemple l'utilisation de composants cloud dans l'application de traçage des contacts COVID-19 et le débat sur l'acquisition d'hyperscalers, a montré qu'un tel principe est nécessaire.

Art. 9 al. 1

Lorsqu'il présente un moyen de preuve électronique, son titulaire doit pouvoir déterminer avec aisance avérée et sans connaissances techniques préalables quels éléments de ce dernier et quelles informations en découlant sont transmis au vérificateur.

Justification : Il est impératif d'assurer la simplicité d'utilisation pour les utilisatrices et utilisateurs afin qu'ils puissent exercer leurs droits. Par conséquent, il

CH++

Olga Baranova, secrétaire générale CH++
Hannes Gassert, président CH++
hello@chplusplus.org

est nécessaire de prouver et de mesurer que cette simplicité est réellement mise en œuvre. Autrement, de nombreuses mesures techniques et organisationnelles mises en place pour contrer la suridentification deviendraient caduques.

Art. 10

L'émetteur et le vérificateur signalent à l'Office fédéral de la cybersécurité toute cyberattaque visant leurs systèmes pouvant avoir des conséquences potentiellement significatives.

Justification : L'obligation de signalement doit être conçue de manière à économiser les ressources. C'est pourquoi nous estimons que les cyberattaques à signaler doivent être précisément définies. Le signalement doit être effectué auprès de l'Office fédéral de la cybersécurité OFCS.

Art. 11 al. 1

L'OFIT publie le code source dans le but d'assurer la traçabilité et la réutilisabilité

Justification : il est important de préciser dans quel but la publication du code source est réalisée. Étant donné que la sécurité du système est renforcée lorsque le plus grand nombre possible de personnes s'appuie sur sa base pour de nouveaux développements, cet objectif doit être clairement énoncé. Sans une telle ouverture, une réussite internationale telle que l'application de traçage des contacts et l'intégration de la technologie suisse dans les principaux systèmes d'exploitation de smartphones n'aurait jamais pu avoir lieu. Nous offrons ainsi également cette opportunité à l'E-ID suisse.

Art. 11 al. 2

Supprimer.

Justification : Les exceptions à l'exigence de transparence doivent être extrêmement limitées, justifiées de manière transparente et très solidement étayées. De plus, de telles raisons de sécurité ne devraient pas être invoquées et défendues par l'OFIT, mais principalement par l'OFCS. Or, la LMETA prévoit déjà que la publication en Open Source peut être interdite pour des raisons de sécurité. Par conséquent, il convient de supprimer ce paragraphe.

Art. 16

Nous recommandons de maintenir la vérification d'identité en ligne tout en rendant la vérification d'identité hors ligne aussi attrayante que possible (par exemple, en offrant la possibilité de demander l'E-ID lors du renouvellement d'une carte d'identité ou d'un passeport). Malgré toutes les préoccupations, un abandon de la délivrance en ligne, comme cela est parfois exigé, signifierait la fin de l'E-ID.

Art. 18 let. f *nouveau*

si sa sécurité ne peut pas être garantie.

Justification : La possibilité de révocation devrait également exister dans le cas où la sécurité de l'ensemble du système ou d'un sous-ensemble des identités est compromise (par exemple, si des vulnérabilités dans la technologie de chiffrement sous-jacente sont découvertes). Les expériences industrielles montrent que des moyens de révocation rapides et évolutifs sont cruciaux dans de tels cas pour prévenir les abus.

Art. 22 al. 1 let. b

la fiabilité de la transaction en dépend de manière impérative

Justification : Nous sommes convaincus que seuls les attributs d'identité réellement et inévitablement nécessaires doivent être demandés. Le critère de fiabilité est assez large, il est donc approprié d'effectuer une qualification et de n'autoriser que les caractéristiques strictement nécessaires.

Art. 22 al. 2

Nous suggérons de clarifier le processus au niveau de l'ordonnance, notamment en ce qui concerne la communication (par exemple, l'avertissement des utilisatrices et utilisateurs en cas d'exclusion d'un vérificateur) et les possibilités de recours. De même, l'implication de l'OFCS doit être réglée.