Hackathon pour la récolte électronique de signatures : Guide

Le hackathon aura lieu du 31 octobre au 1er novembre 2025 à Berne. Il est organisé par l'Institut Public Sector Transformation de la Haute école spécialisée bernoise (BFH) sur mandat de la Chancellerie fédérale.

1. Challenge

L'objectif du hackathon est d'élaborer les variantes les plus prometteuses (celles qui pourraient compter sur le soutient de la population et des milieux politiques) pour la mise en œuvre de la récolte électronique de signatures en Suisse. Les critères d'évaluation pourraient être les suivants : efforts nécessaires à l'introduction et à l'exploitation de la variante (en termes de coûts, de personnel et de temps), convivialité et accessibilité de la variante, fiabilité et sécurité de la variante, multilinguisme et prise en compte d'autres besoins des différents acteurs. L'établissement de liens entre les différentes variantes de mise en œuvre et les thèmes prédéfinis ci-dessous (« Topics » ; cf. chapitre 3) visent à faciliter une évaluation politique dans le cadre du dialogue participatif et une prise de décision des autorités à la lumière des critères mentionnés ci-dessus. L'évaluation n'a pas lieu lors du hackathon.

Les variantes de mise en œuvre doivent indiquer dans quelle mesure et sur la base de quelles caractéristiques elles traitent ou répondent aux questions et aux défis énoncés dans les Topics. Les variantes doivent présenter le parcours utilisateur des différents acteurs (à savoir les électeurs, les comités, les services chargés de la gestion des registres électoraux, la Chancellerie fédérale) par des exemples d'interfaces utilisateur, l'architecture globale, la syntaxe et la sémantique des flux de données entre les acteurs, ainsi que des explications et des justifications relatives à leur conception. Cette présentation doit être la plus compréhensible possible.

Les variantes de mise en œuvre peuvent être présentées (même partiellement) à l'aide de prototypes élaborés lors du hackathon. Il est également possible d'élaborer des variantes de mise en œuvre sans prototype technique. Elles doivent pouvoir être comparées entre elles aussi facilement que possible. Pour leur documentation, il convient donc d'utiliser les outils prescrits (« Mermaid » pour l'architecture et les flux de données). Cette documentation pourrait par exemple comprendre les éléments suivants :

- Acteurs : autorité fédérale (p. ex. Chancellerie fédérale), canton (p. ex. autorité compétente en matière de droits politiques), commune (p. ex. autorité compétente en matière de droits politiques), service chargé de la tenue du registre électoral (généralement rattaché à l'autorité communale compétente en matière de droits politiques), comité, électeurs, personnes au sein des organisations concernées

- Éléments d'infrastructure (appartenant à un acteur) : téléphone portable, tablette, ordinateur portable, serveur, cloud, imprimante, smartcard, papier

- Logiciels (hébergés sur un élément d'infrastructure ; côté client et côté serveur) : système pour la récolte électronique de signatures, registre électoral (peut être hébergé au niveau cantonal en plus du niveau communal – exemple : registre électoral cantonal permanent actualisé quotidiennement sur la base des registres communaux), site web de campagne, base de données, autres logiciels.

- Données (les données doivent également pouvoir être composées d'autres données, une représentation graphique appropriée est nécessaire) : données personnelles nécessaires à la vérification de la qualité d'électeur, numéro AVS, informations

personnelles (prénom, nom, date de naissance, adresse, commune politique), attestation de la qualité d'électeur anonyme, attestation de la qualité d'électeur non anonyme, déclaration de soutien, requête populaire (y compris le texte), référendum, initiative populaire, identifiant du canton, identifiant de la commune, identifiant du comité, clés cryptographiques (privées et publiques, deux pour la signature et deux pour le chiffrement), clé privée particulièrement protégée (illisible ; créée par une puce matérielle), jeu de données chiffrées (composé des données chiffrées ; la clé privée pour le déchiffrement doit être identifiable), preuve (composée d'autres données afin de prouver que ces données ont un rapport particulier les unes avec les autres), signature (composée des données signées ; la clé privée pour la création de la signature doit être identifiable), chiffre, texte, listes de données, publicité pour une initiative populaire.

- Actions : enregistrer les requêtes populaires (initiative populaire ou référendum) dans le système, enregistrer le comité dans le système, vérifier et attester de la qualité d'électeur, enregistrer et transmettre des déclarations de soutien, vérifier des attestations et compter des déclarations de soutien, transmettre des données, vérifier des données à l'aide d'autres données, déchiffrer des données, lire des données, publier des données.

À la suite du hackathon, la documentation des variantes de mise en œuvre sera adaptée si nécessaire afin de permettre leur comparaison. Il est possible que la Chancellerie fédérale complète les variantes de mise en œuvre à partir des travaux réalisés lors du hackathon et d'autres idées qui lui parviendront en dehors de celui-ci. Sur cette base, la Chancellerie fédérale examine la possibilité de réaliser des vidéos afin de faciliter la compréhension d'un public peu familiarisé avec la technologie.

2. Esquisse du déroulement

La BFH dirige le hackathon pour le compte de la Chancellerie fédérale.

Les participants seront invités à présenter à l'assemblée plénière leurs propres propositions de solutions pour relever un ou plusieurs défis décrits dans les Topics. D'autres participants pourront ensuite se joindre à eux et former une équipe qui élaborera une ou plusieurs variantes de mise en œuvre de récolte électronique de signatures adaptée au système suisse sur la base de l'idée présentée.

Les personnes qui souhaitent présenter une proposition de solution au début du hackathon sont priées de la soumettre à la BFH et à la Chancellerie fédérale avant le hackathon. Il est également possible que ce ne soit pas elles, mais une personne faisant partie des organisatrices (« facilitateur ») qui présente l'idée. Dans le cadre de l'appel public à contributions (« Call For Topics ») lancé fin septembre/début octobre 2025, des propositions ont été soumises.

Les participants se verront présenter des outils qu'ils pourront utiliser pour créer des prototypes. Ils sont toutefois libres d'utiliser les outils de leur choix. Des outils prédéterminés pour la documentation des variantes de mise en œuvre leur sont également présentés. Les participants sont priés de les utiliser. Il s'agit pour la Chancellerie fédérale de faciliter la comparaison entre les différentes variantes de mise en œuvre.

Les équipes sont encouragées à échanger entre elles pendant le hackathon. Les équipes ne sont pas en concurrence les unes avec les autres, le hackathon est placé sous le signe de la collaboration.

À la fin du hackathon, les variantes de mise en œuvre sont présentées à l'ensemble des participants. Le hackathon est considéré réussi si les variantes de mise en œuvre élaborées permettent un large choix au sens des critères mentionnés au chapitre 1.

3. Thèmes prédéfinis (« Topics »)

Lecture recommandée pour les participants : chapitres 1 et 2 du rapport du Conseil fédéral sur la récolte électronique de signatures[1].

Les Topics seront affinés et complétés en fonction des contributions éventuelles reçues dans le cadre du « Call for Topics » lancé fin septembre/début octobre 2025.

Topic 1 « De la volonté de soutien à la déclaration de soutien »

À quoi pourrait ressembler le parcours de l'utilisateur entre le moment où il décide d'apporter son soutien et celui où il l'atteste officiellement ? Outre les exemples cités, existe-t-il d'autres situations qui mériteraient une attention particulière dans le cadre de l'élaboration de variantes de mise en œuvre ? Existe-t-il des situations qui devraient être évitées ou du moins ne pas être encouragées ? L'e-collecting doit-il être conçu par exemple uniquement pour une manifestation de soutien locale (à l'occasion d'un échange personnel avec un membre du comité) ?

- Un membre d'un comité se trouve sur le marché, un téléphone portable à la main, et vient de convaincre un électeur de soutenir sa requête populaire. Cette personne souhaite signer immédiatement et sans complication.
    - À prendre en considération : comment empêcher les fraudeurs d'obtenir frauduleusement une attestation de soutien pour une requête populaire autre que celle affichée sur le téléphone portable ?
- Un électeur a entendu parler il y a quelques jours dans les médias d'une requête populaire qu'il souhaite désormais soutenir. Il est assis chez lui sur son canapé, sa tablette à portée de main.
- Un électeur a consulté le site web d'un comité sur son téléphone portable dans le train. Il souhaite signer la requête populaire présentée et clique sur le lien indiqué.
- Un électeur a entendu parler de la nouvelle plateforme de récolte électronique. Il prend son ordinateur portable et regarde quelles requêtes populaires sont en cours et lesquelles il souhaite signer.
    - À prendre en considération : dans quel ordre les requêtes populaires devraient-elles être classées afin d'éviter toute inégalité politique ?

À prendre en considération :

- Les besoins des personnes handicapées
- Conformément à la législation en vigueur, les électeurs signent la requête populaire après avoir pris connaissance du projet et de tous les contenus requis par les exigences formelles (cf. chap. 1.4.1 du rapport en exécution du postulat).
- Comment les électeurs peuvent-ils s'assurer qu'ils communiquent avec le bon interlocuteur (par exemple, plateforme légitime, comité approprié) ? Comment pourraient-ils être informés de la manière dont ils doivent procéder à cette vérification ? (p. ex. vérification de l'URL et du symbole du cadenas, vérification lors de l'installation de l'application)

Topic 2 « Accès aux informations concernant les déclarations de soutien déposées » (cf. en particulier le chapitre 2.8.2 du rapport en exécution du postulat)

[1] https://www.bk.admin.ch/dam/bk/fr/dokumente/pore/e-collecting/rapport%20en%20r%C3%A9ponse%20au%20postulat%20e-collecting.pdf.download.pdf/rapport%20en%20r%C3%A9ponse%20au%20postulat%20e-collecting.pdf

Comment les informations essentielles au suivi de la récolte de signatures par les comités (en particulier le nombre et l'origine géographique des signatures ainsi que les éventuels motifs d'invalidité) pourraient-elles être préparées ? Les informations doivent-elles/peuvent-elles être mises à la disposition uniquement des comités ou également du public ? Quelles sont les éventuelles répercussions sur le secret du vote ?

Les besoins des personnes handicapées doivent être pris en considération.

Topic 3 « Attribution des attestations de soutien aux comités et aux entreprises de récolte »

Contrairement aux initiatives populaires fédérales, il n'existe pas de comités au sens strict du terme pour les référendums. En revanche, différentes organisations de récolte (également appelées « comités » par souci de simplicité) peuvent récolter des attestations de soutien. Les comités qui obtiennent le plus de succès disposent de plus d'espace pour présenter leurs arguments dans les explications du Conseil fédéral que ceux qui ont moins de succès. En outre, tant pour les initiatives populaires que pour les référendums, il existe des entreprises qui soutiennent les comités dans la récolte de signatures contre rémunération.

Comment les attestations de soutien récoltées peuvent-elles être attribuées aux comités ou éventuellement aux organisations de récolte ? Dans quels cas (cf. Topic 1) cela a-t-il un sens ? Quelles sont les éventuelles répercussions sur le secret du vote ?

Topic 4 « Diffusion des arguments des comités via le logiciel de récolte électronique de signatures »

Les formulaires papier peuvent contenir des arguments en faveur du soutien à une requête populaire, sans toutefois dépasser les limites des exigences formelles. Cela garantit que les électeurs déclarent leur soutien en connaissance de cause (p. ex. le titre et le libellé corrects des initiatives, la désignation correcte de l'acte législatif avec la date de la décision de l'Assemblée fédérale ainsi que les dispositions pénales).

Comment permettre aux comités d'afficher les informations de leur choix dans le visuel du logiciel de récolte électronique de signatures tout en empêchant un abus ou une confusion avec les informations pertinentes pour les électeurs ?

Les comités devraient-ils avoir la possibilité de demander aux électeurs de s'identifier via le logiciel de récolte électronique de signatures afin de pouvoir leur envoyer par la suite des informations sur d'autres requêtes populaires ? Comment cela pourrait-il être mis en œuvre ?

Ou bien la diffusion d'informations par les comités devrait-elle être exclue de la récolte électronique de signatures ?

Il convient de prendre en considération les besoins des personnes handicapées.

Topic 5 « Exclusion des attestations de soutien illicites » (cf. chapitre 2.7 du rapport en exécution du postulat)

Il doit être garanti que les attestations de soutien proviennent bien d’un électeur et qu'aucune autre attestation de soutien n'est comptabilisée pour cette personne. Dans le cadre de la récolte de signatures sur papier, cet objectif est atteint grâce à l'obligation de fournir des informations manuscrites, y compris la signature, et à la vérification de leur authenticité par le service chargé de l’attestation de la qualité d’électeur et par la Chancellerie fédérale.

À quoi pourrait ressembler une solution pour la récolte électronique ? Quels éléments de preuve pourraient servir de base à un contrôle juridictionnel ?

Topic 6 « Prévention des attestations de soutien non dépouillées » (cf. chapitre 2.7 du rapport en exécution du postulat)

Il est essentiel de garantir que toutes les attestations de soutien légalement remises soient comptabilisées. Dans le cadre du processus papier, les comités gèrent directement les attestations de soutien, ce qui leur permet, ainsi qu'à d'autres acteurs, de s'assurer dans une large mesure qu'aucune erreur systématique ne se produit lors de l'attestation par le service chargé de l'attestation de la qualité d'électeur et lors du dépouillement par la Chancellerie fédérale.

À quoi pourrait ressembler une solution pour la récolte électronique ? Quels éléments de preuve pourraient servir de base à un contrôle juridictionnel ?

Topic 7 « Respect du secret du vote » (cf. chapitre 2.7 du rapport en exécution du postulat)

L'identité des personnes qui soutiennent une requête populaire ne doit pas être divulguée. Dans le cadre du processus papier, les comités, les services chargés de l'attestation de la qualité d'électeur et la Chancellerie fédérale ont connaissance de l'identité des personnes qui ont apporté leur soutien à une initiative. Cela est inévitable pour des raisons pratiques. La protection des données s'applique. En ce qui concerne la récolte électronique, on ne sait pas encore clairement jusqu'où doivent aller les mesures pour protéger le secret du vote. On peut toutefois affirmer que la récolte électronique offre de nouvelles possibilités pour protéger le secret du vote. Pour déterminer jusqu'où doit aller cette protection, il convient de procéder à une pesée des intérêts, qui peut également tenir compte des coûts.

Comment protéger le secret du vote dans le cadre de la récolte électronique ?

Topic 8 « Intégration avec le processus papier »

Le canal papier restera en place pendant la phase d'essai. Comment les deux canaux peuvent-ils être combinés tout en évitant les signatures multiples ?

Topic 9 « Introduction facilitée pour les communes avec un gain d'efficacité ; sur la base des infrastructures et des processus existants »

Il est possible que certaines communes soient disposées à participer rapidement aux essais, mais ne disposent pas des ressources nécessaires pour adapter leurs logiciels ou en acquérir de nouveaux. Comment garantir que ces communes puissent néanmoins proposer rapidement la récolte électronique et en tirer une valeur ajoutée ?
Information de fond : la plupart des cantons ne disposent actuellement d'aucune centralisation des registres électoraux communaux. Le canton de Genève gère le registre électoral de manière centralisée. Les cantons de Saint-Gall et de Nidwald tiennent un registre centralisé qui est mis à jour quotidiennement à partir des registres électoraux communaux.

Thème 10 « Récolte électronique pour tous les niveaux fédéraux »

Comment le système ou l'interaction entre plusieurs sous-systèmes devrait-il être conçu pour permettre également la récolte au niveau cantonal et communal ?

Annexe « Solutions possibles »

Topic 3 « Attribution des attestations de soutien aux comités et aux entreprises de récolte »

- Les attestations de soutien ne sont pas attribuées aux comités.
- En déclarant leur soutien, les électeurs enregistrent non seulement le référendum soutenu, mais aussi le comité auquel la déclaration de soutien doit être attribuée. À cette fin, les comités (et éventuellement les entreprises de récolte) sont également préenregistrés dans le système de récolte électronique.
    - À prendre en considération : dans quel ordre les comités doivent-ils être affichés afin de ne pas créer d'inégalité politique ? Comment éviter les cas où de nombreux « faux comités » sont créés dans le but de perturber la récolte ?

- Si un électeur est incité à déclarer son soutien sur le site web d'un comité ou dans la rue par un membre du comité, le lien ou le code QR mène à un enregistrement préalable du comité ou de l'entreprise de récolte dans le logiciel utilisé pour la déclaration du soutien.

Topic 5 « Exclusion des attestations de soutien illicites » (cf. chapitre 2.7 du rapport en exécution du postulat)

- Authentification forte des électeurs.
- En outre, les électeurs fournissent une signature numérique (éventuellement anonyme) de leur déclaration de soutien. La signature numérique est vérifiée par un ou plusieurs acteurs. Remarque : les propositions de signature numérique ne doivent pas nécessairement s'inscrire dans le cadre de la signature électronique qualifiée selon la SCSE.

Topic 6 « Prévention des attestations de soutien non dépouillées » (cf. chapitre 2.7 du rapport en exécution du postulat)

- En déclarant leur soutien, les électeurs reçoivent un identifiant personnel et anonyme qui est publié sur un site web officiel. En retrouvant leur identifiant et en additionnant les identifiants publiés, ils peuvent vérifier que leur soutien a bien été pris en compte dans le décompte officiel.

    - À prendre en considération : les électeurs doivent notamment pouvoir s'assurer qu'un identifiant correctement affiché ne peut pas être utilisé par une autre personne pour vérifier sa propre déclaration de soutien. Remarque : les identifiants pourraient être le résultat d'une fonction de hachage à laquelle est également transmise une caractéristique permettant d'identifier l'électeur.

Topic 7 « Respect du secret du vote » (cf. chapitre 2.7 du rapport en exécution du postulat)

- Niveau 0 : outre la sécurisation des infrastructures concernées conformément aux meilleures pratiques, aucune mesure conceptuelle n'est prévue.
- Niveau 1 : les enregistrements indiquant l'identité de l'électeur et la requête populaire soutenue sont immédiatement supprimés ou stockés sous forme chiffrée après réception.
- Niveau 2 : les données que les électeurs joignent à leur déclaration de soutien pour l'attestation de la qualité d'électeur sont anonymes. Cela pourrait par exemple être mis en œuvre en demandant aux électeurs, après avoir prouvé leur identité auprès de la commune, d'obtenir un moyen d'identification anonyme unique qui confirme leur

qualité d’électeur. Ce moyen d'identification pourrait également servir à créer une signature numérique (cf. Topic 5).

- Niveau 3 : Afin d'empêcher tout lien avec l'identité établi via des traces numériques (p. ex. l'adresse IP), les électeurs envoient leur déclaration de soutien chiffrée à l'aide d'un système cryptographique homomorphe au système de récolte électronique. La déclaration de soutien chiffrée est traitée (par exemple additionnée) avec les déclarations de soutien chiffrées des autres électeurs, puis déchiffré à l'aide d'une clé distribuée.

Remarque : les solutions qui protègent particulièrement bien le secret du vote (par exemple en garantissant ce secret même lorsque le service chargé de l’attestation de la qualité d’électeur collabore avec les autres services qui ont accès aux déclarations de soutien) pourraient entrer en conflit avec l'intégration du canal papier (cf. Topic 8). Dans la mesure du possible, ces solutions devraient également garantir, dans la perspective de la première phase d'une éventuelle mise en œuvre, une possibilité d'intégration avec le canal papier, à laquelle il serait ensuite possible de renoncer. Jusqu'à ce renoncement, l'intégration ne fonctionne que si le service chargé de l’attestation de la qualité d’électeur (mais idéalement aucun autre service) peut savoir, comme c'est le cas aujourd'hui, qui a déposé une déclaration de soutien.

Topic 8 « Intégration avec le processus papier »

- À la réception d'une déclaration de soutien sur papier, le service chargé de l’attestation de la qualité d’électeur consulte le système de récolte électronique.
- Il serait également envisageable qu'il enregistre une déclaration de soutien numérique et remplace ainsi celle sur papier.

Topic 9 « Introduction facilitée pour les communes avec un gain d'efficacité ; sur la base des infrastructures et des processus existants »

- Ces communes reçoivent les déclarations de soutien soumises par voie électronique sur papier ou via l'infrastructure existante. Elles impriment les déclarations de soutien reçues par voie électronique. Les communes procèdent manuellement à l’attestation de la qualité d’électeur et enregistrent la déclaration ainsi que les informations relatives à l’électeur sur papier. Comme dans le processus papier, les déclarations de soutien attestées sont transmises à la Chancellerie fédérale par l'intermédiaire du comité pour vérification et dépouillement.