Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Berne, 30 juin 2021

Généraliser la signature électronique pour les documents internes à l'administration fédérale

Rapport donnant suite au postulat 18.3502 Dobler du 12 juin 2018

Table des matières

1 Mandat parlementaire

1.1 Postulat « Généraliser la signature électronique pour les documents internes à l'administration fédérale »

Le 12 juin 2018, le conseiller national Marcel Dobler a déposé le postulat 18.3502, intitulé « Généraliser la signature électronique pour les documents internes à l'administration fédérale », dont la teneur est la suivante :

« Le Conseil fédéral est chargé d'examiner de manière approfondie les possibilités qui s'offrent de généraliser la signature électronique pour tous les documents internes à l'administration fédérale qui doivent être signés, et de rendre compte de ses travaux sous la forme d'un rapport. »

Le développement du postulat est libellé comme suit :

« Intitulée "*Documents internes à l'administration fédérale. Généraliser la signature électronique*", la motion 18.3008 invitait le Conseil fédéral à créer au plus vite les bases légales qui permettront de munir d'une signature électronique, et non plus manuscrite, tous les documents internes à l'administration fédérale qui doivent être signés, l'administration faisant usage dans tous les autres cas des possibilités offertes par la documentation des confirmations gérée par processus, que propose notamment le nouveau produit GEVER standardisé Acta Nova.

Le Conseil fédéral a répondu dans son avis que s'il entendait mettre à profit au sein de l'administration fédérale les possibilités offertes par la documentation des confirmations gérée par processus, que propose notamment le nouveau produit GEVER standardisé Acta Nova, il n'en considérait pas moins que le fait de généraliser et de rendre obligatoire la signature électronique demanderait des éclaircissements plus approfondis. C'est précisément pour l'inviter à procéder à ces éclaircissements que je dépose le présent postulat.

La généralisation dans l'administration de la signature électronique permettra par ailleurs d'accélérer le passage au numérique de l'administration fédérale, d'imposer la dématérialisation intégrale, de contribuer fortement à la banalisation de la signature numérique et enfin d'améliorer l'efficience de l'administration fédérale. L'administration fédérale propose un service nommé validator.ch qui permet à tout moment non seulement de vérifier sans erreur possible la validité d'un document[1], mais aussi permet à tout un chacun de créer et de vérifier aisément une signature électronique. »

Le 29 août 2018, le Conseil fédéral a proposé d'adopter le postulat. Le Conseil national a suivi cette proposition, adoptant le postulat le 28 septembre 2018.

1.2 Rappel des faits

La motion 18.3008 Dobler du 26 février 2018 chargeait le Conseil fédéral de créer au plus vite les bases légales permettant de munir d'une signature électronique tous les documents internes à l'administration fédérale.

Le 1er juin 2018, le Conseil fédéral a proposé de rejeter la motion, indiquant qu'un système de gestion électronique des affaires permet déjà de signer par voie électronique les documents internes à l'administration fédérale qui nécessitent une approbation, ou encore de les transmettre ou de les confirmer par apposition de la mention « Approuvé ». Il a précisé que les conditions techniques permettant de faire usage de ces possibilités étaient déjà réunies et qu'elles se traduiraient, à partir de 2020, par la mise en place d'une solution standardisée pour la gestion électronique des affaires

[1] Remarque : le validateur confirme la validité de la ou des signatures électroniques d'un document. Par contre, il ne dit rien sur la légalité (en allemand « Rechtmässigkeit », terme employé dans la version allemande du postulat. alors que la version française parle plus justement de « validité ») du contenu du document. Dans le cas d'un extrait du casier judiciaire muni d'une signature électronique, il va vérifier par exemple si l'extrait est muni d'une signature qualifiée et d'un horodatage valide, et s'il a été signé avec un certificat prévu à cet effet par le responsable du casier judiciaire. Dans le cas d'un document muni d'une signature qualifiée, le validateur peut vérifier que la signature électronique répond aux exigences fixées à l'art. 14, al. 2bis, du code des obligations (signature manuscrite).

(GEVER) pour quelque 30 000 postes de travail de l'administration fédérale centrale et d'une partie de l'administration fédérale décentralisée.

Le 12 juin 2018, le motionnaire a déposé le postulat 18.3502, mentionné plus haut, avant de retirer la motion 18.3008 le 10 septembre 2018. En août 2021, le système de gestion électronique des affaires (GEVER) Acta Nova sera disponible dans toute l'administration fédérale centrale, sauf dans les représentations du DFAE à l'étranger.

2 Le cadre légal de l'obligation de signature

2.1 Introduction

Si l'on considère l'objectif visé par le postulat et les antécédents de celui-ci, il apparaît que les questions auxquelles il faut répondre sont au nombre de deux : d'une part, quels sont les documents internes à l'administration fédérale pour lesquels la loi prévoit une obligation de signature manuscrite, et d'autre part, dans quels cas cette signature manuscrite peut-elle être remplacée par une signature électronique, et plus précisément par quel type de signature électronique.

La motion 18.3008 « Documents internes à l'administration fédérale. Généraliser la signature électronique » et le postulat 18.3502 « Généraliser la signature électronique pour les documents internes à l'administration fédérale » visent tous deux les documents internes à l'administration fédérale.

Le présent rapport se focalise donc sur les documents internes à l'administration fédérale centrale (ci-après : documents administratifs internes), même s'il est également souvent fait mention de documents dont les destinataires sont extérieurs à l'administration fédérale centrale.

Le chancelier de la Confédération est compétent pour décider des services standard qui font l'objet d'une obligation d'achat pour les unités administratives auxquelles s'applique l'ordonnance sur la transformation numérique et l'informatique (OTNI)[2]. Par services standard, on entend les prestations gérées de manière centralisée, fréquemment utilisées et répondant à des exigences identiques ou similaires, comme la gestion électronique des affaires (GEVER) ou le service standard IAM, qui comprend les services de signature.

2.2 Définition de la signature électronique

Alors qu'il n'existe qu'un seul type de signature manuscrite, il existe différents types ou niveaux de signature électronique. L'art. 2 de la loi fédérale du 18 mars 2016 sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques (loi sur la signature électronique, SCSE)[3] distingue ainsi entre quatre signatures électroniques et le cachet électronique réglementé (étant entendu que si ce dernier constitue techniquement lui aussi une signature électronique, il n'est pas considéré comme tel juridiquement car il n'est pas directement lié à une personne physique en particulier) :

- ***signature électronique*[4] (art. 2, let. a, SCSE) :** elle n'est liée à personne et ne permet donc pas d'identifier une personne.

  La signature électronique simple est définie comme un ensemble de données électroniques qui sont jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier leur authenticité.

- ***signature électronique avancée* (art. 2, let. b, SCSE) :** elle 1) est liée au titulaire, 2) permet d'identifier le titulaire, 3) est créée par des moyens que le titulaire peut garder sous son contrôle

[2] RS **172.010.58**
[3] RS **943.03**
[4] À l'instar de la SCSE, la version française du postulat donnant lieu au présent rapport emploie le terme de « signature électronique », tandis que la version originale allemande du postulat parle de « signature numérique ». C'est ici la même chose.

exclusif et 4) est liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

Tous les employés de l'administration fédérale centrale disposent d'une smartcard munie d'un certificat avancé qui permet d'apposer une signature électronique avancée sur un document.

- ***signature électronique réglementée* (art. 2, let. c, SCSE) :** il s'agit d'une signature électronique avancée créée au moyen d'un dispositif sécurisé de création de signature au sens de l'art. 6 SCSE et fondée sur un certificat réglementé se rapportant à une personne physique et valable au moment de sa création.

  La *Swiss Government PKI* (SGPKI) de l'OFIT ne délivre pas actuellement de signatures réglementées. Rappelons que le certificat de signature de classe B qui est installé sur la smartcard permet uniquement de créer des signatures électroniques avancées, et non des signatures électroniques réglementées telles qu'elles sont définies dans la SCSE.

- ***signature électronique qualifiée* (art. 2, let. e, SCSE) :** un certificat qualifié ne peut être délivré qu'à une personne physique, et il doit contenir la mention qu'il est destiné à n'être utilisé que pour la signature électronique (art. 8, al. 1 et 2, SCSE). Il doit également contenir la mention qu'il est délivré à titre de certificat qualifié (art. 8, al. 3, SCSE).

  Cette signature a en principe les mêmes caractéristiques que la signature électronique avancée visée à l'art. 2, let. b, SCSE, mais elle doit être établie au moyen d'un dispositif sécurisé de création de cachets au sens de l'art. 6 SCSE, et elle est fondée sur un certificat qualifié[5].

  Dans l'administration fédérale, seuls répondent à ces exigences les certificats qualifiés établis au nom d'une personne physique (appelés « certificats qualifiés de classe A » par l'OFIT).

- ***cachet électronique réglementé* (art. 2, let. d, SCSE) :** le certificat concerné est établi au nom, non pas d'une personne physique, mais d'une personne morale ou d'une autorité. Le cachet électronique réglementé (qualifié de « certificat d'autorité réglementé » par l'OFIT et disponible sur smartcard ou sur serveur) permet de garantir l'intégrité et l'origine d'un document, et peut donc être utilisé par l'administration pour signer les documents sortants (y compris les décisions).

  Ce cachet a en principe les mêmes caractéristiques que la signature électronique (art. 2, let. b, SCSE)[6], mais il doit être établi au moyen d'un dispositif sécurisé de création de cachets (art. 6 SCSE) et fondé sur un certificat réglementé se rapportant à une entité IDE au sens de l'art. 3, al. 1, let. c, de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE)[7] et valable au moment de la création du cachet électronique[8]. Il doit également contenir la mention qu'il est délivré à titre de certificat réglementé (art. 7, al. 2, let. b, SCSE).

2.3 Les certificats électroniques utilisés dans l'administration fédérale

À l'interne, lorsqu'elle a recours à la signature électronique, l'administration fédérale utilise surtout la signature électronique avancée au sens de l'art. 2, let. b, SCSE. La smartcard contient en effet les « certificats de classe B » suivants :

- *un certificat de signature avancé* permettant de signer documents (principalement au format PDF) et courriels au moyen d'un logiciel de signature comme l'application Open eGov LocalSigner, encore disponible dans l'administration fédérale, ou des nouveaux services de signature basés sur serveur et d'Outlook (pour les courriels)

---

[5] Aux termes de l'art. 2, let. h, SCSE, un certificat qualifié est un certificat réglementé au sens de la let. g qui remplit les conditions fixées à l'art. 8 SCSE (voir à la note 5 le lien menant aux explications de l'OFIT concernant les types de certificat).

[6] Les exigences que la SCSE prévoit pour l'identification du titulaire du certificat réglementé correspondant vont cependant bien au-delà de celles qui sont associées à un certificat avancé.

[7] RS **431.03**

[8] L'administration fédérale centrale qualifie de certificats de signature de classe A pour personnes morales ou, plus justement, de certificats d'autorité réglementés, les certificats de cachet électronique qu'elle délivre (voir les explications de l'OFIT concernant les différents types de certificat, sous www.bit.admin.ch/bit/fr/home/subsites/generalites-concernant-la-swiss-government-pki/types-de-certificats/classe-a/Geregelte-Behoerdenzertifikate.html).

- *un certificat d'authentification* qui permet d'identifier le titulaire et, après double authentification, lui donne accès au réseau informatique de l'administration fédérale
- *un certificat de chiffrement* permettant de chiffrer documents et courriels.

Les employés des services du personnel et les supérieurs hiérarchiques ayant délégation de signature, soit un nombre relativement restreint de personnes, peuvent en outre demander un certificat de signature qualifié de classe A. Cela suppose techniquement de disposer soit d'une seconde smartcard[9] et d'un lecteur de carte dédié (généralement une clef USB), soit d'un certificat de signature qualifié de classe A pour personnes physiques basé sur serveur, auquel la personne accède au moyen de son certificat d'authentification. Dans ce dernier cas, l'apposition d'une signature qualifiée sur un document (PDF) nécessite de recourir aux applications concernées des services de signature.

Le certificat de signature avancé (de classe B) en usage dans l'administration fédérale répond à un haut niveau de qualité : d'une part, la clef de signature est installée sur la smartcard (et ne peut donc être copiée), d'autre part, le certificat de signature, de même que les certificats de chiffrement et d'authentification, ne sont délivrés à l'employé qu'une fois que son identité a été vérifiée au moyen du passeport ou de la carte d'identité. Une signature générée avec un tel certificat possède une force probante très élevée, même si elle ne répond pas aux exigences de la forme écrite simple au sens du code des obligations (CO, voir ch. 2.4.2).

2.4 Circonstances exigeant la signature manuscrite

2.4.1 La forme électronique

S'agissant de la question de savoir quels documents administratifs internes sous forme papier doivent impérativement comporter une signature manuscrite, et donc comporter une signature qualifiée lorsqu'ils sont émis au format électronique, on constate que les prescriptions applicables sont peu nombreuses. On peut en conclure qu'il n'est que rarement nécessaire d'apposer une signature électronique qualifiée sur les documents (PDF) à caractère strictement interne.

Cela signifie que pour viser et approuver les documents administratifs internes qui sont créés et modifiés dans le système GEVER ou dans une application analogue (par ex. SAP ERP pour les achats, les finances ou les ressources humaines), il est possible de se contenter des « fonctions de confirmation » de GEVER au lieu de devoir les signer électroniquement. Comme les personnes qui visent et approuvent les documents sont connectées au système GEVER via le certificat d'authentification installé sur leur smartcard (double authentification avec certificat de classe B)[10], il est possible de retrouver avec certitude et à tout moment chacune de ces personnes et le moment où elles ont signé ou approuvé au moyen des métadonnées de GEVER, des courriels ou des applications utilisées.

Le SAP ERP est lui aussi un système sécurisé qui rend inutile la signature électronique pour les documents internes, puisque les validations associées aux workflows sont consignées dans le système lui-même – comme c'est le cas dans le système GEVER.

Dans un contexte administratif interne, une signature manuscrite ou électronique n'est nécessaire que pour des documents finaux, et plus particulièrement : a) lorsqu'il s'agit par ex. d'archiver des accords conclus entre deux ou plusieurs parties, ou b) que des documents sont conservés en dehors du système GEVER ou encore c) qu'ils quittent ce système, par ex. pour être archivés. Dans la grande majorité des cas, cependant, une signature électronique avancée avec certificat avancé (classe B) est ici suffisante, sauf lorsqu'il est dit expressément que la validité est subordonnée à la forme écrite, comme c'est par

[9] En raison des exigences techniques élevées auxquelles doit répondre un certificat qualifié (de classe A), la clef de signature correspondante ne peut être installée sur une smartcard comportant déjà un certificat de classe B.
[10] La double authentification, ou authentification à deux facteurs, repose sur deux preuves d'identité distinctes, soit d'une part un support physique attribué au titulaire, en l'occurrence la smartcard, et d'autre part, une information connue du seul titulaire, à savoir le mot de passe Windows ou le code PIN.

ex. le cas pour un contrat de travail, conformément à l'art. 13 de la loi sur le personnel de la Confédération[11].

Si les décisions administratives requièrent elles aussi une signature manuscrite ou une signature électronique qualifiée (voir ch. 2.4.5.1), elles s'adressent cependant généralement à des destinataires qui ne font pas partie de l'administration fédérale, même s'il peut y avoir des exceptions (par ex. dans le cas du licenciement d'un employé). Rappelons aussi que le destinataire d'une décision doit donner son consentement exprès à la remise de cette dernière sous forme électronique, ce qui limite d'autant le nombre des décisions qui sont signées électroniquement.

Conclusion

Au-delà des décisions, rares sont les actes qui, aux termes du droit administratif fédéral, requièrent expressément la forme écrite et donc une signature manuscrite ou, s'ils sont établis sous forme électronique, une signature électronique qualifiée (en lieu et place d'une signature avancée). Il y a lieu d'interpréter cas par cas ce qu'il faut entendre au juste en droit administratif fédéral par « forme écrite » et « signature manuscrite ».

2.4.2 La forme écrite

L'obligation d'établir les documents administratifs internes en la forme écrite garantit la transparence et l'intelligibilité des processus décisionnels de l'administration. Elle découle aussi de la Constitution (Cst.)[12], qui dispose que tous les êtres humains sont égaux devant la loi (art. 8) et qu'ils ont le droit d'être traités par les organes de l'Etat sans arbitraire et conformément aux règles de la bonne foi (art. 9).

Pour que les intéressés puissent au besoin exercer effectivement ces droits, il faut que l'action de l'administration soit régie par des règles claires et qu'elle soit documentée. Cela signifie concrètement que les processus internes à l'administration fédérale doivent avoir été cartographiés et qu'ils soient compréhensibles, notamment lorsqu'il s'agit de savoir qui a décidé quand et comment, et qui a été impliqué dans le processus décisionnel.

Il est par ailleurs possible au sein de l'administration fédérale de remplir cette exigence sans recourir ni à la signature manuscrite ni à la signature électronique qualifiée (qui est son équivalent numérique), au moyen par ex. de GEVER. Le critère décisif est donc la consignation durable au moyen de caractères d'écriture sur un support de déclaration et non la « forme écrite » stricto sensu, qui prévoit que le texte doit être revêtu d'une signature manuscrite.

Conclusion

En conséquence, l'art. 22, al. 1, de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA)[13] fait obligation aux unités administratives de consigner leurs activités au moyen d'une gestion systématique des affaires. L'art. 22, al. 2, OLOGA précise que ces unités utilisent à cet effet des systèmes de gestion électronique des affaires au sens de l'ordonnance du 3 avril 2019 sur la gestion électronique des affaires dans l'administration fédérale (ordonnance GEVER)[14]. Dans les domaines des finances et des ressources humaines, la traçabilité et l'auditabilité sont assurées de manière analogue au moyen du système SAP ERP.

2.4.3 Exigences formelles applicables aux contrats

Aux termes de l'art. 1 CO, un contrat est juridiquement contraignant dès lors que « les parties ont, réciproquement et d'une manière concordante, manifesté leur volonté ». L'art. 11, al. 1, CO précise que la validité d'un contrat n'est subordonnée à l'observation d'une forme particulière que si la loi le prescrit

[11] RS **172.220.1**
[12] RS **101**
[13] RS **172.010.1**
[14] RS **172.010.441**

(selon le principe dit « de la liberté de la forme »)[15]. La loi peut ainsi imposer pour certains actes la forme écrite simple telle qu'elle est prévue par l'art. 12 ss. CO, ce qui signifie que le contrat doit être soit signé à la main par toutes les parties (voir art. 14, al. 1, CO), soit signé électroniquement au moyen d'une « signature électronique qualifiée » au sens de l'art. 2, let. e, SCSE (voir art. 14, al. 2bis, CO). Seule la signature électronique qualifiée est en effet assimilée à la signature manuscrite, et à ce titre cet équivalent numérique est le seul à répondre à l'exigence de la forme écrite simple[16].

Il ne s'ensuit pas nécessairement pour autant qu'un contrat écrit qui n'a pas été signé à la main ou au moyen d'une signature électronique qualifiée ne soit pas juridiquement contraignant. En l'absence d'exigence formelle légale ou contractuelle, en effet, le principe de la liberté de la forme prévaut. Ainsi, est tout aussi juridiquement contraignant un contrat qui a été signé au moyen d'une signature électronique avancée au sens de l'art. 2, let. b, SCSE.

Les différentes formes de signature électronique diffèrent cependant sur le plan de la qualité et donc de leur force probante. Il est vrai qu'il n'y a pas à ce jour de jurisprudence traitant spécifiquement de la question de la force probante à attribuer à une signature électronique avancée, et la question de la validité d'une telle signature doit donc être appréciée cas par cas. Cette appréciation devra également tenir compte des exigences manifestées par les parties contractantes quant à la force probante des documents, de même qu'il y a lieu d'examiner dans chaque cas le degré de sécurité de la procédure de signature, de la conservation de la clef de signature ainsi que des processus d'identification lorsque le niveau de sécurité du certificat délivré est inférieur à celui d'une signature électronique qualifiée ou réglementée.

Compte tenu des difficultés auxquelles se heurte le contrôle de l'authenticité d'une signature manuscrite et de la facilité avec laquelle un document papier peut être manipulé (notamment lorsqu'il comporte plusieurs pages), il est permis de présumer qu'une signature électronique avancée telle qu'elle est définie à l'art. 2, let. b, SCSE présente en termes de garantie d'intégrité et d'authenticité d'un document une force probante au moins équivalente à celle d'une signature manuscrite. Qu'une signature avancée ait une force probante plus faible qu'une signature qualifiée n'entraîne guère de difficultés dans la pratique : les litiges avec les fournisseurs sont en effet dus généralement à des divergences dans l'interprétation des dispositions contractuelles ou portent sur l'évaluation de la qualité des fournitures, l'authenticité ou l'intégrité du texte du contrat lui-même n'étant quasiment jamais remise en cause.

Conclusion

Toutes les unités administratives de la Confédération peuvent donc signer électroniquement au moyen du certificat de signature avancée de classe B enregistré sur la smartcard non seulement les documents strictement internes à l'administration, mais aussi les contrats qui sont conclus avec des acteurs extérieurs à celle-ci – sauf si, et le cas est plutôt rare, la loi prescrit la forme écrite en raison du contenu du texte ou plus généralement de la procédure suivie. Les employés connaissent la qualité élevée de ce certificat (clef de signature sur smartcard et processus d'identification crédible), ce qui explique que les signatures avancées générées avec ce certificat bénéficient d'un haut niveau de confiance mutuelle, du moins au sein de l'administration fédérale.

En ce qui concerne les acteurs extérieurs à l'administration, par contre, c'est moins simple. La SCSE et ses textes d'application, en effet, ne définissent dans tous leurs aspects qualitatifs (sécurité, stockage des clefs, processus d'identification, etc.) ni la signature avancée de l'administration fédérale, ni les signatures avancées du secteur privé – contrairement à ce qui est le cas pour la signature qualifiée. Aussi est-il difficile pour les deux parties d'apprécier si elles peuvent se fier à un document signé par l'autre au moyen d'une signature avancée.

[15] Étant entendu que les parties au contrat peuvent également se mettre d'accord sur une forme particulière (voir art. 16 CO).
[16] Message du 15 janvier 2014 relatif à la révision totale de la loi sur la signature électronique (SCSE) ; FF 2014 957 970

Généraliser la signature électronique pour les documents internes à l'administration fédérale

2.4.4 Digression : contrats des marchés passés par la Confédération

L'ordonnance du 12 février sur les marchés publics (OMP)[17] dispose à l'art. 11, al. 1, que tous les contrats des marchés passés par l'administration fédérale qui relèvent de la loi fédérale du 21 juin 2019 sur les marchés publics (LMP)[18] doivent être conclus « par écrit ».

Or, ce terme n'est pas synonyme de la « forme écrite » exigée par le CO[19], et un marché public peut ainsi être conclu aussi bien par écrit que sous n'importe quelle autre forme établissant le contenu par un texte. Par contre, un contrat d'achat qui serait conclu oralement ou tacitement ne répondrait pas à cette exigence.

Dans le cadre de la mise en œuvre de cette disposition dans la pratique, la Conférence des achats de la Confédération prépare actuellement des recommandations pour la conclusion numérique des contrats de marchés publics.

Certificats qualifiés au sein de l'administration fédérale

Les employés de l'administration fédérale disposent d'un certificat de signature avancé (classe B, non qualifié) délivré par le SGPKI de l'OFIT. Il est également possible en tout temps de demander au SGPKI un certificat de signature qualifié (classe A), mais le processus d'identification actuel est plutôt chronophage, car les employés qui souhaitent obtenir un tel certificat doivent se présenter en personne au SGPKI avec une pièce d'identité officielle, ce qui explique que seuls quelques centaines d'employés en soient dotés à ce jour.

Le processus d'identification devrait toutefois être simplifié à moyen terme, car des travaux sont en cours dans l'Union européenne (UE) pour standardiser les procédures d'identification par vidéo. Il est prévu que la Suisse reprendra la norme européenne concernée (ETSI TS 119 461) pour l'intégrer dans sa législation sur la signature (SCSE). Dans sa réponse à l'interpellation 20.4274 Bellaîche, le Conseil fédéral rappelle que l'art. 7, al. 1, de l'ordonnance du 23 novembre 2016 sur la signature électronique (OSCSE)[20] constitue la base légale autorisant de manière générale l'identification par vidéo.

La mise en œuvre de cette disposition suppose qu'un organisme accrédité évalue la conformité à cette réglementation des méthodes d'identification à distance utilisées par les fournisseurs de services de certification reconnus. Le SGKPI pourra donc lui aussi dans un avenir proche mettre en place pour l'administration fédérale des procédures d'identification vidéo sur cette base, ce qui permettra de simplifier et d'accélérer l'émission de certificats qualifiés.

Certificats qualifiés chez les fournisseurs

La plupart des fournisseurs de l'administration fédérale ne disposent pas actuellement d'une signature électronique qualifiée, principalement parce qu'ils n'en auraient guère l'usage. D'autre part, s'il est devenu plus difficile d'obtenir une signature qualifiée, surtout depuis que La Poste a cessé à la fin 2020 de vendre la SuisseID, les personnes résidant en Suisse peuvent encore s'adresser à deux prestataires reconnus au moins. Le contrôle de l'identité (la personne doit se présenter en personne avec son passeport ou sa carte d'identité) peut être effectué dans certaines boutiques Swisscom, dans un bureau de poste ou devant notaire.

Les fournisseurs européens de l'administration fédérale sont confrontés à cette difficulté qu'un certificat qualifié délivré dans leur pays conformément au droit de l'UE est légalement assimilé en Suisse à un certificat avancé. Il offre pourtant le niveau de sécurité requis pour la signature d'un contrat, notamment en ce qui concerne l'identification du titulaire. Les fournisseurs ne sont du reste pas obligés de se procurer un certificat électronique. Pour répondre à cette situation, il a été mis en place des procédures qui ménagent plusieurs possibilités. Plusieurs unités administratives de la Confédération ont ainsi aménagé leurs processus contractuels de deux façons :

[17] RS **172.056.11**
[18] RS **172.056.1**
[19] Voir le commentaire du 12 février 2020 de l'ordonnance sur les marchés publics (OMP), art. 11, p. 10
[20] RS **943.032**

Généraliser la signature électronique pour les documents internes à l'administration fédérale

Méthode 1

1) le projet de contrat est envoyé au fournisseur par courrier électronique non signé ;
2) le fournisseur signe le contrat au moyen d'une signature électronique qualifiée et le renvoie par courrier électronique ou sécurisé (Secure Mail), ou il imprime le contrat, le signe à la main et le renvoie par courrier postal ;
3) selon qu'il a reçu le contrat sous forme électronique ou papier, le mandant le renvoie par courrier électronique ou sécurisé (Secure Mail) après l'avoir signé électroniquement ou par courrier postal après l'avoir signé à la main.

Avec cette méthode, le fournisseur a le choix entre un contrat signé de manière électronique et un contrat signé à la main.

Méthode 2

1) voir méthode 1
2) voir méthode 1
3) si le contrat a été reçu sur papier, il est scanné dès réception. La version électronique scannée, ou la version reçue et signée par voie électronique, sont revêtues par l'administration d'une signature électronique qualifiée et renvoyées au fournisseur par courrier électronique ou sécurisé (Secure Mail).

Cette méthode implique que l'administration fédérale ne signe plus que de manière électronique les contrats qu'elle conclut, ce qui fait que l'ensemble de la procédure se déroule désormais sous forme numérique. Mais d'autres possibilités sont également envisageables. Comme il a été dit plus haut, la CA prépare actuellement des recommandations pour la conclusion numérique des contrats de marchés publics, auxquelles il est ici renvoyé.

Validation des signatures électroniques

Si le contrat donne lieu à la signature de documents au moyen d'une signature électronique qualifiée ou d'une signature électronique avancée reposant sur le certificat de signature des employés de l'administration fédérale (classe B), cette signature peut être vérifiée au moyen du validateur de l'administration fédérale (validator.ch). Mais celui-ci ne permet pas de vérifier les certificats avancés d'autres prestataires suisses ou européens reconnus, pas plus que les certificats qualifiés de l'UE et d'autres prestataires étrangers. Il est toutefois possible de soumettre ces certificats à un contrôle limité au moyen d'Adobe Acrobat Reader, en activant dans ce programme la liste de confiance approuvée par Adobe (AATL) et les listes de confiance de l'UE (EUTL).

Reconnaissance internationale des certificats suisses

Dans le contexte des marchés publics conclus avec des entreprises étrangères, la question de la reconnaissance mutuelle des certificats qualifiés et des cachets réglementés tels qu'ils sont définis dans la SCSE n'est pas réglée à ce jour. En révisant celle-ci, la Suisse a mis en place une réglementation conforme sur les plans juridique, technique et organisationnel à la réglementation européenne (règlement (UE) n°910/2014, dit règlement eIDAS). Comme les fournisseurs de solutions de signature du secteur privé permettent généralement de créer des signatures réglementées ou qualifiées conformes, au choix, à la SCSE ou au droit européen, une solution possible pourrait résider dans la reconnaissance unilatérale par la Suisse des signatures établies conformément au règlement eIDAS.

Mesure 1

Le DFJP (OFJ) est chargé de déterminer, avec le concours du DEFR (SECO), du DFAE (DDIP et Secrétariat d'État) DFF (AFD) et du DETEC (OFCOM), les moyens de réaliser la reconnaissance unilatérale ou mutuelle des certificats réglementés et qualifiés avec l'UE et avec d'autres Etats importants pour la Suisse et d'informer le Conseil fédéral du résultat d'ici à la fin 2021.

2.4.5 Digression : décisions administratives et factures à caractères de décision

2.4.5.1 Décisions administratives

La loi fédérale du 20 décembre 1968 sur la procédure administrative (PA)[21] dispose à l'art. 34, al. 1, que les décisions sont notifiées par écrit. Mais il y a controverse sur le point de savoir si cette exigence de la forme écrite implique la signature manuscrite d'un collaborateur de l'autorité de décision[22]. De fait, de nombreuses décisions sont même rendues sans aucune signature, comme les décisions de taxation des autorités douanières ou fiscales.

L'art. 34, al. 1bis, PA précise qu'une décision ne peut être notifiée par voie électronique qu'aux parties qui ont accepté cette forme de transmission, la loi n'exigeant pas du reste l'utilisation d'une signature électronique qualifiée (l'équivalent électronique d'une signature manuscrite). Le législateur ayant ainsi laissé à l'exécutif le soin de déterminer le type de signature requis, le Conseil fédéral a d'abord prescrit à l'art. 9, al. 4, de l'ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures administratives (OCEI-PA)[23] que les décisions notifiées par la voie électronique sont munies d'une signature électronique qualifiée. Il a ensuite limité à l'art. 9, al. 5, OCEI-PA l'utilisation du cachet électronique réglementé au sens de l'art. 2, let. d, SCSE, en affirmant que pouvaient être munies de ce cachet uniquement :

a) les copies électroniques de décisions établies sur support papier et signées à la main ;
b) les décisions notifiées selon une procédure automatisée, qui, en raison de leur grand nombre, ne peuvent pas être signées individuellement par un représentant de l'autorité (décisions notifiées en masse) ;
c) les factures électroniques à caractère de décision ; le cachet peut être apposé par les prestataires habituels pour l'échange électronique de factures, sur mandat de l'autorité compétente.

En raison du cadre juridique applicable et de son interprétation frileuse (notamment de l'art. 9, al. 5, let. b, OCEI-PA) par les unités administratives, le cachet électronique réglementé, dont l'usage est pourtant aussi efficace que peu coûteux, n'est que rarement jugé approprié, surtout, justement, dans le cadre des innombrables procédures d'autorisation simples. Et cela alors même qu'aujourd'hui la majeure partie des décisions de l'administration fédérale sont rendues au moyen de procédures automatisées (GEVER ou applications spécialisées) dans lesquelles les employés sont identifiés de toute façon au moyen du certificat d'authentification (classe B). Si un certificat de cachet réglementé était utilisé pour les personnes physiques en lieu et place d'un certificat de signature qualifiée, non seulement cela n'entraînerait aucune dégradation de la traçabilité et de la transparence, mais cette solution serait nettement plus efficace.

Mesure 2a

Le DFJP (OFJ) est chargé d'étudier avec le concours de la ChF (TNI) s'il serait possible, et si oui, comment, de rendre de manière générale les décisions administratives sans les signer mais en les munissant d'un cachet électronique réglementé, et de soumettre le cas échéant au Conseil fédéral le projet d'une modification de l'ordonnance sur la communication électronique dans le cadre de procédures administratives (OCEI-PA, RS 172.021.2 ; art. 9, al. 4 et 5) avant la fin 2021.

[21] RS **172.021**
[22] Voir Kneubühler/Pedretti in Auer et al., VwVG Kommentar, Artikel 34, Rz. 9f. (commentaire PA, art. 34, ch. marg. 34 ; en langue allemande uniquement).
[23] RS **172.021.2**

Généraliser la signature électronique pour les documents internes à l'administration fédérale

2.4.5.2 Factures à caractères de décision

En sa qualité d'unité spécialisée, l'Administration fédérale des finances (AFF) est responsable des processus d'assistance en matière de finances fédérales. Elle s'efforce de gérer les processus financiers fédéraux de manière intégrée et entièrement numérique, et elle est déjà très avancée à cet égard. L'un des rares domaines où existe encore un potentiel d'optimisation important (plusieurs centaines de milliers de factures par an) est l'envoi électronique des factures assorties d'une indication des voies de recours (« factures à caractère de décision »).

La révision de l'OCEI-PA intervenue en 2017 a permis de créer les conditions juridiques autorisant la notification par voie électronique des factures à caractère de décision via l'une des plates-formes courantes de facturation électronique (Postfinance, SIX), après avoir été munies d'un cachet électronique réglementé.

Depuis, l'envoi de factures au format PDF par courrier électronique s'est lui aussi établi, en raison d'abord de sa simplicité et de son faible coût, mais aussi parce que l'AFF a abrogé à la fin 2019 l'ordonnance du DFF concernant les données et informations électroniques (OeIDI)[24], renonçant par là à exiger une signature en matière de TVA. Il est donc aujourd'hui parfaitement légal d'envoyer des factures au format PDF non signées.

S'agissant des fournisseurs de la Confédération et plus particulièrement des petites entreprises, il a été constaté que l'envoi de factures non signées par courriel est pour eux la solution la plus simple et la moins chère, car elle leur permet d'échapper à l'inscription (payante) auprès d'une plate-forme de facturation électronique. L'AFF a mis en place de son côté une adresse électronique unique à laquelle ses fournisseurs peuvent envoyer leurs factures au format PDF, qui est très utilisée et répond donc à leurs attentes. L'AFF a également mis en place pour l'ensemble des unités administratives les conditions techniques permettant de leur envoyer les factures au format PDF par la voie électronique.

En conséquence, en plus de la révision de l'OCEI-PA évoquée au ch. 2.4.5.1, l'AFF propose d'étudier la possibilité de créer les conditions juridiques qui permettraient d'envoyer les factures à caractère de décision au destinataire également par d'autres canaux sous forme de fichier PDF signé ou cacheté. Une telle mesure répondrait à un fort besoin des clients de l'administration fédérale, favoriserait le développement et la transformation numérique des services de l'administration fédérale et irait ainsi dans le sens du postulat Dobler, qui vise à numériser les processus partout où cela est possible.

Mesure 2b

Le DFJP (OFJ) est chargé d'étudier avec le concours de la ChF (TNI) s'il serait possible, et si oui, comment, de simplifier la notification des factures à caractère de décision par rapport à la réglementation actuellement prévue à l'art. 9, al. 2bis et 3, de l'ordonnance sur la communication électronique dans le cadre de procédures administratives (OCEI-PA, RS 172.021.2), et de soumettre le cas échéant un projet au Conseil fédéral avant la fin 2021.

2.4.6 Digression : affaires du Conseil fédéral

La Constitution affirme à l'art. 174 que le Conseil fédéral est l'autorité directoriale et suprême de la Confédération. La loi sur l'organisation du gouvernement et de l'administration (LOGA)[25] affirme de son côté à l'art. 2, al. 1, que l'administration fédérale est subordonnée au Conseil fédéral. Le Conseil fédéral dirige donc l'administration fédérale, mais n'en fait pas lui-même partie. Même si le Conseil fédéral en sa qualité d'autorité collégiale ne fait pas l'objet du présent rapport, revenons néanmoins brièvement sur la forme écrite de son processus de prise de décision, que le Conseil fédéral a décidé en 2019 de mettre en œuvre sous forme numérique.

[24] RS **641.201.511**
[25] RS **172.010**

L'art. 3, al. 1, OLOGA affirme qu'en règle générale, le Conseil fédéral prend ses décisions en se fondant sur des propositions écrites et après la conclusion de la procédure de co-rapport. Il s'ensuit que les documents de conclusion du processus décisionnel – les décisions du Conseil fédéral – doivent eux aussi être signés.

Le processus décisionnel du Conseil fédéral est divisé en deux parties : la procédure écrite de co-rapport d'une part (art. 15 LOGA), et la séance orale du Conseil fédéral qui suit (art. 21 LOGA). La procédure de co-rapport commence le jour où le département compétent signe sa proposition[26] (art. 5, al. 1bis, OLOGA). L'OLOGA ne dit rien de la forme sous laquelle la demande doit être signée, et, par analogie, cette absence de réglementation s'étend aux co-rapports et avis ainsi qu'aux décisions du Conseil fédéral.

L'art. 5, al. 1bis, OLOGA a été inséré dans celle-ci par l'ordonnance du 24 mai 2006 sur le principe de la transparence dans l'administration (OTrans)[27]. Cette disposition devait permettre de définir précisément le moment où débute la procédure de co-rapport, puisque les documents de cette procédure ne sont pas couverts par le droit d'accès prévu par la loi du 17 décembre sur la transparence (LTrans)[28]. Or, peu importe ici que la proposition ait été signée à la main ou par voie électronique, ce qui explique que rien dans les documents préparatoires n'indique que la signature doive absolument être manuscrite.

Même si le Conseil fédéral n'avait pas spécialement en tête la signature électronique lorsque l'art. 5, al. 1bis, a été inséré dans l'OLOGA, il n'en reste pas moins que la formulation ouverte de la disposition laisse place à ce type de signature. C'est ce qui a amené le Conseil fédéral à décider le 30 janvier 2019 que la signature électronique au sens de la SCSE serait assimilée à la signature manuscrite pour ce qui est des documents de préparation (procédure de co-rapport) et de déroulement des séances du Conseil fédéral, tels que les propositions, les co-rapports et les décisions du Conseil fédéral. Relevons que la signature électronique avec certificat de signature avancé de classe B est suffisante pour signer ces différents documents.

2.4.7 Digression : personnel et contrôles de sécurité relatifs aux personnes

2.4.7.1 Gestion du personnel en général

S'il convient en matière de gestion du personnel de distinguer entre le contrat, acte juridique bilatéral, et la résiliation des rapports de travail, acte juridique unilatéral, ils ont en commun de devoir tous deux être établis en la forme écrite (c.-à-d. : en la forme écrite simple au sens du CO) pour être valables, aux termes de l'art. 13 de la loi sur le personnel de la Confédération (LPers)[29]. Cette forme écrite peut être remplacée par la forme électronique (voir ch. 2.2), assimilée à la signature manuscrite en vertu de l'art. 14, al. 2bis, CO pour autant qu'elle consiste en une signature électronique qualifiée avec horodatage électronique qualifié au sens de la SCSE. Il faut relever ici qu'un contrat de travail entre l'employeur Confédération et une personne qu'il est prévu d'engager n'est pas un document strictement interne à l'administration fédérale au sens où l'entend le postulat donnant lieu au présent rapport.

La résiliation des rapports de travail constitue à l'inverse un acte juridique unilatéral. La notification de la résiliation par l'employeur administration doit être faite par écrit (art. 34, al. 1, PA), et elle ne peut être notifiée par voie électronique (avec signature qualifiée) qu'aux parties qui ont accepté cette forme de transmission (art. 34, al. 1bis, PA). Quant à la résiliation du contrat de travail sous forme électronique par l'employé, elle n'est également possible que si celui-ci dispose d'un certificat qualifié.

À cet égard, le Service standard Services de signature de la Confédération (voir ch. 2.1) a effectué en décembre 2020 une analyse des types d'affaire traitées par l'Office fédéral du personnel (OFPER) afin

[26] Il découle de la systématique de la LOGA et de l'OLOGA que les procédures de co-rapport portant sur une note de discussion (art. 17 LOGA, art. 3, al. 4, OLOGA) ou sur une note d'information (art. 12a LOGA, art. 3, al. 5, OLOGA) commencent elles aussi avec cette signature (art. 3 OLOGA).
[27] RS **152.31**
[28] RS **152.3**
[29] RS **172.220.1**

de déterminer s'il y avait lieu de doter tous les employés de l'administration fédérale centrale d'un certificat de signature qualifié (classe A) ou s'il suffisait de fournir un tel certificat aux seuls employés disposant d'une délégation de signature.

Cette analyse a montré que la conclusion du contrat de travail peut difficilement être effectuée par les deux parties au moyen d'une signature électronique qualifiée, les futurs employés ne disposant qu'exceptionnellement d'un certificat de signature qualifié, acquis sur le marché. Seule la modification d'un contrat de travail déjà conclu ou la résiliation d'un commun accord (qui sont des actes juridiques bilatéraux) pourraient être signés par les deux parties au moyen d'une signature qualifiée, pour autant évidemment que tous les employés se voient remettre à leur engagement un certificat de signature qualifiée. Par ailleurs, le certificat de travail devrait lui aussi être signé au moyen d'une signature qualifiée, de façon à permettre à un futur employeur qui ne ferait pas partie de l'administration fédérale centrale de vérifier son validité à l'aide du service Validator.ch.

D'une manière générale, en matière de personnel, il ne suffit pas que toutes les signatures nécessaires soient apposées sous forme électronique pour assurer le traitement entièrement électronique des procédures qui entrent dans le champ d'application de la PA, encore faut-il que la communication intervienne elle aussi électroniquement. Ce dernier point est régi par l'OCEl-PA. Les art. 34, al. 1bis, PA et 8 OCEl-PA disposent ainsi que les destinataires des décisions doivent à cet égard avoir donné leur accord (l'art. 8 OCEl-PA dit ainsi que « l'autorité peut notifier par voie électronique une décision à une partie à condition qu'elle ait expressément accepté cette forme de communication dans la procédure en cause »). L'art. 9, al. 4, OCEl-PA précise que les décisions doivent être munies d'une signature électronique qualifiée.

S'agissant des autres types d'affaire énumérés par l'OFPER, beaucoup plus fréquentes que les précitées (comme par ex. les conventions d'objectifs ou de formation, ou les évaluations du personnel), les modes de conclusion par voie électronique suivants sont en revanche suffisants, puisque le seul aspect à entrer en ligne de compte est celui de l'attestation ou de la preuve :

- message électronique, le cas échéant avec confirmation par le destinataire (éventuellement avec signature email de classe B, voire chiffrement) ;
- visa dans les métadonnées d'un workflow (par ex. Acta Nova) ;
- signature avancée (classe B) sur un PDF au moyen de la smartcard de la Confédération.

Conclusion

Traiter par voie électronique le nombre relativement faible des types d'affaire relevant de la gestion du personnel qui, en raison de l'exigence de la forme écrite, nécessitent de la part des deux parties une signature électronique qualifiée, obligerait à doter tous les employés de l'administration fédérale centrale d'une signature électronique qualifiée. Ce serait là un effort disproportionné qui n'aurait guère de sens à l'heure actuelle. À l'inverse, la grande majorité des types d'affaire traités quotidiennement dans le cadre de la gestion du personnel en général ne nécessitent pas de signature qualifiée et peuvent, lorsqu'une signature est nécessaire, être traitées sur la base du certificat de signature avancée (classe B) des employés.

2.4.7.2 Contrôles de sécurité relatifs aux personnes

Les contrôles de sécurité relatifs aux personnes (CSP) effectués par la ChF et surtout par le Département fédéral de la défense, de la protection de la population et des sports (DDPS) sont relativement nombreux. Ces CSP sont régis par l'ordonnance du 4 mars 2011 sur les contrôles de sécurité relatifs aux personnes (OCSP)[30].

La loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[31] prévoit à l'art. 19, al. 3, qu'un CSP ne peut être effectué qu'avec le consentement de la

[30] RS **120.4**
[31] RS **120**

personne concernée. C'est pourquoi l'OCSP dispose à l'art. 14, al. 5, que la personne à contrôler doit remplir et signer un formulaire ad hoc par lequel elle confirme son consentement.

Ce formulaire devait autrefois être signé à la main par la personne à contrôler. Mais depuis le 1er janvier 2021, le Service spécialisé CSP de la ChF accepte également pour la répétition du contrôle que les employés de la Confédération signent au moyen d'une signature électronique avancée avec certificat de signature de classe B. La signature manuscrite continuera d'être exigée pour un premier emploi, car la personne à contrôler ne dispose généralement pas encore d'un certificat de signature qualifié.

Le Service spécialisé CSP du DDPS estime pour sa part qu'une signature avancée ne suffit pas juridiquement, et exige dans tous les cas une signature manuscrite ou, au cas où le formulaire de contrôle serait remis sous forme électronique, une signature électronique qualifiée. En effet, le DDPS admet certes que l'art. 6 OCEl-PA autoriserait a priori une remise à l'autorité du formulaire sans signature électronique qualifiée (donc même sans signature du tout) pour autant que l'identification de l'expéditeur et l'intégrité de la communication soient assurées par d'autres moyens.

La phrase suivante précise toutefois expressément qu'est réservé le cas où le droit fédéral exige qu'un document spécifique soit signé – condition précisément prévue par l'OCSP. On peut cependant se demander si la signature électronique qualifiée est la seule à pouvoir être considérée comme une signature valide attestant le consentement de la personne concernée, ou si la signature avancée avec certificat de signature de classe B des employés fédéraux ne pourrait l'être elle aussi.

En vertu du droit en vigueur[32], le résultat d'un CSP constitue une décision, qui peut prendre la forme d'une déclaration de sécurité (art. 22, al. 1, let. a, OCSP), d'une déclaration de sécurité sous réserve (art. 22, al. 1, let. b, OCSP), d'une déclaration de risque (art. 22, al. 1, let. c, OCSP) ou d'une constatation (art. 22, al. 1, let. d, OCSP). Ces décisions sont notifiées par écrit (art. 22, al. 2 à 4, OCSP). Comme une personne qui fait l'objet d'un CSP n'est pas encore employée, ce CSP ne constitue pas une procédure interne à l'administration fédérale au sens du postulat donnant lieu au présent rapport, et la décision doit donc soit comme précédemment être revêtue d'une signature manuscrite, soit, pour autant que la personne contrôlée y consente, être signée et notifiée sous forme électronique qualifiée (art. 34, al. 1bis, PA, et 9, al. 4, OCEl-PA). Les répétitions des contrôles de sécurité prévues à l'art. 18 OCSP, en revanche, sont liées à la fonction des personnes concernées, ce qui signifie que cette procédure peut être considérée comme interne à l'administration fédérale au sens où l'entend le postulat donnant lieu au présent rapport.

Conclusion

Il serait possible de traiter par voie entièrement électronique les procédures liées à la répétition des CSP pour les employés déjà en poste au sein de l'administration fédérale, à condition de modifier l'OCSP de façon que celle-ci autorise a) la personne concernée à remettre sans l'avoir revêtu d'une signature électronique qualifiée le formulaire de contrôle qu'elle doit signer, et b) l'autorité à notifier sous forme électronique et chiffrée ses décisions sans avoir à s'assurer au préalable du consentement exprès de la personne concernée.

Il importe cependant de relever que les CSP qui relèvent de la ChF ne représentent qu'une très petite partie de l'ensemble des CSP, ceux-ci étant principalement effectués par le DDPS et sur des personnes extérieures à la Confédération. En ce qui concerne la plupart des CSP, il n'est donc guère envisageable aujourd'hui de les traiter par voie entièrement électronique, car la grande majorité des personnes à contrôler ne disposent probablement pas d'un certificat de signature électronique ou de moyens d'identification électroniques équivalents.

[32] Aux termes de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI), le résultat de l'évaluation effectuée au titre du contrôle de sécurité relatif aux personnes (*déclaration*) constituera un acte matériel au sens de l'art. 25*a* PA, contre lequel il sera possible de recourir auprès du Tribunal administratif fédéral (art. 44, al. 3, LSI). Les déclarations des services spécialisés CSP auront en effet « simplement » valeur de recommandation (art. 41, al. 1, LSI). Notons que le droit en vigueur prévoit d'ores et déjà que l'autorité décisionnelle n'est pas liée par la décision de l'autorité chargée du contrôle de sécurité (art. 23, al. 1, OCSP).

Généraliser la signature électronique pour les documents internes à l'administration fédérale

On a vu toutefois à l'exemple précité que les unités administratives peuvent interpréter de manières diverses le droit qui régit l'usage de la signature électronique. Il convient pour chacun de ces cas de faire établir des avis internes afin de lever autant que possible les obstacles auxquels se heurte une transformation numérique rapide, au moyen soit d'une interprétation des textes, soit de propositions d'ajustements susceptibles d'être mis en œuvre sans délai à l'échelon de l'ordonnance.

Mesure 3

Le DDPS (SG-DDPS) est chargé de s'assurer, avec le concours de la ChF (service spécialisé CSP), que l'élaboration de la législation d'application de la loi sur la sécurité de l'information actuellement en cours sera mise à profit pour abroger l'obligation formelle de demander à la personne assujettie à un contrôle de sécurité qu'elle signe le formulaire par lequel elle consent au contrôle, du moins en ce qui concerne les répétitions des contrôles. Le consentement devra toutefois comme précédemment être donné par écrit et être vérifiable.

2.4.8 Digression : légalisations

La « légalisation » d'un document vise à lui conférer l'équivalence avec un acte authentique d'un autre pays. Cette démarche suppose souvent une « authentification » de ce document par une autorité de l'État de provenance.

En Suisse, c'est la ChF qui est compétente pour légaliser les signatures des unités de l'administration fédérale (y compris des ambassades et des consulats de Suisse), celles des chancelleries d'État des cantons et des organisations qui assument des tâches publiques dans l'intérêt du pays tout entier. Cette procédure formelle de la légalisation a été remplacée pour certains États par la procédure un peu plus simple de l'apostille, en vertu de la Convention de La Haye du 5 octobre 1961 supprimant l'exigence de la légalisation des actes publics étrangers[33]. La ChF est également chargée de délivrer l'apostille prévue à l'art. 3 de ladite Convention, dans la mesure où il s'agit d'un acte émanant d'une unité de l'administration fédérale.

La légalisation et la délivrance de l'apostille supposent toutes deux que la ChF dispose de copies de la signature à authentifier ou, en vue de l'apposition d'une apostille, à certifier. La mise à jour en continu du registre des spécimens de signatures et la comparaison manuelle des signatures sont des tâches fastidieuses.

Si la légalisation et l'apposition d'une apostille sont en Suisse des procédures entièrement analogiques, le droit international prévoit depuis près de 15 ans la possibilité de les mener sous forme électronique, avec par ex. la numérisation de l'acte sous-jacent et sa signature au moyen d'une apostille électronique[34]. Cette apostille électronique a été mise en place dans plus de 40 pays, mais non en Suisse.

Il est en revanche déjà possible aujourd'hui de vérifier les signatures numériques de l'administration fédérale. On trouve en effet à l'adresse validator.ch un service de l'administration fédérale qui permet de vérifier à tout moment et de partout la validité des signatures électroniques apposées sur les documents des autorités suisses. Selon le type de document, seront vérifiés la signature et l'intégrité du fichier signé, le statut du certificat de signature (révoqué / non révoqué) et, le cas échéant, la validité de l'horodatage.

[33] RS **0.172.030.4**
[34] Pour en savoir plus, voir : www.hcch.net > Instruments > Conventions > 12 > apostille électronique

3 Analyse technique et conditions générales

3.1 Gestion électronique des affaires dans l'administration fédérale

L'ordonnance GEVER, qui se fonde sur l'art. 57*h*, al. 3, LOGA, dispose que l'administration fédérale doit traiter les informations importantes pour les affaires au moyen de systèmes de gestion électronique des affaires (systèmes GEVER) (art. 2, al. 1). Pour ce faire, les unités administratives utilisent GEVER standardisé (art. 3, al. 1). La solution standardisée GEVER Acta Nova a été installée entre-temps pour quelque 30 000 postes de travail de l'administration fédérale centrale (voir ch. 1.2 ci-dessus). Côté personnel, ont notamment été mis en service le système d'information pour la gestion des données du personnel (IGDP) et le E-Dossier personnel.

3.2 Confirmations électroniques dans Acta Nova

L'art. 14 de l'ordonnance GEVER dispose que les systèmes GEVER doivent permettre de *confirmer* des informations *par voie électronique*, notamment pour confirmer une prise de connaissance, pour requérir une approbation et pour donner son approbation. Comme cela a déjà été mentionné, tous les employés de l'administration fédérale sont identifiés au cours de ces processus par un certificat d'authentification sur leur smartcard via une double authentification. Il est ainsi possible de déterminer avec précision qui a procédé à quelle confirmation GEVER, et quand précisément.

En termes de traçabilité, la confirmation GEVER est ainsi comparable à une signature électronique munie d'un certificat de signature avancé (classe B). En l'occurrence, l'authenticité est attestée indirectement par le certificat d'authentification avec lequel les employés se connectent au système GEVER, et l'intégrité du document est garantie par l'établissement des versions successives.

Le système GEVER prévoit les trois confirmations suivantes[35] :
a) « pour information », pour confirmer une prise de connaissance ;
b) « pour visa », pour requérir l'aval d'un tiers avant l'approbation ;
c) « pour approbation », pour approuver.

Ces confirmations servent à gérer des processus plus ou moins standardisés basés sur la division du travail. Des exemples typiques de processus internes à l'administration fédérale sont le traitement des propositions adressées aux départements ou au Conseil fédéral dans le cadre de la *préparation* de la procédure de co-rapport (voir ch. 2.4.6 ci-dessus) ou l'élaboration d'actes normatifs. Dans le cadre de ces processus, des projets initiaux sont établis par certaines personnes ou certains services, lesquels sont ensuite complétés, retravaillés ou vérifiés par d'autres personnes ou services en fonction de certains impératifs, avant d'être finalement approuvés à différents niveaux hiérarchiques. Ces processus électroniques automatisés ont remplacé depuis longtemps dans de nombreux domaines, mais pas encore dans tous, le travail sur papier et donc, le cas échéant, les signatures manuscrites ou les sigles des collaborateurs.

3.3 Signature électronique dans Acta Nova

Acta Nova permet d'effectuer non seulement des *confirmations GEVER*, mais aussi des signatures électroniques avec des certificats de signature avancés (classe B), avec des cachets électroniques réglementés (appelés certificats d'autorité, de classe A) et avec des certificats de signature qualifiés (classe A) au sens de la SCSE. Les documents (PDF) eux-mêmes sont signés électroniquement, et la signature forme avec le document une unité indissociable, contrairement aux confirmations GEVER, qui figurent dans les métadonnées, c'est-à-dire en dehors du document. Par conséquent, les métadonnées ne sont pas transmises en étant intégrées dans le document lorsqu'un document quitte le système GEVER. C'est pourquoi il faudrait munir d'une signature électronique les documents déjà approuvés qui

[35] P. 14 du rapport explicatif de la ChF relatif à l'ordonnance GEVER du 3 avril 2019.

quittent le système GEVER ou qui sont acheminés à l'extérieur, et dont l'intégrité et l'authenticité requièrent une protection particulière.

Depuis 2018, il est possible de générer des signatures électroniques dans les systèmes GEVER (notamment dans Acta Nova) avec le logiciel Open eGov LocalSigner, qui est développé pour l'administration fédérale depuis 2008. Les fonctionnalités sont certes limitées, mais la création d'une signature électronique ne nécessite que quelques clics. Dans le cadre du développement d'Acta Nova, il est prévu de remplacer le logiciel Open eGov LocalSigner et d'intégrer le service de signature basé sur serveur. L'extension de la signature unique actuelle par une fonctionnalité de signature par lots débutera probablement à l'échelle fédérale à partir de l'automne 2021. En automne 2020, il a déjà été possible d'introduire la fonctionnalité de cachetage en masse à partir d'applications spécialisées, laquelle est activement utilisée par des applications spécialisées depuis mars 2021. Par conséquent, d'ici là, la création d'une signature électronique via Open eGov LocalSigner ou sa vérification à l'aide du validateur est certes possible, mais elle plus compliquée et plus coûteuse que l'utilisation de confirmations GEVER.

Des processus administratifs efficaces et allégés supposent que les moyens les plus exigeants sur les plans pratique et technique ne soient utilisés que dans les cas où ils sont réellement nécessaires. Dans les échanges administratifs internes à l'administration fédérale, de simples confirmations GEVER sont généralement suffisantes ; les signatures et les cachets électroniques ne sont généralement pas requis au sein de l'administration fédérale, mais ils sont néanmoins – comme il a été indiqué au ch. 2.4 ci-dessus – judicieux, voire nécessaires, dans certains cas. L'utilisation de signatures électroniques se justifie donc surtout dans les documents juridiquement importants qui sont échangés avec des personnes et des services avant tout *extérieurs* à l'administration fédérale[36].

4 Synthèse

4.1 Avantages de la confirmation électronique par rapport à la signature électronique

Pour disposer de processus administratifs efficaces et allégés, il est important de n'utiliser le moyen le plus complexe d'un point de vue pratique et technique – c'est-à-dire la signature électronique personnelle ou le cachet électronique – que dans les cas où cela est nécessaire. Dans le cas des échanges au sein de l'administration fédérale, les confirmations GEVER et, si nécessaire, les signatures électroniques avancées (classe B), qui peuvent être considérées comme comparables en termes de traçabilité, sont généralement suffisantes. La signature qualifiée ou le cachet réglementé doit ou devrait – hormis les exceptions au sein de l'administration fédérale énoncées au ch. 2.4 – être utilisé en priorité pour les documents juridiquement importants qui sont échangés avec des personnes et des services *extérieurs* à l'administration fédérale.

Le grand avantage d'une confirmation électronique est sa simplicité. Les signatures électroniques, qui prennent plus de temps, ne doivent être utilisées que lorsque cela est nécessaire ou judicieux.

4.2 Lever les « obstacles » juridiques et autres mesures requises

Comme il a été indiqué au ch. 2.4, les conditions nécessaires à la gestion électronique des affaires au sein de l'administration fédérale sont en place, que ce soit sous la forme de confirmations électroniques (ch. 3.2) ou de signatures électroniques (ch. 3.3). En ce qui concerne les confirmations électroniques, les employés fédéraux peuvent utiliser le système de gestion électronique des affaires Acta Nova. C'est

[36] Ainsi, les contrats de droit privé et les décisions administratives pour lesquels une signature électronique qualifiée est requise par la loi ne peuvent pas être délivrés avec une simple confirmation GEVER. Cette exigence formelle est le cas normal pour les décisions administratives (art. 34, al. 1bis, PA et art. 9, al. 4 et 5, OCEl-PA).
En revanche, l'utilisation de la forme écrite, même si elle n'est pas exigée par la loi, est nécessaire dans de nombreux cas pour des raisons pratiques afin de clarifier le contenu du contrat et de savoir s'il s'agit seulement d'un projet ou déjà d'un contrat accepté par toutes les parties, donc contraignant.

précisément pendant la pandémie de coronavirus et pendant la période de travail à domicile qui s'en est suivie qu'on s'est rendu compte que l'échange de documents sous forme papier est largement inutile et que la gestion purement électronique des affaires est possible. Cette situation a abouti en fin de compte à une prise de conscience accrue du facteur le plus important dans l'utilisation de la gestion électronique des affaires, à savoir le facteur humain. La crise du coronavirus a ainsi énormément accéléré la transition vers une gestion purement numérique des affaires.

Enfin, le Conseil fédéral lui-même a envoyé un signal fort en faveur de la transition numérique, le 30 janvier 2019, en décidant que les signatures manuscrites et les signatures électroniques seraient équivalentes pour la procédure de co-rapport (voir ch. 2.4.6).

5 Conclusions

L'administration fédérale a connu une évolution technique rapide non seulement depuis la transmission du postulat 18.3502 Dobler, intitulé « Généraliser la signature électronique pour les documents internes à l'administration fédérale », mais aussi à la faveur, d'une part, de l'introduction – désormais achevée – du système unifié GEVER Acta Nova, et, d'autre part, du développement et de l'intégration des nouveaux services de signature basés sur serveur.

Dans l'ensemble, le présent rapport conclut qu'il n'est guère nécessaire d'agir. Les bases légales des signatures électroniques sont suffisantes pour le domaine interne à l'administration fédérale. Par contre, il est apparu que les exigences techniques applicables à l'utilisation de la signature électronique pourraient encore être améliorées (remplacement du logiciel Open eGov LocalSigner, qui est dépassé). Toutefois, les travaux visant à le remplacer par les services de signature 2.0 et à relier ces derniers à Acta Nova et à certaines applications spécialisées importantes sont en cours et seront vraisemblablement achevés avant la fin 2021 (ch. 3.3).

Dans toute la mesure du possible, il convient de renoncer à l'utilisation de signatures électroniques pour les transactions internes à l'administration fédérale et d'utiliser plutôt les fonctions Acta Nova des confirmations GEVER et les fonctions analogues du système SAP ERP. Les signatures électroniques ne doivent être utilisées que pour les documents finaux (contrats, conventions, décisions internes) et uniquement dans les cas où les documents quittent le système/l'entité GEVER ou sont stockés en dehors du système GEVER, et où leur intégrité et leur authenticité requièrent une protection particulière. Cette procédure est réglée dans la directive interne E018, mise à jour en continu, intitulée « Utilisation et validation des signatures électroniques dans des documents PDF ».

Comme les employés peuvent soit travailler avec leur certificat d'authentification identifié (double authentification avec certificat de classe B) dans le système GEVER ou dans des applications spécialisées, soit signer des documents (PDF) et des courriels avec leur certificat de signature avancé (classe B), il n'y a aucun déficit de sécurité en ce qui concerne la signature électronique des documents administratifs internes et des processus d'affaires électroniques, que ce soit au niveau de l'infrastructure ou des réglementations. Dans les cas où les confirmations GEVER ne conviennent pas, les signatures avec des certificats de signature avancés (classe B) sont suffisantes dans quasiment tous les cas pour le domaine interne à l'administration fédérale.

Chaque unité administrative est tenue non seulement d'analyser en détail les réglementations juridiques auxquelles elle est soumise, mais aussi de simplifier le déroulement des processus. À cet égard, il convient de déterminer les rares cas dans lesquels les documents administratifs internes doivent être munis d'une signature *qualifiée* (voir par ex. ch. 2.3.5). Par conséquent, les personnes qui sont chargées de cette tâche doivent disposer d'un certificat de signature qualifié (classe A), qui peut être commandé à tout moment auprès de l'OFIT.

Par ailleurs, le secteur TNI de la ChF continue d'épauler les Services du Parlement en vue de l'achat éventuel des services standard de la Confédération afin d'instaurer une correspondance sans papier

entre l'exécutif et le parlement, par exemple dans le domaine de la documentation supplémentaire afférente au budget et au compte d'État.

Ainsi, l'objectif visé par le postulat donnant lieu au présent rapport a été atteint puisqu'il est possible d'utiliser la signature électronique partout, sans que ce soit pour autant obligatoire (c.-à-d. sans qu'il faille renoncer à la signature manuscrite). Outre les trois mesures précitées, quatre mesures supplémentaires seront mises en œuvre afin de renforcer encore davantage l'efficacité du recours à la signature électronique dans l'administration fédérale.

L'art. 29 OLOGA dispose que les départements et la ChF doivent se doter d'un règlement d'organisation contenant notamment des règles régissant les signatures (al. 1) et que ces règlements doivent être publics (al. 3). L'art. 49, al. 3, LOGA dispose quant à lui non seulement que les directeurs de groupement ou d'office et les secrétaires généraux doivent régler la délégation de signature dans leur domaine de compétence, mais aussi que les contrats, les décisions et les autres engagements formels de la Confédération portant sur un montant supérieur à 100 000 francs requièrent une double signature.

Mesure 4

Tous les départements et la ChF sont chargés, à la faveur de la révision des lois et des ordonnances qui sont de leur ressort, de faire en sorte que des solutions électroniques privilégiant la forme numérique (*digital first*) soient proposées pour la gestion des affaires avec des personnes ou des entités internes ou externes, en tenant compte de la directive interne E018.

Les réglementations relatives aux signatures doivent être adaptées au domaine électronique de façon à ce que soient déterminées les affaires pour lesquelles il est permis d'utiliser une signature électronique qualifiée, une signature électronique avancée (classe B) ou un cachet électronique réglementé. À cet égard, les art. 37 ss de l'ordonnance sur les finances de la Confédération (OFC)[37], qui régissent la signature des pièces justificatives et la signature des autorisations d'exécuter des ordres de paiement, doivent également être respectés. Enfin, les éventuelles exigences formelles relevant du droit civil doivent elles aussi être observées.

Mesure 5

Les départements et la ChF sont chargés de réviser leurs réglementations relatives aux signatures avant la fin 2022 de façon à simplifier autant que possible les procédures. Les signatures formelles au sens juridique du terme (signatures manuscrites ou qualifiées au sens de la SCSE) ne seront plus exigées dans le cadre des processus d'affaires internes à l'administration fédérale que si elles sont nécessaires en raison d'une exigence de validité explicite ou d'exigences formelles relevant du droit civil. Dans les autres cas, les décisions seront prises et documentées au moyen de certificats avancés de classe B ou au moyen de confirmations ou de visas dans le cadre des processus d'affaires (par ex. GEVER ou SAP). Les départements et la ChF s'assurent que les réglementations révisées sont mises en œuvre dans leurs unités respectives.

Pour garantir une utilisation efficace des différentes possibilités qui existent relativement à la signature électronique qualifiée, à la signature avancée, au cachet électronique et à la consignation des processus d'affaires, des outils d'aide seront développés et proposés aux unités administratives. Les personnes et les entités internes ou externes à l'administration fédérale trouveront toutes les informations nécessaires concernant la signature électronique sur la page Internet de l'OFIT[38] et sur celle de l'OFCOM[39].

[37] RS **611.01**
[38] www.bit.admin.ch/bit/fr/home/themes/elektronische-signatur.html
[39] www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-numerique-et-internet/communication-numerique/signature-electronique.html

Généraliser la signature électronique pour les documents internes à l'administration fédérale

Mesure 6

La ChF (TNI) est chargée de développer avant la fin 2021 un outil d'aide qui permette de répondre aux questions autour des formes de déclaration de volonté qui, à la lumière de l'expérience, sont susceptibles d'être mises en œuvre en fonction des différentes modalités de collaboration interne ou externe.

Le processus d'identification prescrit par la loi pour la délivrance d'un certificat qualifié sera rendu plus efficace et, surtout, plus convivial. Il s'agira notamment d'examiner s'il est possible de faire en sorte que les collaborateurs qui ne travaillent pas à Berne n'aient plus à se rendre en personne sur place (c'est-à-dire à la *Swiss Government* PKI de l'OFIT) à chaque fois qu'un certificat doit leur être délivré, compte tenu qu'ils ont déjà fait l'objet d'une identification personnelle à leur entrée en fonctions.

Mesure 7

La ChF (TNI) est chargée, avec le concours du DFF (OFIT), de veiller à ce que, avant la fin 2022, les processus de gestion certifiés des certificats électroniques, en particulier des certificats qualifiés et des cachets électroniques réglementés, soient rendus plus efficaces et plus efficients au sein de l'administration fédérale centrale.