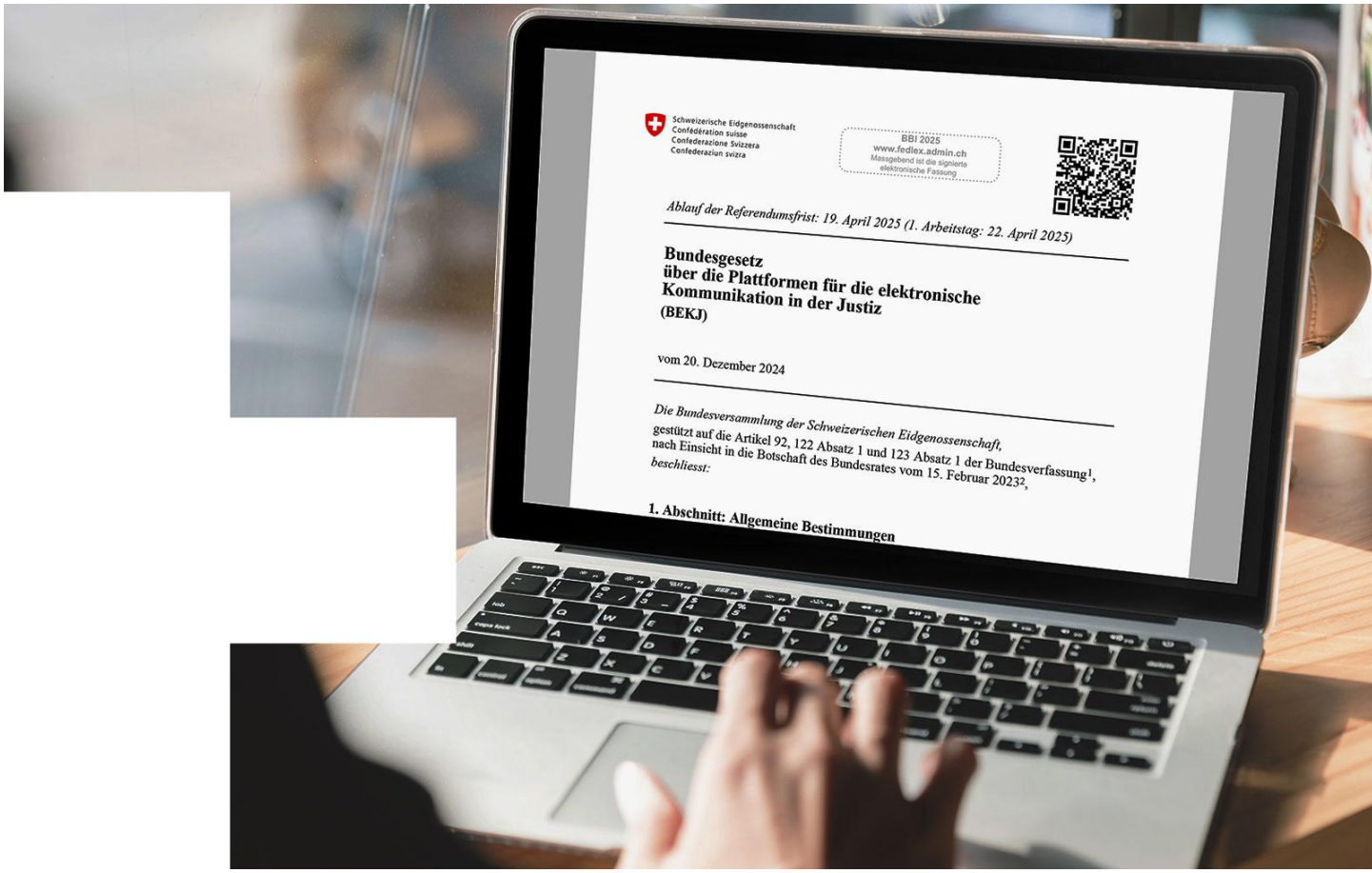
PROJET
Justitia 4.0



Guide pratique

Cachet d'autorité (art. 22, al. 2, LPCJ)

Le présent guide pratique s'adresse aux **autorités judiciaires** assurant la direction de la procédure qui doivent **apposer un cachet sur certains documents** avant de procéder à une **notification via la plateforme justitia.swiss**.

Conformément à l'art. 22, al. 2, LPCJ, les autorités apposent sur les documents, avant leur transmission à une plateforme, un *cachet électronique réglementé* et un *horodatage électronique qualifié* au sens de la loi du 18 mars 2016 sur la signature électronique (SCSE). Si le cachet ou l'horodatage manque, la plateforme refuse les documents.

Contrairement à la **s**ignature **é**lectronique **q**ualifiée (SEQ), un **cachet électronique réglementé** (cachet d'autorité) n'est exigé que d'une **personne morale** (corporation, autorité, cantons, communes, entreprises de droit privé). Ce cachet d'autorité atteste de l'authenticité des documents et de l'identité d'une personne morale.

En revanche, la SEQ[1] remplace la signature manuscrite d'une personne physique. Elle atteste de l'authenticité des documents et de l'identité de la personne physique signataire dans l'échange électronique de données.

1 Qu'est-ce qu'un cachet électronique réglementé avec horodatage électronique ?

Un **cachet électronique réglementé** est un type de signature électronique spécifique prescrit par la loi, utilisé par les autorités et les personnes morales pour signer des documents numériques et identifier l'autorité ayant créé et envoyé le document (authentification).

L'art. 2, al. b, en relation avec l'art. 7 de la loi fédérale sur les services de certification dans le domaine de la signature électronique et des autres applications des certificats numériques du 18 mars 2016, état au 1er janvier 2020, (SCSE), définit la signature électronique avancée comme suit :
Une signature électronique avancée créée au moyen d'un dispositif sécurisé de création de cachet au sens de l'art. 6 SCSE et fondée 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 et valable au moment de la création du cachet électronique.

L'horodatage qualifié[2] fourni avec le cachet électronique réglementé garantit l'intégrité du document.

En outre, à des fins de conservation des preuves à long terme, chaque cachet électronique réglementé (et chaque signature électronique qualifiée [SEQ]) est également assorti d'un horodatage électronique qualifié.

Il est recommandé d'apposer une image visible sur le document cacheté.

La Chancellerie fédérale avait par exemple mis en œuvre cette mesure jusqu'à la fin de l'année 2025 lors de la publication de la version PDF de la Feuille fédérale.

	
Image d'un cachet électronique réglementé de Zurich	*Feuille fédérale, FF 2025 19, message LPCJ*

[1] cf. Guide pratique Signature électronique qualifiée (SEQ)

[2] cf. art. 2, let. j, SCSE du 18 mars 2016 (état au 1er janvier 2020)

Un cachet d'autorité avec horodatage au sens de la LPCJ ou de la SCSE est synonyme de :

Valeur légale : *en Suisse, les cachets électroniques qualifiés sont reconnus par la loi et sont juridiquement contraignants.*

Authenticité : *le cachet électronique confirme que le document provient effectivement de l'autorité indiquée.*

Intégrité : *il garantit que le document n'a pas été modifié depuis sa création ou depuis l'apposition du cachet.*

Confiance dans les processus numériques : *les cachets électroniques renforcent la confiance dans les documents électroniques et les processus administratifs numériques.*

Efficacité et numérisation : *ils permettent de mettre en place des processus sans papier, car les documents numériques peuvent être utilisés de manière juridiquement valable, sans authentification physique ni cachet.*

Les documents munis d'une signature électronique et d'un cachet électronique qualifiés peuvent faire l'objet d'un contrôle d'origine et d'intégrité à l'aide d'un logiciel approprié (voir ch. 5, validateur). L'impression de ce document muni d'un cachet numérique entraîne la perte des garanties techniques d'authenticité et d'intégrité : il s'agit donc d'une simple copie qui ne répond pas aux exigences de la forme écrite. Ces caractéristiques qualifiantes sont donc perdues en cas de changement de support, il n'est alors plus possible de reconnaître une falsification. Il y a rupture de transmission lorsque le **document doit être imprimé et envoyé par la poste**. Pour ces raisons, les lois fédérales de procédure exigent, dès l'entrée en vigueur de la LPCJ, **la signature manuscrite** (des personnes compétentes) **en cas d'envoi postal traditionnel**.[3]

2 À partir de quand les autorités doivent-elles utiliser le cachet électronique réglementé avec horodatage ?

Les autorités judiciaires ont besoin d'un cachet d'autorité à partir de l'entrée en vigueur de la LPCJ si, à partir de cette date, elles souhaitent également **transmettre des notifications électroniques aux avocat-e-s et aux parties à la procédure** via la plateforme justitia.swiss.[3] La plateforme vérifie si le cachet d'autorité figure sur un document. Le cachet d'autorité doit correspondre au cachet que l'autorité a communiqué lors de l'enregistrement de son profil.

Dans tous les cas, les autorités judiciaires ont besoin d'un cachet d'autorité à partir de la date à laquelle le canton décide que les procédures en vertu de la LPCJ devront **obligatoirement** être transmises **par voie électronique** via la plateforme justitia.swiss (ce que l'on appelle « l'obligation cantonale »), ou à l'expiration de la période de transition de cinq ans après l'entrée en vigueur de la LPCJ, conformément à l'art. 37, al. 1, LPCJ.

Pendant la phase pilote, et avant l'entrée en vigueur de la LPCJ, le document principal d'un envoi nécessite une SEQ, mais le cachet de l'autorité n'est pas encore requis.

En l'état actuel des connaissances, aucun cachet d'autorité n'est requis pour l'événement de processus « **consultation des dossiers** ».

[3] L'entrée en vigueur de la LPCJ entraîne la modification des lois mentionnées dans les annexes (p. ex. art. 201, al. 2, CPP, art. 353, al. 1, let. k, CPP, art. 133, let. g et h, CPC, art. 235, al. 1, let. f, CPC, art. 238, let. h, CPC, etc.).

3 Conseils à l'intention des autorités judiciaires

Avec l'entrée en vigueur de la LPCJ, un cachet d'autorité doit être apposé sur un document, en règle générale sur la décision (jugement, ordonnance, prononcé, mandat de comparution ou ordonnance pénale, etc.) des autorités judiciaires (art. 22, al. 2, LPCJ), si ce document est envoyé via la plateforme justitia.swiss. Les annexes jointes et les autres documents ne nécessitent pas de cachet d'autorité (en l'état actuel des connaissances, un cachet par notification est suffisant)[4].

Outre **l'acquisition du futur cachet d'autorité et de l'horodatage** auprès d'un émetteur de certificat reconnu, les autorités judiciaires doivent réfléchir à la manière dont l'apposition de ces cachets d'autorité sera intégrée dans les processus de travail de leurs divisions et de leurs chancelleries.

Les réflexions suivantes se posent :

- Le pouvoir judiciaire dispose-t-il d'un cachet visuel différent de celui des autres autorités administratives cantonales ?
- Qui est habilité à apposer le cachet d'autorité et à quelle étape de travail celui-ci est-il apposé sur un document ?
- Quels membres du personnel ont besoin du cachet d'autorité à leur poste de travail pour l'apposer sur les documents prévus ?
- Certains documents nécessitent-ils en outre des signatures électroniques qualifiées (SEQ) en raison d'une base légale cantonale ou interne à l'autorité ?
- Qui appose les éventuelles SEQ nécessaires et sur quels documents ? Des instructions internes existent-elles à ce sujet et comment les processus de travail sont-ils organisés ?
- À l'avenir, le cachet d'autorité sera-t-il apposé à partir de l'application métier ou de l'ADJ ? Comment résoudre la question de l'apposition des cachets et des éventuelles SEQ nécessaires pendant la période de transition, jusqu'à ce que l'application métier ou l'ADJ soit mise à disposition ?
- Justitia 4.0 ou la corporation de droit public justitia.swiss a-t-elle été informée des caractéristiques d'identification nécessaires au cachet d'autorité avant le début des notifications via la plateforme justitia.swiss ?
- Quelles autres **directives concernant la gestion hybride des dossiers** doivent être respectées si les jugements, les ordonnances, les ordonnances pénales, les mandats de comparution, etc. ne sont **pas** envoyés aux parties non représentées par un-e avocat-e via la plateforme justitia.swiss, **mais par la poste comme auparavant** ?[5] Les processus de travail à cet égard doivent être discutés et documentés suffisamment tôt avec le personnel des chancelleries.

[4] Les dispositions d'exécution de la LPCJ sont actuellement en consultation. Il n'est donc pas encore possible de répondre définitivement à la question de savoir si un seul document muni d'un cachet suffit, ni quelles autorités doivent apposer un cachet sur leurs documents.

[5] Par exemple, les modifications de la loi prévues dans les annexes avec l'entrée en vigueur de la LPCJ, à l'art. 201, al. 2, CPP, à l'art. 353, al. 1, let. k, CPP, à l'art. 133, let. g et h, CPC, à l'art. 235, al. 1, let. f, CPC, à l'art. 238, let. h, CPC, etc.

4 Comment une autorité se procure-t-elle un cachet électronique réglementé avec horodatage ?

En Suisse, les autorités et organisations se procurent le cachet électronique réglementé et l'horodatage électronique réglementé en s'adressant à des services de certification reconnus, appelés fournisseurs de services de certification CSP (Certification Service Providers).

Émetteurs reconnus de certificats SEQ conformément à la SCSE, voir le site Internet de la Confédération[6] : Swisscom, SwissSign, DigiCert, OFIT.

L'acquisition d'un cachet nécessite toutefois **l'attribution d'un numéro IDE valable**. L'activité du ministère public et des tribunaux relève de la souveraineté et n'est donc pas soumise à la TVA. En règle générale, le canton dispose d'un numéro IDE, mais pas les autorités judiciaires. Toutefois, ces dernières peuvent utiliser le cachet du canton en tant que « sous-unité ».

eOperations Suisse SA[7] a lancé un appel d'offres pour l'acquisition de cachets et de signatures auprès d'éditeurs de cachets d'autorités, afin que les cantons et leurs communes puissent se procurer des cachets et des signatures. Les bénéficiaires sont les cantons (23, à l'exception de BE, GE, VD) ayant rejoint eOperations Suisse SA ainsi que leurs quelque 1500 communes/districts.[8]

5 Questions issues de la pratique

Les autorités judiciaires peuvent-elles créer deux profils distincts sur la plateforme et déposer le même cachet d'autorité pour les deux profils ?

Exemple : le tribunal régional / d'arrondissement / de district et le tribunal des mesures de contrainte sont organisés ensemble sur le plan institutionnel au sein d'une même autorité judiciaire. En raison de leurs compétences distinctes, ils souhaitent toutefois disposer de deux profils séparés sur la plateforme justitia.swiss. Toutefois, pour des raisons organisationnelles, ils ne possèdent qu'un seul **cachet d'autorité** pour leurs organisations : tribunal régional / d'arrondissement / de district et tribunal des mesures de contrainte.

Réponse : oui, c'est tout à fait possible.

Pour chaque profil, le cachet d'autorité (ou, s'il existe des cachets multilingues, les versions en allemand, français et italien) doit être communiqué à Justitia 4.0 ou à la corporation de droit public justitia.swiss avant toute utilisation de la plateforme justitia.swiss pour les notifications.

---

[6] https://www.sas.admin.ch/sas/fr/home/akkreditiertestellen/akkrstellensuchesas/pki1.html État au 24.03.2026 ou https://actuel.easygov.swiss/solutions-de-signature/signature-electronique-2/ (État au 20.01.2026)

[7] **eOperations Suisse SA**, dont le siège est à Berne, a été fondée en 2018 par la Conférence suisse sur l'informatique. Elle est aujourd'hui la propriété exclusive de sa fondatrice, la CSI, et de 87 autres actionnaires du secteur public, dont tous les cantons et de nombreuses communes. eOperations Suisse a pour but de mettre en place et d'exploiter des solutions informatiques communes pour les prestations numérisées des autorités de la Confédération, des cantons et des communes, ainsi que d'organiser des appels d'offres communs. L'activité opérationnelle d'eOperations Suisse, qui est une entreprise publique, est sans but lucratif. www.eoperations.ch

[8] Voir Communiqué de presse sur les appels d'offres : https://www.eoperations.ch/wp-content/uploads/2023/11/231113-Communique_de_presse_adjucations_pour-les-signatures_electroniques_cachets_et_horodatages.pdf

La plateforme justitia.swiss peut-elle transmettre des documents qui contiennent, outre le cachet d'autorité réglementé, une ou deux signatures électroniques qualifiées ?

La plateforme justitia.swiss ne vérifie que le cachet d'autorité. Les signatures électroniques qualifiées (SEQ) apposées en plus sur le document ne sont pas vérifiées par la plateforme justitia.swiss ; elles ne perturbent pas le processus de transmission.

Le cachet d'autorité est-il lié à une adresse de notification spécifique sur la plateforme justitia.swiss ?

Chaque profil d'autorité dispose d'une adresse de notification unique (VGer ZH, tribunal administratif de ZH). Les autorités judiciaires doivent communiquer à temps à Justitia 4.0 ou à la corporation de droit public justitia.swiss le futur cachet d'autorité ainsi que ses caractéristiques d'identification, de préférence lors du processus d'enregistrement, mais au plus tard avant la première notification via la plateforme justitia.swiss.

Où et comment l'apposition du cachet d'autorité devrait-elle être intégrée dans le travail quotidien des autorités judiciaires ?

L'application dossier judiciaire électronique (ADJ) de Justitia 4.0 comprendra une intégration avec l'émetteur de certificat (discret[9]). Il est également possible d'intégrer l'apposition du cachet dans une application métier, ou, en attendant que celle-ci soit prête, dans une solution alternative.

Les documents portant un cachet d'autorité peuvent-ils être vérifiés à l'aide d'un validateur ?

Les citoyen-ne-s et les entreprises ainsi que les avocat-e-s doivent pouvoir vérifier les documents officiels émis par les autorités et cachetés ou signés numériquement par celles-ci, afin de s'assurer que ces documents officiels proviennent effectivement de l'autorité concernée et qu'ils n'ont subi aucune modification au moment de la vérification. À cet effet, il est nécessaire de disposer d'un **validateur** permettant de vérifier les documents comportant une ou plusieurs signatures ou un ou plusieurs cachets apposés par voie électronique, conformément aux prescriptions de la SCSE (RS 943.03) et de l'OAAE (RS 211.435.1) (Validateur de signature - Valider un document).

En raison de dispositions relatives au **respect du secret professionnel, du secret de fonction** ou **à la protection des données**, il peut être interdit de télécharger sur un système externe des documents dont le contenu est sensible, même si le système externe n'effectue qu'un traitement purement automatique et qu'aucune donnée n'y est enregistrée ou consignée. Dans ce cas, il convient d'utiliser une méthode de validation locale qui ne nécessite pas de télécharger le document sur un système externe.[10] Lors de l'entrée en vigueur de la LPCJ (nouvel art. 16*a* SCSE)[11], un validateur gratuit, public et discret sera mis à disposition.

---

[9] L'émetteur de certificat **discret** fait référence à un fournisseur de signatures électroniques discrètes ou de cachets électroniques réglementés permettant de signer électroniquement des documents sans transmettre l'intégralité du document. Le logiciel de signature discrète ne transmet que la valeur de hachage du document, ce qui permet de respecter les dispositions relatives à la protection des données ainsi que le secret de fonction ou le secret professionnel.

[10] Le service en ligne du validateur discret

[11] FF 2023 679 – Message concernant la loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire | Fedlex et FF 2025 19 - Loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire | Fedlex à l'annexe 18. Loi du 18 mars 2016 sur la signature électronique.

Les autorités cantonales sont priées de prendre contact avec eOperations Suisse SA https://www.eoperations.ch/fr/service/validateurdesignature/. Les autorités communales s'adressent à l'interlocuteur correspondant dans leur canton.

Les services officiels de l'administration fédérale s'adressent au domaine « Transformation numérique et gouvernance de l'informatique » (TNI) de la Chancellerie fédérale.

Sources : Message relatif à la révision totale de la loi sur la signature électronique (SCSE) du 15 janvier 2014, disponible sous https://www.fedlex.admin.ch/eli/fga/2014/171/fr

Loi fédérale sur les plateformes de communication électronique dans le domaine judiciaire du 20 décembre 2024 ; Feuille fédérale, FF 2025 19, message LPCJ

Site Internet de l'Office fédéral de l'informatique et de la télécommunication et https://www.bit.admin.ch/fr/le-validateur (état au 20.01.2026)

Concept Certificat réglementé délivré à une autorité V1.5 **Certificat d'autorité**

Vous trouverez des informations complémentaires et des informations sur des thèmes associés via info@justitia.swiss et/ou sur le site Internet www.justitia40.ch