Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de la justice OFJ
Domaine de direction Services centraux
Unité Informatique juridique

Conditions de la reconnaissance des plateformes de messagerie sécurisée utilisées dans le cadre de procédures (liste des critères)

du 16 septembre 2014 (version 2.0)

Annexe de l'ordonnance du DFJP du du 16 septembre 2014 sur la reconnaissance des plateformes de messagerie sécurisée utilisées dans le cadre de procédures (Ordonnance sur la reconnaissance des plateformes de messagerie; RS 272.11)

Table des matières

1 Objet et contenu

[1] La liste des critères définit les exigences que doivent remplir les plateformes de messagerie sécurisée pour être reconnues au sens de l'art. 2 de l'ordonnance sur la reconnaissance des plateformes de messagerie.

[2] Les plateformes de messagerie reconnues peuvent être utilisées pour transmettre par voie électronique des documents dans le cadre d'une procédure administrative. La reconnaissance d'une plateforme de messagerie par le Département fédéral de justice et police (DFJP) a aussi valeur de reconnaissance au sens de l'ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures administratives (OCEI-PA; RS 172.021.2).

2 Composantes d'un message électronique

Un message électronique comporte un en-tête et le corps du message, éventuellement complété d'annexes. Le corps du message et les annexes sont qualifiés de composantes du message.

3 Recours à des tiers

Le titulaire de la reconnaissance (fournisseur de prestations) peut déléguer l'exploitation technique de la plateforme à des tiers, en tout ou en partie. Il continue d'assumer la responsabilité de la plateforme sur les plans technique, administratif et juridique.

4 Exigences liées à la sécurité de l'information

4.1 Exigences de base pour les entreprises privées

[1] Si le fournisseur de prestations est une entreprise privée, la sécurité de l'information doit être garantie par l'établissement, l'implémentation, l'exploitation, la surveillance, la vérification, l'entretien et l'amélioration d'un système de management de la sécurité de l'information (SMSI) satisfaisant aux critères de la norme SN EN ISO/CEI 27001 2013 (Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information – Exigences[1]).

[2] L'efficacité et l'adéquation du SMSI doivent être attestées par un certificat conforme à la norme SN EN ISO/CEI 27001, 2013, délivré par un service de certification reconnu par le Service d'accréditation suisse (SAS). Les services offerts par la plateforme doivent s'inscrire dans le cadre défini pour le SMSI certifié. Les certificats SN EN ISO/CEI 27001, 2005 sont reconnus jusqu'à l'échéance du délai transitoire fixé par le SAS (Technologies de

[1] La norme indiquée peut être consultée ou commandée à l'Association suisse de normalisation (SNV), Bürglistrasse 29, 8400 Winterthour, www.snv.ch.

l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information – Exigences[2]).

[3] Lorsqu'une nouvelle version de la norme ISO/CEI 27001 est publiée, la conformité du certificat du SMSI doit être attestée au plus tard à l'échéance du délai transitoire. L'offre de prestations de la plateforme doit se maintenir dans le domaine couvert par le SMSI certifié.

4.2 Exigences de base pour les autorités

[1] Si le fournisseur de prestations est une autorité publique, le recours à un SMSI répondant à la norme SN EN ISO/CEI 27001/2013 reste indispensable, mais il est possible de renoncer, dans des cas exceptionnels et dûment motivés, à un certificat validé par un service de certification. Dans ce cas, l'efficacité et l'adéquation du SMSI doivent être attestées par un rapport contenant les résultats d'un audit formel interne réalisé conformément à la clause 9.2 de la norme SN EN ISO/CEI 27001, 2013. Le rapport d'audit ne doit contenir aucun élément qui s'opposerait à une certification. Jusqu'à l'échéance du délai transitoire fixé par la SAS, la reconnaissance pourra aussi être obtenue sur présentation d'un rapport contenant les résultats de l'audit formel interne réalisé sur le SMSI conforme à la clause 6 de la norme SN EN ISO/CEI 27001, 2005.

[2] Les principes et la réalisation de l'audit et les compétences et l'expérience des auditeurs s'appuient sur la norme SN EN ISO/CEI 19011, 2011, sur les Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information[3] et sur la norme SN EN ISO/CEI 27007, 2011 (Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information[4]). L'audit doit être effectué au moins une fois par an et les rapports d'audit doivent être présentés à l'OFJ.

[3] Lorsqu'une nouvelle version de la norme ISO/CEI 27001 est publiée, la conformité du SMSI avec cette dernière doit être attestée au plus tard à la fin du délai transitoire. L'offre de prestations de la plateforme doit se maintenir dans le domaine couvert par le SMSI certifié.

4.3 Exigences supplémentaires pour les entreprises privées et les autorités

La gestion des risques au sens de la norme SN EN ISO/CEI 27005, 2011, doit s'effectuer en tenant compte des exigences décrites aux points 4.3.1 à 4.3.3.

4.3.1 Gestion de l'exploitation et de la communication

[1] La gestion de l'exploitation de la plateforme et des communications pour lesquelles elle est utilisée doit s'effectuer en application des dernières avancées technologiques et faire l'objet d'une description complète, qui en illustre toutes les étapes, ainsi que de vérifications et d'adaptations périodiques.

---

2 La norme indiquée peut être consultée ou commandée à l'Association suisse de normalisation (SNV), Bürglistrasse 29, 8400 Winterthour, www.snv.ch.

3 La norme indiquée peut être consultée ou commandée à l'Association suisse de normalisation (SNV), Bürglistrasse 29, 8400 Winterthour, www.snv.ch.

4 La norme indiquée peut être consultée ou commandée à l'Association suisse de normalisation (SNV), Bürglistrasse 29, 8400 Winterthour, www.snv.ch.

[2] Les exigences particulières suivantes doivent être remplies:

a. Les plateformes de développement, de test et de production sont séparées les unes des autres.
b. Le réseau est segmenté selon les résultats d'une évaluation des risques. Les serveurs utilisés pour exploiter la plateforme sont répartis entre les différents segments en fonction du niveau de protection dont ils doivent bénéficier.
c. Les messages électroniques sont transmis et stockés exclusivement sous une forme chiffrée. Un déchiffrage de bout en bout (end-to-end) n'est pas nécessaire.
d. Les mots de passe ne sont pas stockés de manière non chiffrée et ne sont pas journalisés.
e. Les méthodes et les systèmes de chiffrement utilisés s'appuient sur les techniques les plus récentes et sont capables de parer aux menaces actuelles. Ils répondent à des normes telles qu'on en trouve par ex. dans la publication officielle « Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung »[5] de l'Agence allemande pour l'électricité, le gaz, les télécommunications, la poste et les chemins de fer (« Bundesagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen »). Cette dernière publie une liste d'algorithmes à utiliser pour la signature électronique au sens de la loi et de l'ordonnance sur la signature électronique allemande. Tout recours à des normes spéciales doit être dûment justifié et faire l'objet d'un examen quant à son adéquation et à son efficacité. Les méthodes et les systèmes propriétaires utilisés doivent être certifiés comme étant résistants aux attaques cryptanalytiques connues.
f. La conception de la plateforme doit permettre de renouveler les méthodes et les systèmes de chiffrement et de modifier la longueur des clés de manière relativement simple et économique.
g. Lors du transfert des messages, il est interdit de recourir à un chiffrement réalisé uniquement au moyen de clés dérivées de mots-de-passe, afin d'empêcher les attaques de craquage hors ligne.
h. La solidité des méthodes et des systèmes de chiffrement utilisés fait l'objet d'une description complète et détaillée au moment de la conception de l'architecture de sécurité globale. Les méthodes et les systèmes de chiffrement sont régulièrement vérifiés et le cas échéant adaptés, dans le cadre d'un processus d'amélioration permanent.

4.3.2 Gestion des accès

[1] Les mesures prévues pour la gestion des accès à la plateforme doivent satisfaire aux normes techniques les plus récentes et garantir une protection contre les menaces actuelles ; elles doivent faire l'objet d'une description complète et détaillée et être régulièrement vérifiées. Elles sont adaptées si nécessaire.

[2] Les exigences particulières suivantes doivent être remplies:

a. L'accès aux messages électroniques transférés s'effectue au moyen de méthodes d'authentification forte (p. ex. certificats numériques ou cartes à puce individuelles). L'information d'authentification n'est pas transmise en clair afin de prévenir les attaques visant sa récupération et sa reproduction.
b. Si l'authentification se fait au moyen de mots de passe, ces derniers doivent être transmis de manière chiffrée, par ex. dans le cadre d'une connexion SSL (Secure Sockets

[5] La liste des algorithmes et des paramètres qui conviennent est publiée à l'adresse: www.bundesnetzagentur.de > Qualifizierte elektronische Signatur > Aufgaben der Bundesnetzagentur / Veröffentlichungen > Festlegung geeigneter Algorithmen.

Layer) / TLS (Transport Layer Security). Le recours à ces protocoles permet de renoncer à limiter la durée de validité des mots de passe, qui doivent remplir les critères usuels et actuels de sécurité.

c. Des mesures sont à prendre pour prévenir les attaques de craquage des mots de passe et pour empêcher l'utilisation de mots de passe triviaux. Les utilisateurs sont invités à définir des mots de passe forts (par ex. au moyen d'une échelle permettant de visualiser leur degré de fiabilité) ; un mot de passe fort comprend au moins 8 positions et se compose d'au moins trois des quatre catégories d'éléments suivants : majuscules, minuscules, chiffres et caractères spéciaux. Il est personnel et n'est jamais communiqué.

4.3.3 Acquisition, développement et entretien des éléments de la plateforme

a. Les serveurs accessibles via Internet doivent être correctement sécurisés. On tiendra compte des bonnes pratiques pertinentes, par ex. des *Security Configuration Benchmarks* du *Center for Internet Security*[6].

b. Les éléments de la plateforme sont à l'épreuve des techniques d'attaque connues, telles que les décrit par ex. le projet *Open Web Application Security*[7].

4.4 Exceptions pour les autorités

Les plateformes qui sont contrôlées exclusivement par une autorité peuvent stocker des messages électroniques non chiffrés et les transmettre à des systèmes internes. L'autorité doit toutefois prendre des mesures administratives, des mesures de gestion ou des mesures techniques afin de réduire suffisamment le risque découlant de cette faiblesse technique. Pour déterminer ces mesures, l'autorité procède à une évaluation des risques basée sur la norme ISO/CEI 27001, 2013.

6 www.cisecurity.org
7 www.owasp.org

5 Exigences liées aux quittances

5.1 Contenu de la quittance

Une quittance doit contenir les éléments suivants:

a. Informations sur la quittance
   1. Nom de la plateforme qui délivre la quittance,
   2. Indication du type de quittance (dépôt, réception, péremption ou refus).

b. Informations sur le message électronique
   1. Informations sur l'expéditeur (nom, adresse de courriel),
   2. Informations sur le destinataire (nom, adresse de courriel),
   3. Champ « Objet » (si existant),
   4. Horodatage.

c. Composantes du message ou informations sur ces composantes (lorsque le message n'est pas chiffré de bout en bout)
   1. Noms des composantes (si existantes),
   2. Types et formats des composantes,
   3. Taille des composantes en Bytes,
   4. Valeur(s) de hachage des composantes; le hachage doit si possible avoir été réalisé à l'aide de deux techniques de chiffrement différentes.

d. Moment où la quittance est délivrée.

e. Signature électronique avancée, conformément à la loi fédérale du 19 décembre 2003 sur la signature électronique (SCSE; RS 943.03).

5.2 Indications de temps

a. La signature électronique de la quittance se fonde sur un certificat d'un fournisseur reconnu au sens de la SCSE et est liée à un horodateur.

b. Les heures indiquées sur la quittance proviennent du système d'horodatage de la plateforme du fournisseur et correspondent aux moments du dépôt et de la réception des communications.

5.3 Chronologie des étapes de la communication

D'un point de vue chronologique, les étapes de la communication sont définies de la manière suivante:

a. Envoi d'un écrit à un tribunal ou à une autorité:
   1. *Heure du dépôt:* moment où la plateforme utilisée par l'expéditeur confirme que le document a été téléchargé sur la plateforme d'envoi;
   2. *Heure de la réception:* moment où la plateforme utilisée par le tribunal ou l'autorité destinataire confirme que l'écrit a bien été reçu.

b. Notification d'un mandat de comparution, d'une décision ou d'une autre communication par un tribunal ou une autorité:
   1. *Heure du dépôt:* moment où la plateforme utilisée par le tribunal ou l'autorité confirme que la notification a été téléchargée sur la plateforme d'envoi;
   2. *Heure de la distribution:* moment où la plateforme utilisée par le destinataire prépare et enclenche la procédure d'envoi du message ou met le message à la disposition du destinataire pour téléchargement;
   3. *Heure de la réception:* lorsque le message est réceptionné dans le délai légal de réception, moment où la plateforme utilisée par le destinataire confirme que le message a bien été reçu.
   4. *Heure de la péremption:* lorsque le message n'est pas réceptionné dans le délai légal de réception, la fin de ce délai a valeur d'heure de péremption;
   5. *Heure du refus:* dans le délai légal de réception applicable, moment où la communication est refusée.

5.4 Quittances délivrées

[1] Les plateformes délivrent les quittances suivantes:

a. Envoi d'écrits à un tribunal ou une autorité:
   1. Quittance assortie de l'heure de dépôt (quittance de dépôt);
   2. Quittance assortie de l'heure de la réception (quittance de réception).
b. Notifications par un tribunal ou une autorité:
   1. Quittance assortie de l'heure de dépôt (quittance de dépôt);
   2. Quittance assortie de
      - l'heure de réception, lorsque le message est réceptionné par son destinataire dans le délai légal de réception (quittance de réception);
      - l'heure de péremption, lorsque le message n'est pas réceptionné dans le délai légal de réception (quittance de péremption);
      - l'heure du refus, lorsque le message est refusé par son destinataire dans le délai légal de réception (quittance de refus).

[2] Si une plateforme n'est reconnue que pour l'envoi d'écrits aux autorités, elle ne délivrera qu'une quittance de dépôt, en dérogation à l'al. 1, let. a.

5.5 Création et envoi des quittances

a. La quittance est créée par la plateforme sous la forme d'un fichier PDF signé.
b. L'horodatage figurant dans la signature de la quittance ne diffère pas de plus d'une minute de celui indiqué sur la quittance. En d'autres termes, la quittance est établie dans la minute suivant la signature.
   Il s'agit là de délais réglementaires. Tout dépassement doit être journalisé ; s'il excède cinq minutes, l'autorité de certification doit en être informée par écrit le jour ouvrable suivant.
c. Lors de la remise d'un écrit à un tribunal ou à une autorité, l'expéditeur et le tribunal ou l'autorité reçoivent chacun la même quittance, indiquée au ch. 5.4, al.1, let. a.
   L'expéditeur peut indiquer à la plateforme qu'il renonce, lors de la remise d'un écrit, à

l’envoi d’une quittance de réception ou, lors d'une notification, à l’envoi d’une quittance de dépôt.

d. Lors d’une notification par un tribunal ou une autorité, ce dernier ou cette dernière et l’expéditeur reçoivent chacun la même quittance, parmi celles indiquées au ch. 5.4, al. 1, let. b.
Le tribunal ou l’autorité peut indiquer à la plateforme qu’il renonce, en cas de réception d’un écrit, à l’envoi d’une quittance de réception ou, en cas de notification, à l'envoi d’une quittance de dépôt. Si la plateforme dispose d’une fonction "Autoaccept", la réception peut être confirmée sans indication de l’heure.

e. Si un message électronique est adressé simultanément à plusieurs destinataires, il est possible de regrouper les différentes heures de dépôt sur une quittance unique. L’heure indiquée sur la quittance unique est la même que l’heure qui clôt la liste journalisée des heures de dépôt.

f. Les quittances sont rendues accessibles à leurs destinataires via la plateforme qu’ils utilisent.

g. Les quittances peuvent être envoyées de manière non chiffrée si elles ne contiennent que la mention prévue au ch. 5.1, mais aucun détail sur le contenu de la notification ou de la communication.

h. Les plateformes peuvent envoyer les quittances à toutes les adresses de courriel spécifiées par les participants à l’envoi, à la demande de ces derniers.

i. Le nom de fichier de la quittance doit permettre de l’identifier sans ambiguïté comme telle. Voici un exemple de format recommandé :
[YYMMDD]_[Message Identifier]_[Plateforme]_[Type de quittance].

6 Exigences liées au système de management des services informatiques

6.1 Exigences de base

[1] Pour garantir une bonne exploitation de la plateforme, il faut démontrer que les processus suivants sont documentés, introduits, exploités, surveillés de manière permanente, vérifiés périodiquement, entretenus et améliorés:

a. Processus de fourniture des services
   1. Gestion des niveaux de services,
   2. Etablissement de rapports de services,
   3. Gestion de la continuité et de la disponibilité des services,
   4. Budgétisation et comptabilisation des services informatiques,
   5. Gestion de la capacité,
   6. Gestion de la sécurité des informations;

b. Processus de gestion des relations
   1. Gestion des relations entre fournisseurs de prestations et clients,
   2. Gestion des fournisseurs;

c. Processus de résolution
   1. Gestion des incidents et des demandes de services,
   2. Gestion des problèmes;

d. Processus de pilotage
   1. Gestion des configurations,
   2. Gestion des changements,
   3. Gestion des mises en production et du déploiement.

[2] Les processus doivent répondre aux normes internationales SN EN ISO/CEI 20000-1, 2011 (Technologies de l'information – Gestion des services – Partie 1 : Exigences du système de management des services[8]) et SN EN ISO/CEI 20000-2, 2012 (Technologies de l'information – Gestion des services – Partie 2: Guide pour l'application de systèmes de management de services[9]) ou à des normes comparables. Leur certification selon ces normes est souhaitable, mais pas indispensable.

[3] En outre, une fonction de centre de services (Service Desk) doit être créée, exploitée, surveillée en permanence, vérifiée périodiquement, entretenue et améliorée.

6.2 Disponibilité

[1] La disponibilité de la plateforme doit être garantie en principe 24 heures sur 24. Des interruptions pour son entretien peuvent être prévues entre 0h15 et 7h00 (heure suisse) ou le week-end. Elles doivent être annoncées sur la plateforme au moins 72 heures à l'avance.

---

8 La norme indiquée peut être consultée ou commandée à l'Association suisse de normalisation (SNV), Bürglistrasse 29, 8400 Winterthour, www.snv.ch.

9 La norme indiquée peut être consultée ou commandée à l'Association suisse de normalisation (SNV), Bürglistrasse 29, 8400 Winterthuur, www.snv.ch.

[2] La disponibilité de la plateforme est indiquée sur un procès-verbal, à publier sur cette dernière.

6.3 Synchronisation de l'horloge

L'horloge de la plateforme doit être synchronisée avec un serveur de référence de sorte qu'elle ne s'écarte jamais de plus de cinq secondes de l'heure de ce dernier. La synchronisation et les écarts de temps constatés sont journalisés.

6.4 Taille des messages électroniques

La plateforme doit pouvoir traiter des messages électroniques d'une taille de 15 MB et permettre l'envoi et la réception de fichiers atteignant 25 MB.

6.5 Informations aux utilisateurs

[1] Le fournisseur de prestations doit publier sur la plateforme, en des termes compréhensibles pour les non-spécialistes, les principales caractéristiques des éléments suivants:

a. l'architecture de la plateforme;
b. le contrôle des accès à celle-ci;
c. les méthodes et les systèmes de chiffrement utilisés.

[2] Le chiffrement bout à bout des messages électroniques n'est pas absolument indispensable. A cet égard, on fera figurer sur la plateforme le message suivant:
Il peut arriver que la plateforme contienne des messages non chiffrés, qui peuvent être lus par le fournisseur de prestations ou les tiers mandatés (même si cela n'est pas autorisé). Les utilisateurs qui ne souhaitent pas courir ce risque doivent renoncer à utiliser la plateforme ou renforcer le chiffrement du message (par. ex. en utilisant une clé numérique publique du destinataire).

[3] Les utilisateurs de la plateforme doivent être informés de leurs obligations, notamment en matière de diligence, et du fait que les données les concernant sont visibles dans le répertoire principal des participants, consultable par ces derniers (cf. ch. 7). Ils doivent également être informés de la force de leur mot de passe (cf. ch. 4.3.2, al. 2, let. c) ainsi que du fait que l'objet du message et les noms de fichier des éventuelles annexes sont transmis sans être chiffrés.

7 Exigences liées au répertoire principal des participants

[1] Pour permettre l'envoi de messages électroniques entre les plateformes, l'OFJ crée un répertoire non public des participants, appelé répertoire principal des participants, qui ne peut être consulté qu'à partir de plateformes reconnues. L'utilisation à des fins publicitaires ou commerciales des adresses qu'il contient est interdite.

[2] Le répertoire principal des participants comprend plusieurs arborescences correspondant chacune à un sous-répertoire de participants et à des droits d'écriture spécifiques. Ces sous-arborescences, qui appartiennent à la classe d'objets LDAP (Lightweight Directory Access Protocol), comprennent les attributs suivants (d'autres attributs sont possibles, comme les coordonnées d'un service desk, le paramétrage de préférences d'affichage ou de recherche, la limitation de la taille des messages et des commentaires):

Nom de l'attribut	Signification	Exemples
Ou	Nom usuel de la plateforme.	ekomm, Incamail, canton de Berne, PrivaSphere
platformUri	URI à laquelle la plateforme peut être jointe.	https://www.bla.ch:8080/
smtpUri	Adresse du MTA de la plateforme créé pour permettre l'interopérabilité.	smtps://smtp.bla.ch:25001/
smimeSignCertificate smimeEncryptionCertificate	Certificats X.509 destinés aux clés publiques utilisées par le protocole S/MIME de signature et de chiffrement / déchiffrement (les deux certificats peuvent être identiques). Format: PKCS#7 SignedData	
smtpCertificate	Certificat X.509 destiné à la clé publique utilisée par le protocole MTA pour la distribution sécurisée des messages. Format: PKCS#7 Signed-Data.	

[3] Les données figurant dans les sous-arborescences du répertoire se fondent sur la classe d'objets inet-OrgPerson correspondant à RFC 2798. Les deux attributs suivants doivent être indiqués dans tous les cas:

a. Mail (mail);
b. Distinguished Name (dn).

[4] Chaque participant doit être identifié de manière univoque au moyen de l'attribut mail. Cet attribut sert par exemple à constituer le Distinguished Name.

[5] Chaque plateforme publie sur le répertoire principal les données des participants qu'elle détient; elle les actualise au moins une fois par jour.

[6] Les exploitants de la plateforme doivent identifier les participants. Ils disposent de différentes méthodes pour ce faire:

a. identification personnelle selon les critères définis à l'art. 5 de l'ordonnance du 3 décembre 2004 sur la signature électronique (OSCSE, RS 943.032);
b. identification au moyen de SuisseID;
c. validation par lettre de l'adresse de domicile;
d. contrat écrit entre le participant et l'exploitant de la plateforme;
e. enregistrement du groupe (confirmation des identités par l'association cantonale des avocats ou enregistrement et identification des avocats).

[7] La communication dans les deux sens entre le répertoire principal des participants et les répertoires des participants des plateformes s'effectue par une procédure d'authentification forte, idéalement basée sur un protocole LDAPS (LDAP over SSL) et sur des certificats reconnus par un service de certification au sens de la SCSE.

[8] Si une autorité propose sur Internet un formulaire permettant de lui transmettre des écrits, on indiquera également dans le répertoire principal des participants l'URL menant à ce formulaire.

8 Exigences liées à la communication entre les plateformes

[1] Si l'expéditeur et le destinataire d'un message électronique sont enregistrés sur la même plateforme, le transfert s'effectue sans quitter cette dernière. S'ils sont enregistrés sur des plateformes différentes, le message est transmis de l'une à l'autre. Normalement, la communication s'effectue entre deux plateformes; il peut cependant arriver qu'un message transite par un plus grand nombre de plateformes.

[2] Ci-après, A désigne l'expéditeur et P_A la plateforme sur laquelle A est enregistré (ou par laquelle transite le message), B désigne le destinataire du message et P_B la plateforme sur laquelle il est enregistré ($P_A \neq P_B$). P_A et P_B sont normalement connectées entre elles et peuvent échanger des messages. En l'absence d'une connexion directe, d'autres plateformes jouent le rôle d'intermédiaires.

8.1 Exigences de base

[1] La communication entre les plateformes doit être protégée par chiffrement. Il existe deux couches de protection:

1. Sur la couche « transport », les données sont chiffrées selon la norme RFC 3207 (Secure Simple Mail Transfer Protocol [SMTP] over TLS). Il faut pour cela que toutes les plateformes disposent d'un MTA (SMTP Mail Transfer Agent) exploitant Secure SMTP over TLS. L'adresse du MTA doit être publiée dans le répertoire principal des participants, de même que le certificat X.509 smtpCertificate correspondant. Les certificats X.509 permettent aux MTA de s'identifier mutuellement.
2. Sur la couche « utilisateurs », le chiffrement des messages sur la plateforme d'envoi s'effectue selon la norme S/MIME (Secure Multipurpose Internet Mail Extensions) : le message est signé par la plateforme d'envoi au moyen d'une clé privée et est chiffré au moyen d'une clé de chiffrement publique de la plateforme de réception. Les certificats X.509 smimeSignCertificate et smimeEncryptionCertificate correspondants doivent être publiés dans le répertoire principal des participants.

[2] Chaque plateforme doit par conséquent disposer de trois paires de clés: une paire pour la couche transport, pour le chiffrement, et deux paires pour la couche « utilisateurs », pour la signature et l'authentification et pour le chiffrement (voir les certificats correspondants – smtpCertificate, smimeSignCertificate et smimeEncryptionCertificate – dans le tableau du point 7). Un certificat peut être utilisé à différentes fins dans l'application.

[3] Le présent document n'aborde pas plus avant le chiffrement de la couche « transport », qui pour l'essentiel détermine la configuration utilisée par les MTA pour gérer le protocole STARTTLS (Secure SMTP over TLS). En ce qui concerne le chiffrement des messages sur la couche « utilisateurs », voici une description du protocole de communication à utiliser.

8.2 Protocole de communication

[1] Considérons l'exemple d'un message envoyé entre les plateformes P_A et P_B. P_B doit délivrer une quittance de réception et verbaliser le moment de la distribution du message, P_A doit délivrer une quittance de dépôt.

a. La communication entre P_A et P_B s'effectue de la manière suivante:

1. P_A reçoit le message à transmettre, envoie une quittance de dépôt pour le confirmer et l'insère dans un message conforme au protocole S/MIME comportant les en-têtes SMTP suivants:
   - To: adresse mail de B;
   - From: adresse mail de A;
   - Message-ID: identifiant univoque du message défini par P_A et commun à toutes les plateformes;
   - X-ZP-MsgType: type de message ; dans le cas d'un message électronique, on utilisera simplement « message » ;
   - Heure de dépôt, heure de réception ou heure de péremption ou de rejet (cf. ch. 5.3; date, heure et minute) en millisecondes depuis le 1.1.1970 («X-ZP-IntakeTimeStampMillis», «X-ZP-ReceiveTimeStampMillis»)[10], pour que l'indication du temps puisse se faire de manière correcte sur toutes les plateformes participantes[11];
   - Nom de la plateforme d'envoi («X-ZP-FromPlatform»), contenant la dénomination «OU» univoque figurant dans le répertoire supérieur.

   Des en-têtes supplémentaires sont possibles (par ex. pour indiquer l'heure locale de P_A ou pour préciser si l'objet de l'envoi est un acte officiel ou une simple communication[12]). Le message électronique à envoyer constitue le corps d'un message conforme au protocole S/MIME.
2. P_A signe le message conforme au protocole S/MIME avec sa clé de signature privée et chiffre le tout avec la clé de chiffrement public de P_B.
3. Le message signé et chiffré est transféré du MTA de P_A au MTA de P_B, après avoir été encore une fois chiffré sur la couche « transport » (STARTTLS ou Secure SMTP over TLS). Il n'y a pas lieu de tenir compte des éventuelles signatures utilisées pour garantir la sécurité sur la couche « transport ». Si le message ne peut pas être délivré à son destinataire, la seule chose à faire est d'en avertir immédiatement A.
4. P_B déchiffre le message reçu, vérifie et efface la signature, journalise le moment de sa distribution et envoie la quittance de distribution à P_A. Simultanément, le message est déposé dans la boîte de B, qui peut le télécharger, ou qui le reçoit directement s'il y a explicitement consenti.
5. La plateforme destinataire P_B s'assure que les messages signés par l'expéditeur peuvent être lus lorsqu'elle les reçoit via une interface web.
6. P_B accepte le message indépendamment du statut de l'expéditeur dans le répertoire principal des participants.

---

10 Pour simplifier le traitement, il faudrait reproduire ces indications de temps sous une forme lisible par l'homme dans un autre en-tête X.

11 On pourra indiquer les heures de dépôt et de distribution de la plateforme locale sur le WEB-GUI de la plateforme, de manière à ce qu'elles s'affichent au passage du pointeur ou dans une fenêtre pop-up. Le non-initié ne verra de prime abord que les indications de temps coordonnées entre les plateformes.

12 A titre d'exemple, si l'expéditeur et le destinataire sont tous deux des autorités, la question se pose de savoir si l'on a affaire à un écrit ou à un jugement (ou une décision). Pour garantir le bon fonctionnement de la fonction « receipt-auto-delivered », on aura avantage à compléter l'en-tête optionnel « X ZP TypeOfCommunication » des valeurs « ENQUIRY » et « AUTHORITY_RESPONSE ».

b. Une fois l'envoi effectué, le message se trouve dans la sphère d'influence de P_B. Il revient à ce dernier d'informer P_A de tout événement qui pourrait affecter le message A cet effet, P_B peut créer un message S/MIME doté des indications d'en-tête SMTP suivantes, puis l'envoyer à P_A:
   1. To: adresse mail de A.
   2. From: adresse mail de B.
   3. Message-ID: identificateur de message défini par P_B (univoque et commun à toutes les plateformes).
   4. In-Reply-To: valeur indiquée par P_A dans le champ Message-ID.
   5. X-ZP-MsgType: un des types de message suivants:
      - receipt-deposited: le message se trouve dans la boîte de B;
      - receipt-delivered: le message a été retiré par B;
      - receipt-auto-delivered: le message a été automatiquement transféré à B (qui peut être une autorité). P_B peut renoncer à recevoir une quittance de réception;
      - receipt-timed-out: le délai de remise du message est échu sans que celui-ci ait été retiré;
      - receipt-refused: B a refusé de réceptionner le message;
      - receipt-invalid-signature: la signature du message n'est pas valable;
      - receipt-error: message d'erreur générique, indépendant de la signature;
      - confidential: ce type de message est utilisé par ex. pour la quittance de dépôt, lorsque celle-ci est envoyée par l'autre plateforme.
        Pour garantir la plus grande robustesse possible, ces messages compatibles entre opérateurs ne doivent être impérativement protégés que sur la couche « transports » sans le smimeEncryptionCertificate (mandatory TLS).

c. Si X-ZP-MsgType a la valeur «receipt-delivered», le corps du message doit contenir la quittance de distribution correspondante, accompagnée le cas échéant d'informations supplémentaires (par ex. sous la forme d'indications d'en-tête SMTP supplémentaires). Si X-ZP-MsgType a la valeur «receipt-error», le corps du message peut contenir des informations complémentaires sur l'erreur survenue. En cas d'utilisation de l'en-tête X-Zp-ERROR-To-User, celui-ci s'affiche aux yeux de l'utilisateur concerné. Dans ce cas comme dans les autres, le corps du message peut aussi être vide.

d. Dans tous les cas, P_B signe le message au moyen de sa clé privée et chiffre le résultat au moyen de la clé de chiffrement publique de P_A. Le MTA envoie le message signé et chiffré de P_B à P_A (là aussi sur la couche transport et par un canal chiffré au moyen de Secure SMTP over TLS). P_A déchiffre le message, vérifie et supprime la signature et rend compte à A du résultat, sous une forme adapée (ou en lui remettant une quittance).

[2] Assistance pour les autorités: lorsque la plateforme d'envoi constate après deux jours (ouvrables) que l'autorité de destination n'a pas encore retiré un message qui lui est adressé, elle peut ouvrir un ticket d'alerte sur la plateforme de réception. Cette dernière s'assure de l'ouverture, dans le délai restant, d'un tel ticket auprès du service d'assistance sous contrat avec l'autorité en question. La plateforme de réception communique le statut à la plateforme d'envoi avant que le délai ne soit écoulé.

8.3 Interopérabilité et accès au répertoire principal des participants

[1] Chaque plateforme garantit gratuitement vis-à-vis des autres plateformes le transfert des messages selon le protocole décrit plus haut et l'accès à son répertoire principal des participants.

[2] L'utilisateur final est autorisé à utiliser des métacaractères dans ses recherches dans le répertoire principal des participants.