CONVENTION INDIVIDUELLE D'ADHÉSION COLLECTIVE GATEWAY

Description des prestations

La convention individuelle d'adhésion collective Gateway fait partie du contrat-cadre et de ses annexes. Sauf accord contraire dans la présente convention individuelle, le contrat-cadre et ses annexes s'appliquent.

Introduction et domaine d'utilisation

L'objet de la présente convention individuelle est le produit HIN Gateway (HIN GW). En utilisant HIN GW, les utilisateurs travaillent et communiquent de manière conforme à la protection des données au sein des établissements et avec d'autres membres HIN raccordés (secret professionnel/secret médical, LPD).

La convention individuelle règle les droits et obligations de HIN et du client concernant le raccordement et l'utilisation de la plate-forme HIN via HIN GW.

Les indications sur les technologies, systèmes d'exploitation, etc. supportés et utilisés se réfèrent à l'état au moment de l'élaboration de la présente convention individuelle.

1. Prestations de HIN

Selon sa configuration, HIN GW comprend les composants HIN Mail Gateway (MGW) et/ou HIN Access Gateway (AGW), qui peuvent être gérés de manière centralisée et qui sont intégrés dans le paysage informatique existant.

HIN GW permet d'utiliser HIN Mail et HIN Access. HIN Mail protège la communication par e-mail dans tout le domaine de messagerie. Les e-mails envoyés aux membres HIN et les e-mails désignés comme «confidentiels», mais aussi les e-mails vers les destinataires sans adhésion à HIN, sont automatiquement cryptés. HIN Access permet d'accéder aux applications protégées par HIN au moyen de l'identité HIN sans qu'il soit nécessaire d'installer un logiciel ou des certificats sur les postes de travail.

HIN Mail

- **Fonctionnement**
  Échange d'e-mails automatiquement sécurisé (cryptage basé sur le domaine entre les Gateways) avec la communauté HIN et toutes les adresses e-mail raccordées à HIN.

  Cryptage automatique des e-mails marqués comme «confidentiels» à tout destinataire.
- **Conditions d'utilisation**
  Le composant MGW est intégré dans l'infrastructure informatique du client en tant qu'appliance virtuelle (VM), ou également appliance matérielle (HW), conformément aux instructions (manuel technique de l'utilisateur).
- **Étendue des prestations MGW**
  - Utilisation d'une signature pour vérifier l'authenticité (vérification de l'expéditeur) et l'intégrité (détecter d'éventuelles modifications du contenu).

- Signature et cryptage (en fonction de la version MGW) des e-mails sortants.
- Vérification de l'intégrité et de l'authenticité ainsi que décryptage (en fonction de la version MGW) des e-mails entrants.

HIN Access

- **Fonctionnement**
  Accès sécurisé et conforme à la protection des données aux services du répertoire HIN et aux applications protégées par HIN via Single Sign-on (SSO).
- **Conditions d'utilisation**

  Le composant AGW est intégré dans l'infrastructure informatique du client en tant qu'appliance virtuelle VM, conformément aux instructions (manuel technique de l'utilisateur).

- **Étendue des prestations AGW**
  - Établissement et mise à disposition d'identités électroniques HIN pour l'institution, des groupes d'utilisateurs ou des utilisateurs individuels (en fonction de la version AGW et de l'offre concrète)
  - Vérification de l'intégrité et de l'authenticité lors de l'accès aux applications protégées par HIN (authentification, SSO).

La HIN Private Key Infrastructure (PKI) règle l'enregistrement des clés publiques, les gère avec les certificats correspondants et vérifie leur validité.

HIN et le client s'engagent à gérer de manière sécurisée toutes les identifications et clés. En cas de divulgation involontaire de mots de passe ou de vol, d'utilisation abusive ou d'accès non autorisé à la clé privée, HIN autorise le client à se faire établir une nouvelle clé (nouvel enregistrement) ou à faire bloquer définitivement l'identité.

Mise en service

HIN s'engage à mettre HIN GW en service pour le client à la date convenue et à prendre toutes les dispositions nécessaires pour que le client puisse utiliser le service dans son intégralité.

L'installation peut être effectuée de manière autonome par l'administrateur du client, sur la base de la documentation mise à disposition. L'installation de la VM ou de la HW et l'intégration dans l'environnement informatique du client (pare-feu, serveur de messagerie) ne font pas partie de l'offre de HIN, sauf dispositions contraires expressément stipulées dans celle-ci. Des prestations d'ingénierie et de mise en œuvre peuvent toutefois être fournies sur demande et sont facturées au tarif horaire actuellement en vigueur.

Piste d'audit

La piste d'audit est l'enregistrement continu de toutes les actions et de tous les événements déclenchés par les utilisateurs ou les composants système sur la plate-forme HIN. Chaque entrée de la piste d'audit comprend la date et l'heure, l'application ou le composant système, la désignation de l'action, l'utilisateur qui l'a déclenchée, etc.

Un extrait de la piste d'audit est fourni au client sur demande et dans la mesure du possible. L'extrait contient les données et attributs de la piste d'audit qui sont nécessaires pour répondre à la question posée et que le client est autorisé à consulter.

Les dispositions générales définies dans le contrat-cadre s'appliquent systématiquement.

3. Dispositions particulières

HIN recommande d'installer les correctifs ou mises à niveau des logiciels fournis le plus rapidement possible, au plus tard dans les 2 mois. Les frais de maintenance et de support pour les anciennes versions peuvent être facturés à partir du 3e mois suivant la sortie des correctifs et des mises à niveau.

Les dysfonctionnements ou problèmes résultant du paramétrage de HIN Gateway ou de l'interaction de HIN Gateway avec l'infrastructure, le matériel ou les logiciels utilisés par le client, et dus à des erreurs de manipulation ou causés par des interventions dans HIN Gateway ne sont pas considérés comme des défauts de HIN Gateway.

Le client est responsable envers HIN des dommages dus au non-respect de ses obligations contractuelles, à moins qu'il ne prouve qu'aucune faute ne lui est imputable.

4. Obligations de coopération du client

Au cours du processus d'enregistrement, le client génère une clé publique et une clé privée (public/private key). La clé publique est transmise à HIN. Cette clé permet d'identifier les membres ou collaborateurs de l'organisation concernée comme appartenant à cette organisation.

Les caractéristiques d'authentification telles que clé privée, certificat, phrase de passe, etc. ne doivent pas être transmises ou vendues à des tiers. Elles ne doivent pas non plus être reprises dans une autre entreprise. Le client assume les conséquences résultant d'une utilisation abusive des caractéristiques d'authentification. En cas de vol, d'utilisation abusive, d'accès non autorisé aux clés privées ou de divulgation de la phrase de passe, HIN autorise le client à générer de nouvelles clés privées et à s'enregistrer de nouveau ou à faire bloquer le login.

Obligation de diligence

Le client informe toutes les personnes du fonctionnement décrit et des obligations de diligence dans le traitement des informations sensibles. Le client est responsable de la sécurité de la transmission de messages au sein de son réseau ou de son système de messagerie.

Le client installe les mises à jour rapidement après leur sortie et informe HIN de manière proactive des éventuels incidents de sécurité.

Le client octroie à HIN des droits d'audit sur HIN Gateway et Active Directory (AD), ce qui permet à HIN de vérifier, sur la base des «AGW Security Guidelines», si une protection adéquate est garantie.

5. Conditions d'utilisation

L'utilisation du composant MGW pour l'envoi système n'est pas autorisée ou requiert une licence spécifique.

6. Rémunération

Les frais uniques (coûts initiaux) sont facturés après la conclusion du contrat.

HEALTH INFO NET SA

Janvier 2024