ACCORDO INDIVIDUALE GATEWAY COLLETTIVO

Descrizione delle prestazioni

L'Accordo individuale Gateway collettivo fa parte del contratto quadro e dei suoi allegati. Se non diversamente indicato nel presente Accordo individuale, si applicano il contratto quadro e i suoi allegati.

Introduzione e campo di applicazione

Oggetto del presente Accordo individuale è il prodotto HIN Gateway (HIN GW). Utilizzando HIN GW, gli utenti lavorano e comunicano all'interno della propria istituzione e con altri membri HIN collegati in modo conforme alle norme in materia di protezione dei dati (segreto professionale / segreto medico, LPD).

L'Accordo individuale disciplina i diritti e i doveri di HIN e del cliente in relazione al collegamento e all'utilizzo della piattaforma HIN tramite HIN GW.

Le informazioni su tecnologie, sistemi operativi ecc. supportati e utilizzati si riferiscono allo stato al momento della redazione del presente Accordo individuale.

1. Prestazioni di HIN

A seconda della versione, HIN GW comprende i componenti HIN Mail Gateway (MGW) e/o HIN Access Gateway (AGW) gestibili in maniera centralizzata e integrabili nel sistema informatico esistente.

HIN GW consente l'utilizzo di HIN Mail e HIN Access. HIN Mail protegge la comunicazione e-mail dell'intero dominio di posta elettronica. Le e-mail inviate ai membri HIN e quelle contrassegnate come «confidenziali» inviate a destinatari che non sono membri HIN vengono automaticamente crittografate. HIN Access consente di accedere alle applicazioni protette HIN tramite l'identità HIN senza bisogno di installare software o certificati sulle postazioni di lavoro.

HIN Mail

- **Funzionamento**

  Scambio mail automaticamente protetto (crittografia basata sul dominio tra i gateway) con la HIN Community o con tutti gli indirizzi e-mail collegati a HIN.

  Le e-mail indirizzate a qualsiasi destinatario contrassegnate come «confidenziali» vengono crittografate in automatico.

- **Requisiti per l'utilizzo**

  Il componente MGW viene integrato nell'infrastruttura informatica del cliente in base alle istruzioni (manuale tecnico d'uso) come appliance virtuali (VM) o, in alternativa, come appliance hardware (HW).

- **Portata dei servizi MGW**
  - Impiego di una firma per verificare l'autenticità (verifica del mittente) e l'integrità (verifica delle modifiche al contenuto).
  - Firma e crittografia (a seconda della versione di MGW) delle e-mail in uscita.

- Verifica dell'integrità e dell'autenticità nonché la decrittografia (a seconda della versione di MGW) delle e-mail in arrivo.

HIN Access

- **Funzionamento**
  Accesso sicuro e conforme alle norme in materia di protezione dei dati ai servizi di directory HIN e alle applicazioni protette HIN tramite Single Sign-On (SSO).
- **Requisiti per l'utilizzo**

  Il componente AGW viene integrato nell'infrastruttura informatica del cliente in base alle istruzioni (manuale tecnico d'uso) come appliance virtuale (VM).

- **Portata dei servizi AGW**
  - Emissione e fornitura di identità elettroniche HIN per l'istituzione, gruppi di utenti o singoli utenti (a seconda della versione di AGW e dell'offerta specifica).
  - Verifica dell'integrità e dell'autenticità in fase di accesso ad applicazioni protette HIN (autenticazione, SSO).

La Private Key Infrastructure (PKI) di HIN regola la registrazione delle chiavi pubbliche, le gestisce insieme ai certificati associati e ne verifica la validità.

HIN e il cliente si impegnano a gestire in modo sicuro tutte le identificazioni e le chiavi. In caso di divulgazione involontaria delle password o di furto, uso improprio o accesso non autorizzato alla chiave privata, HIN accorda al cliente il diritto di impostare una nuova chiave (nuova registrazione) o di far bloccare definitivamente l'identità.

Attivazione

HIN si impegna ad attivare HIN GW al cliente alla data concordata e a prendere tutte le precauzioni per garantire che il cliente possa utilizzare il servizio nella sua interezza.

L'installazione può essere eseguita autonomamente dall'amministratore del cliente sulla base della documentazione fornita. L'installazione della VM o della HW e l'integrazione nell'ambiente informatico (firewall, server di posta) del cliente non fanno parte dell'offerta di HIN, a meno che non siano espressamente inclusi nell'offerta. Su richiesta possono però essere fornite prestazioni di engineering o implementazione che vengono fatturate in base alle tariffe orarie in vigore.

Audit trail

L'Audit trail fornisce una registrazione completa di tutte le azioni e gli eventi attivati dagli utenti o dai componenti del sistema nella piattaforma HIN. Una voce dell'Audit trail è caratterizzata da data e ora, applicazione o componente del sistema, denominazione dell'azione, utente che l'ha attivata ecc.

Su richiesta e ove possibile, al cliente viene fornito un estratto dell'Audit trail. L'estratto contiene i dati e gli attributi dell'Audit trail necessari per la questione specifica e che il cliente è autorizzato a visualizzare.

In linea di principio, si applicano le disposizioni generali stabilite nel contratto quadro.

3. Disposizioni particolari

HIN raccomanda di installare il prima possibile le patch o gli aggiornamenti del software rilasciati al massimo entro 2 mesi. I costi di manutenzione e assistenza per le versioni precedenti possono essere fatturati a partire dal terzo mese successivo al rilascio di patch e aggiornamenti.

I malfunzionamenti o i problemi derivanti dalla parametrizzazione di HIN Gateway o dall'interazione di HIN Gateway con l'infrastruttura, l'hardware o il software utilizzati dal cliente che sono riconducibili a errori operativi o causati da interventi all'interno di HIN Gateway, non devono essere considerati difetti di HIN Gateway.

Il cliente risponde nei confronti di HIN per i danni riconducibili al mancato adempimento dei suoi obblighi contrattuali, qualora non dimostri di non avere colpa.

4. Obblighi di collaborazione del cliente

Durante il processo di registrazione, il cliente genera una chiave pubblica e una privata (Public/Private Key). La chiave pubblica viene inviata a HIN. I membri o il personale dell'organizzazione interessata sono identificati come appartenenti a tale organizzazione sulla base di questa chiave.

Gli elementi di autenticazione, come ad esempio chiave privata, certificato, passphrase ecc. non devono essere trasmessi o venduti a terzi. Inoltre, non possono essere trasferiti a un'altra azienda. Il cliente è responsabile delle conseguenze derivanti dall'uso improprio degli elementi di autenticazione. In caso di furto, uso improprio, accesso non autorizzato alle chiavi private o divulgazione delle passphrase, HIN accorda al cliente il diritto di generare nuove chiavi private e di registrarsi nuovamente o di far bloccare l'accesso.

Obbligo di diligenza

Il cliente informa tutte le persone sul funzionamento descritto e sugli obblighi di diligenza nel trattamento di informazioni sensibili. Il cliente è responsabile della sicurezza della comunicazione all'interno della propria rete o del proprio sistema di posta.

Il cliente installa gli aggiornamenti subito dopo il rilascio e informa HIN in modo proattivo di eventuali accadimenti correlati alla sicurezza.

Il cliente concede a HIN i diritti di audit su HIN Gateway e sull'Active Directory (AD) che consentono a HIN di verificare l'esistenza di una protezione adeguata in base alle «AGW Security Guidelines».

5. Disposizioni di utilizzo

L'utilizzo del componente MGW per invii di sistema non è consentito o richiede una licenza separata.

6. Compenso

Le quote una tantum (costi iniziali) vengono fatturate dopo la conclusione del contratto.

HEALTH INFO NET SA

Gennaio 2024