EINZELVEREINBARUNG KOLLEKTIV GATEWAY

Leistungsbeschreibung

Die Einzelvereinbarung Kollektiv Gateway ist Teil des Rahmenvertrags und seiner Anhänge. Steht in dieser Einzelvereinbarung nichts Anderweitiges, gilt der Rahmenvertrag mit seinen Anhängen.

Einleitung und Anwendungsbereich

Gegenstand dieser Einzelvereinbarung ist das Produkt HIN Gateway (HIN GW). Durch den Einsatz des HIN GW arbeiten und kommunizieren Nutzer innerhalb ihrer Institution und mit anderen angeschlossenen HIN Mitgliedern datenschutzkonform (Berufsgeheimnis/Arztgeheimnis, DSG).

Die Einzelvereinbarung regelt die Rechte und Pflichten von HIN und dem Kunden betreffend Anschluss und Nutzung der HIN Plattform mittels HIN GW.

Angaben über unterstützte und eingesetzte Technologien, Betriebssysteme etc. beziehen sich auf den Stand zum Zeitpunkt der Erstellung dieser Einzelvereinbarung.

1. Leistungen von HIN

Das HIN GW umfasst je nach Ausprägung die zentral bewirtschaftbaren und in die bestehende IT-Landschaft integrierbaren Komponenten HIN Mail Gateway (MGW) und/oder HIN Access Gateway (AGW).

Das HIN GW ermöglicht die Nutzung von HIN Mail und HIN Access. HIN Mail schützt die E-Mail-Kommunikation der gesamten Maildomäne. E-Mails an HIN Mitglieder und als «vertraulich» markierte E-Mails an Empfänger ohne HIN Mitgliedschaft werden automatisch verschlüsselt. HIN Access ermöglicht den Zugriff auf HIN geschützte Anwendungen mittels HIN Identität ohne Installation von Software oder Zertifikaten auf den Arbeitsstationen.

HIN Mail

- **Funktionsweise**

  Automatisch gesicherter Mailverkehr (domänenbasierte Verschlüsselung zwischen Gateways) mit der HIN Community resp. allen an HIN angeschlossenen E-Mail-Adressen.

  Automatische Verschlüsselung von als «vertraulich» markierten E-Mails an beliebige Empfänger.

- **Nutzungsvoraussetzungen**

  Die Komponente MGW wird gemäss Anleitung (technisches Benutzerhandbuch) als virtuelle Appliance (VM), alternativ auch als Hardware Appliance (HW), in die IT-Infrastruktur des Kunden integriert.

- **Leistungsumfang MGW**
  - Einsatz einer Signatur zur Überprüfung von Authentizität (Absenderüberprüfung) und Integrität (Prüfung auf Veränderung des Inhaltes).
  - Signierung und Verschlüsselung (abhängig von MGW-Version) von ausgehenden E-Mails.

- Überprüfung von Integrität und Authentizität sowie Entschlüsselung (abhängig von MGW-Version) von eingehenden E Mails.

HIN Access

- **Funktionsweise**
  Gesicherter und datenschutzkonformer Zugriff auf die HIN Verzeichnisdienste und HIN geschützten Anwendungen mittels Single Sign-on (SSO).
- **Nutzungsvoraussetzungen**

  Die Komponente AGW wird gemäss Anleitung (technisches Benutzerhandbuch) als virtuelle Appliance VM in der IT-Infrastruktur des Kunden integriert.

- **Leistungsumfang AGW**
  - Ausstellen und Bereitstellen elektronischer HIN Identitäten für die Institution, Benutzergruppen oder einzelne Benutzer (abhängig von der AGW-Version und der konkreten Offerte)
  - Überprüfung von Integrität und Authentizität bei Zugriffen auf HIN geschützte Anwendungen (Authentisierung, SSO).

Die HIN Private Key Infrastructure (PKI) regelt die Registrierung der öffentlichen Schlüssel, verwaltet diese zusammen mit den dazugehörigen Zertifikaten und verifiziert deren Gültigkeit.

HIN und der Kunde verpflichten sich zur sicheren Verwaltung aller Identifikationen und Schlüssel. Im Falle von unbeabsichtigtem Bekanntwerden von Passwörtern oder Entwendung, Missbrauch oder unerlaubtem Zugriff auf den privaten Schlüssel gibt HIN dem Kunden das Recht, sich einen neuen Schlüssel einrichten (erneute Registrierung) oder die Identität definitiv sperren zu lassen.

Aufschaltung

HIN verpflichtet sich, dem Kunden das HIN GW auf den vereinbarten Termin aufzuschalten und alle Vorkehrungen zu treffen, damit der Kunde den Dienst vollumfänglich nutzen kann.

Die Installation kann vom Kunden-Administrator basierend auf der zur Verfügung gestellten Dokumentation selbständig durchgeführt werden. Die Installation der VM oder HW und die Integration in die IT-Umgebung (Firewall, Mailserver) des Kunden ist nicht Bestandteil des Angebotes von HIN, falls nicht ausdrücklich mitofferiert. Engineering- bzw. Implementierungsleistungen können jedoch auf Anfrage vermittelt werden und werden nach aktuell geltenden Stundenansätzen in Rechnung gestellt.

Audit Trail

Der Audit Trail stellt die lückenlose Aufzeichnung aller Aktionen und Ereignisse dar, die von Benutzern oder Systemkomponenten in der HIN Plattform ausgelöst werden. Ein Audit Trail Eintrag ist charakterisiert durch Datum und Zeit, Applikation bzw. Systemkomponente, Bezeichnung der Aktion, auslösender Benutzer u.a.

Dem Kunden wird auf Verlangen und nach Möglichkeit ein Auszug aus dem Audit Trail zur Verfügung gestellt. Der Auszug enthält diejenigen Daten und Attribute des Audit Trails, welche für die konkrete Fragestellung benötigt werden, und zu deren Einsicht der Kunde berechtigt ist.

Es gelten grundsätzlich die allgemeinen im Rahmenvertrag festgelegten Bestimmungen.

3. Besondere Bestimmungen

HIN empfiehlt zur Verfügung gestellte Software Patches oder Updates so rasch als möglich, spätestens innert 2 Monaten einzuspielen. Wartungs- und Supportaufwände für ältere Versionen, können ab dem 3. Monat nach Erscheinen der Patches und Upgrades in Rechnung gestellt werden.

Fehlfunktionen oder Probleme, die sich aus der Parametrisierung des HIN Gateways oder aus dem Zusammenspiel HIN Gateway mit der von dem Kunden eingesetzten Infrastruktur, Hard- oder Software ergeben, die auf Bedienungsfehler zurückzuführen sind oder durch Eingriffe in HIN Gateway verursacht werden, gelten nicht als Fehler von HIN Gateway.

Der Kunde haftet gegenüber HIN für Schäden, die auf die Nichterfüllung seiner vertraglichen Verpflichtungen zurückzuführen sind, wenn er nicht beweist, dass ihn kein Verschulden trifft.

4. Mitwirkungspflichten des Kunden

Der Kunde generiert im Verlauf des Registrations-Prozesses einen öffentlichen und einen privaten Schlüssel (Public/Private Key). Der öffentliche Schlüssel wird bei HIN eingereicht. Die Mitglieder oder Mitarbeiter der betreffenden Organisation werden anhand dieses Schlüssels als zu dieser Organisation zugehörig ausgewiesen.

Die Authentisierungsmerkmale wie z.B. Privater Schlüssel, Zertifikat, Passphrase, etc. dürfen nicht an Dritte übertragen oder verkauft werden. Sie dürfen auch nicht in eine andere Firma übernommen werden. Der Kunde trägt die Folgen, die sich aus missbräuchlicher Verwendung von Authentisierungsmerkmalen ergeben. HIN gibt dem Kunden das Recht im Falle der Entwendung, des Missbrauchs, des unerlaubten Zugriffs auf die privaten Schlüssel oder des Bekanntwerdens der Passphrase das Recht, neue private Schlüssel zu generieren und sich erneut zu registrieren oder das Login sperren zu lassen.

Sorgfaltspflicht

Der Kunde informiert alle Personen über die beschriebene Funktionsweise und Sorgfaltspflichten im Umgang mit sensiblen Informationen. Der Kunde ist für die Sicherheit der Nachrichtenübermittlung innerhalb seines Netzwerks bzw. Mailsystems verantwortlich.

Der Kunde installiert Updates zeitnahe nach Release und informiert HIN proaktiv über allfällige Sicherheitsvorfälle.

Der Kunde räumt HIN auf dem HIN Gateway sowie dem Active Directory (AD) Auditrechte ein, welche es HIN erlauben, anhand der «AGW Security Guidelines» zu überprüfen, ob adäquater Schutz gegeben ist.

5. Nutzungsbestimmungen

Die Nutzung der Komponente MGW für den Systemversand ist nicht gestattet bzw. bedingt eine separate Lizenzierung.

6. Vergütung

Die einmaligen Gebühren (Initialkosten) werden nach Vertragsabschluss in Rechnung gestellt.

HEALTH INFO NET AG

Januar 2024