NetUSE E-Mail Encryption

Spezielle Leistungsbeschreibung, Version 1.0, 24.05.2018

1 Leistungsmerkmale NetUSE E-Mail Encryption

1.1 Allgemeine Dienstbeschreibung

Dieser Dienst umfasst die Bereitstellung, den Betrieb, die Überwachung, die Lizenzen, die notwendigen Updates und das Backup eines redundanten Mailgateways zur benutzerbasierenden Verschlüsselung und Signierung von E-Mails auf Basis des Protokolls SMTP (Simple Mail Transfer Protocol) in den Rechenzentren der NetUSE AG. Der Dienst wird durch Mailrouting integriert. Die Bereitstellung erfolgt auf gemeinsam genutzter Infrastruktur.

1.2 Mailtransport

Der Dienst NetUSE E-Mail Encryption ermöglicht dem Kunden den Austausch von elektronischen Nachrichten im Store- and-Forward-Verfahren aufder Basis international anerkannter Normen (Simple Mail Transfer Protocol (SMTP), Extended SMTP (ESMTP)) für den Mailtransport zwischen demMailsystem des Kunden und den NetUSE Mailrelay-Gateways für aus Sicht des Kunden ein- und ausgehende E-Mails. Die NetUSE Mailrelay-Gateways unterstützen eine verschlüsselte Übertragung von E-Mails via TLS (Transport Layer Security).

Die NetUSE Mailrelay-Server nehmen dabei im Rahmen dieses Services ausschließlich E-Mails von ausgewählten IP-Adressen (Mailservern) des Kunden und nur für die konfigurierten Mail-Domains des Kunden an. Alternativ kann der Kunde über den Service NetUSE Mailrelay ein vollständiges Mailrelay (primärer MX) für seine Mail-Domains beauftragen.

1.3 Generelle Vorgehensweise

NetUSE E-Mail Encryption wird in den ein- und ausgehenden Mailverkehr des Kunden eingebunden. Aus Sicht des Kunden eingehende E-Mails werden entschlüsselt sowie ggf. vorhandene kryptografische Signaturen geprüft, ausgehende E-Mails werden signiert und soweit möglich (siehe 1.5.3)verschlüsselt. Durch eine hinterlegte Policy (Secure-Mail-Policy) kann zum Beispiel vorgegeben werden, zu welchen Empfängern (E-Mail-Adressen bzw. Domains) eine Verschlüsselung verpflichtend ist. E-Mails, die trotz verpflichtender Verschlüsselung nicht verschlüsselt werden können, können in ein SecureMail Messenger System umgeleitet und dort vom Empfänger mit Hilfe eines Web-Browsers abgeholt werden. Alle kryptografischen Schlüssel werden auf dem Mailgateway gespeichert, so dass keine Anpassungen an den Mailclients des Kunden erforderlich sind.

1.4 Unterstützte E-Mail-Verschlüsselungsverfahren

Der Service NetUSE E-Mail Encryption unterstützt als E-Mail-Verschlüsselungsverfahren bzw. Protokolle S/MIME (Secure/Multipurpose Internet Mail Extensions) und OpenPGP (Pretty Good Privay), die beide auf einer asymmetrischen Verschlüsselung basieren und ein Public-Private-Schlüsselpaar je E-Mail-Adresse des Kunden erfordern. Bei S/MIME sind digitale X.509-basierte User-Zertifikate für die Verifizierung der Schlüssel für den Betrieb notwendig. X.509 Zertifikate müssen zusätzlich kostenpflichtig beschafft werden. Dies kann über den CA-Connector automatisiert erfolgen (siehe 1.7).

1.5 Behandlung von öffentlichen Schlüsseln, E-Mails und Lizenzen

1.5.1 Lizenzierung von Benutzern

Ver- oder Entschlüsselung sowie Erstellung oder Überprüfung von Signaturen erfordern eine Benutzerlizenz. Die Verwaltung der Benutzerlizenzen erfolgt manuell durch die NetUSE AG oder automatisiert durch den ERP-Connector (siehe 1.6). Maßgeblich für die Zuordnung der Benutzerlizenz ist die E-Mail-Adresse. Für einen lizenzierten Benutzer hinterlegte E-Mail-Alias-Adressen erfordern keine weitere Benutzerlizenz. Ist für den Benutzer keine Lizenz hinterlegt, wird die Mail unverarbeitet weitergeleitet.

1.5.2 Suche nach öffentlichen Schlüsseln von Kommunikationspartnern.

Ausgehende E-Mails können nur verschlüsselt werden, wenn der öffentliche Schlüssel des Kommunikationspartners dem Service bekannt ist. Der Service NetUSE E-Mail Encryption unterstützt den Benutzer durch eine automatische Suche nach öffentlichen Schlüsseln in diversen öffentlichen Verzeichnissen. Das Auffinden eines öffentlichen Schlüssels des Kommunikationspartners kann nicht garantiert werden, auch wenn einer existiert.

1.5.3 Ausgehende E-Mails

Ausgehende E-Mails werden auf Basis der im Mailgateway hinterlegten Policy oder in Folge eines Benutzer-Befehls in der E-Mail verschlüsselt und signiert. Kann für den Kommunikationspartner kein öffentlicher Schlüssel gefunden werden, lassen sich die Mails in einen SecureMail Messenger (siehe 1.5.5) umleiten.

1.5.4 Eingehende Mails

Verschlüsselte Mails werden automatisch entschlüsselt. Eine an einer eingehenden E-Mail vorhandene kryptografische Signatur der E-Mail wird geprüft. Bei der Überprüfung der Signatur wird der Inhalt der Mail auf Unversehrtheit geprüft. Die Signatur wird anhand in der NetUSE E-Mail Encryption hinterlegter TrustCenter Zertifikate validiert. Weitere TrustCenter Zertifikate von Kommunikationspartnern können durch NetUSE geprüft und hinterlegt werden. Ein Anrecht auf Hinterlegung weiterer TrustCenter Zertifikate besteht nicht. Fehler bei der Überprüfung der Signatur (auch Signatur nicht validierbar) oder beim Entschlüsseln der Mail werden (konfigurierbar je Kunde) im Betreff oder im Inhalt der Mail kenntlich gemacht, um den Empfänger darüber zu informieren.

1.5.5 SecureMail Messenger

Ausgehende E-Mails, die aufgrund einer im Mailgateway hinterlegten Policy oder eines Benutzer-Befehls in der E-Mail nicht unverschlüsselt übertragen werden dürfen, können entweder abgelehnt (Fehlermeldung an den Absender) oder in den SecureMail Messenger umgeleitet werden. Der SecureMail Messenger stellt ein per HTTPS gesichertes Webmail-Interface zur Verfügung, über das die E-Mails mit einem Web-Browser über eine verschlüsselte Verbindung vom Kommunikationspartner abgeholt werden können. Der Kommunikationspartner (Empfänger-E-Mail-Adresse) erhält beim ersten Eintreffen einer E-Mail im SecureMail Messenger eine unverschlüsselte Informations-E-Mail mit einem Registrierungslink. Nach einmaliger Registrierung im SecureMail Messenger kann der Kommunikationspartner den SecureMail Messenger als Web-Mailer zum Austausch geschützter Informationen mit den E-Mail-Adressen des Kunden nutzen. Beim Eintreffen neuer E-Mails vom Kunden im SecureMail Messenger für denselben Kommunikationspartner erhält der Kommunikationspartner jeweils eine Informations-E-Mail, die ihn über das Vorliegen einer neuen Nachricht informiert.

Standardmäßig ist das im Rahmen von NetUSE E-Mail Encryption bereitgestellte SecureMail Messenger Portal unter einer URL (Uniform Resource Locator) aus einer Domain der NetUSE AG erreichbar.

1.6 ERP-Connector

Der ERP-Connector (Enterprise Resource Planning) fragt automatisiert die Informationen über die vorhandenen Benutzer des Kunden aus einer LDAP-Datenquelle des Kunden ab. Die Datenquelle kann ein Microsoft Active Directory oder jeder andere LDAP-Dienst des Kunden sein. Zu einem Benutzer werden dabei seine E-Mail-Adresse und alle E-Mail-Alias-Adressen abgefragt, so dass eine automatische Zuordnung der Alias-Adressen zu Benutzern erfolgen kann. Über die Definition von verschiedenen Policy-Gruppen im LDAP kann eine Unterscheidung der verwendeten Secure-Mail-Policy des Kunden erwirkt werden. Die Zuordnung einer Gruppe im LDAP des Kunden zu einer Secure-Mail-Policy erfolgt in der NetUSE E-Mail Encryption. So können z.B. unterschiedliche Policies für verschiedene Personengruppen oder Unternehmensbereiche des Kunden genutzt werden. Im Zusammenwirken mit dem CA-Connector kann über die Gruppenzuordnung ebenfalls gesteuert werden, für welchen Benutzer ein Zertifikat beschafft werden soll. Eine Zuordnung eines Benutzers zu mehreren Policy-Gruppen ist nicht zulässig.

Durch Verwendung des ERP-Connectors kann eine automatische Zuweisung von Benutzer-Lizenzen aufgrund der Policy erfolgen.

Die Nutzung des ERP-Connectors ist optional. Für den ERP-Connector entstehen keine zusätzlichen monatlichen Kosten.

1.7 CA-Connector

Über den CA-Connector können aus dem Service NetUSE E-Mail Encryption heraus automatisiert User-Zertifikate für die konfigurierten Benutzer des Kunden bestellt werden. Hierbei kann eine eigene Certificate Authority (CA) des Kunden (self-signed) verwendet werden, oder es wird über das Datacenter des Technologiepartners Zertificon Solutions GmbH ein Zertifikat eines TrustCenters bestellt. Zertificon bietet dabei verschiedene TrustCenter zur Auswahl, von denen die Zertifikate bezogen werden können.

Die Nutzung des CA-Connectors ist optional. Für den CA-Connector entstehen zusätzliche monatliche Kosten bei der NetUSE AG.

1.7.1 CA-Connector-Vertrag

Damit eine automatisierte Zertifikatsbestellung mit einer offiziellen CA erfolgen kann, muss ein Vertrag zwischen dem Kunden und der Zertificon Solutions GmbH geschlossen werden, der die Zertificon beauftragt und berechtigt die User-Zertifikate für den Kunden einzukaufen. Die Zertifikate haben eine Mindestvertragslaufzeit von 1 Jahr. Eine automatische Zertifikatsbestellung und -Verlängerung kann konfiguriert werden.

Die einzelnen Zertifikate werden dem Kunden gesondert in Rechnung gestellt, entweder über die NetUSE AG oder direkt von der Zertificon Solutions GmbH.

1.7.2 Eigene Public Key Infratructure (PKI) in NetUSE E-Mail Encryption

Über eine im Rahmen von NetUSE E-Mail Encryption optional bereitgestellte eigene PKI für den Kunden kann eine automatische Generierung von Zertifikaten erfolgen. Bei der Verwendung einer eigenen PKI kann der Kommunikationspartner die E-Mail beim Empfang nicht automatisch verifizieren. Für die Nutzung entstehen keine zusätzlichen monatlichen Kosten,

1.8 Rahmenparameter

Dr.-Hell-Straße
24107 Kiel

Sitz der AG: Kiel
HRB 5358 AG Kiel

Telefon: 0431- 2390 400
Telefax: 0431- 2390 499

service@NetUSE.de
www.NetUSE.de

HypoVereinsbank für €:
IBAN DE36 **20030000** 000 **2366565**
BIC HYVEDEMM300
HypoVereinsbank nur für $:
IBAN DE16 **20030000** 00 **15559701**
BIC HYVEDEMM300

Förde Sparkasse Kiel für €:
IBAN DE45 **21050170** 00 **24002776**
BIC NOLADE21KIE
Commerzbank für €:
IBAN DE91 **21040010** 0 **749671400**
BIC COBADEFFXXX

Sydbank für €:
IBAN DE88 **21020600 1000477957**
BIC SYBKDE22KIE
Sydbank nur für $:
IBAN DE66 **21020600 1000477965**
BIC SYBKDE22

USt.-ID: DE156073942
Gläubiger-ID: 97ZZZ00000021988

Aufsichtsrat: Dr. Dirk Lukas (Vorsitz)

Vorstand:
Dr. Jörg Posewang (Vorsitz)
Dr. Roland Kaltefleiter
Andreas Seeger

Die Nutzung des Dienstes NetUSE E-Mail Encryption setzt voraus, dass für alle Mail-Domains, für die die E-Mails bearbeitet werden sollen, der Service NetUSE Mailrelay beauftragt ist oder alternativ alle ein- und ausgehenden Mails von definierten IP-Adressen des Kunden per SMTP über die NetUSE Mailsysteme geleitet werden. NetUSE E-Mail Encryption kann nur für ganze Mail-Domains oder Subdomains des Kunden realisiert werden, so dass alle Mails von bzw. an eine Mail-Domain durch NetUSE E-Mail Encryption geroutet werden müssen; eine selektive Abschaltung dieses Dienstes auf der Basis von Usern bzw. E-Mail-Adressen ist im Rahmen der Secure-Mail-Policy möglich. E-Mails, die der Kunde zwischen verschiedenen E-Mail-Adressen innerhalb seiner Maildomains verschickt, werden vom Service NetUSE E-Mail Encryption nicht verschlüsselt, entschlüsselt oder signiert. Ebenso werden die E-Mails zwischen zwei Mandanten innerhalb des Services NetUSE E-Mail Encryption nicht verschlüsselt, entschlüsselt oder signiert.

1.9 Verzögerung der Mailzustellung

NetUSE E-Mail Encryption arbeitet mit sogenannten Mail-Queues, die die E-Mails annehmen und in der Regel sofort ggf. aber zeitverzögert weiterleiten. Dabei kann diese Zeitverzögerung von wenigen Sekunden bis hin zu mehreren Stunden variieren, wenn das System z.B. durch Spam-Wellen stark belastet wird. Eine zeitverzögerte Zustellung ist kein Mangel.

1.10 Veränderung von Mailinhalten

Der Vorgang der Ver- oder Entschlüsselung bzw. Signierung von E-Mails durch NetUSE E-Mail Encryption kann zur Veränderung von Inhalten führen, zum Beispiel durch Anhängen von Informations-Headern in den Mail-Headern, Erweitern des Betreffs (Subjects) einer E-Mail durch einen Hinweistext oder Anfügen von Bearbeitungsinformationen (Verschlüsselungsstatus, Signaturstatus, ...) an den Mailinhalt. Dies kann in der Folge auch dazu führen, dass eine bereits vorhandene kryptographische Signatur an einer aus Sicht des Kunden ausgehenden E-Mail entfernt werden muss. Der Kunde erklärt hierzu sein Einverständnis.
Eine weitergehende Information (z.B. an den Absender der E-Mail) erfolgt nicht.

1.11 Verschlüsselte Daten

Wird NetUSE E-Mail Encryption zusammen mit NetUSE Spam-Filter, NetUSE Virus-Scan-E-Mail oder NetUSE Threat Emulation E-Mail betrieben, so erfolgt für eingehende E-Mails aus Sicht des Kunden zuerst die Entschlüsselung der E-Mails und danach erst die weitere Bearbeitung durch die anderen genannten NetUSE Services.
Im Rahmen der Secure-Mail-Policy ist u.a. zu definieren, wie der Service NetUSE E-Mail Encryption mit bereits vom Kunden signierten und verschlüsselten aus Sicht des Kunden ausgehenden E-Mails umgehen soll.

1.12 E-Mail-Größenbeschränkung

E-Mails größer als 100 MB (1 MB =10^6 Bytes) werden vom Service NetUSE E-Mail Encryption abgelehnt. Eine kundenspezifische Anpassung der maximalen Mailgröße ist nicht möglich.

1.13 E-Mail-Aufbewahrung

Die NetUSE AG kann für die Speicherung von E-Mail, die die NetUSE AG dem Kunden nicht binnen eines Zeitraums von 8 Stunden zustellen kann, keine Garantie übernehmen. Sofern der Speicherplatzbedarf im Einzelfall ein zumutbares Maß überschreitet, behält sich die NetUSE AG vor, die weiteren für einen Kunden eingehenden Nachrichten abzulehnen.
Falls der Kunde für die entsprechenden Mail-Domains einen Vertrag über NetUSE Mailrelay hat, gelten die dort vereinbarten deutlich längeren Aufbewahrungsfristen.

1.14 Delivery Status Notification Messages (Bounces)

Delivery Status Notification Messages (auch bezeichnet als Postmaster/Mailerdaemon-E-Mails bzw. Error-Bounces), d.h. E-Mails mit den Absendern <> oder MAILER-DAEMON im Envelope-FROM, können bereits nach 4 Stunden (Verweilzeit auf NetUSE-Systemen) gelöscht werden, sofern mindestens ein Zustellversuch fehlgeschlagen ist.

1.15 Fehlercodes bei eingehendem Mailrelay

Liefert ein Mailserver des Kunden bei einem Zustellversuch durch NetUSE-Mailserver bei (aus Sicht des Kunden) eingehendem Mailrelay einen temporären Fehlercode (dies betrifft alle 4er Codes), dann hat die NetUSE AG das Recht, diese gegenüber dem Absender der E-Mail auf einen 5er Code (permanenter Fehler) umzuschreiben.

1.16 ??

.

1.17 Abrechnungsverfahren

Die Abrechnung des Services NetUSE E-Mail Encryption erfolgt in Form einer monatlichen Grundgebühr je Benutzerlizenz sowie ggf. zusätzlich einer nutzungsabhängigen Gebühr für sogenannte HighVolume-User, die anhand der ein- und ausgehenden Mails der HighVolume-User ermittelt wird

1.17.1 Abrechnung je Benutzer bzw. Mailverteiler

Die Abrechnung des Service NetUSE E-Mail Encryption erfolgt je Benutzer bzw. Mailverteiler des Kunden, dem (via statischer Konfiguration oder ERP-Connector) explizit eine Lizenz zugeordnet wurde. Dabei wird prinzipiell jede E-Mail-Adresse, für die aufgrund der Benutzerlizenz Verschlüsselungs-, Entschlüsselungs- oder Signatur-Operationen durchgeführt werden können, als kostenpflichtiger Benutzer gezählt. Dazu wird bei Abschluss des Vertrages die zu schützende Benutzeranzahl (inkl. Mailverteiler) des Kunden vereinbart (Commitment). Grundlage für die Abrechnung ist die im Laufe des Monats maximal genutzte Anzahl lizensierter E-Mail-Adressen, welche sich auf das vom Kunden vorbestellte Commitment (Mindestabnahme) und eventuell darüberliegende genutzte Lizenzen verteilt.Die NetUSE AG ist berechtigt, die Anzahl zu prüfen und gegenüber ihren Zulieferern offen zu legen.
Da der Service NetUSE E-Mail Encryption keine Benutzer, sondern nur E-Mail-Adressen identifizieren kann, werden für die Abrechnung prinzipiell alle E-Mail-Adressen des Kunden als Benutzer gezählt. Ausschließlich E-Mail-Adressen, die als E-Mail-Alias-Adresse einer primären Benutzer-E-Mail-Adresse zugeordnet sind, werden von der Zählung ausgenommen. Diese Zuordnung kann entweder manuell nach Vorgabe des Kunden erfolgen (Konfigurationsänderung) oder aber automatisiert über den ERP-Connector.

1.17.2 Abrechnung für HighVolume-User

Zusätzlich zu der Abrechnung je Benutzer bzw. Mailverteiler entstehen weitere Kosten für sogenannte HighVolume/Automation-User. Das sind alle User mit mehr als 3000 (durch den Service NetUSE E-Mail Encryption gerouteten, also in der Regel externen) E-Mails pro Monat (Summe aus ein- & ausgehenden Mails), sowie alle Mails von/an E-Mail-Adressen, die automatisierten Systemen zugeordnet sind (z.B. E-Business-Systemen wie Online-Shops, Online-Auktionshäusern, Portalen, Buchhaltungssystemen, CRM Systemen, Lösungen für Zulieferer, Newsletter und ERP-Systeme (z.B. SAP)).
Die Abrechnung erfolgt je angefangene 1000 E-Mails pro Monat als Summe über alle HighVolume/Automation-User des Kunden.

1.18 Einrichtung, Änderungen

Im Rahmen der Ersteinrichtung von NetUSE E-Mail Encryption für einen Mandanten werden für alle zeitgleich beauftragten Mail-Domains sowie Benutzer bzw. Mailverteiler die vom Kunden gewünschten Maßnahmen und Einstellungen (Secure-Mail-Policy) konfiguriert. In der Ersteinrichtung eines Mandanten ist die Einrichtung für bis zu 10 Mail-Domains des Mandanten mit einer für alle Mail-Domains identischen Policy enthalten.

1.18.1 Mail-Domains

Die Einrichtung weiterer (über 10 hinausgehende oder aber später beauftragter) Mail-Domains sowie die Einrichtung weiterer Policies ist kostenpflichtig. Das Löschen von Mail-Domains oder Policies ist kostenfrei.

1.18.2 Benutzer bzw. Mailverteiler

Die Ersteinrichtung des Service NetUSE E-Mail Encryption für einen Mandanten umfasst noch keine Einrichtung von Benutzern bzw. Mailverteilern. Diese ist zusätzlich kostenpflichtig je Benutzer bzw. Mailverteiler. Prinzipiell wird dabei jede E-Mail-Adresse als Benutzer gezählt. Falls E-Mail-Alias-Adressen bei der Beauftragung als solche vom Kunden gekennzeichnet und einer primären E-Mail-Adresse zugeordnet worden sind, fallen für die Einrichtung von E-Mail-Alias-Adressen keine zusätzlichen Einrichtungsgebühren an.
Wird der ERP-Connector zur Abfrage der E-Mail-Adressen aus dem LDAP des Kunden verwendet und ein CA-Connector Vertrag abgeschlossen, können die Einrichtungsgebühren pro Benutzer entfallen.
Die manuelle Einrichtung von Benutzern wird als Festpreis pro Benutzer abgerechnet.

1.18.3 ERP-Connector

Die optionale Einrichtung des ERP-Connectors erfolgt nach Aufwand und wird gemäß der jeweils gültigen NetUSE-Service-Preisliste berechnet.

1.18.4 CA-Connector

Die optionale Einrichtung des CA-Connectors erfolgt nach Aufwand und wird gemäß der jeweils gültigen NetUSE-Service-Preisliste berechnet.

1.18.5 eigene Public Key Infratructure (PKI)

Es ist möglich, im Rahmen des Service NetUSE E-Mail Encryption eine eigene PKI für den Kunden anzubinden.

1.18.5.1 eigene PKI in NetUSE E-Mail Encryption

Im Rahmen des Service NetUSE E-Mail Encryption kann eine eigene PKI für den Kunden auf Basis von X.509 oder OpenPGP bereitgestellt und angebunden werden. Die Einrichtung wird als Festpreis abgerechnet.

1.18.5.2 eigene PKI beim Kunden

Die optionale Anbindung einer beim Kunden vorhandenen PKI auf Basis von X.509 erfolgt nach Aufwand und wird gemäß der jeweils gültigen NetUSE-Service-Preisliste berechnet.

1.18.6 Dedizierte URL für SecureMail Messenger

Der Kunde kann optional seinen Kommunikationspartnern den von ihm im Rahmen von NetUSE E-Mail Encryption genutzten SecureMail Messenger unter einer eigenen URL aus einer Domain den Kunden bereitstellen. Die Nutzung dieser Option ist mit zusätzlichen einmaligen und monatlichen Kosten verbunden.

1.18.7 Konfigurationsänderungen

Sollten während der Vertragslaufzeit vom Kunden gewünschte Konfigurationen oder Änderungen anfallen, wird die NetUSE AG diese nach Aufwand durchführen und gemäß der jeweils gültigen NetUSE-Service-Preisliste berechnen. Die manuelle Verlängerung von Zertifikaten zählt als Konfigurationsänderung wird nach Aufwand gemäß der jeweils gültigen NetUSE-Service-Preisliste berechnet.

2 Mitwirkungspflichten des Kunden

2.1 Datenschutz

Im Rahmen der von der NetUSE AG betriebenen Lösung fallen beim Betrieb datenschutzrechtlich relevante Daten an, z.B.:

- E-Mail-Adressen des Kunden, an die E-Mails gesendet werden.
- E-Mail-Adressen, die E-Mails an den Kunden senden.
- Ggf. datenschutzrechtlich relevante Inhalte innerhalb der E-Mails.

Es obliegt dem Kunden sicherzustellen, dass die datenschutzrechtlichen Regularien (z.B. der Europäischen Datenschutzgrundverordnung (DS-GVO)) eingehalten werden und dass seine Mitarbeiter über die Erhebung der Daten informiert werden und die gesetzlichen Bestimmungen in Bezug auf die betriebliche Mitbestimmung eingehalten werden.

2.2 Automatische Veröffentlichung von Zertifikaten

Der Kunde willigt ein, dass alle für ihn erstellten Benutzer-Zertifikate in öffentlichen Verzeichnissen der Certificon Solutions GmbH veröffentlicht werden. Durch diese Veröffentlichung ist es Geschäftspartnern des Kunden möglich, die öffentlichen Schlüssel aufzufinden, zu verifizieren und eine verschlüsselte E-Mail-Kommunikation mit dem Kunden aufzunehmen.

2.3 Mail-Domains des Kunden

Der Service NetUSE E-Mail Encryption kann nur für im Voraus festgelegte Mail-Domains des Kunden genutzt werden. Dementsprechend muss der Kunde der NetUSE AG bei Beauftragung alle Mail-Domains benennen, für die er den Dienst nutzen möchte. Eine nachträgliche Änderung der Liste der geschützten Mail-Domains wird gemäß 1.18.1 abgerechnet.

2.4 Konfiguration auf Mailservern des Kunden

Konfigurationen auf den Mailservern des Kunden sind nicht Bestandteil dieser Leistung, sondern liegen im Verantwortungsbereich des Kunden. Auf Wunsch des Kunden unterstützt die NetUSE AG bei derartigen Konfigurationsarbeiten nach Aufwand gemäß der jeweils gültigen NetUSE-Service-Preisliste.

2.5 E-Mail-Routing

Für die Integration von NetUSE E-Mail Encryption in den Mail-Datenverkehr ist der Kunde verantwortlich. Sofern der Kunde nicht NetUSE Mailrelay für die entsprechenden Mail-Domains beauftragt hat, muss er der NetUSE AG bei der Beauftragung folgende Informationen benennen:

- bis zu 5 IP-Adressen der einliefernden Mailserver des Kunden für die Übergabe von zu behandelnden E-Mails an die NetUSE AG
- bis zu 5 IP-Adressen oder Hostnamen der annehmenden Mailserver des Kunden für die Übergabe bereits von NetUSE E-Mail Encryption behandelten E-Mails an den Kunden

2.6 Absicherung der Mailboxserver

Um die Funktion von NetUSE E-Mail Encryption zu gewährleisten, ist es erforderlich, dass der gesamte zu ver- bzw. entschlüsselnde sowie zu signierende E-Mail-Datenverkehr über die von der NetUSE AG vorgegebenen Systeme geroutet wird und dass direkte Verbindungen am Service vorbei aus dem Internet durch Access-Listen oder Firewallregeln unterbunden werden. Diese Konfiguration erfolgt kundenseitig und ist nicht Bestandteil dieses Services.

2.7 Secure-Mail-Policy

Ausgehend von der Secure-Mail-Policy des Kunden wird im Rahmen des Services NetUSE E-Mail Encryption konfiguriert, welche Sicherheitsverfahren (Verschlüsselung optional oder verpflichtend; Behandlung von nicht verschlüsselungsfähigen E-Mails (mangels öffentlicher Schlüssel der Empfänger); ...) für die Kommunikation eingehalten werden müssen. Diese Definition kann auf Basis von Empfänger- oder Absender-E-Mail-Adressen bzw. -Domains erfolgen und muss vom Kunden zeitnah nach der Beauftragung bereitgestellt werden. Solange vom Kunden keine eigene Secure-Mail-Policy bereitgestellt worden ist, nutzt der Service NetUSE E-Mail Encryption eine Default-Policy (für alle lizensierten Benutzer bzw. Mailverteiler werden bei aus Sicht des Kunden eingehenden E-Mails die Signatur geprüft und, sofern ein Zertifikat eingespielt ist, diese entschlüsselt; ausgehende E-Mails werden signiert, sofern ein Zertifikat hinterlegt ist, und verschlüsselt, sofern möglich).

Die NetUSE kann im Rahmen eines kostenpflichtigen Workshops bei der Formulierung dieser Policy unterstützen.

2.8 Private Keys und Zertifikate

Der Service NetUSE E-Mail Encryption benötigt für die Signierung und Entschlüsselung von E-Mails den dazugehörigen Private Key. Die Kommunikationspartner des Kunden benötigen für die Verschlüsselung von E-Mails an den Kunden und die Verifizierung der E-Mails vom Kunden ein X.509 Zertifikat oder den PGP-Public Key mit den Web-of-Trust Signaturen. Mit der Beauftragung des Service (oder der nachträglichen Beauftragung für weitere Benutzer bzw. Mailverteiler) hat der Kunde für alle E-Mail-Adressen (Benutzer bzw. Mailverteiler), für die Verschlüsselungs-, Entschlüsselungs- oder Signatur-Operationen durchgeführt werden können sollen, die User-Zertifikate sowie die zugehörigen Schlüssel an die NetUSE AG zu übergeben. Dasselbe gilt bei jeder Verlängerung von auslaufenden User-Zertifikaten. Zeiten, die durch nicht zeitgleiche Beauftragung des Benutzers und Lieferung des Zertifikats entstehen, werden nach Aufwand gemäß der jeweils gültigen NetUSE-Service-Preisliste abgerechnet.

Alternativ kann der Kunden einen sogenannten CA-Connector-Vertrag (gemäß 1.7.1) abschließen, über den die User-Zertifikate automatisch in den Service NetUSE E-Mail Encryption importiert werden können. Ebenso können darüber auslaufende Zertifikate automatisch verlängert werden.

2.9 E-Mail-Adressen automatisierter Systeme

Für die korrekte Lizenzierung muss der Kunde mit der Übergabe der E-Mail-Adressen für die Einrichtung des Service markieren, welche dieser E-Mail-Adressen sogenannten automatisierten Systemen (gemäß 1.17.2) zugeordnet sind.

2.10 Nutzung des CA-Connector Vertrages

Falls der Kunde einen CA-Connector-Vertrag abschließen möchte, hat er die notwendigen Dokumente beizustellen, die in Abhängigkeit des gewählten Trust-Centers von der Zertificon Solutions GmbH für den Abschluss bzw. die Umsetzung des Vertrages gefordert werden.

2.11 Nutzung des ERP-Connectors

Für die Nutzung des ERP-Connectors ist ein LDAP-Zugriff (IP-Adresse, ggf. Benutzername und Passwort, Search-Base) auf einen LDAP-Dienst des Kunden notwendig. Der Kunde gewährt den Systemen der NetUSE Zugriff auf seine LDAP-Datenquelle(n) und sorgt ggf. für notwendige Firewallfreischaltungen in seinem Verantwortungsbereich. Im Rahmen dieses LDAP-Dienstes muss der Kunde folgende Informationen bereitstellen: Gruppennamen (DN)

2.12 Nutzung des CA-Connectors in Verbindung mit dem ERP-Connector

Bei Nutzung des CA-Connectors zusammen mit dem ERP-Connector können automatisch Zertifikate bestellt und verlängert werden. Die Benutzerverwaltung und Zuordnung der Benutzer zu den Policy-Gruppen im LDAP des Kunden obliegt dem Kunden. Der Kunde hat sicherzustellen, dass keine Zertifikate automatisiert für Benutzer bestellt werden, die kein Zertifikat erhalten sollen. Die Kosten für irrtümlich bestellte Zertifikate durch falsche Benutzerzuordnung im LDAP-System des Kunden trägt der Kunde.

2.13 Nutzung einer eigenen PKI

Bei der Nutzung einer eigenen PKI ist der Kunde für die Veröffentlichung des Root-Zertifikats (z.B. auf seiner Webseite) verantwortlich.

2.14 DNS Hosteintrag für Nutzung einer dedizierten URL für SecureMail Messenger

Um die Nutzung einer dedizierten URL für den SecureMail Messenger zu ermöglichen, ist es erforderlich, dass HTTPS-Zugriffe auf die URL des kunden-dedizierten SecureMail Messenger Portals auf dem von der NetUSE AG bereitgestellten Server ankommen. Dazu muss für den in der URL verwendeten Hostnamen ein Hosteintrag (A-Record) in der DNS-Zone der zugehörigen Domain angelegt werden, der auf die IP-Adresse des von der NetUSE AG betriebenen SecureMail Messenger Servers zeigt. Diese Konfiguration erfolgt kundenseitig und ist nicht Bestandteil dieses Services, sofern diese Domain nicht von der NetUSE AG betrieben wird.

2.15 Empfängercheck

Falls der Kunde für die betreffenden Mail-Domains nicht NetUSE Mailrelay beauftragt hat, hat er sicherzustellen, dass seine Mailserver, an die NetUSE E-Mail Encryption E-Mails zustellen soll, auch alle E-Mails annehmen, die vom Kunden zuvor an NetUSE E-Mail Encryption übergeben wurden. Wenn also ein Empfängercheck bei der Annahme von E-Mails beim Kunden implementiert ist, so ist er vom Kunden vor der Übergabe von E-Mails an NetUSE E-Mail Encryption durchzuführen.

3 Verfahren bei Störungen

Die NetUSE AG leistet innerhalb der Geschäftszeiten (Montag bis Freitag von 8:00 bis 18:00 Uhr; ausgenommen gesetzliche Feiertage) kostenlosen Telefonservice, sofern die Störungen durch die NetUSE AG zu verantworten sind. Stellt sich im Laufe der Bearbeitung heraus, dass die Störungsursache nicht von der NetUSE AG zu verantworten ist, so wird die NetUSE AG dem Kunden die Bearbeitung in Rechnung stellen. Die Berechnung erfolgt dabei nach Aufwand gemäß der jeweils gültigen NetUSE-Service-Preisliste.

4 Spezielle Leistungsbeschreibung, allgemeine Leistungsbeschreibung und AGB

Bei Vertragsschluss oder spätestens bei Nutzung des Dienstes NetUSE E-Mail Encryption werden folgende Bestimmungen in angegebener Reihenfolge Vertragsbestandteil: der Vertrag, die Bestimmungen dieser speziellen Leistungsbeschreibung, die allgemeine Leistungsbeschreibung für NetUSE IP-Dienstleistungen, die NetUSE-Service-Preisliste und die Allgemeinen Geschäftsbedingungen der NetUSE AG.

Dr.-Hell-Straße
24107 Kiel

Sitz der AG: Kiel
HRB 5358 AG Kiel

Telefon: 0431- 2390 400
Telefax: 0431- 2390 499

service@NetUSE.de
www.NetUSE.de

HypoVereinsbank für €:
IBAN DE36 **20030000** 000 **2366565**
BIC HYVEDEMM300
HypoVereinsbank nur für $:
IBAN DE16 **20030000** 00 **15559701**
BIC HYVEDEMM300

Förde Sparkasse Kiel für €:
IBAN DE45 **21050170** 00 **24002776**
BIC NOLADE21KIE
Commerzbank für €:
IBAN DE91 **21040010** 0 **749671400**
BIC COBADEFFXXX

Sydbank für €:
IBAN DE88 **21020600 1000477957**
BIC SYBKDE22KIE
Sydbank nur für $:
IBAN DE66 **21020600 1000477965**
BIC SYBKDE22

USt.-ID: DE156073942
Gläubiger-ID: 97ZZZ00000021988

Aufsichtsrat: Dr. Dirk Lukas (Vorsitz)

Vorstand:
Dr. Jörg Posewang (Vorsitz)
Dr. Roland Kaltefleiter
Andreas Seeger