Beantragung der Einrichtung einer Schnittstelle zur SEN-Cloud

Mittels der Schnittstelle werden kontrollierte und gesicherte Zugangspunkte zu den IT-Systeme der SEN-Cloud bereitgestellt. Die Schnittstelle zur SEN-Cloud ist ein Bestandteil der ISO 27001-Zertifizierung SEN-Cloud. Aufgrund dessen müssen zur Einrichtung einer Schnittstelle zur SEN-Cloud alle in diesem Formular aufgelisteten Anforderungen umgesetzt werden.
Zudem muss das VPN-Datenblatt SEN-Cloud Infrastruktur vollständig ausgefüllt sein.

Anforderungen:

Bitte bestätigen Sie durch das Setzen eines Häkchens, dass die beschriebene Anforderung umgesetzt bzw. akzeptiert werden.

- ☐ Gemäß der ISO 27001 Annex A.12.1.4 sind Entwicklungs-, Test- und Produktivumgebung voneinander getrennt. Passive EMT haben die Trennung in ihrem Sicherheitskonzept, welches anhand der Vorgaben der Certificate Policy des BSI und der SEN.CA erstellt wurde, dokumentiert. Jedem Kunden wird pro benötigter Systemlandschaft mindestens ein Mandant ausgeprägt, der exklusiv auf die Daten der zugewiesenen Systemlandschaft zugreifen kann. Zur Durchführung von Tests sind die Test- und ggf. Entwicklungsumgebung einzusetzen.
- ☐ Die Anbindung der technischen Systemlinien des Kunden über die Schnittstelle erfolgt über eine gesicherte IPSec-Netzwerkverbindung (VPN-Verbindung), welche mit den im VPN Datenblatt SEN-Cloud Infrastruktur angegebenen Daten aufgebaut wird.
- ☐ Der Zugang zu der Schnittstelle erfolgt über geeignete Zugangskennungen, die eine Authentisierung des zugreifenden Systems erfordern. Anwenderkennungen sind zur Authentisierung nicht erlaubt. Die Zugangskennungen werden für jede Systemlinien DEV, TEST und PROD und für jeden Mandanten einer Systemlinie unterschiedlich gewählt. Die verwendeten Authentifizierungsinformationen werden nicht unverschlüsselt in den angebundenen Systemen gespeichert. Der Zugriff auf die Authentifizierungsinformationen ist auf ein Minimum an Personen beim Servicenehmer beschränkt. Die zur Authentifizierung benötigten Anmeldeinformationen werden immer verschlüsselt übertragen.
- ☐ Bei der Verwendung von http Schnittstellen wird eine https Verschlüsselung verwendet.
- ☐ Jeder Zugriff auf die Schnittstelle wird auf Seite des Kunden protokolliert.

☐ Jeder erkannte Sicherheitsmangel oder -vorfall im relevanten Kontext der Schnittstelle wird den Betreibern der SEN-Cloud unmittelbar mitgeteilt.

☐ Änderungen an den Funktionen der Schnittstelle unterliegen auf Seite des Betreibers der SEN-Cloud einem geregelten Release – und Änderungsverfahren. Ein neuer Releasestand der Schnittstelle durchläuft vor der Bereitstellung in der Produktivumgebung Tests in der Entwicklungs- und Testumgebung. Jeder Schnittstellennutzer testet die Schnittstelle in einem definierten Zeitraum und meldet gefundene Fehlern den Betreibern der SEN-Cloud. Sind die Fehler schwerwiegend, wird das Release nicht in die nächsthöhere Systemlinie überführt.

☐ Anforderungen an Nutzer der MSB oder IM4G API:
Das verwendete SSL Zertifikat wurde von einer öffentlichen, vertrauenswürdigen CA signiert. Dabei ist darauf zu achten, dass ein Subject-Alternative Name des Zertifikats mit dem Hostnamen aus der Callback-URL der Webservices übereinstimmt. Da öffentliche CAs keine Zertifikate für IP-Adressen aus dem privaten Adressbereichen ausstellen dürfen, ist es daher erforderlich als API-Endpunkte offizielle IPv4 Adressen zu verwenden. Diese müssen aus dem Netzbereich des Kunden kommen. Als Alternative kann ein Zertifikat über die interne SEN-Cloud CA beantragt werden. In diesem Zertifikat können interne IP Adressen verwendet werden.

Können Sie Anforderungen nicht akzeptieren oder umsetzen, beschreiben Sie hier die betroffene Anforderung und den Grund der Ablehnung:

Unterschrift des Ansprechpartners[1]:

Ort, Datum, Vorname, Name, Unterschrift, Firmenstempel

1 Die Ansprechpartner müssen mit denen aus dem Antragsformular zur Teilnahme an der PKI des Dienstleisters identisch sein.