

Leistungsbeschreibung

Krypto-Plattform

Stand 28.04.2026

Inhaltsverzeichnis

1	Rahmenbedingungen und Zielsetzung	4
1.1	Unternehmen (Auftraggeber)	4
1.2	Kurzbeschreibung des Auftragsgegenstandes	4
1.3	IST-Zustand	4
2	Allgemeine Anforderungen an die HSM-Infrastruktur	5
2.1	Infrastruktur On-Premise	5
3	Allgemeine Anforderungen an die Entrust KMS Infrastruktur	5
3.1	Infrastruktur On-Premise	5
3.1	Hochverfügbarkeit und Stabilität	5
3.2	Anbindung an das Microsoft Active Directory	5
3.3	Lifecycle Management	5
3.4	Compliance Manager	5
3.5	Unterstützte Use Cases	6
4	Allgemeine Anforderungen an die Portal Architektur	6
4.1	Infrastruktur	6
4.2	Anbindung an das Microsoft Active Directory	6
4.3	Anbindung Ansible Automation Plattform	7
4.4	Schlüssellänge	7
4.5	On Premises Installation	7
4.6	Anbindung externer Zertifikate	7
4.7	Integration Mobile Device Management (MDM)	7
4.8	Integration ACME v2	7
4.9	Anforderungen an den Funktionsumfang	7
4.10	Benötigte Formate	8
4.11	Graphische Übersicht	8
4.12	Reports	8
4.13	Verlauf	8
4.14	Ablaufbenachrichtigungen und E-Mail-Verteiler	8
4.15	Standardprotokolle	8
4.16	Verwaltung mehrerer Domänen	8
4.17	Genehmigungsworkflow	8
4.18	Usability	8
4.19	IP-Adresse als SAN-Eintrag	8
4.20	Hochverfügbarkeit und Stabilität	9
5	Mengen	9
6	Lieferung	9
7	Dienstleistungen auf Abruf	10

7.1	Anforderungen an das eingesetzte Personal	10
7.2	Inbetriebnahme	11
7.2.1	Assessment	11
7.2.2	Schulung	11
8	Instandhaltung der Hardware und Pflege der Software	11
9	Treiber und Firmware	12
10	Zertifizierungen	12
11	Optionen und Abrufe	12
12	Kaufmännischer Ansprechpartner	12

1 Rahmenbedingungen und Zielsetzung

1.1 Unternehmen (Auftraggeber)

Die Techniker Krankenkasse (TK) ist eine bundesweite Krankenkasse mit über 12 Millionen Versicherten. Als gesetzliche Krankenversicherung ist die TK eine Körperschaft des öffentlichen Rechts mit Selbstverwaltung.

1.2 Kurzbeschreibung des Auftragsgegenstandes

Die Beschaffung besteht aus Hardware, Software und Dienstleistung:

1.3 IST-Zustand

1.3.1 HSM

Derzeit werden für die verschiedenen Domänen nShield XC HSM-Module eingesetzt. Insgesamt sind derzeit 5 HSM-Module mit insg. 55 Client-Lizenzen und 5 ECC-Lizenzen im Einsatz. Für die Steuerung und Verwaltung wird das Module Keysafe v5 eingesetzt.

1.3.2 Certificate Hub - Certificate Lifecycle Management (PKI Portal)

Entrust CSP Hub

Das bestehende Entrust CSP Portal ist eine im TK-Intranet verfügbar gemachte Appli-
ance. Die dahinter liegende Infrastruktur der PKI basiert auf einer ins Active Directory (AD) eingebundenen Microsoft Certificate Authority (CA). Wir haben insg. 4 MS Certificate Authority Umgebungen im Einsatz.

1.3.3 KMS

Wir setzen mehrere Entrust KMS Appliances ein, welche jeweils zu einem Cluster zusammengefügt worden sind.

- 3 x Compliance Server
- 2 x Vault-Server Produktion
- 2 x Vault Server DMZ

Auf den Vault Servern laufen die folgenden Module:

- KeyControl for Oracle TDE
- KeyControl for Microsoft TDE
- KeyControl Secrets
- KeyControl KMIP
- KeyControl Multicloud Bring Your Own Key

2 Allgemeine Anforderungen an die HSM-Infrastruktur

2.1 Infrastruktur On-Premise

Die Anzahl der zukünftigen HSM-Module soll reduziert werden. Dazu müssen diese in der Lage sein, eine Multi-Tenant Umgebung bereitzustellen. Die HSM-Module sind als Cluster-Lösung zu betreiben und werden in mehreren Rechenzentren gehostet. Insgesamt werden derzeit 5 eigene Secure World Umgebungen benötigt, eine Erweiterung muss möglich sein. Die Module müssen den zukünftigen Post-Quantum Standard unterstützen. Sobald der Standard feststeht, ist der AN verpflichtet, seine Software daran anzupassen. Die Verwaltung der HSM-Lösung muss über ein zentrales Management Tool möglich sein. Der AN gewährleistet, dass die vertraglich gemäß Preisblatt vereinbarten Hardware-Komponenten über die gesamte Vertragslaufzeit lieferbar sind. Dies gilt sowohl bei Nachbestellung einer Hardware-Komponente im Rahmen einer vertraglichen Option als auch im Falle eines notwendigen Hardwareaustausches nach einer Störung. Der Wechsel eines Hardware-Produkts ist nur unter den Voraussetzungen von § 17 des Vertrags möglich.

3 Allgemeine Anforderungen an die Entrust KMS Infrastruktur

3.1 Infrastruktur On-Premise

Die derzeitige Infrastruktur wird weiterhin in ihrer aktuellen Form betrieben. Jegliche bereitgestellte Software inkl. zugehöriger Dienste müssen in den eigenen Rechenzentren der TK betrieben werden. Cloudbasierte Lösungen dürfen nicht zum Einsatz kommen und werden ausgeschlossen. Die Lösung muss über Windows Server 2025, über Red Hat Enterprise Linux 8/9 (RHEL) und auch über eine in sich geschlossene Appliance bereitstellbar sein. Weitere Hinweise befinden sich im Kapitel Plattform-Konformität in der Anlage L1, Vorgaben aus IT-Sicht.

3.1 Hochverfügbarkeit und Stabilität

Die TK wird die Lösung in 2 örtlich separierten Rechenzentren betreiben. Die Lösung muss daher hochverfügbar aufgebaut sein. Sollte eine Instanz ausfallen, muss ohne Daten- und Zeitverlust auf die andere Instanz (automatisiert) gewechselt werden.

3.2 Anbindung an das Microsoft Active Directory

Die Anbindung an das Microsoft Active Directory muss gewährleistet sein. Das Berechtigungskonzept muss an das AD der TK angebunden werden. Die Plattform muss eine rollenbasierte Zugriffskontrolle (RBAC) bieten, um den Userzugriff auf bestimmte Datensätze und Funktionen (Rollen) zu steuern. Ergänzend gelten die Anforderungen aus dem Abschnitt „Identity und Access Management der Anlage L1.

3.3 Lifecycle Management

Die Lösung muss zwingend ein Lebenszyklusmanagement für Schlüssel und Geheimnis-Treasure und ein dezentrales Schlüssel- und Geheimnislebenszyklusmanagement zur Erfüllung geschäftlicher und regulatorischer Anforderungen beinhalten.

3.4 Compliance Manager

Ein einheitliches Dashboard für Inventar, Risiko und Compliance kryptografischer Assets ist zwingende Anforderung zur Durchsetzung von Richtlinien gemäß TK-Vorgaben.

3.5 Unterstützte Use Cases

- Vault for KMIP
 - o Database Protection
 - o Virtual Machine Protection
 - o Data Security
 - o Storage Protection
- Vault for Secrets
 - o SSH Session Protection
 - o Privileged Account and Session Management
- Vault for VM Encryption
 - o Agent-Based VM Encryption
 - o Cloud
 - o On Premises
- Vault for Databases-TDE
 - o Database Protection for Oracle
 - o Database Protection for MS SQL
 - o Database Protection for Postgres DB
 - o Database Protection for Mongo DB
- Vault for Cloud Keys
 - o BYOK
 - o HYOK
 - o Customer Managed Keys
- Vault for Application Security
 - o Data Tokenization
 - o Data Encryption
 - o Signing

4 Allgemeine Anforderungen an die Portal Architektur

4.1 Infrastruktur

Die zukünftige Lösung muss mit der bestehenden Infrastruktur kompatibel sein. Diese basiert auf einer Microsoft PKI mit Entrust Hardwaresicherheitsmodulen. Im zugehörigen Portal müssen 30.000 Zertifikate verwaltet werden können, die sich überwiegend aus Webserver- und Druckerzertifikaten zusammensetzen. Zusätzlich muss die Erhöhung der Zertifikatsmenge möglich sein. Der geschätzte Umfang der Leistung ist dem Preisblatt (Anlage A1) zu entnehmen.

4.2 Anbindung an das Microsoft Active Directory.

Die Anbindung an das MS Active Directory muss gewährleistet sein. User- und Maschineninformationen müssen für das Erzeugen von Zertifikaten aus dem AD bezogen werden können. Das Berechtigungskonzept muss an das AD angebunden werden. Die Plattform muss eine rollenbasierte Zugriffskontrolle (RBAC) bieten, um den Userzugriff auf bestimmte Datensätze und Funktionen zu steuern. Ergänzend gelten die Anforderungen aus dem Abschnitt „Identity und Access Management der Anlage L1.

4.3 Anbindung Ansible Automation Plattform

In der IT-Architektur der Techniker Krankenkasse wird die Ansible Automation Plattform (AAP) eingesetzt. Die Lösung muss in der Lage sein dort integriert zu werden.

4.4 Schlüssellänge

In der IT-Architektur der Techniker Krankenkasse wird derzeit mit 4K und ECC-Zertifikaten gearbeitet, daher muss die Plattform in der Lage sein, mit Schlüssellängen von mindestens 4K und ECC umzugehen. Zukünftige Schlüssellängen wie z.B. Post-Quanten-Sicherheit sollen zeitnah über Updates zur Verfügung gestellt werden.

4.5 On Premises Installation

Jegliche bereitgestellte Software inkl. zugehöriger Dienste müssen in den eigenen Rechenzentren der TK betrieben werden können. Cloudbasierte Lösungen dürfen nicht zum Einsatz kommen und werden ausgeschlossen. Das Produkt muss über Windows Server 2025, über Red Hat Enterprise Linux 8/9 (RHEL) und auch über eine in sich geschlossene Appliance bereitstellbar sein. Für die Lauffähigkeit gelten die folgenden Vorgaben:

- Windows Server zum Angebotszeitpunkt aktuelles Major-Release im Long Term Servicing Channel (LTSC) und Vorgängerversion (auch im LTSC)
- Red Hat Enterprise Linux, zum Angebotszeitpunkt aktuelles Major-Release und Vorgängerversion
- Red Hat OpenShift 4.x (aktuelles Minor-Release)
- Open Virtual Appliance auf VMware ESX 8.0

4.6 Anbindung externer Zertifikate

Es muss eine Anbindung externer Zertifikatsanbietenden (derzeit DigiCert) für die Domäne der Techniker Krankenkasse möglich sein. Darüber hinaus muss die Möglichkeit der Verwaltung externer Zertifikate der Domäne der Techniker Krankenkasse in der Oberfläche der Zertifikatsverwaltung gegeben sein. Bestellungen von externen Zertifikaten mittels API bei Dritt-anbietenden müssen innerhalb des bereitgestellten Portals ausführbar sein.

4.7 Integration Mobile Device Management (MDM)

Das zur Verfügung gestellte Portal muss eine MDM-Integration unterstützen, insbesondere für Microsoft Intune und Jamf.

4.8 Integration ACME v2

Das zur Verfügung gestellte Portal muss eine ACME-Integration unterstützen, insbesondere für Linux.

4.9 Anforderungen an den Funktionsumfang

Folgende Funktionen müssen aus dem Portal mit oben beschriebener PKI-Infrastruktur erfüllt werden:

- Zertifikate müssen von Endanwender: innen über das Portal bestellt werden können
- Certificate Signing Request (CSR) müssen vom Portal verarbeitet werden können
- Zertifikate müssen von den Administrierenden widerrufen werden können
- Endanwender: innen müssen einen Antrag zum Widerruf von Zertifikaten stellen können.

4.10 Benötigte Formate

Die Zertifikate müssen in allen angebundenen Domänen in folgenden Formaten ausgestellt werden können:

Zertifikate: „.pfx/p12“, oder „.pem“,

4.11 Graphische Übersicht

Zur optimalen Verwaltung muss den PKI-Administrierenden über die Weboberfläche eine graphische Übersicht über eingesetzte Zertifikate geliefert werden. Diese muss individualisierbar sein, beispielsweise durch Filter. Das Interface der Verwaltungsoberfläche für Administrierende und Endanwender: innen muss graphisch, browserbasiert und über das Intranet der TK erreichbar sein.

4.12 Reports

Es müssen Berichte/Reports in der Weboberfläche angezeigt werden können. Darüber hinaus sollen diese im PDF erzeugt werden können und individualisierbar sein.

4.13 Verlauf

Es muss in der Weboberfläche des Portals zur Zertifikatsverwaltung einen Aktivitätsverlauf über ausgestellte und revozierte Zertifikate geben.

4.14 Ablaufbenachrichtigungen und E-Mail-Verteiler

Benachrichtigung über ablaufende Zertifikate müssen aus der Benutzeroberfläche der Zertifikatsverwaltungssoftware per E-Mail und mit Hilfe von E-Mail-Verteilern automatisiert an Zertifikatsinhaber: innen, deren Vertreter: innen und Teamleiter: innen verschickt werden können.

4.15 Standardprotokolle

Folgende Standards müssen unterstützt werden: ACME v2, SCEP, LDAP, Intune und REST API.

4.16 Verwaltung mehrerer Domänen

Aufgrund der Arbeit mit weiteren Domänen neben der Produktivumgebung, muss die Oberfläche des Portals für die Verwaltung und Beantragung von Zertifikaten für mind. vier verschiedenen Domänen geeignet sein.

4.17 Genehmigungsworkflow

Es muss ein individueller Genehmigungsworkflow zur Freigabe von (Zertifikats-)Anforderungen sowie zum Widerruf vorliegen. Der Prozess muss so gestaltet werden können, dass es einer manuellen Zustimmung der PKI-Administrierenden bedarf. Zertifikatslebenszyklen müssen dennoch automatisierbar sein.

4.18 Usability

Das Interface der Verwaltungsoberfläche muss grafisch, browserbasiert und über das Intranet der TK erreichbar sein. Relevante Elemente und Funktionen der Oberfläche müssen im Sinne gelungener User-Experience gut zu finden und leicht erreichbar sein. Es muss ein responsives Design verwendet werden. Generell gelten die Hinweise zu dem Kapitel Vorgaben zu Clients aus der Anlage L1, Vorgaben aus IT-Sicht.

4.19 IP-Adresse als SAN-Eintrag

Das Portal muss neben DNS-Einträgen auch IPv4 und IPv6 Adressen als SAN-Eintrag unterstützen.

4.20 Hochverfügbarkeit und Stabilität

Die TK wird das Portal in 2 örtlich separierten Rechenzentren betreiben. Das Portal muss daher hochverfügbar aufgebaut sein. Sollte eine Instanz ausfallen, muss ohne Daten- und Zeitverlust auf die andere Instanz gewechselt werden.

5 Mengen

Die zu liefernde Anzahl an Hardware-Komponenten sowie an Software-Komponenten ergibt sich aus dem Preisblatt (Anlage A1). Darüber hinaus hat die TK die Möglichkeit, einzelne Leistungen in der Vertragslaufzeit als Option nachzubestellen. Diese optionalen Leistungen sowie deren maximale Anzahl ergeben sich ebenfalls aus dem Preisblatt (Anlage A1), dort Spalte „optionale Erweiterung“. Zudem ist die TK berechtigt, Dienstleistungen abzurufen, siehe dazu im Einzelnen unten Ziffer 7.

Hinsichtlich der optionalen Erweiterungen sowie der Abrufleistungen hat der AN keinen Anspruch auf Abnahme.

6 Lieferung

Die Hardware-Komponenten sind vom AN originalverpackt innerhalb von 4 Wochen nach Zuschlagserteilung und im Falle der optionalen Erweiterung innerhalb von 8 Wochen nach Anforderung (vgl. Ziff. 12) an die TK-Unternehmenszentrale oder dem 2. Rechenzentrum in Hamburg zu liefern, es sei denn die Vertragsparteien vereinbaren eine hiervon abweichende Lieferfrist.

Alle Lieferungen erfolgen frei Haus, d.h. sie ist an der jeweils von der TK benannten Lieferadresse dem zuständigen Personal zu übergeben.

Die Liefertermine sind mit dem RZ-Operating (Tel. 040/6909-1842, rz-operating@tk.de und v-rz-infra@tk.de) mit einem Vorlauf von 5 Arbeitstagen abzustimmen. Teillieferungen sind zu vermeiden.

Die Lieferungen erfolgen in Abhängigkeit vom geplanten Aufstellort an folgende Lieferadressen:

TK-Unternehmenszentrale

Techniker Krankenkasse Warenannahme Habichtstraße 28 22305 Hamburg

Durchfahrthöhe: 4,00m

Eine Hebebühne ist vorhanden. LKW mit Hebebühne und Hubwagen wird empfohlen. Anlieferung täglich 08:00 - 17:00 Uhr, freitags bis 15:00 Uhr

Spezifikationen Lastenfahrstuhl:

Traglast: 2250kg Breite: 1,54m Höhe: 2,20m Tiefe: 2,10m

Ab einem Gewicht von 500kg sind für den Transportweg vom Lastenfahrstuhl bis hin zum Aufstellort Bodenplatten auszulegen.

q.beyond AG

Techniker Krankenkasse im Hause q.beyond AG RZ4 oder RZ2 Grasweg 62 22303 Hamburg
LKW mit Hebebühne und Hubwagen ist erforderlich.

Spezifikationen Lastenfahrstuhl:

Traglast: 3000kg

Breite: 1,80m, innen 2,25m

Höhe: 2,48m, innen 2,60m

Tiefe: 2,40m

Ab einem Gewicht von 400kg sind für den Transportweg vom Lastenfahrstuhl bis hin zum Aufstellort Bodenplatten auszulegen.

7 Dienstleistungen auf Abruf

Innerhalb der Laufzeit des Vertrages hat der Auftragnehmer (AN) auf Abruf Dienstleistungen zu erbringen. Der geschätzte Umfang der Leistung ist dem Preisblatt (Anlage A1) zu entnehmen.

Die Dienstleistungen werden in der Regel im Zeitraum zwischen 06 bis 20 Uhr von Montag bis Freitag (Ausnahmen: bundeseinheitliche Feiertage) erbracht. In Ausnahmefällen muss die Dienstleistung auch an Samstagen erbracht werden. Die Erbringung der Dienstleistung an Samstagen wird dem AN mit einer Vorlaufzeit von 2 Wochen angekündigt.

Der AN unterstützt bei der Durchführung von Wartungsarbeiten ca. 2-4 x im Jahr auf Abruf für die einzelnen Produkte wie HSM, KMS, CSP und ADCS. Die Unterstützungsleistungen können sich zum Beispiel auf Updates, Softwareanpassungen/-aktualisierungen, Automatisierungen, Health-Check und Optimierungen beziehen.

Unterstützungsleistungen werden ausschließlich remote durchgeführt und können über unterschiedliche Wege erfolgen, z.B. Video-Konferenzen über Microsoft Teams, TeamViewer oder ein Remote Access VPN. Die Details werden zwischen der TK und dem AN nach Zuschlagserteilung abgestimmt.

7.1 Anforderungen an das eingesetzte Personal

Die vom AN eingesetzten Spezialist: innen müssen mindestens über folgende Qualifikationen und Erfahrungen verfügen:

- Betrieb eines Entrust CSP-PKI-Portals
- Verwaltung von mindestens 5.000 Zertifikaten
- Betrieb und Anbindung eines Microsoft Active Directory Certificate Services (AD CS)
- Einrichtung oder Betrieb Entrust HSM
- Erfahrungen bei der Implementation des angebotenen Portals
- Erfahrungen bei der Migration von Zertifikaten in das angebotene Portal
- Administrations- und Betriebserfahrung im Umgang und der Nutzung des angebotenen Portals
- Die o. a. Qualifikationen und Erfahrungen müssen innerhalb der letzten zwei Jahre bei mindestens zwei durchgeführten Projekten im Enterprise Business Umfeld erworben worden sein.
- Erfahrung mit Multitenant HSM Umgebungen

oder

Erfahrungen mit dem angebotenen Portal:

- Implementierung, Administration und Betrieb eines Entrust CSP-PKI-Portals
- Migration und Verwaltung von mindestens 5.000 Zertifikaten
- Betrieb und Anbindung eines Microsoft Active Directory Certificate Services (AD CS)
- Einrichtung und Betrieb Entrust HSM
- Erfahrung mit Multitenant HSM Umgebungen

- Die o. a. Qualifikationen und Erfahrungen müssen innerhalb der letzten zwei Jahre bei mindestens zwei durchgeführten Projekten im Enterprise Business Umfeld erworben worden sein.

Die Qualifikationsprofile sind von dem AN auf Verlangen der TK vorzulegen.

7.2 Inbetriebnahme

Die Software wird einmalig von dem AN in Betrieb genommen, inkl. Import bestehender Zertifikate. Das Vorgehen wird zwischen der TK und dem AN nach Zuschlagserteilung abgestimmt. Die Migration aus der bestehenden Umgebung muss automatisiert erfolgen können. Der Migrationsprozess ist einmalig vom AN bei der Inbetriebnahme der Umgebung vorzunehmen. Die Inbetriebnahme beginnt mit einer Abstimmung zwischen TK und AN. Die Abstimmung erfolgt spätestens nach Ablauf von fünf Werktagen, nachdem die TK die Leistung angefordert hat. Die Inbetriebnahme mit Migration ist spätestens innerhalb von 30 Werktagen abzuschließen.

Bestandteil der Inbetriebnahme ist auch die Erstellung der technischen Dokumentation. Diese ist in deutscher Sprache zu erstellen und der TK in elektronischer Form zur Verfügung zu stellen.

Bei weiteren technischen Änderungen innerhalb der Vertragslaufzeit, die durch den AN durchgeführt werden, ist die Dokumentation von diesem entsprechend anzupassen / zu aktualisieren.

7.2.1 Assessment

Der Auftragnehmer verpflichtet sich, ein strukturiertes Assessment durchzuführen, um die aktuellen Anforderungen, Kompetenzen und Risiken zu identifizieren und zu bewerten. Die Ergebnisse sind in einem Bericht zu dokumentieren.

Vor der Implementierung ist ein technisches Assessment zur IST-Analyse der bestehenden Systemlandschaft durchzuführen. Dies umfasst die Bewertung von [z.B. IT-Sicherheit, Skalierbarkeit, Dokumentation] und die Vorlage eines Migrationskonzepts.

7.2.2 Schulung

Für die genutzte Hard- und Software führt der AN während oder nach der Inbetriebnahme eine individualisierte Schulung der TK MA erfolgen. Der Schulungszeitpunkt, der Inhalt und der Leistungsumfang der Schulung werden im Vorwege mit der TK abgestimmt.

8 Instandhaltung der Hardware und Pflege der Software

Während der Vertragslaufzeit ist der AN verpflichtet, die Hardware und Software instand zu halten und zu pflegen. Im Fehlerfall leistet der AN Support und stellt die Betriebsbereitschaft wieder her.

Der Support muss Deutsch- oder Englisch- sprachig zur Verfügung gestellt werden. Die Support-Leistungen ergeben sich im Einzelnen aus dem Vertrag sowie aus untenstehender Tabelle.

Die Service-, Reaktions- und Wiederherstellungszeiten ergeben sich aus den §§ 11 und 12 des Vertrags.

Der AN stellt der TK eine Möglichkeit für die Meldung von Hardware- und Softwarestörungen per Telefon, Mail und Ticketsystem zur Verfügung. Die Anforderungen an die Störungsmeldungen ergeben sich aus § 13 des Vertrags.

9 Treiber und Firmware

Für alle o.g. angebotenen systemrelevanten Einzelkomponenten müssen für Microsoft Windows 11 64Bit bzw. Windows Server 2022 / 2025 oder höher zertifizierte bzw. signierte Treiber vorliegen.

Für die angebotenen HSM-Objekte **muss** die Möglichkeit der Firmware- Aktualisierung, mind. skriptbasiert, ggf. auch via GUI, verfügbar sein.

Für die angebotenen CSP-Objekte **muss** die Möglichkeit der Firmware- Aktualisierung, mind. skriptbasiert, ggf. auch via GUI, verfügbar sein.

10 Zertifizierungen

Die eingesetzte Hardware muss gem. EMV zertifiziert und CE gekennzeichnet sein.

Die angebotenen Softwareobjekte und Komponenten müssen alle einschlägigen Gesetze, Verordnungen und Normen, insbesondere das GPSG (Geräte- und Produktsicherheitsgesetz) erfüllen.

11 Optionen und Abrufe

Die TK fordert die Leistung in Textform an. Hierzu nutzt die TK ein internes Bestellwesen. Das Bestellformular wird dem AN per E-Mail als Dateianhang im PDF- oder XML-Format übersandt.

Aus der Bestellung Abruf ergeben sich folgende Angaben:

- Ansprechpartner mit Telefonnummer
- Anzahl und Typen der aus dem Preisblatt zu liefernden Hard- oder/und Software-Komponenten
- Im Falle von Hardware-Komponenten zusätzlich Lieferanschrift und Anlieferungstermin

Im Übrigen gelten für die Optionen und Abrufe die Regelungen aus den §§ 15 und 16 des Vertrags.

12 Kaufmännischer Ansprechpartner

Der AN stellt für die Vertragslaufzeit einen kaufmännischen Ansprechpartner zur Verfügung.