

## Elektronische Gesundheitskarte und Telematikinfrastruktur

# Spezifikation Healthcare Confidential Computing (HCC)

Version: 0.9.1\_CC  
Revision: 1617869  
Stand: 01.06.2026  
Status: zur Abstimmung  
freigegeben  
Klassifizierung: öffentlich\_Entwurf  
Referenzierung: gemSpec\_HCC

## Dokumentinformationen

Bei dieser Version des Dokumentes handelt es sich um die Grundlage für die Abstimmung zwischen der gematik und ihren Gesellschaftern sowie mit BSI / BfDI.

### Gender-Hinweis

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument überwiegend die männliche Form verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

### Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

### Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.9.0	18.11.202 4		Erstentwurf / Diskussionsgrundlage	gematik
0.9.1_CC	01.06.202 6		Grundlegend Überarbeitet, Grundlage für Erstabstimmung mit Gesellschaftern, BSI, BfDI	gematik

## Inhaltsverzeichnis

<b>1 Einordnung des Dokuments.....</b>	<b>6</b>
<b>1.1 Zielsetzung.....</b>	<b>6</b>
<b>1.2 Zielgruppe.....</b>	<b>6</b>
<b>1.3 Geltungsbereich.....</b>	<b>6</b>
<b>1.4 Abgrenzung des Dokuments.....</b>	<b>6</b>
<b>1.5 Methodik.....</b>	<b>7</b>
1.5.1 Normative Festlegungen.....	7
1.5.2 Hinweis auf offene Punkte.....	7
<b>2 Übersicht.....</b>	<b>8</b>
<b>3 Einleitung.....</b>	<b>9</b>
<b>3.1 Inhaltlicher Aufbau dieser Spezifikation.....</b>	<b>10</b>
<b>3.2 Formaler Aufbau dieser Spezifikation.....</b>	<b>10</b>
<b>3.3 Fortschreibung dieser Spezifikation.....</b>	<b>11</b>
<b>3.4 Standardisierung des Confidential Computing Ansatzes.....</b>	<b>12</b>
<b>4 Sicherheitsziel.....</b>	<b>15</b>
<b>5 Begriffsdefinitionen.....</b>	<b>16</b>
<b>6 Konzepte, Systemkontext und Akteure.....</b>	<b>20</b>
<b>6.1 Confidential Computing.....</b>	<b>20</b>
<b>6.2 Cloud Computing.....</b>	<b>21</b>
<b>6.3 Shared Responsibility Model.....</b>	<b>22</b>
<b>6.4 Implementierte HCC-Governance.....</b>	<b>23</b>
<b>6.5 Integration mit Diensten außerhalb von HCC.....</b>	<b>24</b>
<b>7 Sicherheitsarchitektur von HCC.....</b>	<b>26</b>
<b>7.1 Trennung zwischen Designtime und Runtime.....</b>	<b>27</b>
<b>7.2 Attestation des Sicherheitszustands.....</b>	<b>28</b>
<b>7.3 Bootstrapping der technischen Sicherheitsarchitektur.....</b>	<b>32</b>
<b>7.4 Umfang und Grenzen der Initialisierungszeremonie.....</b>	<b>33</b>
<b>7.5 HCC Plattform Services.....</b>	<b>33</b>
7.5.1 HSM-Cluster (Runtime).....	34
7.5.2 Trust Domain Configuration & Attestation Service (Runtime).....	35
7.5.3 Key Management Service (Runtime).....	37
7.5.4 Trust Domain Deployment Repository (Runtime).....	37
7.5.5 HCC-Provider Deployment Repository (Runtime).....	38

78	7.5.6 TI Policy Administration Point (Designtime).....	38
79	7.5.7 TI Design & Configuration Repository (Designtime).....	38
80	7.5.8 TI Verification & Build Service (Designtime).....	39
81	7.5.9 Trust Domain Build Service (Designtime).....	40
82	<b>7.6 Schlüsselmanagement.....</b>	<b>40</b>
83	7.6.1 Öffentliche HCC-Service-Identität.....	40
84	7.6.2 TI-Identität von HCC-Services.....	41
85	7.6.3 Session-Cache-Schlüssel.....	41
86	7.6.4 Persistenz-Schlüssel.....	42
87	<b>7.7 Ausschluss der Betreiber und anderer Angreifer.....</b>	<b>42</b>
88	7.7.1 Physische Sicherheit der Rechenzentrums Umgebung.....	43
89	7.7.2 Isolation von Mandanten im Netz.....	43
90	7.7.3 Prozessisolation.....	44
91	7.7.4 Sichere Hardware-Komponenten der Runtime TCB.....	46
92	7.7.5 Sichere Software-Komponenten der Runtime TCB.....	47
93	7.7.6 Validierung des Mandantenkontextes.....	47
94	<b>7.8 Service Runtime.....</b>	<b>48</b>
95	<b>7.9 Integration mit den Zero Trust Services der TI.....</b>	<b>49</b>
96	<b>7.10 Erreichbarkeit aus dem Internet.....</b>	<b>49</b>
97	<b>7.11 Abwehr von Überlastungsangriffen aus dem Internet.....</b>	<b>49</b>
98	<b>8 Organisatorische Sicherheit.....</b>	<b>51</b>
99	8.1 Rollen und Verantwortlichkeiten.....	51
100	<b>9 Zulassungen und Bestätigungen.....</b>	<b>57</b>
101	<b>10 Interoperabilität.....</b>	<b>59</b>
102	<b>11 Integration in das SIEM der TI.....</b>	<b>60</b>
103	<b>12 Integration in das Testing Framework der TI.....</b>	<b>61</b>
104	12.1 Tests der HCC Cloud Plattform.....	61
105	12.2 Tests mit der HCC Cloud Plattform.....	62
106	<b>13 Integration in die betriebliche Steuerung der TI.....</b>	<b>66</b>
107	13.1 Verfügbarkeit und Performance.....	66
108	13.2 Logging- und Monitoringsysteme.....	67
109	13.3 Betriebliche Rollen und Verantwortung.....	67
110	13.4 Betriebliche Schnittstellen.....	68
111	13.5 Provisionierung und Service-Fulfillment.....	68
112	13.6 Anwendbarkeit betrieblicher Prozesse (TI-ITSM).....	68
113	13.6.1 Change Management.....	69
114	13.6.2 Incident Management.....	69
115	13.6.3 ITSM-Toolanbindung.....	70
116	<b>14 Anforderungen an HCC.....</b>	<b>71</b>

117	<b>14.1 HCC-Provider - marktoffenes Angebot.....</b>	<b>71</b>
118	<b>14.2 HCC-Provider - Bereitstellung HCC-Infrastruktur.....</b>	<b>72</b>
119	14.2.1 Cloud-Infrastruktur.....	72
120	14.2.2 DDoS-Abwehr.....	73
121	<b>14.3 HCC-Provider - Integration mit gematik.....</b>	<b>74</b>
122	<b>14.4 HCC-Provider - Mandanten für HCC-Dienstanbieter.....</b>	<b>76</b>
123	<b>14.5 HCC-Provider - HCC-Sicherheitsfunktionalität.....</b>	<b>79</b>
124	<b>14.6 HCC-Provider - Sicherheitsanforderungen.....</b>	<b>82</b>
125	14.6.1 Bereitstellung geeigneter Hardware.....	82
126	14.6.2 Schutz der Integrität der VAU.....	85
127	14.6.3 Schutz der Datenverarbeitung.....	86
128	14.6.4 Schutz der Daten bei Speicherung.....	87
129	14.6.5 Schutz der Daten beim verteilten Caching.....	88
130	14.6.6 Schutz der Daten beim Transport.....	89
131	14.6.7 Konsistenz des Systemzustands, Logging und Monitoring.....	90
132	<b>14.7 HCC-Provider - Trust Domain Services und Komponenten.....</b>	<b>90</b>
133	14.7.1 Trust Domain Deployment Repository.....	90
134	14.7.2 Trust Domain Configuration & Attestation Service.....	91
135	14.7.3 Trust Domain Build Service.....	93
136	14.7.4 HSM-Cluster.....	94
137	14.7.5 HCC-Hosts.....	96
138	14.7.6 HCC-Stack.....	96
139	14.7.7 Key Management Service.....	97
140	14.7.8 Weitere Dienste.....	98
141	14.7.9 Sicherheitsgutachten.....	98
142	14.7.10 Herstellererklärung funktionale Eignung.....	99
143	14.7.11 Herstellererklärung sicherheitstechnische Eignung.....	101
144	<b>14.8 Anforderungen an HCC-Dienstanbieter.....</b>	<b>103</b>
145	<b>14.9 Anforderungen an die HCC-Dienste der gematik.....</b>	<b>103</b>
146	<b>14.10 Anforderungen an HCC-Clients.....</b>	<b>103</b>
147	<b>15 Anhang A - Verzeichnisse.....</b>	<b>104</b>
148	<b>15.1 A1 - Abkürzungen.....</b>	<b>104</b>
149	<b>15.2 A2 - Glossar.....</b>	<b>104</b>
150	<b>15.3 A3 - Abbildungsverzeichnis.....</b>	<b>105</b>
151	<b>15.4 A4 - Tabellenverzeichnis.....</b>	<b>105</b>
152	<b>15.5 A5 - Referenzierte Dokumente.....</b>	<b>105</b>
153	15.5.1 Dokumente der gematik.....	105
154	15.5.2 Weitere Dokumente.....	107
155		
156		

## 1 Einordnung des Dokuments

### 1.1 Zielsetzung

Das Dokument definiert den Produkttyp Healthcare Confidential Computing (HCC) einschließlich der Sicherheits- und Datenschutzanforderungen. HCC stellt eine Cloud-basierte Form einer Vertrauenswürdigen Ausführungsumgebungen dar. Die Anforderungen richten sich an Hersteller von für HCC verwendete Komponenten, an Anbieter von HCC-Infrastrukturen sowie an Anbieter, die HCC als Plattform für den Betrieb von Diensten in der TI nutzen.

### 1.2 Zielgruppe

Das Dokument richtet sich an Anbieter, Hersteller und Betreiber von HCC-Infrastrukturen (HCC-Provider), an HCC-Dienstanbieter, die einen HCC-Provider nutzen, HCC-Workload-Hersteller, die eine Implementierung für einen HCC-Dienst liefern, sowie an ihre Sicherheitsgutachter.

### 1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des Deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. gemPTV\_ATV\_Festlegungen, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

#### Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

### 1.4 Abgrenzung des Dokuments

Diese Spezifikation ersetzt keine der bereits existierenden Anforderungslagen zur VAU, wie sie im Kontext verschiedener Anwendungen und in verschiedenen Formen definiert worden sind. Der Umstieg einer Anwendung von ihrer bisherigen Anforderungslage bzgl. der VAU auf HCC erfolgt bei Bedarf seitens der Anwendung und explizit im Zuge einer

Änderung ihrer Spezifikation und dann durch Referenz auf das vorliegende Dokument  
bzw. seine zukünftigen Releases.

## 1.5 Methodik

### 1.5.1 Normative Festlegungen

Anforderungen und Anwendungsfälle als Ausdruck normativer Festlegungen werden  
durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119]  
entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS,  
DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Da in dem Beispielsatz „Eine leere Liste DARF NICHT ein Element besitzen.“ die Phrase  
„DARF NICHT“ semantisch irreführend wäre (wenn nicht ein, dann vielleicht zwei?), wird  
in diesem Dokument stattdessen „Eine leere Liste DARF KEIN Element besitzen.“  
verwendet. Die Schlüsselworte werden außerdem um Pronomen in Großbuchstaben  
ergänzt, wenn dies den Sprachfluss verbessert oder die Semantik verdeutlicht.

Anforderungen und Anwendungsfälle werden im Dokument wie folgt dargestellt:

**<ID> - <Titel der Afo>**

Text / Beschreibung

[<=]

Dabei umfasst die Anforderung / der Anwendungsfall sämtliche zwischen ID und  
Textmarke [<=] angeführten Inhalte.

Der Identifier (ID) bei Anforderungen hat in der Regel die Vorsilbe "A\_", bei  
Anwendungsfällen die Vorsilbe "AF\_" gefolgt von einer Nummer.

### 1.5.2 Hinweis auf offene Punkte

Themen, die noch intern geklärt werden müssen oder eine Entscheidung seitens der  
Gesellschafter erfordern, sind wie folgt im Dokument gekennzeichnet:

*Beispiel für einen offenen Punkt.*

## 2 Übersicht

Die Verarbeitung von personenbezogenen medizinischen Daten im Rechenzentrum erfordert Maßnahmen, die ihre Sicherheit und Vertraulichkeit gewährleisten. Mit diesem Ziel werden schon aktive Anwendungen (u. a. ePA und eRezept) in Vertrauenswürdigen Ausführungsumgebungen betrieben. Healthcare Confidential Computing (HCC) ist eine Ausprägung der Vertrauenswürdigen Ausführungsumgebung, die in Cloud-Infrastrukturen umgesetzt werden kann.

HCC baut auf der etablierten Technologie von Confidential Virtual Machines (cVM) auf. Diese nutzt spezielle Hardwarefunktionen im Prozessor für eine Arbeitsspeicherverschlüsselung, wodurch die Daten auch während der Verarbeitung geschützt sind. In Verbindung mit konsequenter Transportverschlüsselung und verschlüsselter Speicherung der Daten wird ein Datenzugriff durch Personen beim Cloud-Provider ausgeschlossen.

Für die Verarbeitung von medizinischen Daten genügt der Ausschluss des Cloud-Providers jedoch nicht, sondern es muss auch der Datenzugriff durch den Dienstbetreiber ausgeschlossen werden.

Neben der Arbeitsspeicherverschlüsselung unterstützen die Prozessoren daher auch, das Speicherabbild einer cVM mit der darin enthaltenen Dienstsoftware zu messen und diese Information zur Verfügung zu stellen (Remote Attestation). Dadurch wird ein unabhängiger Dritter wie die gematik in die Lage versetzt, gültig betriebene Dienste eindeutig zu identifizieren und nur solche mit dem Zugriff auf die für die Datenverarbeitung notwendigen kryptographischen Identitäten in HSMs auszustatten.

HCC stellt ein Framework für die Nutzung der Confidential Computing Technologie in einer Cloud dar, das einen kryptographischen Vertrauensraum für die TI bei Cloud-Providern etabliert und damit drei Probleme technisch löst:

- Die gematik kann als unabhängiger Dritter ihre Policies in der Betriebsumgebung durchsetzen und damit die Rolle eines Trust Domain Providers einnehmen.
- Nur als zulässig registrierte Dienste (Workloads) können mit TI-Identitäten gestartet werden.
- Manipulationen oder Verletzungen der Sorgfaltspflichten in der Betriebsumgebung führen nicht zu Datenschutzverletzungen, weil die verarbeiteten Daten durchgängig durch Verschlüsselung geschützt sind.

HCC stellt auch einen Rahmen für die Prüfung und Einbringung der Dienstsoftware bereit, mit dem sichergestellt wird, dass alle Dienstsoftware die sicherheitstechnischen Anforderungen erfüllt.

HCC wird durch eine Reihe von in Cloud betriebenen sicherheitsfunktionalen Dienste umgesetzt.

Eine Reihe von Anforderungen an den Cloud-Provider adressiert die Grenzen der Sicherheitsgarantien der Confidential Computing Technologie, indem eine geschützte und korrekt betriebene Cloud-Umgebung durchgesetzt wird.

**Offen: Übersichtsbild**



---

## **3 Einleitung**

---

Die Architektur der TI 2.0 ist u. a. durch die Abkehr von der rein dezentralen Verarbeitung der medizinischen Daten (im Klartext) geprägt. Die Datenverarbeitung wird in Zukunft primär in professionell betriebenen Rechenzentrumsinfrastrukturen stattfinden, um die Mehrwerte digitaler Prozesse und Daten im Gesundheitswesen schneller und mit höherer Verfügbarkeit und Qualität erschließen und funktionale Erweiterungen und Fixes schnell, flexibel, kontrolliert und kosteneffizient in der Breite verfügbar machen zu können.

Während die Nutzer der TI der zentralen Infrastruktur im Sinne des Datenschutzes bisher nur ein begrenztes Vertrauen entgegenbringen mussten, steigt in der TI 2.0 der Bedarf, die Vertrauenswürdigkeit der zentralisierten Datenverarbeitung sicherzustellen und für die Nutzer transparent und glaubhaft darstellbar zu machen. Dieser Bedarf soll mit Confidential Computing adressiert werden, ergänzt durch weitere Mechanismen und Maßnahmen.

Gleichzeitig – und unabhängig von Anforderungen an die Vertrauenswürdigkeit der Infrastruktur im engeren Sinne – befinden sich Rechenzentrumsinfrastrukturen im Wandel zum Cloud Computing. Dedizierte Systeme zur Bereitstellung von Netzwerk-, Verarbeitungs- und Speicherressourcen gehen in hochskalierten Multi-Mandanten-Infrastrukturen auf, in denen Ressourcen bedarfsgesteuert dynamisch bereitgestellt werden.

Lösungsanbieter in der TI, die Cloud-Infrastrukturen nutzen, können auf diesem Weg Up-Front-Investitionen in anwendungsbezogene Infrastruktur vermeiden. Compute-, Speicher-, Zugangs- und Transport-Ressourcen – inkl. Redundanz und Reservekapazitäten – werden anwendungs- und mandantenübergreifend ausgelastet und damit die Kosten pro Anwendungsfall gesenkt.

Die Infrastruktur für die Bereitstellung der TI-Dienste wird längerfristig eine Konsolidierung erfahren, die in Verbindung mit höherer Automatisierung und Ausreifung von Infrastruktur- Betriebsprozessen – aufgrund von Skalierungseffekten – wesentlich zur Verbesserung der betrieblichen Stabilität der TI beitragen werden.

Höherwertige Funktionalitäten, z. B. Datenbanksysteme, werden als mandantenfähige Managed Services vom Cloud-Anbieter bereitgestellt, skaliert, administriert, überwacht und aktuell gehalten, um betriebliche Aufwände für die Lösungsanbieter zu verringern, Fehlerquellen zu eliminieren und das beim Lösungsanbieter erforderliche technische Know-how zu reduzieren.

Dem Lösungsanbieter werden Werkzeuge zur eigenständigen Verwaltung der von ihm benötigten Ressourcen zur Verfügung gestellt, wobei auch Ressourcen bereitgestellt werden, bspw. für Confidential Compute, die im Rahmen definierter Grenzen automatisch mit dem Aufkommen an Requests hoch- und herunterskalieren.

Healthcare Confidential Computing ist als Begriff für die Verbindung von Cloud Computing mit dem für die Verarbeitung von Klartextdaten im Gesundheitswesen erforderlichen Vertrauensniveau definiert.

Die Datenverarbeitung soll anbieterübergreifende Standards in einem existierenden Markt für Verarbeitungs-, Speicher- und Zugangsressourcen nutzen und zur Erreichung des erforderlichen Vertrauensniveaus ggf. ergänzen.

Mit Healthcare Confidential Computing soll die Weiterentwicklung der fachlichen Funktionalität der TI von der Bereitstellung der physischen Infrastruktur entkoppelt

werden, um die Umsetzung neuer Dienste der TI für ihre Anbieter substantiell zu vereinfachen.

### **3.1 Inhaltlicher Aufbau dieser Spezifikation**

Healthcare Confidential Computing definiert eine Plattform für die vertrauenswürdige Ausführung von Diensten der TI, jedoch keine fachliche Funktionalität. Diese wird mit den Spezifikationen für die Fachanwendungen oder für unterstützende Funktionen der TI geliefert. Zur Erreichung der Sicherheitsziele von Healthcare Confidential Computing wird jedoch umfangreiche Sicherheitsfunktionalität benötigt, z. B. zur Attestation, für die Verwaltung der Umgebungen etc.

Gleichzeitig soll Healthcare Confidential Computing ein gewisses Maß an anbieterübergreifender Portabilität für (Fach-) Dienste sowie die Interoperabilität von Client-Zugriffs-Protokollen gewährleisten. Hieraus ergeben sich weitere funktionale Festlegungen und damit auch die Form des vorliegenden Dokuments als Produktypspezifikation.

Healthcare Confidential Computing als Produkttyp ist zudem durch die Zuständigkeit der gematik für die Governance der TI motiviert, sowie durch das Ziel, Dienstanbieter auf der Plattform von vielen sicherheitstechnischen und betrieblichen Nachweispflichten sowie von der eigenen Umsetzung von Governance-Schnittstellen zu entlasten. Die gematik muss dazu die Anbieter von Healthcare Confidential Computing direkt zulassen, so dass Dienstanbieter mit der Wahl eines zugelassenen Anbieters die Zusicherungen von Healthcare Confidential Computing unmittelbar nutzen können.

Der Fokus von Healthcare Confidential Computing auf technische Sicherheitsmechanismen, auf einen anbieter- und anwendungsübergreifenden Plattformcharakter sowie auf das Ziel einer möglichst weitgehenden Bündelung der Verantwortung für die Verfügbarkeit der Dienste beim Plattformanbieter motivieren darüber hinaus die direkte Integration der Governance-Funktionen der gematik in die Healthcare Confidential Computing Infrastrukturen der Anbieter und damit auch ihre Darstellung als Teil der vorliegenden Spezifikation.

Die Abbildung der Governance-Rolle der gematik über integrierte technische Mechanismen zielt auch darauf ab, das Automatisierungspotenzial der digitalen Transformation zu erschließen und den organisatorischen Aufwand zur Aufrechterhaltung des Betriebs und der Garantien von Healthcare Confidential Computing zu begrenzen.

Die Sicherheitsleistung von Healthcare Confidential Computing bestimmt den Aufbau der vorliegenden Spezifikation. Die Sicherheitsfunktionalitäten werden aus ihrem jeweiligen Sicherheitskontext motiviert. Interoperabilitätsanforderungen werden unabhängig begründet. Betriebliche Anforderungen berücksichtigen die neue Anbieterstruktur mit ihren Rollen und Verantwortlichkeiten.

### **3.2 Formaler Aufbau dieser Spezifikation**

Der sicherheitsfunktionale Aufbau von Healthcare Confidential Computing erfordert eine Darstellung der funktionalen Komponenten. Diese Darstellung bestimmt den ersten Teil des Dokuments, formuliert keine normativen Anforderungen im Sinne von RFC 2119 und dient dem Gesamtverständnis. Die normativen Anforderungen werden im zweiten Teil des Dokuments nach Adressaten gebündelt gestellt.

### 3.3 Fortschreibung dieser Spezifikation

Confidential Computing ist ein noch neues Paradigma zur Gewährleistung von Vertraulichkeit bei der Datenverarbeitung in IT-Infrastrukturen Dritter:

- Die technischen Mechanismen von Confidential Computing ändern sich noch stark von einer Hardware-Generation zur nächsten. Zudem unterscheiden sich die Confidential Computing Modelle verschiedener Hersteller. Damit unterscheiden sich auch die Wege zur Erreichung der Sicherheitsziele der TI auf Basis dieser Modelle. Die gematik setzt in Zukunft auf Confidential Virtual Machine Technologien, da diese von den verschiedenen Hardware-Herstellern unterstützt werden.
- Die Umsetzung der Hardware-gestützten On-Chip Mechanismen für Confidential Computing sind proprietär und damit nur eingeschränkt einer unabhängigen Begutachtung zugänglich. Dem Hersteller der Hardware muss damit ein gewisses Vertrauen entgegengebracht werden. Dieses Vertrauen ist jedoch dadurch begrenzt, dass die Systeme bei einem unabhängigen Betreiber genutzt werden und nur zu sehr begrenzten Zwecken (z. B. Plattform-Attestation, TCB-Recovery) über Proxies mit dem Hersteller in Verbindung gebracht werden.
- Die notwendige Ausrichtung der Hardware (z. B. CPUs) auf optimale Performance erfordert viele Optimierungen auf Hardware-Ebene mit von Prozessen gemeinsam genutzten Ressourcen (wie Pipelines, Page Tables, Caches, Translation Lookaside Buffers, Branch Predictors etc.) und einer eigenen Semantik, die bisher nicht klar mit einer Semantik zur Isolation von Verarbeitungsprozessen zusammengesetzt werden konnte. Hierbei könnte es sich um ein prinzipielles Problem handeln. So ergeben sich regelmäßig neue Schwachstellen, die für Angreifer ein „Window of Opportunity“ darstellen können. Die Schwachstellen müssen durch den Infrastrukturbetreiber gepatcht werden und nehmen diesen damit wieder organisatorisch in die Pflicht. Maßnahmen zur Begrenzung der resultierenden Risiken können Einschränkungen hinsichtlich der Flexibilität des Deployments von Workloads beim Cloud-Computing mit sich bringen. Konkret: Die Isolationsgarantien von Enklaven oder Confidential VMs werden regelmäßig durch neu entdeckte Schwachstellen, insbesondere durch Seitenkanäle, infrage gestellt. Dies wird auch für die Zukunft erwartet und es resultiert in Anforderungen zur Ausführung von HCC-Workloads auf exklusiv für HCC bereitgestellten Hosts und zur Attestation und Offenlegung des Host-OS. Es wird davon ausgegangen, dass sich hieran in absehbarer Zukunft nichts ändern wird.
- Die industriellen Möglichkeiten zur Abbildung einer anbieterunabhängigen Governance-Rolle befinden sich noch in der Entstehung. Das vorliegende Dokument stellt gerade hierzu einen Entwurf dar. Die Integration dieser Rolle innerhalb der gematik wird ein fortwährender Prozess sein, der sich auch auf die Schnittstellen zu HCC-Providern auswirken wird.
- Standards z. B. für die Formate, Inhalte und Protokolle für Remote Attestation befinden sich noch im Entstehungsprozess. Die gematik wird diesem Prozess auf der Ebene ihrer Spezifikationen folgen, wo es sinnvoll erscheint.

Die vorliegende Spezifikation versucht bereits die genannten Einschränkungen durch geeignete Anforderungen und TI-spezifische Festlegungen zu adressieren. Gleichwohl muss sich jeder Anbieter, der eine Zulassung als HCC-Provider gemäß dieser Spezifikation anstrebt, darauf einstellen, dass die Spezifikation mit dem sich weiter entwickelnden Stand von Technik und Forschung fortgeschrieben wird, und dass damit in Zukunft eventuell zusätzliche Anforderungen oder Änderungen an bestehenden Anforderungen verbunden sein werden, die er in der Folge umsetzen muss, um seine Zulassung zu erhalten.

Weitere Quellen zukünftiger Änderungen an dieser Spezifikation betreffen folgende Aspekte:

- Standardisierungsbemühungen internationaler Organisationen, wie IETF und Confidential Computing Consortium.  
Diese betreffen kryptographische Primitiven, Attestationsprotokolle, Attestation Evidence sowie Trust und Provisioning, Insbesondere die Integration von Confidential Computing mit den dominierenden Technologien im Cloud-Stack (z. B. Kubernetes) erscheint derzeit noch kein standardisiertes Modell hervorgebracht zu haben,
- die schrittweise Integration und Automatisierung der Governance-Rolle der gematik im Rahmen der Einführung der TI 2.0.  
Hiervon werden primär Formate, Protokolle und Prozesse an der Schnittstelle zur gematik betroffen sein,
- Veränderungen am organisatorischen Rahmen der gematik für Zulassung und Betriebsprozesse,
- die Erweiterung von Steuerungsmöglichkeiten, die der HCC-Provider seinen Kunden zur Verfügung stellen, insbesondere Möglichkeiten zur Kombination der (fachlichen) Lösung des Kunden mit generischen Komponenten der TI 2.0, z. B. Komponenten der anwendungsübergreifenden Zero Trust Architektur (Policy Enforcement, Policy Decision) sowie
- die Erweiterungen der Service Portfolios der HCC-Anbieter z. B. mit Cloud-native Services.

Die Integration von Healthcare Confidential Computing mit Cloud-native Services, d. h. mit Subsystemen in der Cloud-Infrastruktur, die auf eine Nutzung der Systemressourcen durch viele Kunden des Cloud Providers optimiert sind, bedarf in jedem Einzelfall einer Überprüfung ihrer Vereinbarkeit mit den Sicherheitsgarantien.

### **3.4 Standardisierung des Confidential Computing Ansatzes**

Die gematik hat traditionell ihre Spezifikationen möglichst technologie-neutral zu gestalten versucht. Dieser Ansatz war insbesondere im Falle von "Gesamtlösungen aus einer Hand", wie bei den bisher umgesetzten (Fach-)Dienstleistungen, plausibel.

Mit der Nutzung von Confidential Computing Technologie und insbesondere der Attestation von Systemen durch Dienste in der (Co-) Hoheit der gematik, wird eine neue Konstruktion für den Vertrauensraum in der TI möglich, die eine erhebliche Steigerung der Transparenz aus Sicht der Nutzer der TI und aus Sicht der gematik als öffentlichem Garanten für Datenschutz und Sicherheit darstellt.

Attestation wird bereits seit der ersten Implementierung der elektronischen Patientenakte in einer vertrauenswürdigen Ausführungsumgebung als Basis für die Ermöglichung der Klartextverarbeitung von personenbezogenen medizinischen Daten der TI in Rechenzentren genutzt und mit der vorliegenden Spezifikation für Cloud-Umgebungen nutzbar gemacht sowie weiter ausgebaut (siehe [6.3- Shared Responsibility Model](#)).

Dies erfordert ein gewisses Maß an technologischer Standardisierung, um:

- die erforderliche Transparenz auf einem einheitlichen Sicherheitsniveau zu erreichen,
- die Plattform steuerungsfähig zu machen und
- im Zuge der schrittweisen Weiterentwicklung der Plattform eine Fragmentierung des Designs, technische Barrieren sowie ausufernde Aufwände zu verhindern.

Darüber hinaus müssen die bereits in 3.3- Fortschreibung dieser Spezifikation genannten industriellen Entwicklungen beim Confidential Computing berücksichtigt und mit der für Cloud-Computing erforderlichen Trennung zwischen Plattform und Diensten (sowie ihren jeweiligen Anbietern) in Einklang gebracht werden. Diese Trennung bringt einen Bedarf an Interfaces mit sich, der stark von der genutzten Confidential Computing Technologie abhängt.

In der Industrie hat sich im Verlauf der letzten Jahre eine Präferenz für Confidential Virtual Machines etabliert, die insbesondere auf die Nutzung in der Cloud ausgerichtet ist. Confidential Virtual Machines werden daher von der gematik als Grundlage für die Standardisierung genutzt.

Die mit diesem Trend verbundenen Herausforderungen (z. B. deutlich vergrößerte Trusted Computing Base im Sinne der industrieüblichen Definition für Confidential Computing) werden in Kauf genommen (und adressiert), um keine der am weitesten verbreiteten Hardware-Plattformen (Intel, AMD, ARM, NVIDIA, IBM, etc.) auszuschließen und gleichzeitig eine einheitliche Abgrenzung zwischen (Cloud-) Plattform und Workloads (confidential laufende Virtual Machines, in denen die Dienstkomponenten laufen) zu erhalten.

Im Einklang mit der weiteren Strategie für die TI 2.0 wird gleichzeitig die Interoperabilität mit Kubernetes als Mechanismus für das Provisionieren und zur Steuerung von Workloads insbesondere in der Cloud berücksichtigt. Kubernetes handhabt Workloads auf Basis von Containern gemäß OCI (Open Container Initiative).

Aus der Kombination von Confidential VMs (cVM) und Managed Containers resultiert ein Design-Problem, für das es verschiedene Lösungsansätze aus der Industrie gibt, jedoch derzeit noch keinen Ansatz, der sowohl hinsichtlich Sicherheit, als auch Performance, als auch Verbreitung gut etabliert ist. Hierbei spielt es eine Rolle, dass Kubernetes von sich aus z. B. keinen verschlüsselten Transport von Konfigurationsdaten vorsieht und dass die Control Plane von Kubernetes generell die Pods steuert, die bei cVMs innerhalb des Verarbeitungskontextes laufen, was dem Betreiberausschluss entgegensteht.

Um diesem Problem auszuweichen, wird der Integrationspunkt zwischen containerisierter Workload und cVM-basierter Ausführungsumgebung in der Cloud aus der Laufzeitumgebung heraus in eine Build-Umgebung für HCC-Dienste verlagert, die kontinuierlich weiterentwickelt wird.

HCC-Provider implementieren ihre Laufzeitumgebungen auf der Grundlage von (attestierbaren) cVMs und gemäß den Sicherheitsanforderungen auf in Teilen jeweils eigene Weise und stellen eine Provider-spezifische Build-Pipeline bereit, die standardmäßig containerisierte Workloads von Diensteanbietern in bei dem jeweiligen Provider attestierbare und ausführbare cVMs transformiert und - nach Freigabe - an seine Cloud-Systeme (Deployment Repository, Attestation Service) übermittelt, damit sie in der Cloud instanziiert werden können.

Im Laufe der Zeit können sich herausbildende Standards oder Verbesserungen der bestehenden Lösungen seitens der HCC-Provider umgesetzt werden. Auch wird zum aktuellen Zeitpunkt eine starre Auslegung der Standardisierung hinsichtlich Kubernetes vermieden, damit HCC-Provider das Workload-Deployment selbst gestalten und optimieren können.

## 4 Sicherheitsziel

Personenbezogene medizinische Daten besitzen einen sehr hohen Schutzbedarf und erfordern daher besondere Maßnahmen zu ihrem Schutz, wenn sie von Anbietern in der TI verarbeitet, gespeichert oder transportiert werden.

Wenn darüber hinaus (und bei der Nutzung von Cloud-Computing anzunehmen) eine sehr große Zahl von Personen von unberechtigten Zugriffen in der Betriebsumgebung eines Anbieters betroffen sein könnten, ist eine noch größere Sorgfalt bei der Festlegung und Umsetzung der Maßnahmen gerechtfertigt.

Rein organisatorische Maßnahmen bei Betreibern von Diensten, die solche Daten verarbeiten, sowie bei den Betreibern der darunterliegenden Infrastrukturen werden als nicht ausreichend angesehen, um unberechtigte Zugriffe ausreichend zu unterbinden.

Das Sicherheitsziel für Healthcare Confidential Computing entspricht dem Sicherheitsziel für die Vertrauenswürdige Ausführungsumgebung:

**Bei der Klartext-Verarbeitung von Daten mit sehr hohem Schutzbedarf in Diensten der Telematikinfrastruktur sind unberechtigte Zugriffe mit technischen Maßnahmen auszuschließen.**

**Hierbei sind alle Arten von Zugriffen unberechtigt, die nicht in der den Dienst spezifizierenden fachlichen Anwendung als berechtigte Zugriffe definiert sind.**

**Als Zugriff gilt hierbei auch jede Form der Profilbildung, d. h. die Gewinnung von personenbezogenen Informationen aus Mustern des Datenverkehrs, der Datenverarbeitung oder der Datenspeicherung.**

**Technische Maßnahmen sind hierbei Maßnahmen, die technische Mechanismen zur Verschlüsselung oder Komponenten mit physischem Schutz für verarbeitete, transportierte oder gespeicherte Daten innerhalb der Laufzeitumgebung eines Dienstes etablieren. Die zur Etablierung und Aufrechterhaltung der technischen Mechanismen erforderlichen organisatorischen Prozesse müssen dabei so ausgestaltet sein, dass die technischen Mechanismen durch keinen der im Bedrohungsmodell berücksichtigten Angreifer so weitgehend unwirksam gemacht werden können, dass unberechtigte Zugriffe möglich werden.**

Das Sicherheitsziel für Healthcare Confidential Computing baut auf den in der TI bereits geltenden Anforderungen für den Schutz von transportierten Daten durch Verschlüsselung und von gespeicherten Daten durch Verschlüsselung und geeignete Speichersysteme auf (siehe [gemSpec\_Krypt] und die Spezifikation der jeweiligen Anwendung).

Die Übergänge in den Verarbeitungskontext mit Klartextverarbeitung (Entschlüsselung von eingehenden Client-Requests und von Daten aus der Speicherung) und aus ihm heraus (Verschlüsselung von Responses und von Daten, die gespeichert werden) werden als Teil der vertrauenswürdigen Verarbeitung innerhalb des Dienstes betrachtet.



## 5 Begriffsdefinitionen

Dieser Abschnitt führt die in diesem Dokument genutzten Begriffe ein.

**Schützenswerte Daten:** Umfasst alle Daten einer Anwendung mit sehr hohem Schutzbedarf, die kein Unbefugter einsehen oder ändern darf.

Der Anbieter des Dienstes, in dem die Daten im Klartext verarbeitet werden, sowie der Anbieter der betrieblichen Infrastruktur des Dienstes zählen als unbefugt, sofern sie nicht gemäß Spezifikation der Anwendung auf Daten zugreifen dürfen. Zu den Unbefugten zählen des Weiteren externe Angreifer sowie ggf. andere Dienstanbieter innerhalb oder außerhalb der TI, deren Dienste in einer gemeinsamen Betriebsumgebung mit dem Anwendungsdienst betrieben werden.

**Vertrauenswürdige Ausführungsumgebung (VAU):** Gesamtheit der für eine sichere Klartextverarbeitung erforderlichen Software und Hardware beim Betreiber eines VAU-Dienstes.

**Healthcare Confidential Computing (HCC):** Das im vorliegenden Dokument spezifizierte sicherheitstechnische Rahmenwerk der gematik zur Definition von Anforderungen an Anbieter, Infrastrukturen, Anwendungen und Prozesse in der TI, die eine VAU bei nach den Prinzipien des Cloud-Computings operierenden Anbietern realisieren.

HCC setzt voraus, dass der Anbieter (**HCC-Provider**) am Markt auftritt und für jeden seiner Kunden einen Mandantenkontext bereitstellt, in dem die administrativen Funktionen für die Ressourcenallokation, für das Deployment und zur weiteren Steuerung des Betriebs von Diensten verfügbar sind. Weiterhin wird vorausgesetzt, dass Dienste bis zu einem gewissen Grad automatisch skalieren. Die Sicherheitsleistungen des HCC-Providers sollen seine Mandanten (die Anbieter von HCC-Diensten in der HCC-Infrastruktur) im Hinblick auf die an sie gerichteten Anforderungen zum Nachweis der Sicherheit ihrer Dienste weitgehend entlasten. Der HCC-Provider unterhält eine direkte Beziehung mit der gematik und stellt für diese einen Mandantenkontext bzw. geeignete Schnittstellen bereit, die dazu dienen, den kryptographischen Vertrauensraum der TI für HCC (**HCC-Trust-Domain**) in seiner Infrastruktur verfügbar zu machen.

**HCC-Dienst:** Fachdienst oder anderer Dienst der TI. Enthält die Anwendungslogik und alle Logik, die zu ihrer Steuerung notwendig ist. Der Dienst wird auf einer HCC-Infrastruktur betrieben, um schützenswerte Daten im Klartext zu verarbeiten.

**HCC-Infrastruktur:** Gesamtheit der für eine sichere Klartextverarbeitung erforderlichen Software und Hardware bei einem Cloud-Anbieter.

HCC-Infrastruktur stellt eine Cloud-basierte Form der VAU-Infrastruktur dar. Zur Hardware gehören insbesondere die HCC-Server sowie alle für ihre betriebliche Steuerung erforderlichen Komponenten. Zur HCC-Infrastruktur gehören Komponenten für das Routing von Requests aus dem Internet (oder - solange dieses noch erforderlich ist - aus dem Netz der TI) an den HCC-Dienst und das Routing der Responses zurück an Clients, wenn solche Komponenten dem Betreiber oder Angreifern Einblick in individuelles Nutzerverhalten ermöglichen könnten und daher regulatorisch relevant sind. Zur HCC-Infrastruktur gehören die Systeme zur verschlüsselten Speicherung von Daten insoweit, als auch für die verschlüsselten Daten sichergestellt werden muss, dass diese nicht in Systeme außerhalb zugelassener Regionen oder nicht zugelassener Anbieter abfließen.

**Trusted Computing Base (TCB):** Gesamtheit der Software und Hardware beim Betreiber, deren sicherheitstechnische Korrektheit gegeben sein muss, um den Ausschluss unbefugter Zugriffe sicherzustellen.

Ein grundlegendes Prinzip bei der Konstruktion von HCC-Infrastruktur besteht darin, die

TCB möglichst klein zu halten, um die Angriffsfläche zu minimieren und um zu ermöglichen, dass z. B. ein Gutachter die Sicherheitsgarantien mit möglichst großer Gewissheit feststellen kann. Die TCB ist der wesentliche Teil der Gesamtheit der HCC-Infrastruktur aus der Perspektive der Sicherheit. Neben der TCB umfasst die Gesamtheit der HCC-Infrastruktur Komponenten, die ihren Betrieb ermöglichen und steuern und somit zur Gewährleistung der Verfügbarkeit beitragen, jedoch keine Auswirkung auf Vertraulichkeit und Integrität der Klartext-Datenverarbeitung haben. Die TCB umfasst grundsätzlich die Komponente, die die fachliche Verarbeitung implementiert, d. h. den fachlichen Kern des HCC-Dienstes.

**HCC-Host:** Für die Ausführung von HCC-Diensten (als Workloads) geeignete und genutzte Server-Hardware.

HCC-Hosts implementieren eine Confidential Computing Technologie und die für eine Attestation des gesamten Servers sowie aller darauf installierten Workloads erforderlichen Mechanismen. Hierzu gehören mindestens Measured Boot, ein Hardware-geschützter Root of Trust für die Attestation sowie ein Mechanismus für die sichere Trennung der Klartextdatenverarbeitung von den Funktionen zur betrieblichen Steuerung des Servers durch den Betreiber. Es wird davon ausgegangen, dass HCC-Hosts als virtualisierte Ablaufumgebungen für Workloads konfiguriert sind.

**Workload-Image:** Container Image oder Virtual Machine Image, das die Implementierung der Verarbeitung der Anwendungsdaten im Klartext im HCC-Dienst umfasst.

Das Workload-Image stellt die Workload zur Ausführung in der virtualisierten Infrastruktur bereit. Im Zuge der Attestation wird für jedes vom HCC-Host geladene Workload-Image eine eindeutige **Workload Identity** (in Form von Hardware-signierten Hash-Werten) ermittelt, die mit Soll-Werten in einer Konfigurationsdatenbank abgeglichen werden kann, um die Berechtigung der Workload zur Verwendung der kryptographischen Identität (X.509-Zertifikat) des durch sie implementierten HCC-Dienstes und von weiterem Schlüsselmaterial zu erteilen.

**Verarbeitungskontext:** Der Verarbeitung eines Requests im HCC-Dienst zugeordneter Prozess, Thread oder Scope einschließlich aller sicherheitsrelevanten Abhängigkeiten. Client-Requests erreichen den Verarbeitungskontext verschlüsselt. Im Scope des Verarbeitungskontextes sind alle für die Verarbeitung des Client-Requests erforderlichen Schlüssel erreichbar. Der Verarbeitungskontext führt die fachliche Logik (inkl. Autorisierung) zur Behandlung des Requests aus und antwortet dem Client mit einer verschlüsselten Response. Falls im Rahmen der Request-Verarbeitung schützenswerte Daten persistiert oder mit anderen Diensten bzw. anderen Verarbeitungskontexten ausgetauscht werden müssen, so verschlüsselt der Verarbeitungskontext diese Daten vorher. Der Verarbeitungskontext stellt den technischen Kern der TCB dar.

**HCC-Client:** Software-Client, der das Protokoll zum Zugriff auf einen Verarbeitungskontext umsetzt.

Der Software-Client nutzt Mechanismen der Hardware, des Betriebssystems oder der Plattform des Client-Gerätes, auf dem er läuft, um Schlüsselmaterial zu schützen oder die im Kontext von Zero Trust erforderlichen Nachweise (Client-Attestation) zu erzeugen. Der HCC-Client spielt in der vorliegenden Spezifikation u. A. deshalb eine Rolle, weil die HCC-Infrastruktur als Plattform für verschiedene Dienste der TI mindestens ein anwendungs- und anbieterübergreifend interoperables Zugriffsprotokoll für HCC-Clients unterstützen muss.

**Anwendungs-Client:** Software-Client einer Anwendung.

Der Anwendungs-Client nutzt einen HCC-Client zum Zugriff auf einen HCC-Dienst. Anwendungs-Clients können den HCC-Client als Komponente integrieren.

**HCC-Kanal:** Durchgehend verschlüsselte Verbindung zwischen HCC-Client und Verarbeitungskontext.

Der HCC-Kanal kommt in zwei Ausprägungen vor, als reiner TLS-Kanal sowie als TLS-Kanal



mit zusätzlicher Verschlüsselung auf Anwendungsebene mittels des VAU-Protokolls bzw. ZETA/ASL (siehe [gemSpec\_Krypt], Kap. 7). Insbesondere die Möglichkeit zur Verwendung von reinem TLS kann sich auf die dem Verarbeitungskontext vorgelagerten Infrastrukturkomponenten auswirken, da in diesem Fall DDoS-Schutzkomponenten, Firewalls, Load Balancer, API- und Ingress-Gateways keine TLS-Entschlüsselung von Requests durchführen können.

**Persistenzschlüssel:** Kryptographische(r) Schlüssel, mit dem Daten bei ihrer Speicherung außerhalb der TCB (in Dateisystemen, Datenbanken, etc.) vor dem Zugriff Unbefugter geschützt werden.

Persistenzschlüssel werden anwendungsspezifisch gebildet und im Verarbeitungskontext oder aus ihm heraus in einem HSM-Cluster oder einem HCC-Host-lokalen Hardware-Krypto-Modul generiert und genutzt.

**HCC-Dienst-Hersteller:** Entwickelt die Software für den HCC-Dienst, beauftragt ihre Begutachtung und beantragt ihre Zulassung. Zu der Software zählt insbesondere das Workload-Image. Die Entwicklung von HCC-Workloads zielt auf ihre Lauffähigkeit bei einem oder mehreren HCC-Providern ab. Hieraus ergeben sich Anforderungen hinsichtlich der Interoperabilität der Laufzeitumgebungen von HCC-Providern, aber ggf. auch Anforderungen zur Nutzung HCC-Provider spezifischer Templates (z. B. für confidential Virtual Machines) durch den HCC-Workload-Hersteller.

**HCC-Dienstanbieter:** Bietet einen HCC-Dienst in der TI an. Die Rolle des HCC-Dienstanbieters ist eine primär geschäftlich-organisatorische und umfasst die Konfiguration des Mandantenkontextes sowie den User-Rollout und den Support.

**HCC-Provider:** Durch die gematik zugelassener Anbieter, der eine mandantenfähige Infrastruktur für den Betrieb von HCC-Diensten bereitstellt. Dies umfasst Kapazitäten für die Datenverarbeitung, die Datenspeicherung, den Netzwerktransport inkl. Anbindung an das Internet (und ggf. das bisherige Netz der TI) sowie Cloud-Services. Kunden bzw. Mandanten des HCC-Providers sind HCC-Dienstanbieter. Wenn ein Cloud Provider neben seiner Rolle als HCC-Provider auch andere Sektoren, Märkte oder Kunden adressiert, so werden nur die HCC-spezifischen Teile seiner Infrastruktur, Services, Komponenten und Prozesse dem HCC-Provider zugerechnet. Wenn ein Anbieter gleichzeitig als HCC-Provider und als HCC-Dienstanbieter auftritt, dann können organisatorische Trennungsanforderungen zum Tragen kommen.

**HCC-Mandant:** Kunde bzw. Mandant eines HCC-Providers, der mittels Konfiguration des durch den HCC-Provider bereitgestellten Mandantenkontextes die Dienste (eigene oder Dienste aus dem Portfolio des HCC-Providers oder von Dritten) definiert und parametrisiert, welche für ihn in der Infrastruktur des HCC-Providers laufen. HCC-Mandanten sind HCC-Dienstanbieter aus der Perspektive des HCC-Providers betrachtet.

**HCC-Trust-Domain (HCC-TD):** Der HCC-Provider-übergreifend implementierte und durch die gematik verantwortete kryptographische Vertrauensraum aller HCC-Dienste und Komponenten. Die HCC-TD baut auf einer oder mehreren (auch externer) PKI auf und spannt das Netz kryptographisch prüfbarer Beziehungs-, Verbindungs- und Nutzungsmöglichkeiten auf. Eine Besonderheit von Confidential Computing besteht darin, dass Confidential Services als vollständige Automaten mit kryptographischer Workload Identity und einer zugeordneten Signer Identity ausgestattet werden können. Von solchen Services generierte und signierte Artefakte können dann eingesetzt werden, um Vertrauensbeziehungen über komplexe Regelwerke (Policies oder Code) zu etablieren.

648

649 **Confidential Computing Stack (CC-Stack):** Integrierter Satz von Technologien, die  
650 eine Implementierung von Confidential Computing realisieren.

651 Ein solcher Stack kann auf verschiedene Weise aufgebaut sein, um u. a. sein Ziel der  
652 Abwehr von Angriffen aus dem betrieblichen Umfeld des HCC-Providers zu erreichen. Er  
653 muss mittels Hardware-Unterstützung mindestens die folgenden Eigenschaften  
654 aufweisen:

- 655 • Verschlüsselung des Arbeitsspeichers zur Abwehr von Angriffen auf Daten im  
656 Arbeitsspeicher mittels Entnahme des Arbeitsspeichers und Auslesens außerhalb des  
657 Schutzes durch den Server sowie
- 658 • Fähigkeit zur Attestation des Systems inkl. Hardware, Firmware, Hypervisor,  
659 Betriebssystem, Plattformkomponenten und Anwendungskomponenten (Workloads)  
660 auf der Basis von Hardware-geschützten Host-lokalen Vertrauensankern.

---

## 6 Konzepte, Systemkontext und Akteure

---

In den folgenden Abschnitten werden die grundlegenden Konzepte dargestellt, die Healthcare Confidential Computing definieren und begründen.

### 6.1 Confidential Computing

Confidential Computing ist eine aus Sicht des Datenschutzes zwingende Voraussetzung für die Zulässigkeit einer aus dem Verantwortungsbereich der Akteure des Gesundheitswesens ausgelagerten Verarbeitung personenbezogener medizinischer Klartextdaten in der TI.

Der Grundgedanke des Confidential Computings ist bereits in den Vertrauenswürdigen Ausführungsumgebungen der Fachdienste der ePA, des E-Rezepts und der sektoralen Identity Provider umgesetzt. Er besteht darin, die Klartextverarbeitung (von personenbezogenen medizinischen Daten) innerhalb der physischen Infrastruktur mit technischen Mitteln so weit zu isolieren, dass es selbst einem Angreifer aus dem betrieblichen Umfeld der Infrastruktur nicht möglich ist, Vertraulichkeit, Integrität oder Authentizität der Datenverarbeitung bzw. der Daten selbst zu verletzen. Confidential Computing liefert Schutz für Data in Use.

Die Klartextverarbeitung erfolgt damit in isolierten Verarbeitungskontexten. Nur innerhalb dieser Verarbeitungskontexte können die schützenswerten Nutzdaten im Klartext vorliegen und für den Transport und die Speicherung der Nutzdaten benötigtes Schlüsselmaterial zur Ver- und Entschlüsselung verwendet werden. Gleichzeitig ist die Code-Basis der Verarbeitungskontexte, die Trusted Computing Base (TCB), möglichst klein gehalten, um in der Begutachtung eine starke Zusicherung über die Sicherheitseigenschaften erzielen zu können.

Daneben gelten weitere Anforderungen:

- **Schutz für Data at Rest:** Nutzdaten werden verschlüsselt gespeichert und ein Abfluss der Nutzdaten aus der geschützten Infrastruktur wird mittels baulich-physikalischer und organisatorischer Maßnahmen ausgeschlossen.
- **Schutz für Data in Transit:** Nutzdaten werden grundsätzlich verschlüsselt und nur zwischen wechselseitig authentisierten und zulässigen (autorisierten) Systemen transportiert.
- **Verbot von Nutzertracking und Profilbildung:** Die Auswertung nutzer- bzw. institutionsbezogenen Verhaltens durch den Anbieter ist im Confidential Computing weitgehend systematisch durch die Gesamtarchitektur auszuschließen. Notwendige und zulässige Auswertungen sind auf Anwendungsebene umgesetzt und damit Teil der spezifizierten Autorisierungsmodelle der Anwendungen. Hierzu gehören auch alle erforderlichen Mechanismen zur Entstörung soweit sie einen Umgang mit den verarbeiteten Nutzdaten oder Einblick in Nutzerverhalten erfordern.
- **Sichere Entwicklung und Inbetriebnahme:** Die Software der Dienste und an der Verarbeitung der Nutzdaten beteiligter Komponenten wird mittels sicherer Prozesse entwickelt, durch anerkannte Prüfstellen begutachtet und authentisiert sowie integritätsgeschützt in die Betriebsumgebung eingebracht.

- **Sichere Hardware:** Die Hardware von an der Verarbeitung der Nutzdaten beteiligten Systemen ist hinsichtlich ihrer Eignung für das erforderliche Vertrauensniveau geprüft und wird über sichere Prozesse beschafft und verwaltet.
- **Governance durch gematik:** De Wirksamkeit der technischen Mittel wird durch die gematik, als unabhängige Institution und Governance-Verantwortliche für die TI, möglichst öffentlich, kontinuierlich und prüfbar dargestellt.
- **Datenschutzgarantien:** Die gematik gründet ihre Datenschutzgarantien auf einer (Produkt-)Zulassung für die HCC-Infrastruktur, auf geeigneten weiteren Zulassungs-, Begutachtungs- und Zertifizierungsprozessen, die den Anbietern auferlegt sind, sowie auf der Attestation der laufenden Dienste.
- **Schutz vor Seitenkanalangriffen:** Aufgrund der Grenzen der Schutzwirkung der als Confidential Computing vermarkteten Technologien gegenüber Seitenkanalangriffen muss ausgeschlossen werden, dass Nicht-HCC-Prozesse auf derselben CPU parallel mit HCC-Prozessen laufen. Prozesse des Infrastrukturbetreibers, die aus technischen (z. B. Hypervisor) oder betrieblichen Gründen (z. B. Observability-Funktionen) mit auf der CPU laufen müssen, müssen als Teil der TCB betrachtet, mit begutachtet und mit attestiert werden.

Dem Anbieter der Confidential Computing Infrastruktur obliegt damit im Betrieb primär die Sicherstellung der Verfügbarkeit seiner Infrastruktur und der darauf laufenden Dienste, d. h. die Erfüllung von betrieblichen Service Level Agreements bezüglich Erreichbarkeit der HCC-Dienste aus dem Internet (und ggf. noch aus dem zentralen Netz der TI) und Verfügbarkeit der Transport-, Verarbeitungs- und Speicherkapazitäten sowie die bedarfsgerechte Provisionierung der HCC-Dienste. Seine eigenen administrativen Eingriffsmöglichkeiten enden an den Grenzen der Trusted Computing Base.

## 6.2 Cloud Computing

Im Unterschied zu den bisher anwendungsspezifisch umgesetzten Infrastrukturen u. a. der ePA und des E-Rezepts ist Healthcare Confidential Computing darauf ausgerichtet, eine generische Infrastruktur für die Umsetzung von Basis- und Fachdiensten bereitzustellen und damit eine Form des Cloud Computing zu ermöglichen sowie auch tatsächlich in hochskalierten (Public) Cloud Infrastrukturen betrieben zu werden. Mit dieser Ausrichtung werden verschiedene Ziele verfolgt:

- Verbesserungen der betrieblichen Stabilität der TI durch längerfristige Konsolidierung, Standardisierung und Integration der Infrastruktur,
- Verringerung der personellen und prozessualen Aufwände für die Bereitstellung der Infrastruktur für die TI-Dienste, die exklusiv durch das Gesundheitswesen getragen werden müssen,
- Nachnutzung der Weiterentwicklung der Technologien, der Automatisierung, der Qualitätssteigerungen, der Verfügbarkeit und des wachsenden nativen Service-Portfolios in der Cloud für die Dienste der TI sowie
- Nutzung der elastischen Skalierbarkeit von Diensten in der Cloud.

Anbieter von Healthcare Confidential Computing (HCC-Provider) bieten ihre Infrastrukturen marktoffen für die Anbieter von (Fach-) Diensten der TI an.

Ein TI-Dienstanbieter tritt als Kunde mit seinem HCC-Provider in eine Geschäftsbeziehung und erhält damit Zugang zu einem Mandantenkontext innerhalb der Infrastruktur. Er erhält damit auch die Werkzeuge zur eigenständigen Buchung von Systemressourcen, zur Konfiguration und zur betrieblichen Überwachung der Systemressourcen und seiner Dienste sowie für die Aufnahme seiner Dienste in den Vertrauensraum von HCC bzw. der

TI 2.0. Charakteristisch für Cloud Computing ist dabei insbesondere, dass die Bereitstellung der Infrastruktur-Ressourcen auf bereits betriebsbereiten Systemen automatisiert erfolgt, sobald der Kunde dies via Web-Schnittstelle oder über APIs angefordert hat. Darüber können Dienste mit dem Volumen der an sie gerichteten Anfragen automatisch hoch- und herunterskaliert werden. Dem Dienstanbieter werden generell nur die tatsächlich genutzten Ressourcen in Rechnung gestellt.

Der Dienstanbieter kann für seinen Dienst damit die vom HCC-Provider bereitgestellten Systemressourcen nutzen und darauf verzichten entsprechende eigene Infrastruktur aufzubauen. Er kann darüber hinaus die Funktionalitäten von Cloud-Services nachnutzen, indem diese in seinem Mandantenkontext für ihn instanziiert oder als Shared Cloud-native Services für den Dienstanbieter konfiguriert werden, und muss daher solche Funktionalitäten nicht selbst entwickeln. Der Dienstanbieter nutzt dabei (ggf. teilweise automatisch) die in der Infrastruktur umgesetzten Sicherheits- und Betriebsmechanismen, die Schnittstellen zu den TI-spezifischen SIEM und Monitoringsystemen der gematik sowie die erteilten Zulassungen und Zertifizierungen des HCC-Providers nach und kann damit die Zulassungsprozesse für seinen Fachdienst substanziell vereinfachen.

Cloud Computing liefert mit seinen Container- oder VM-basierten Deployment-Möglichkeiten auch die Grundlage für eine Integration (durch Konfiguration in der Laufzeitumgebung) von fertigen Komponenten in (Fach-) Dienste. Für eine solche Nutzung sind z. B. Komponenten zur Autorisierung vorgesehen, die im Rahmen der Einführung der Zero Trust Architektur der TI 2.0 durch die gematik bereitgestellt werden sollen. Sie werden im Dienstkontext instanziiert und liefern z. B. eine Integration in die Sicherheitsadministration der TI mit.

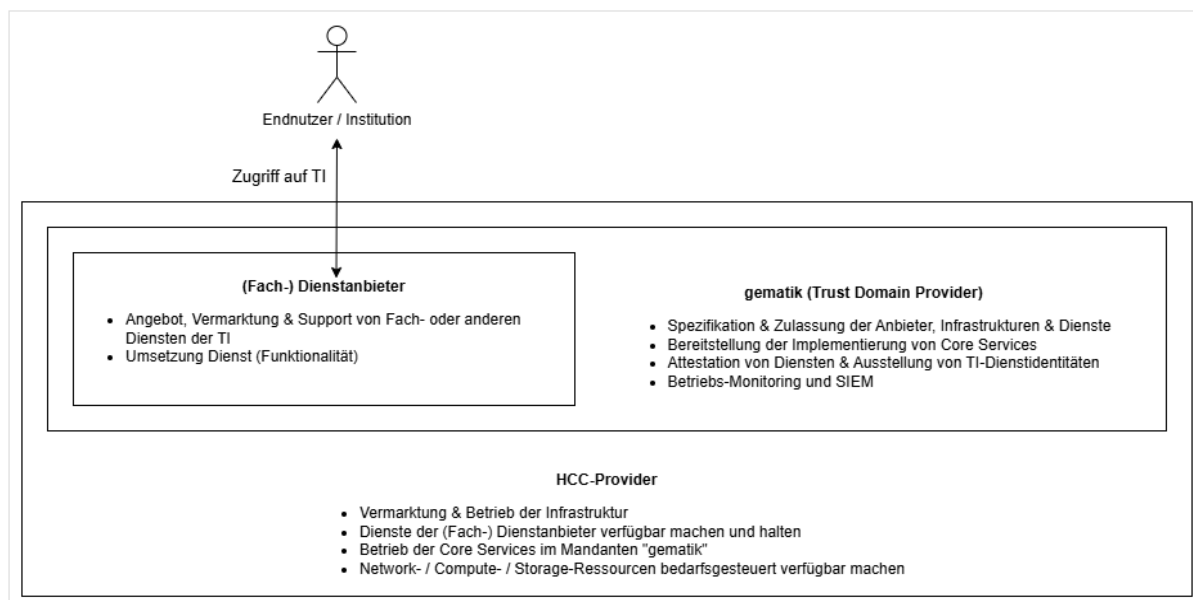
## 6.3 Shared Responsibility Model

Für die Bereitstellung von Diensten resultiert beim Confidential Computing in der Cloud ein Modell von „Shared Responsibility“ in dem der Dienstanbieter die Verantwortung für die funktionale Korrektheit und Sicherheit der von ihm eingebrachten Implementierung seines Dienstes trägt und diese auch begutachten lässt und zur Zulassung einreicht. Dabei muss er den durch die Infrastruktur gesetzten rechtlichen, betrieblichen und sicherheitstechnischen Rahmen berücksichtigen. Der HCC-Provider unterstützt dies, indem er offene, industrieübliche und stabile Schnittstellen für die Nutzung seiner HCC-Infrastruktur anbietet.

Die geteilte Verantwortlichkeit zwischen HCC-Dienstanbieter und HCC-Provider wird durch die Verantwortung der gematik als Garant für Verfügbarkeit, Performance und Sicherheit der TI erweitert:

- **Verfügbarkeit:** Die Abgrenzung der Verantwortlichkeiten von Dienstanbietern und HCC-Provider erfolgt technisch durch geeignete "Übergabemesspunkte" (z. B. "Request an die Eingangsschnittstelle der Dienst-Workload geroutet", "Request durch Dienst-Workload verarbeitet") im Rahmen der Festlegungen zur Gesamtverfügbarkeit des Dienstes.
- **Performance:** Optimierung der HCC-Plattformen hinsichtlich dienstübergreifender Stabilität und Performance (im Sinne der Effizienz) seitens der HCC-Providers gemeinsam mit der gematik in einem fortlaufenden Prozess.
- **Sicherheit:** Implementierung des dienstübergreifenden souveränen HCC-Vertrauensraums (HCC Trust Domain) einschließlich des Policy Managements unter (Co-)Hoheit der gematik in der Infrastruktur des HCC-Providers.

Die Verantwortlichkeit der gematik bildet sich bei HCC über technische Mittel zur direkten Überwachung der beteiligten Systeme ab. Sie erstreckt sich damit von der Ebene der Zulassung über die Sicherheits- und Betriebsüberwachung bis in die Ebene der Infrastruktur, ohne HCC-Provider oder Fachdienstanbieter aus ihrer jeweiligen Verantwortung zu entbinden.



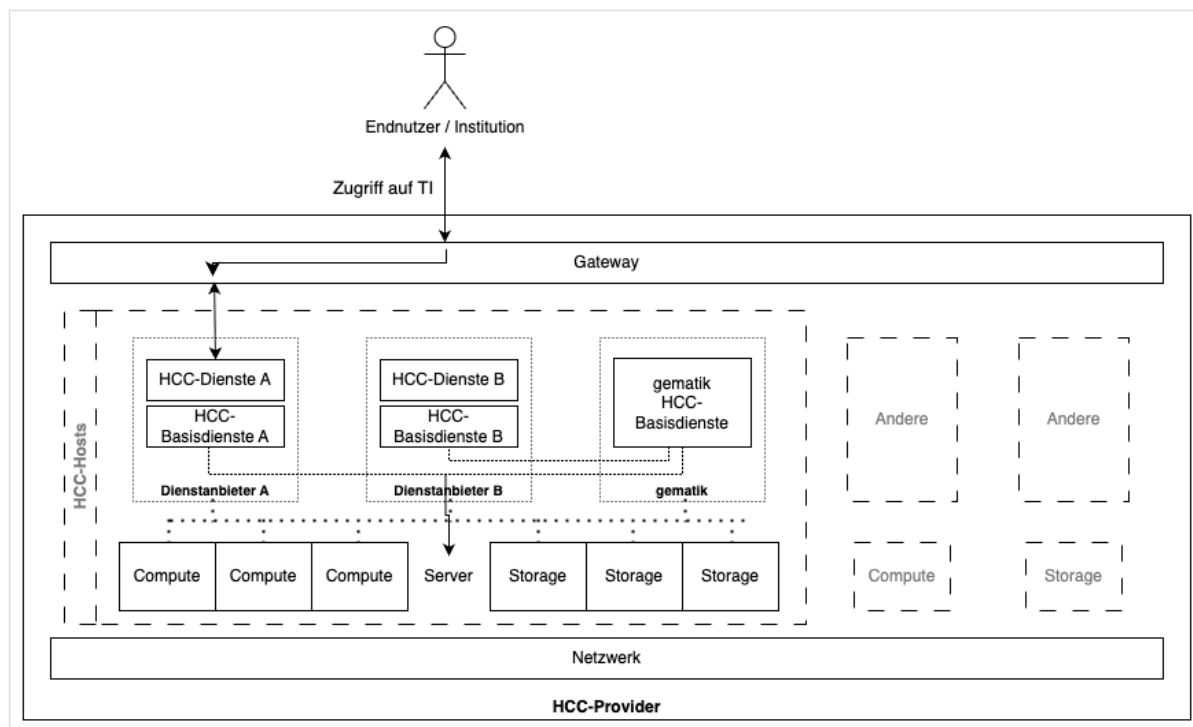
**Abbildung 1: Shared Responsibility - Verteilung der Aufgaben**

Ein möglichst großer Teil der querschnittlich benötigten Plattformdienste soll im Mandantenkontext des Dienstansbieters instanziiert werden, um komplexe Cost Sharing Modelle zu vermeiden und ein immer noch hohes Maß an organisatorischer Trennung zwischen Dienstansbiestern auch innerhalb einer HCC-Infrastruktur zu gewährleisten.

## 6.4 Implementierte HCC-Governance

Die Zulassung eines HCC-Dienstes zur TI impliziert seinen Betrieb bei einem zugelassenen HCC-Provider sowie die Integration des Dienstes in die vom HCC-Provider bereitgestellten (oder angebotenen) und von der gematik gesteuerten HCC-Basisdienste der TI, die sowohl den HCC-Dienst als auch die HCC-Infrastruktur zur Laufzeit den Governance-Prozessen der gematik unterstellen.





**Abbildung 2: Governance - Deployment View**

Die HCC-Basisdienste werden direkt in der Infrastruktur der HCC-Provider bereitgestellt, damit gleichzeitig die hohen Schutzbedarfe für die verarbeiteten Daten erfüllt und eine hohe Verfügbarkeit aller Schnittstellen innerhalb der Betriebsverantwortung des HCC-Providers erreicht werden.

HCC-Basisdienste sind die im Kapitel [HCC Platform Services](#) definierten Dienste zur Verwaltung der HCC-Infrastruktur.

Um die HCC-Basisdienste hoheitlich steuern zu können, stellt der HCC-Provider der gematik einen spezifischen Mandantenkontext oder einen Plattformzugang zur Verfügung in dem die HCC-Basisdienste verwaltet werden. Die (sicherheits-) funktionalen Schnittstellen der HCC-Basisdienste müssen für HCC-Dienste der (Fach-)Dienstleister erreichbar sein.

Alle dargestellten Beziehungen und die zugehörigen Konfigurationen werden über die TI-Policy definiert und zur Laufzeit automatisiert um- und durchgesetzt. Die TI-Policy wird dazu, falls erforderlich, auf Schnittstellen des Cloud Management Systems des HCC-Providers abgebildet, d. h. verteilt und ggf. vorher übersetzt.

## 6.5 Integration mit Diensten außerhalb von HCC

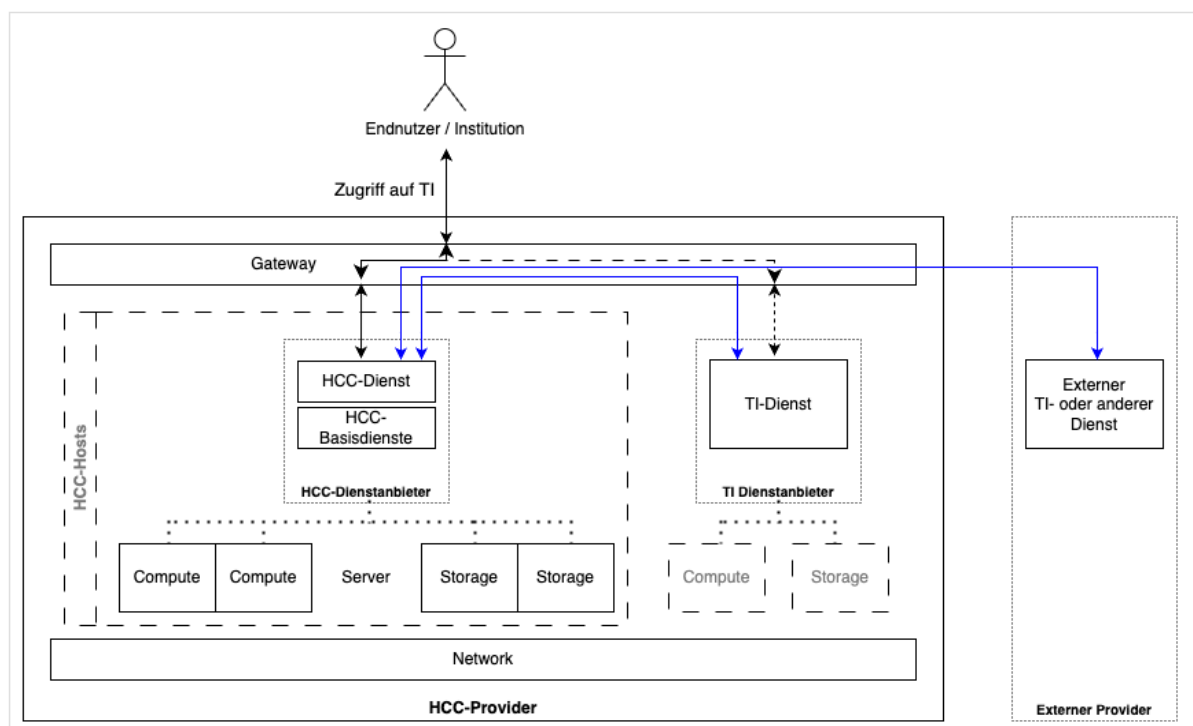
Während die Bereitstellung von generischer Infrastruktur durch HCC-Provider die Verfügbarkeit von Ressourcen zur Verarbeitung besonders vertraulicher Gesundheitsdaten sicherstellt und standardisiert, gibt es angrenzende Bedarfe für IT-Infrastruktur und Lösungen, die nicht auf dieses spezifische Vertrauensniveau angewiesen sind, aber in der Cloud betrieben werden.

Diese Bedarfe können seitens der Akteure flexibel über einen Mix aus Cloud-Angeboten, anwendungsspezifischen Managed Services und On-Premises Systemen aufgebaut werden und mit HCC-Diensten integriert werden, soweit dies datenschutzrechtlich

zulässig ist und keine Verletzung von Sicherheitsanforderungen bzgl. der in HCC verarbeiteten Daten impliziert. Hierbei müssen alle Kommunikationspartner der HCC-Dienste mindestens authentifiziert werden können.

Beispiele sind Entwicklungs- und Testplattformen, Verwaltungswerkzeuge, Primärsysteme der Leistungserbringer und Systeme der Kostenträger, die in der Hoheit anderer Akteure im Gesundheitswesen liegen sowie Dienste, die keine personenbezogenen Daten verarbeiten. Auch Bestandssysteme verschiedenster Art, die weder nach den Prinzipien des Confidential Computing noch als Cloud-Lösungen entwickelt worden sind, müssen eingebunden werden können.

Die Integration von HCC-Diensten mit diesen anderen Diensten erfolgt über Gateway-Funktionen beim HCC-Provider, die neben der Datenverkehrssteuerung auch eine erste Stufe des Ausschlusses von unbekannten externen Verbindungspartnern umsetzen. Die Verwendung solcher Gateways im Kontext eines HCC-Dienstes setzt damit Konfigurationseinstellungen auf Policy- und Netzwerkebene voraus. Diese Konfigurationseinstellungen sollen im Mandantenkontext angesiedelt sein.



**Abbildung 3: Integration von HCC-Diensten mit TI-Diensten und externen Diensten**



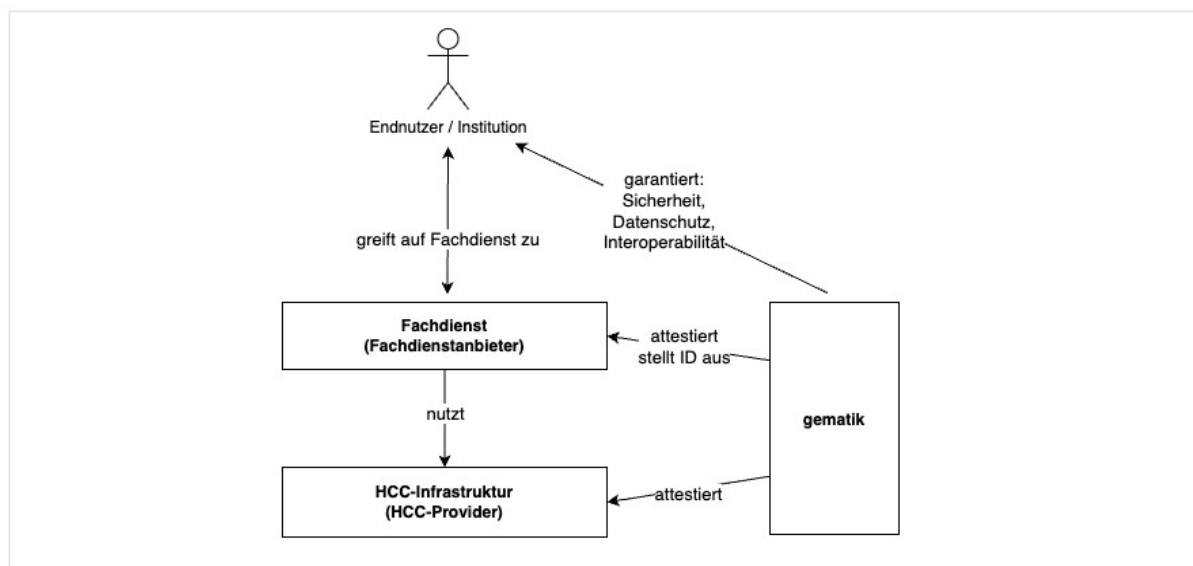
## 7 Sicherheitsarchitektur von HCC

HCC ist eine Sicherheitsarchitektur für den Betrieb von Diensten im Rechenzentrum, die konsequent nach den Prinzipien von Security by Design aufgebaut ist. Sie hat zum Ziel, neben allen weiteren Unberechtigten, auch den Betreiber der physischen Infrastruktur mit technischen Mitteln daran zu hindern, auf die verarbeiteten Klartextdaten oder auf laufende Verarbeitungsprozesse zuzugreifen.

Die Sicherheitsarchitektur von HCC ist eingebettet in die umfangreichen baulichen, technischen, personellen und prozeduralen Sicherheitsmaßnahmen, die für größere Rechenzentrumsinfrastrukturen ohnehin üblich und durch ihre gutachterlich bestätigte Konformität mit geeigneten Normen abgesichert sind. Ein entsprechendes betriebliches Umfeld wird vorausgesetzt (siehe Kapitel 9- Zulassungen und Bestätigungen).

Die Sicherheitsarchitektur von HCC beschreibt daher primär den Aufbau und die Komponenten, die innerhalb der Rechenzentrumsumgebung das substanziell oberhalb einer üblichen Zertifizierung liegende Schutzniveau abbilden, welches für die Klartextdatenverarbeitung von personenbezogenen medizinischen Daten erforderlich ist. Entscheidend für dieses höhere Schutzniveau sind die technischen Mechanismen von Confidential Computing und die Einbeziehung der gematik als vom Betreiber unabhängige Stelle in diese Mechanismen.

HCC stellt einen Sonderfall von Confidential Computing in der Cloud dar, da Confidential Cloud Computing i. A. keinen unabhängigen Dritten (hier die gematik) als technisch in die Laufzeitumgebung integrierten Garanten für die Sicherheits- und Privacy-Eigenschaften und keinen technischen Ausschluss des Anwendungsbetreibers von der Datenverarbeitung vorsieht. Vergleichbare Konstellationen könnten jedoch auch für andere Anwendungsbereiche mit staatlicher Aufsicht und hohem Schutzbedarf entstehen.



**Abbildung 4: gematik als Garant für HCC**

In den folgenden Unterkapiteln wird die Sicherheitsarchitektur von HCC dargestellt und begründet.

## **7.1 Trennung zwischen Designtime und Runtime**

Der Gesamtaufbau des Systems trennt die zur Laufzeit der Basis- und Anwendungsdienste erforderlichen Komponenten und Artefakte (beim HCC-Provider) von den Designtime-Systemen zur organisatorischen Handhabung und Bereitstellung dieser Artefakte. Dadurch wird die Komplexität der Steuerung von HCC aus der Laufzeitumgebung so weit wie möglich herausgehalten und die Angriffsfläche der Laufzeitumgebung minimiert.

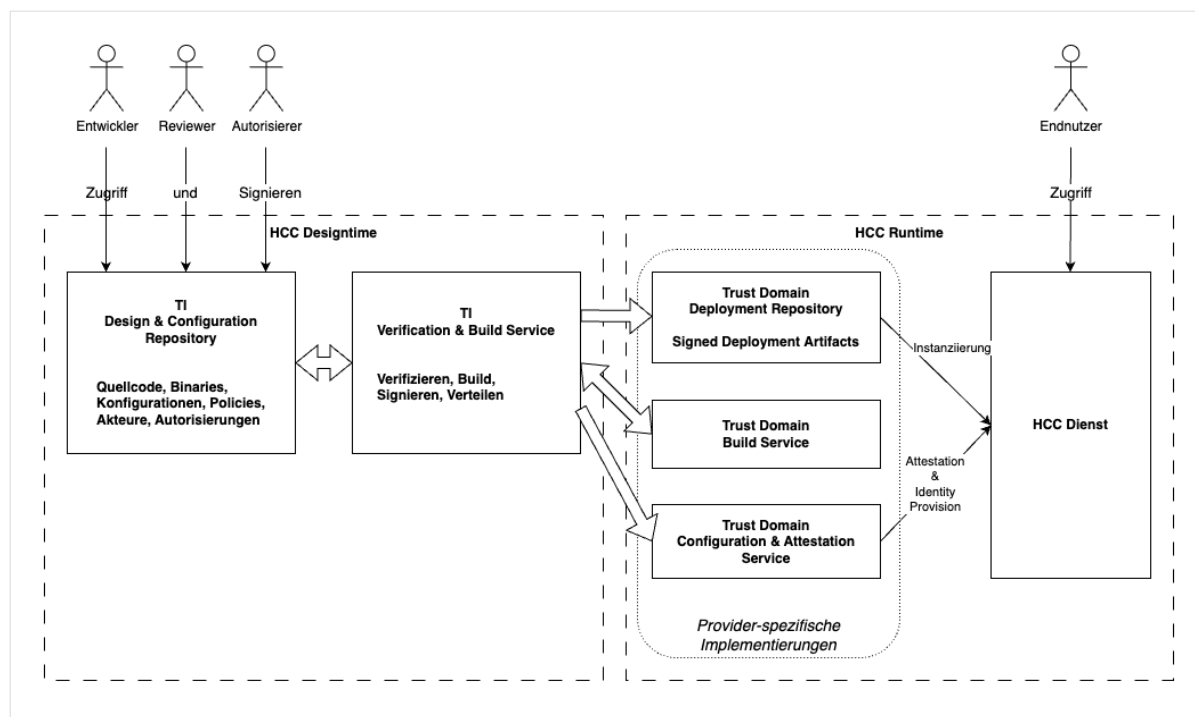
Die Verbindung zwischen Designtime und Runtime wird mittels Signierung der zur Laufzeit benötigten Artefakte in der Designtime erreicht.

Ein TI Design & Configuration Repository in dem ggf. komplexe organisatorische Abläufe umgesetzt werden müssen, um die Qualität der bereitgestellten Artefakte und bspw. eine Umsetzung des Mehraugenprinzips sicherstellen zu können, liefert die zur Laufzeit benötigten Artefakte in signierter Form.

Artefakte werden als Endresultat so weit wie möglich automatisierter Prüfprozesse signiert – durch Sign-off seitens autorisierter Akteure oder durch vertrauenswürdige Dienste der Plattform automatisiert. Vertrauenswürdige Dienste werden genutzt, wenn Artefakte als Ergebnis automatisierter Verarbeitungs- und Prüfprozesse entstehen (z. B. im TI Verification & Build Service) oder wenn eine Vielzahl verschiedener Akteure an den Prozessen in den Designtime-Systemen beteiligt ist und deren Signaturen zur Vereinfachung auf wenige in der Laufzeitumgebung zu prüfende Signaturen reduziert werden müssen.

Dienstsoftware soll zunächst unabhängig von den spezifischen Confidential Computing Implementierungen der HCC-Provider entwickelt und in einem zweiten Schritt für die Ausführung bei einem HCC-Provider vorbereitet werden können. Jeder HCC-Provider stellt dazu einen Trust Domain Build Service bereit (bzw. ein Plug-in für eine Build Pipeline der gematik, wie in 3.4- Standardisierung des Confidential Computing Ansatzes dargestellt), der die Umwandlung durchführt, die umgewandelten Artefakte zurückliefert (und ggf. signiert) und gleichzeitig die Referenzwerte für die Attestation ermittelt. Der Vorgang soll automatisiert durchgeführt werden können, aber zu Test- und Prüfzwecken auch manuell angestoßen werden können.

Ein Trust Domain Deployment Repository je HCC-Provider nimmt die fertigen Artefakte aus dem TI Verification & Build Service auf. Jede Laufzeitumgebung bzw. jeder Standort eines HCC-Providers, enthält eine für die dort verfügbaren Anwendungen vollständige Replik des Deployment Repositories, um zeitlich begrenzte Unterbrechungen in der Verfügbarkeit der Designtime-Systeme überbrücken zu können.



**Abbildung 5: Designtime- und Runtime-Umgebung**

Die Trennung von Runtime und Designtime wird auch auf der betrieblichen Ebene der Designtime-Services umgesetzt. Die Designtime-Services benötigen eine Laufzeitumgebung, die die gematik z. B. bei einem HCC-Provider beziehen kann. Confidential Computing wird für den TI Verification & Build Service benötigt, da dieser Prozesse zur automatisierten Erzeugung von geprüften Artefakten und zur automatisierten Signierung bereitstellt. Für Designtime-Services ist ein gesonderter Mandantenkontext der gematik – neben dem Kontext für den Betrieb der Trust Domain Runtime-Services – erforderlich.

## 7.2 Attestation des Sicherheitszustands

Basis für die Erreichung der Sicherheitsziele von HCC ist ein wohldefinierter Soll-Zustand und eine stets aktuelle und gegen den Soll-Zustand validierte Erfassung des Ist-Zustands aller Systeme in der Trusted Computing Base.

Die Definition des Soll-Zustands ist durch Referenzwerte der geprüften technischen Artefakte (Software-Pakete, Konfigurationsdatensätze) und durch Attribute von registrierten Komponenten in der Betriebsumgebung (Server-Typ, Betriebszustand, Signaturschlüssel, etc.) gegeben.

Die Funktionen zur Erfassung des Ist-Zustands, zum Abgleich mit dem Soll-Zustand sowie zur Aufnahme von Diensten in die HCC Trust Domain wird in den Infrastrukturen der HCC-Provider jeweils durch einen Attestations- und Konfigurationsdienst (Trust Domain Configuration & Attestation Service, TDCAS) übernommen.

Da die Attestation auf Mechanismen der Hardware und Software aufbaut, die von den seitens des Anbieters verwendeten Systemkomponenten abhängen, ist der TDCAS anbieterspezifisch umgesetzt. HCC-Provider können ihre HCC-Stacks auf der Basis der Technologien Intel TDX, AMD SEV-SNP, ARM CCA, IBM Z und äquivalenten zukünftigen Technologien aufbauen, da diese Technologien sowohl die Speicherverschlüsselung als

auch die Attestation der HCC-Workloads (cVMs) unterstützen. Hinzu kommt eine Attestation der HCC-Hosts (Hardware, Firmware, Hypervisor, Host-Services) mittels TPM oder einem anderen Verfahren, das einen vom HCC-Provider unabhängigen Vertrauensanker in Hardware und eine Messung mittels Komponenten der TCB bieten. Beide Ebenen der Attestation müssen miteinander integriert sein, um sicherzustellen, dass attestierte Workloads auf attestierten Hosts laufen.

Der TDCAS wird der gematik vom HCC-Provider zur Verfügung gestellt, von HCC-Provider und gematik gemeinsam in Betrieb genommen und dabei mit dem Vertrauensanker im HSM-Cluster verbunden.

In der Konfigurationsdatenbank des TDCAS sind stets die HCC-Hosts bzw. ihre Signer Identities, die aktuell zugelassenen Versionen aller zur TCB gehörenden Software-Komponenten und Konfigurationen sowie weitere Daten registriert. Die Konfigurationsdatenbank bildet den Soll-Zustand ab und wird über administrative Prozesse gefüllt, die in der Design-time-Umgebung liegen.

Die Attestation erfolgt in zwei Stufen:

1. Attestation des Hosts inkl. Firmware und Hypervisor und
2. Attestation je gestarteter Workload.

Für jeden für den HCC-Vertrauensraum gestarteten Host wird mittels TPM und Secure Boot Attestationsfähigkeit erreicht. Der Hypervisor bzw. ein damit gestarteter Dienst ist für den Abruf und die Weitergabe der signierten PCR-Werte aus dem TPM zuständig. Der Hypervisor muss sicherstellen, dass Workloads, die nicht aus dem HCC-Vertrauensraum stammen, auf HCC-Hosts nicht gestartet werden können.

Für jede HCC-Dienstinstanz wird das Speicherabbild gemessen, während sie als Confidential VM gestartet wird. Anschließend ruft sie einen lokalen Attestation Report ab, der von der Hardware und Firmware der CPU des registrierten HCC-Hosts produziert und mit einem in der Hardware verankerten Schlüssel signiert ist. Der Report enthält auch die für Confidential Computing notwendigen Angaben zur Konfiguration des Hosts bzw. der CPU.

Der Signer Key in der CPU sowie der Signer Key des TPM müssen von HCC-Provider-unabhängigen Hardware-Herstellern stammen, um sie jedem Einfluss seitens des HCC-Providers zu entziehen.

Eine Kombination der Attestation Reports aus CPU und TPM wird als Nachweis über einen bestimmungsgemäßen Betriebszustand an den lokalen TDCAS übermittelt und vom TDCAS gegen seine Konfigurationsdatenbank geprüft. Die Konfigurationsdatenbank des TDCAS enthält dazu neben den Referenzwerten die Hardware-Signer-Identitäten aller beim HCC-Provider in der jeweiligen Location für die potenzielle Nutzung für HCC registrierten Server. Damit kann der TDCAS die Signaturen der Attestation Reports prüfen und damit gleichzeitig feststellen, dass es sich um Server in der sicheren Betriebsumgebung handelt.

Die Attestation auf der Grundlage der kombinierten Reports auf Ebene der cVM und der Host-Software kann auf verschiedene Arten umgesetzt sein, muss aber sicherstellen, dass beide signierte Reports "fresh" sind und von demselben Host stammen (inkl. Abwehr von z. B. "Kuckucksangriffen").

Die Datenbank des TDCAS enthält die Signer-Identität des TI Verification & Build Service, so dass der TDCAS die Authentizität der Konfigurationseinträge stets selbst prüfen kann. Im einfachsten Fall sind alle Registrierungseinträge von nur einer Service-Identität signiert, die als Teil des TI Verification & Build Service den Übergang der Einträge von der Design-time- in die Runtime-Umgebungen automatisiert.

Erst im Anschluss an eine erfolgreiche Verifikation der Attestation Reports durch den TDCAS wird ein HCC-Dienst in den HCC-Vertrauensraum aufgenommen. Hierzu werden

der HCC-Dienstinstanz vom TDCAS Credentials zum Zugriff auf den privaten Schlüssel für die TLS-Identität (X.509-Zertifikat) des HCC-Dienstes und ggf. auf weiteres benötigtes Schlüsselmaterial im HSM-Cluster übermittelt. Kurzlebige Zertifikate bzw. Schlüssel können auch direkt in den Verarbeitungskontext des HCC-Dienstes eingebracht werden. Die konkreten Vorgaben hierzu liefert die Spezifikation des HCC-Dienstes.

Der TDCAS erzeugt über jeden Attestationsvorgang einen kryptographisch gegen Veränderungen geschützten Log-Eintrag.

Der TDCAS kann gegenüber den HCC-Diensten als Sub-CA der PKI der TI arbeiten und dann dienstspezifische Zertifikate ausstellen, die mit seinem Sub-CA-Zertifikat signiert sind. Damit eröffnen sich Möglichkeiten für:

- Dienstzertifikate mit kurzer Laufzeit
- Das Setzen eines erweiterten Attributs im Dienstzertifikat, dass eine Referenz auf den Log-Eintrag des spezifischen Attestationsvorgangs darstellt. Clients können eine Funktion zur Interpretation der Referenz als URL sowie zum Abruf und zur Anzeige des Log-Eintrags implementieren.

Die Konfigurationsdatenbank des TDCAS wird durch den TDCAS selbst verwaltet und ist mittels Signaturen und Hardware-basierten Sicherheitsfunktionen der TDCAS-Hosts gegen Manipulationen (z. B. Veränderungen an Datenbankdateien, Laden einer ungültigen Datenbank) und gegen Rollback geschützt, z. B. mittels monotoner Versionszähler.

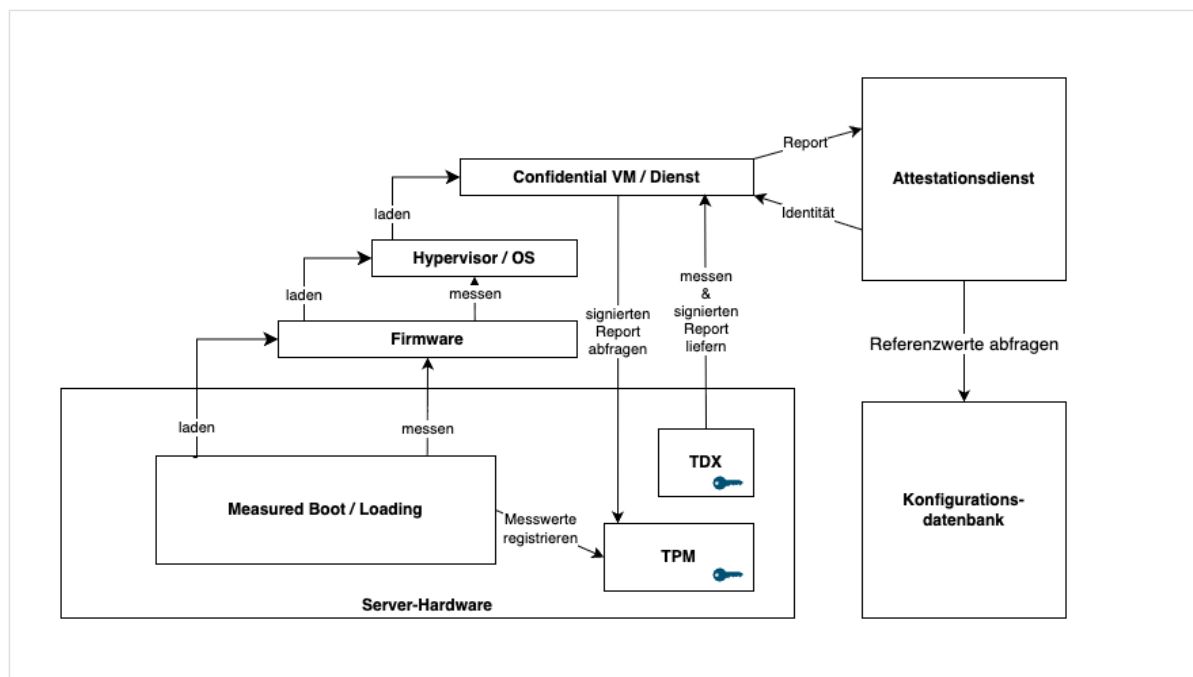
Der TDCAS ist mit dem HCC-Vertrauensanker der TI beim HCC-Provider kryptographisch verknüpft. Über diese Verknüpfung wird auch seine Identität abgesichert und seine Authentisierung gegenüber dem HCC-Vertrauensanker ermöglicht.

Der HCC-Vertrauensanker besteht aus einem unter Einbeziehung der gematik und ggf. weiterer Akteure zeremoniell administrierten HSM-Cluster. Um auch die initiale Zeremonie remote durchführen zu können – eine Möglichkeit, die insbesondere für Cloud-Provider relevant ist – sollten die HSMs Key Attestation unterstützen. Damit kann in der Zeremonie auch ohne physischen Zugang überprüft werden, dass die Erzeugung des Schlüsselmaterials tatsächlich in einem HSM stattfindet.

Während des Betriebs der HCC-Service-Instanzen können weitere Mechanismen zum Schutz der Integrität der attestierten Systeme eingesetzt werden, bspw. die Linux Integrity Measurement Architecture.

Der Hardware-geschützte Signer-Schlüssel für die Workload-Attestation ist in die CPU integriert, für die Host-Attestation in ein TPM. In der Kombination können diese Schlüssel die Anforderung zur Erfassung des gesamten CC-Stacks umsetzen.

Die folgende Abbildung zeigt ein vereinfachtes Beispiel einer kombinierten Attestation auf Basis von Intel TGX und einem TPM:



**Abbildung 6: Attestation beispielhaft, vereinfacht**

Die genaue Ausgestaltung der Attestation durch die HCC-Provider ist system- und technologiespezifisch und wird in der vorliegenden Spezifikation daher nicht weiter im Detail standardisiert. Ein Standard könnte jedoch im Zuge internationaler Strukturen, wie dem Confidential Computing Consortium oder der IETF, entstehen und längerfristig für die TI adaptiert werden.

Als wichtigste Anforderung an jede Umsetzung der Attestation wird nur gefordert, dass die Attestation den Sicherheitszustand der TCB vollständig abbilden muss. Hierbei ist die Annahme zulässig, dass gut gehärtete Komponenten ihren Sicherheitszustand erhalten, nachdem sie korrekt gestartet und attestiert wurden. Die Anforderungen an den Nachweis einer entsprechenden Härtung können jedoch hoch sein. Im Ergebnis werden Mechanismen zur kontinuierlichen bzw. häufig wiederholten Attestation nicht zwingend gefordert.

Für alle außerhalb der Confidential VMs laufenden Software-Komponenten der HCC-Host-Plattform – wie Firmware, Hypervisor, Betriebssystem und Provisionierungskomponenten – muss nachgewiesen sein, dass diese Komponenten keine Angriffe aus dem Betriebsumfeld auf die Confidential VMs ermöglichen und dass nur entsprechend geprüfte Software-Komponenten laufen können.

Die Attestation der Host-Plattform außerhalb der cVMs dient primär dem Integritätsschutz der HCC-Hosts. Dieser ist erforderlich, da cVMs keinen perfekten Schutz vor Angriffen bieten, falls es einem Angreifer (Innentäter aus dem betrieblichen Umfeld) gelingt, spezifischen Angriffs-Code auf dem Host einzuschleusen, der die in cVMs laufenden Verarbeitungen über Seitenkanäle angreift. Der TPM-basierte Attestationsreport wird in die Attestation cVMs eingebettet oder anderweitig kryptographisch sicher verknüpft in das Attestationsschema eingebunden.

TPM-basierte Attestation wird in Verbindung mit einer organisatorischen Trennung innerhalb der Organisation des HCC-Providers – zwischen Verantwortlichen für den physischen Betrieb der Hosts einerseits und Verantwortlichen für die Bereitstellung der Host-Software andererseits – dazu genutzt, um das Angriffspotential von Innentätern zu reduzieren. Die Referenzwerte für das TI-Design & Configuration Repository werden von



der verantwortlichen Stelle für die Bereitstellung der Software-Komponenten mittels einer in der HCC-Trust-Domain registrierten Identität signiert übermittelt.

Um die attestierte Integrität der Betriebssystemumgebung über den gesamten Boot-Zyklus eines Hosts zu erhalten, muss die Host-Plattform so aufgebaut sein, dass sie nicht aus betrieblichen Gründen während der Laufzeit verändert werden muss.

Wenn ein neuer HCC-Host ins Rechenzentrum eingebracht wird, müssen die Signaturschlüssel seines TPMs und seiner CPU im TI-Design & Configuration Repository registriert werden, damit diese nachfolgend vom TDCAS erkannt werden können. Darüber hinaus muss die Attestation gegenüber dem Hardware-Hersteller durchgeführt werden, z. B., um zu bestätigen, dass es sich um eine originale CPU des Herstellers handelt. So weit wie möglich sollen auch Daten zur Lieferkette und zum Prozess der Einbringung des Servers in die Umgebung erfasst werden (z. B. im Rahmen des regulären Asset Managements). Diese Daten werden, ggf. auszugsweise, zusammen mit einer eindeutigen Host-ID und ggf. weiteren Daten an das TI-Design & Configuration Repository übermittelt und ggf. im Rahmen von Audits verwendet.

Für HCC-Hosts wird auf der Grundlage ihrer Registrierung angenommen, dass sie sich in der gegen physische Eingriffe geschützten Betriebsumgebung des HCC-Providers befinden. Der HCC-Provider muss mit organisatorischen Mitteln das Einbringen manipulierter Einträge verhindern. Dies bedeutet insbesondere, dass es ausgeschlossen sein muss, Server zu registrieren, die sich außerhalb der geschützten Betriebsumgebung des HCC-Providers befinden.

### **7.3 Bootstrapping der technischen Sicherheitsarchitektur**

Die technischen Mittel zur Abwehr von Innentätern müssen derart gestaltet sein, dass sie die HCC-Plattform während des Betriebs zur autonomen Aufrechterhaltung ihrer Sicherheitsgarantien in die Lage versetzen. Sie müssen die HCC-Plattform daher mit der Fähigkeit zur Introspektion und Attestation ihres Sicherheitszustands ausstatten. Die TCB muss sowohl möglichst klein als auch möglichst transparent gehalten sein. Sämtliche Mechanismen müssen auf wirksamen kryptographischen Verfahren in Kombination mit physischen Schutzmaßnahmen und mit Rollentrennung aufbauen. Alle Prozesse zur Umsetzung, zum Rollout und zur Veränderung der TCB müssen damit selbstevident aufgebaut sein und für alle kritischen Änderungen ein Zusammenwirken geeigneter unabhängiger Akteure erfordern.

Den Ausgangspunkt für die kryptographische Absicherung der Prozesse bildet der HCC Root of Trust, ein privater Schlüssel in einem HSM-Cluster beim HCC-Provider. Dieser gewinnt seine Legitimität im Rahmen einer Initialisierungszeremonie, an der hinreichend viele, geeignete und voneinander unabhängige Akteure inkl. der gematik beteiligt sind. Dieser organisatorische Rahmen ist noch zu definieren. Die initiale Zeremonie wird einmal pro HCC-Anbieter durchgeführt und für Dritte nachprüfbar protokolliert. Das Zertifikat des HCC Root of Trust wird von einer hoheitlichen PKI der TI abgeleitet. Die Replikation des Root of Trust auf HSM-Cluster an anderen Standorten wird innerhalb der Zeremonie vorbereitet und nutzt die Mechanismen der verwendeten HSMs oder auch spezifisch dafür entwickelter, gehärteter Erweiterungssoftware.

Die Zeremonie zur Instanziierung eines HCC-Anbieters und seiner Infrastruktur ist darauf ausgelegt, nachfolgende administrative Aktivitäten lückenlos als kryptographisch gesicherte (delegierte) Fortsetzungen der Zeremonie abzubilden. Dies bedeutet insbesondere, dass die im Anschluss erforderliche Bereitstellung von Schlüsselmaterial, Zertifikaten, Softwarekomponenten, Konfigurationen und Policies für den Betrieb von Plattform- und Fachdiensten nicht dem Anbieter der Infrastruktur allein überantwortet und nur mittels organisatorischer Vorgaben abgesichert wird, sondern dass ein

Mehraugenprinzip systematisch als kryptographisch gesicherte Kette von Delegationen als Teil der Plattform umgesetzt wird. Hierzu ist es notwendig, bereits in der Zeremonie die administrativen Möglichkeiten über die des HSM-Clusters hinaus zu erweitern.

Daher wird in der Zeremonie bereits der TDCAS initialisiert, d. h. mit seinem kryptographischen Credential zur Anmeldung am HSM-Cluster ausgestattet und auf diese Weise an den Root of Trust gebunden (Pairing). Wie im Abschnitt 7.2- Attestation des Sicherheitszustands dargestellt, verbindet der TDCAS den Sollzustand des Systems mit den während der Instanziierung von Services gemessenen Istzuständen. Für den sicheren Import der Referenzwerte für den Sollzustand in die Konfigurationsdatenbank muss der TDCAS ihren Signer kryptographisch prüfen können. Der TDCAS wird also bereits in der Zeremonie z. B. mit dem Signer-Zertifikat des TI Verification & Build Service konfiguriert.

## **7.4 Umfang und Grenzen der Initialisierungszeremonie**

Innerhalb der Initialisierungszeremonie für den Root of Trust muss das System genau so weit initialisiert, konfiguriert und mit Identitäten ausgestattet werden, dass im Anschluss Erweiterungen durch verteilt arbeitende Akteure auch von außerhalb der Rechenzentrumsumgebung auf der Grundlage der registrierten Identitäten umgesetzt werden können.

Bei den Erweiterungen bzw. Änderungen handelt es sich um:

- die Registrierung oder Deregistrierung von HCC-Diensteanbietern und HCC-Diensten unter der Aufsicht der gematik,
- die Registrierung oder Deregistrierung von Software-Komponenten zur funktionalen Erweiterung der Plattform,
- die Registrierung oder Deregistrierung von HCC-Hosts und ggf. von anderen Komponenten der TCB. Sie erfolgt durch den HCC-Provider im Zuge der Einbringung solcher Komponenten in die Rechenzentrumsumgebung und mittels abgesicherter Prozesse sowie
- die Registrierung oder Deregistrierung administrativer Identitäten, Rollen und Zuordnungen.

Mit jeder Art von Erweiterung sind Akteure bzw. Rollen verbunden, die als Signer der jeweiligen Registrierungseinträge autorisiert werden müssen. Auch diese (Meta-)Ebene der Autorisierung wird mittels signierter Einträge im Policy Administration System für HCC (als Teil des TI Design & Configuration Repositories) realisiert.

## **7.5 HCC Plattform Services**

Im Folgenden werden die Dienste der HCC-Plattform dargestellt, die für die Bereitstellung der Software- und Konfigurationsartefakte der TCB von HCC sowie für die Instanziierung der HCC-Services benötigt werden. Sie stellen im Verbund sicher, dass nur gültig autorisierte und konfigurierte Software auf HCC-Hosts ausgeführt wird.

Aus logischer Sicht könnten alle Änderungen an der HCC-Plattform über ein einziges Repository gesteuert werden. Dies erscheint jedoch weder aus technischer noch aus betrieblicher oder organisatorischer Sicht sinnvoll. Daher werden die verschiedenen Arten der Erweiterung auf einen Satz von Basisdiensten verteilt. Diensttypen sind jeweils einem an der Bereitstellung der Plattform beteiligten Akteur zugeordnet. Wenn Diensttypen keinem Akteur zugeordnet sind, dann sind sie oder ihre Inhalte durch die Inhalte anderer



Dienste vollständig definiert. Die Dienste sind entweder der HCC-Runtime oder der HCC-Designtime zugeordnet.

**HCC Runtime Services** sind Teil jeder Laufzeitumgebung, d. h. sie werden in jeder Rechenzentrums-Location instanziiert, um die Verfügbarkeit aller weiteren Dienste abzusichern. Sie werden vom HCC-Provider als Teil seines HCC-Angebots bereitgestellt. Ihre Bereitstellungs- und Betriebskosten werden nutzungsbezogen durch die HCC-Mandanten getragen, auch wenn sie aus Gründen der Governance in einem der gematik zugeordneten Mandantenkontext betrieben werden.

**HCC Designtime Services** sind einmalige Dienste zur Steuerung administrativer Prozesse der HCC-Plattform. Sie können im Auftrag der gematik bei einem der HCC-Provider betrieben werden. Änderungen, die sich auf die Laufzeitumgebungen beziehen, müssen ausgehend von diesen Systemen auf die Runtime Services verteilt werden.

Die folgende Abbildung liefert einen Überblick über die Services, ihre Zuordnung zur Runtime bzw. zur Designtime sowie die wichtigsten Beziehungen zwischen den Services:

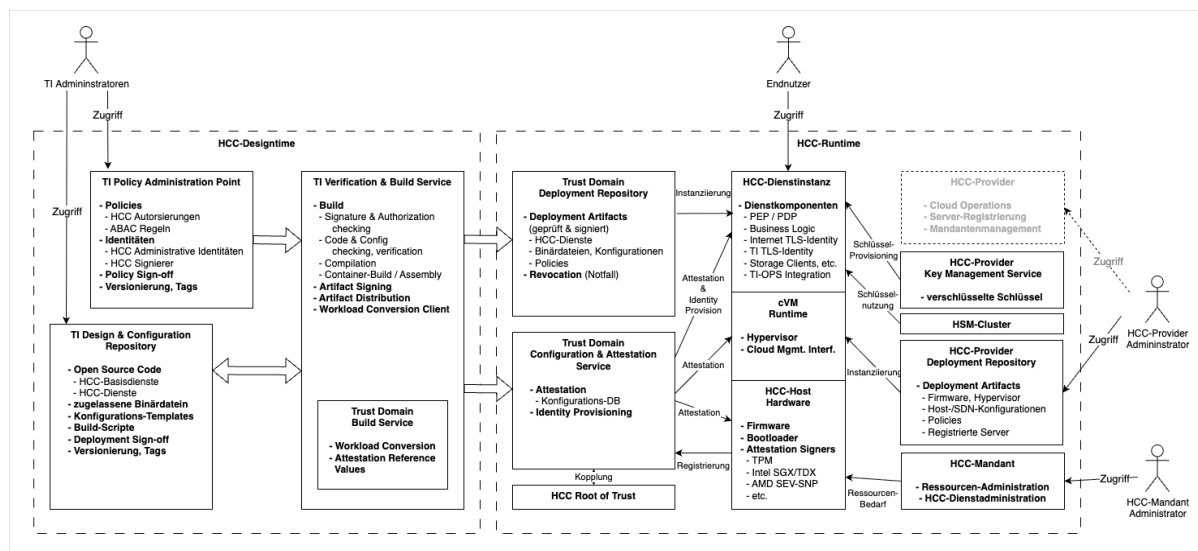


Abbildung 7: HCC-Services in Designtime- und Runtime-Umgebung

### 7.5.1 HSM-Cluster (Runtime)

Der Vertrauensanker für HCC in der jeweiligen Infrastruktur eines HCC-Providers liegt in einem standortübergreifend synchronisierten HSM-Cluster mit mehreren HSM-Appliances pro Location. Er ist Basis des HSM-Service für HCC, der neben dem Vertrauensanker weitere kryptographische Operationen bereitstellt.

Der HSM-Cluster kann Funktionen für Trust Domains außerhalb von HCC oder der TI übernehmen, solange eine Partitionierung sicherstellt, dass der HSM-Service für HCC exklusiv unter der HCC-Governance liegt.

Der HSM-Service wird für die Verwaltung des Vertrauensankers und weiteren Schlüsselmaterials im Kontext der HCC-Plattform oder der HCC-Dienste genutzt. Der Zugriff auf den Cluster durch eine HCC-Dienstinstanz erfolgt immer lokal innerhalb des Rechenzentrums, in dem sie läuft.

Um die Vertrauenskette auch remote bis auf den Vertrauensanker zurückverfolgen zu können, sollen HSMs eingesetzt werden, die Key Attestation für die im HSM-Cluster verwalteten asymmetrischen Schlüssel unterstützen. Hiermit wird insbesondere auch nachvollziehbar, dass die Verwaltung der wichtigsten Schlüssel der Einflussnahme durch

den HCC-Provider entzogen ist, da der Vertrauensanker für die Key Attestation beim unabhängigen Hersteller der HSMs liegt.

Die Nutzung des HSM-Clusters durch HCC-Dienste wird z. B. mittels einer Client-Library zur Integration in das Workload-Image realisiert. HCC-Diensthersteller müssen solche Client-Libraries in ihre Workloads integrieren können (operativ und rechtlich). Alternativ kann ein separat als HCC-Dienst betriebener HSM-Proxy zum Einsatz kommen, der es ermöglicht, HCC-Dienste ohne Integration einer ggf. vom HSM-Hersteller abhängigen Client-Library zu entwickeln und der gleichzeitig eine Abstraktion über herstellerspezifische funktionale Merkmale von HSMs bieten kann.

## **7.5.2 Trust Domain Configuration & Attestation Service (Runtime)**

Während der Root of Trust HSM-Cluster mit den im Rahmen der Zeremonie initialisierten und personalisierten Smartcards der HSM-Administratoren den ersten Ring der TCB bildet, stellt der Trust Domain Configuration & Attestation Service (TDCAS) den zweiten Ring dar. Seine Initialisierung und das Pairing mit dem HSM-Cluster bilden den zweiten Schritt im Bootstrapping des Vertrauensraums.

Das Pairing des TDCAS mit dem Root of Trust basiert auf der Einrichtung von Credentials in den TDCAS auf dedizierten TDCAS-Hosts. TDCAS-Hosts können damit eine Untergruppe der HCC-Hosts darstellen, aber auch als HSMs mit TDCAS-Funktionalität ausgeführt sein. Der TDCAS wird als Confidential Service ausgeführt. Die Credentials werden als Sealed Secrets, d. h. mittels eines in der Hardware verankerten Schlüssels verschlüsselt, durch den TDCAS gespeichert, so dass sie nach einem Neustart des TDCAS-Hosts und des TDCAS-Dienstes wieder verfügbar sind. Das Sealing berücksichtigt die Werte aus dem Measured Boot Process, so dass die Credentials nur dann wiederhergestellt werden können, wenn dieselbe Software auf demselben Host gestartet wurde. Key Rolling und Update der Software werden durch einen darauf aufbauenden Mechanismus unterstützt.

Bei den auf diese Weise in den TDCAS eingebrachten Credentials handelt es sich in erster Linie um Authentisierungsschlüssel für den HSM-Cluster bzw. für dort eingerichtete Rollen. Je nach genauer Ausgestaltung des Aufbaus des Vertrauensraums kann jedoch auch Schlüsselmaterial dazugehören, das es dem TDCAS ermöglicht, Credentials für den HSM-Zugriff für andere Dienste zu generieren.

Zu den für den Attestationsdienst notwendigen Konfigurationsdaten gehören das Sub-CA-Zertifikat für die Ausstellung der HCC-Dienstidentitäten sowie die kryptographische Identität des vom TI Verification & Build Service verwendeten Signers der vom TDCAS benötigten Attestations-Referenzdaten zur Prüfung der Authentizität dieser Daten. Das Schlüsselpaar des Sub-CA-Zertifikats wird während der Zeremonie im HSM-Cluster erzeugt, von einer Sub-CA der Komponenten-PKI der TI zertifiziert und dem TDCAS zugänglich gemacht. Das Zertifikat des TI Verification & Build Service wird während der Zeremonie eingebracht. Die Gesamtheit der für die Zeremonie erforderlichen Zuordnungen von Signer- und Service-Identitäten zu Autorisierungen bilden die initiale Policy der HCC-Plattform für den HCC-Provider.

Der TDCAS und Repliken seiner Konfigurationsdatenbank werden in alle Rechenzentrumsstandorte des HCC-Providers verteilt. Der TDCAS in einer Location kann nur HCC-Workloads in derselben Location attestieren.

Je nach eingesetztem CC-Stack kann die spätere Attestation der HCC-Dienste verschiedene Formen annehmen. Im Beispiel der Nutzung von Intel TDX in Kombination mit einem TPM werden folgende Schritte durchlaufen:

- Der TDCAS wird von jedem HCC-Host zunächst nach Beendigung der Bootphase kontaktiert. Er erhält die vom TPM des Hosts signierten Werte aus dem Measured Boot Process und prüft diese gegen registrierte Referenzwerte in seiner

Konfigurationsdatenbank (die aus dem TI Design & Configuration Repository stammen und ggf. auch aus der Host Registry des HCC-Providers), um festzustellen, ob der Host mit zulässiger Firmware und einem zulässigen Boot Image inkl. aller für den Betrieb als cVM-Runtime erforderlichen Software-Komponenten gestartet wurde.

- Wenn das der Fall ist, wird angenommen, dass weiteres Laden von Software-Komponenten, z. B. das Laden der cVM-Images, von einer bekannten und vertrauenswürdigen Software-Komponente auf dem Host ausgeführt wird, so dass nur korrekt signierte cVMs gestartet werden. Hierdurch wird sichergestellt, dass auf HCC-Hosts keine unbekannte Software gestartet werden kann.
- Downgrade-Angriffe werden mit der nächsten Stufe, der Attestation, abgewehrt. In dieser Stufe kontaktiert jeder HCC-Dienst nach seinem Start den TDCAS erneut, um die vom registrierten TDX-Signer-Key des Hosts der cVM signierten Attestation Reports gegen Referenzwerte für cVMs prüfen zu lassen. Im Erfolgsfall provisioniert der TDCAS die Service-Identitäten für die cVM bzw. die Access Credentials für die entsprechenden Funktionsaufrufe im HSM-Cluster. Hierbei handelt es sich um das HCC-interne TLS-Zertifikat für die Service-to-Service Kommunikation sowie, falls der Service aus dem Internet erreichbar ist, ein TLS-Zertifikat aus einer öffentlichen CA. Mit dem HCC-internen TLS-Zertifikat fungiert der TDCAS als Sub-CA einer hoheitlichen PKI der gematik für die Services von HCC.

Eine derzeit noch ungelöste Schwierigkeit für die Umsetzung des kombinierten Attestationsverfahrens für Host und cVMs auf dem Host besteht darin, dass die Virtualisierung mittels cVMs gerade verhindern soll, dass cVMs (genau wie normale VMs) die Spezifika der darunterliegenden Hardware-Plattform kennen müssen bzw. direkt ermitteln können. Bei einer möglichen Umsetzung mittels eines vom Hypervisor gestarteten Moduls mit lokaler Netzwerkschnittstelle ergibt sich ein Angriffsszenario durch einen manipulierten Hypervisor, der Anfragen an das eigene TPM an einen anderen Host mit korrektem Hypervisor weiterreicht und der cVM mit dessen Rückgabewerten einen eigenen zulässigen Zustand bestätigt (Kuckucksangriff).

Es wird davon ausgegangen, dass sich eine geeignete Konstruktion mittels der Registrierung der individuellen Signer-Keys für die TPMs und die cVMs aller HCC-Hosts (genutzt durch den TDCAS) sowie mit geeigneter Ausgestaltung eines TPM-Attestierungsmoduls umsetzen lässt. Da diese Konstruktion jedoch eng mit den betrieblichen Gegebenheiten des jeweiligen HCC-Providers abgestimmt sein muss, wird hierfür derzeit keine technische Vorgabe gemacht. Eine Konkretisierung wird im Rahmen der ersten Umsetzungen bei HCC-Providern erfolgen.

Der TDCAS muss eine Schnittstelle für den Empfang von Konfigurationsdaten aus dem TI Verification & Build Service anbieten.

### **7.5.3 Key Management Service (Runtime)**

Der Key Management Service (KMS) übermittelt verschlüsseltes Schlüsselmaterial zwischen HCC-Dienstinstanzen. Der mit der HCC-Plattform direkt verknüpfte Anwendungsfall ist die HCC-Host-individuelle Bereitstellung von dienst- bzw. anwendungsspezifischen Schlüsseln. Der KMS kann jedoch auch für weitere anwendungsspezifische Zwecke seitens der Workload-Hersteller genutzt werden.

Das vom KMS vorgehaltene und übermittelte Schlüsselmaterial ist für diesen selbst nicht zu entschlüsseln. Weil der KMS nur mit verschlüsseltem Schlüsselmaterial arbeitet, gehört er nicht zur TCB. Es muss trotzdem sichergestellt sein, dass (verschlüsseltes) Schlüsselmaterial nur innerhalb der für HCC qualifizierten Rechenzentrumsumgebungen verwaltet wird und diese nicht verlässt.

1286 Workloads verwenden den KMS des HCC-Providers entweder mittels einer Remote-API  
1287 oder mittels einer lokal eingebundenen Library. Eine Provider-übergreifende  
1288 Standardisierung dieser Schnittstellen ist derzeit nicht vorgesehen.

#### 1289 **7.5.4 Trust Domain Deployment Repository (Runtime)**

1290 Das Trust Domain Deployment Repository enthält die Binaries der Software-Komponenten  
1291 für Core Services, Anwendungsdienste und Dienstkomponenten inkl.  
1292 Konfigurationsschemata in signierter Form. Den Großteil dieser Artefakte bilden die  
1293 Workload Images für HCC-Dienste. Die Software-Komponenten können in mehreren zum  
1294 jeweiligen Zeitpunkt für den Einsatz freigegebenen Versionen vorliegen. Das Deployment  
1295 Repository bietet Funktionalitäten für die Steuerung der Deployment-Lifecycles, z. B. für  
1296 eine Revokation im Notfall.

1297 Das Trust Domain Deployment Repository kann auch als Policy Hub dienen und dann alle  
1298 für eine HCC-Umgebung benötigten Policies für die Zero Trust Komponenten und den  
1299 TDCAS in der Laufzeitumgebung als signierte und gebündelte Artefakte bereitstellen. Es  
1300 empfängt alle Änderungen an Policies vom Policy Administration Point der TI.

1301 Das Trust Domain Deployment Repository gehört nicht zur TCB, da die Gültigkeit der  
1302 Artefakte über Signaturen abgesichert wird. Es muss jedoch gegen unautorisierte  
1303 Einträge geschützt sein, um seine Funktionsfähigkeit zu schützen und jederzeit den  
1304 gültigen Stand der Deployment-Basis von HCC abzubilden. Es kann als Teil des  
1305 Deployment Management Systems des HCC-Providers (HCC-Provider Deployment  
1306 Repository) umgesetzt sein, muss dann jedoch eine prüfbare Abgrenzung zwischen  
1307 Artefakten für den Vertrauensraum der TI und anderen Artefakten umsetzen, um den  
1308 Schutz der Funktionsfähigkeit gewährleisten zu können und um HCC-spezifische Abfragen  
1309 zu ermöglichen.

1310 Das Trust Domain Deployment Repository hat Repliken an allen  
1311 Rechenzentrumsstandorten des HCC-Providers, um ein performantes Deployment der  
1312 Dienste ohne externe betriebliche Abhängigkeit zu ermöglichen. Nur die beim jeweiligen  
1313 HCC-Provider nutzbaren Artefakte aus dem HCC-Gesamtportfolio der TI müssen in der  
1314 jeweiligen (selektiven) Replik vorhanden sein.

1315 Das Trust Domain Deployment Repository muss eine Schnittstelle für den TI Verification &  
1316 Build Service bereitstellen, über die Deployment-Artefakte eingebracht werden können.

#### 1317 **7.5.5 HCC-Provider Deployment Repository (Runtime)**

1318 Das HCC-Provider Deployment Repository ist der (logische) Teil des betrieblichen  
1319 Steuerungssystems des HCC-Providers, der die Software-Komponenten und  
1320 Konfigurationen zur Bereitstellung der HCC-Laufzeitumgebungen sowie die  
1321 Registrierungsdaten für alle beim HCC-Provider eingesetzten HCC-Hosts umfasst. Es kann  
1322 durch verschiedene Systeme des HCC-Providers realisiert sein, wird von ihm verwaltet  
1323 und gehört nicht zur unmittelbaren TCB.

1324

#### 1325 **7.5.6 TI Policy Administration Point (Design-time)**

1326 Der TI Policy Administration Point stellt das Verwaltungssystem für die Policy des  
1327 Vertrauensraums im Kontext der Zero Trust Architektur für HCC dar.

1328 Der TI Policy Administration Point stellt alle Funktionalitäten zur Administration der Policy  
1329 der HCC Trust Domain inkl. der Abgrenzung von Teilen der Policy, Delegation von

Verantwortlichkeiten für die abgegrenzten Teile und integritätsgeschützter Änderungsverfolgung bereit. Er ist so strukturiert, dass er den an der Verwaltung der Policy beteiligten Akteuren ihre jeweilige Sicht auf die Policy ermöglicht und er unterstützt den Sign-off von Policies mittels Multi-Party-Signaturen, bspw. Threshold Signature Schemes.

Der TI Policy Administration Point enthält Registrierungsdaten für alle Identitäten menschlicher oder institutioneller Akteure oder Dienste, die an der Verwaltung der HCC Trust Domain beteiligt sind. Er enthält nicht die Registrierungsdaten der Endnutzeridentitäten der TI oder der an den fachlichen Prozessen der TI beteiligten Institutions- oder Organisationsidentitäten. Diese werden durch TI Identity Provider bereitgestellt und in Policies nur genutzt oder referenziert. Spezifisch für HCC bilden Policies auch die Identitäten der Hosts und Workloads (auf Basis ihrer gemessenen Hash-Werte) sowie deren Zugriff auf Schlüssel und Schnittstellen ab. Attribute based Access Control wird auf diese Weise auch auf die Steuerung des HCC-Vertrauensraums angewendet.

Der TI Policy Administration Point bietet die Administrationsfunktionalität für die Verwaltung der für HCC und Zero Trust benötigten Identitäten, Rollen und Zuordnungen, wird initial mit den Identitäten der an der Zeremonie teilnehmenden Personen sowie dem Root of Trust Public Key und den Public Keys der Core Services befüllt und bildet die Kette der Verantwortlichkeiten für jede Operation (z. B. Registrierung einer neuen Identität) dadurch ab, dass nur von registrierten und (via Policy) autorisierten Autoren und Reviewern signierte Einträge akzeptiert werden. Alle Veränderungen werden auditfähig versioniert.

Der TI Policy Administration Point ist ein Dienst der gematik. Er wird von der gematik verantwortet, entwickelt und weiterentwickelt. Er ist daher nicht Gegenstand der Zulassung von HCC-Providern, jedoch notwendig für das Verständnis und das Funktionieren der Sicherheitsarchitektur von HCC und daher hier dargestellt.

### **7.5.7 TI Design & Configuration Repository (Designtime)**

Das TI Design & Configuration Repository enthält den Quellcode von Plattformdiensten und von Open Source Anwendungsdiensten inkl. Build Scripts, Revision Tags und Konfigurationsschemata für Software-Komponenten, die für Laufzeitumgebungen konfiguriert werden müssen, sowie weitere Software-Artefakte. Es enthält daneben auch binäre Artefakte, z. B. Dienst-Software, die unabhängig begutachtet und auf dieser Grundlage durch die gematik zugelassen wurden.

Das TI Design & Configuration Repository bietet Code Management Funktionalität inkl. Review und Sign-off im Mehraugenprinzip. Es basiert auf einer Git-Versionsverwaltung und bietet die Möglichkeit externe Quellen einzubinden. Commits, Tags und Imports sind nur mit Signatur eines in der Trust Domain registrierten und autorisierten „Importeurs“ gültig. Der „Importeur“ kann selbst ein Dienst sein. Auch Komponenten, die nur in binärer Form zur Verfügung stehen, werden über das Repository mittels autorisiertem (signiertem) Import registriert und damit verfügbar gemacht.

Das TI Design & Configuration Repository bildet, gemeinsam mit dem im folgenden Absatz dargestellten TI Verification & Build Service, die Grundlage für sichere Zulassungs- und ggf. auch Entwicklungsprozesse für HCC-Dienste. Die Entwicklungsprozesse waren bisher den Anbietern oder Herstellern von Diensten überlassen. Aufgrund der Shared Responsibility und des Charakters von HCC als Plattform sowie im Sinne der Open Source Strategie ist es notwendig, sichere (Teil-)Entwicklungsprozesse auch als Teil der Plattform zu verankern. Sie werden zunächst in einem funktional wie organisatorisch einfachen Modell umgesetzt und später verfeinert und ausgebaut.



Das TI Design & Configuration Repository ist ein einmaliger Dienst der gematik. Es wird von der gematik verantwortet, entwickelt und weiterentwickelt. Es ist daher nicht Gegenstand der Zulassung von HCC-Providern, jedoch notwendig für das Verständnis und das Funktionieren der Sicherheitsarchitektur von HCC und daher hier dargestellt. Der Dienst selbst gehört nicht zur TCB, muss jedoch gegen unautorisierte Einträge geschützt sein, um seine Funktionsfähigkeit zu schützen und jederzeit den gültigen Stand der Code-Basis der HCC-Services abzubilden.

## **7.5.8 TI Verification & Build Service (Designtime)**

Der TI Verification & Build Service besteht aus Build-Diensten, die Software-Artefakte aus dem TI Design & Configuration Repository und dem TI Policy Administration Point verifizieren, bauen und als signierte Container Images, Binaries, Konfigurationsdateien oder Policy Sets in die Trust Domain Deployment Repositories und die Trust Domain Configuration & Attestation Services verteilen. Builds führen über die eingeflossenen Quellen Buch und sind im besten Fall (Bit für Bit) reproduzierbar. Quelldateien werden vor der Verwendung auf valide Signaturen von für das jeweilige Artefakt autorisierten Identitäten geprüft.

Im Zuge des Builds werden Verfahren zur automatisierten Prüfung und Verifikation der Quellen eingesetzt. Prüf- und Verifikationscode wird selbst als Quelle interpretiert. Es kommen für die verwendeten Sprachen relevante Compiler, Checker und Build-Tools zum Einsatz. Der TI Verification & Build Service besteht daher aus einer Mehrzahl von Services, die in ihrer Gesamtheit und im Zusammenspiel das Build System der Plattform darstellen. Damit sind auch die Provider-spezifischen Trust Domain Build Services (siehe 7.5.9- Trust Domain Build Service (Designtime)) Teil des TI Verification & Build Service.

Referenzwerte für Binaries und Konfigurationen werden durch den Build Service (bzw. durch eingebundene Trust Domain Build Services) in einer Form erzeugt, die für den Abgleich mit den Messwerten während des Starts der jeweiligen Dienste geeignet sind. Dazu werden die Measured Boot Hash-Werte z. B. durch Instanziierung in einer vertrauenswürdigen Mess-cVM und Erzeugung des Attestation Reports (oder mittels eines anderen geeigneten Tools zur Bestimmung derselben Werte) ermittelt und anschließend signiert.

Der TI Verification & Build Service ist ein einmaliger Dienst in der Verantwortung der gematik. Der Dienst gehört zur TCB. Er erfordert daher eine Begutachtung durch eine qualifizierte und unabhängige Stelle. Er wird als Confidential Service mit einer Signer-Identität betrieben, die während einer Zeremonie erstellt wird, die den Start der HCC Trust Domain markiert. Die Zeremonie wird bei dem HCC-Provider durchgeführt, bei dem die Designtime-Dienste betrieben werden, hat aber einen HCC-Provider-unabhängigen Charakter.

Der TI Verification & Build Service ist nicht Gegenstand der Zulassung von HCC-Providern, jedoch notwendig für das Verständnis und das Funktionieren der Sicherheitsarchitektur von HCC und daher hier dargestellt.

## **7.5.9 Trust Domain Build Service (Designtime)**

Der Trust Domain Build Service ist ein vom HCC-Provider bereitgestelltes Werkzeug zur Konvertierung von Workload Images in die vom HCC-Provider genutzte Confidential-Computing-Technologie bzw. -Lösung und zur Ermittlung der Referenzwerte für die Attestation. Die Konvertierung kann auf einem cVM-Template basieren. Der Dienst kann als Plug-in für den TI Verification & Build Service umgesetzt werden. Standardmäßig wird er via API durch den TI Verification & Build Service angesteuert. Der Trust Domain Build

Service kann von der gematik, von HCC-Diensteanbietern oder von HCC-Workload Herstellern zu Testzwecken auch manuell genutzt werden.

Als Input verarbeitet der Trust Domain Build Service OCI-standardkonforme Container Images.

Der Trust Domain Build Service ist ein einmaliger Dienst je HCC-Provider. Er ist ein HCC-Dienst, weil die Referenzwerte vertrauenswürdig ermittelt werden müssen und um eine manipulationsgeschützte Signer-Identität für den Dienst zu ermöglichen, die seine Verwendung innerhalb von automatisierten Abläufen ermöglicht.

## 7.6 Schlüsselmanagement

Instanzen von HCC-Services benötigen Zugriff auf eine Reihe von Schlüsseln, um Daten beim Transport sowie bei der Speicherung abzusichern. Es wurde bereits dargestellt, dass dieser Zugriff durch den TDCAS bereitgestellt wird und dass dies nur nach einer erfolgreichen Attestation geschieht. Als Quelle des Schlüsselmaterials kommen der HSM-Cluster (Schlüssel verbleiben in den HSMs und werden über Zugriffskontrollierte Schnittstellen genutzt) und der Key Management Service (Schlüssel werden für jeden Ziel-Host individuell verschlüsselt gehalten und übermittelt) infrage. Im Folgenden wird die Bereitstellung von Schlüsselmaterial im Hinblick auf die verschiedenen Einsatzzwecke dargestellt.

### 7.6.1 Öffentliche HCC-Service-Identität

Jede für Clients erreichbare Instanz eines HCC-Service benötigt eine für diese Clients zu authentisierende, Instanz-übergreifende Service-Identität, die an den Zugriff auf den privaten Schlüssel zum TLS-Zertifikat des Service gebunden ist. Es kommen **zwei** Modelle der Bereitstellung infrage:

- Nach erfolgreicher Attestierung wird an die HCC-Service-Instanz ein kryptographisches Zugriffs-Credential übermittelt, mit dem sie TLS-Challenges durch den HSM-Service signieren lassen kann. Das private Schlüsselmaterial zur Service-Identität verbleibt im HSM-Cluster. Der pro Standort bereitgestellte HSM-Cluster muss die Last bewältigen können, die für alle Vorgänge zum Aufbau von TLS-Sessions über alle öffentlich erreichbaren HCC-Services am Standort anfällt. Dies gilt auch, wenn z. B. andere Standorte unerreichbar sind, d. h. im Fall von erhöhter Last beim Failover.
- Nach erfolgreicher Attestierung wird an die HCC-Service-Instanz der private Schlüssel für die Service-Identität übermittelt. Hierbei ist der HSM-Service nur einmal beim Start involviert und es muss eine entsprechend geringere Kapazität bereitgestellt werden. Voraussetzung für dieses Modell der Schlüsselbereitstellung ist das Vorhandensein eines in die HCC-Hosts integrierten kryptographischen Hardware-Moduls, um die privaten Schlüssel der Service-Identitäten aus der Angriffsfläche des CC-Stacks zu entfernen. Die Provisionierung des Schlüsselmaterials muss für den individuellen Host verschlüsselt erfolgen. Das Hardware-Modul muss sicherheitstechnisch zertifiziert sein.
- *Offene dritte Option: Bereitstellung kurzlebiger Service-Identitäten, wie es durch die Konstruktion mit der Sub-CA im TDCAS bereits möglich geworden ist. Welche Gültigkeitszeiträume wären dann angemessen?*

## 7.6.2 TI-Identität von HCC-Services

Für die Service-to-Service Kommunikation innerhalb der Trust Domain werden dienstspezifische Zertifikate aus einer hoheitlichen PKI der TI verwendet. Die Bereitstellung der Schlüssel erfolgt entsprechend der ersten Variante (aus Abschnitt 5.6.1), d. h. die Schlüssel verbleiben im HSM-Cluster. Zwischen Services müssen pro Instanz nur eine begrenzte Anzahl von TLS-Verbindungen aufgebaut werden und diese können mittels Session Resumption aktiv gehalten werden, so dass nur eine vergleichsweise geringe HSM-Last zustande kommt.

## 7.6.3 Session-Cache-Schlüssel

Damit HCC-Dienste hochverfügbar als (zustandsloser) Cluster funktionieren können, müssen die Session-Daten der Nutzer Instanz-übergreifend in einem Shared Cache gehalten werden. Alle Instanzen eines HCC-Dienstes nutzen in einem Standort-übergreifend synchronisierten Cache denselben symmetrischen Schlüssel, so dass jede Instanz von einer anderen Instanz angelegte oder aktualisierte Session-Daten entschlüsseln kann. Das Caching von Session-Daten ist anwendungsspezifisch, d. h. je Typ von HCC-Dienst wird ein eigener Schlüssel verwendet. Session-Cache-Schlüssel müssen in regelmäßigen Abständen getauscht werden.

*Offene Frage: Diese Konstruktion erzeugt eine noch relativ große Angriffsfläche. da jeder Verarbeitungskontext eines Dienstes denselben Schlüssel erhält. Wie könnte hier eine bessere Trennung realisiert werden?*

Der Schlüssel wird je HCC-Host in einer an die Server-Hardware und die Attestation des CC-Stacks (inkl. Anwendung) gebundenen Form – d. h. individuell für diese verschlüsselt – bereitgestellt. Bei der Registrierung von HCC-Hosts durch den HCC-Provider werden deren Hardware-Schlüssel registriert. Bei der Registrierung eines HCC-Dienstes wird ein Schlüssel im HSM-Cluster erzeugt und je registriertem Host verschlüsselt an den Key Management Service exportiert. Für nachträglich hinzugefügte Hosts wird diese Hinterlegung für alle registrierten HCC-Dienste ergänzt.

Der symmetrische Session-Cache-Schlüssel kann zusätzlich nutzer- oder Session-spezifisch ausgestaltet werden. Eine Entscheidung hierzu ist noch zu treffen und sollte sich an bereits erprobten Verfahren orientieren. In diesem Fall wird anstelle eines übergreifend gültigen symmetrischen Session-Cache-Schlüssels vom Key Management Service ein Key Derivation Key an die HCC-Dienstinstanz übergeben, von dem die nutzer- oder Session-spezifischen symmetrischen Schlüssel lokal abgeleitet werden können, indem Nutzer- bzw. Session-Identifizier als Parameter für die Schlüsselableitung verwendet werden.

*Offene Frage: Ist das wirklich eine bessere Lösung? Lässt sie sich ohne große Komplikationen umsetzen?*

## 7.6.4 Persistenz-Schlüssel

Daten, die aus dem Verarbeitungskontext einer HCC-Dienstinstanz an ein System zur Persistierung der Daten übergeben werden, müssen mittels eines symmetrischen Schlüssels geschützt werden. Dieser Schlüssel ist spezifisch für den HCC-Dienst und ggf. für den Daten-Owner. Daten-Owner-spezifische Schlüssel werden generiert, wenn der Daten-Owner den HCC-Dienst erstmalig nutzt. Jede Instanz desselben HCC-Dienstes muss den Schlüssel rekonstruieren oder anderweitig (wieder)erlangen können, um nachfolgende Requests desselben Nutzers verarbeiten zu können.



Die Persistenz-Schlüssel (ggf. Master Keys für eine Schlüsselableitungsfunktion) werden vom Key Management Service bereitgestellt. Sie sind mittels eines vergleichbaren Mechanismus geschützt wie die Session-Cache-Schlüssel, d. h. im KMS an die registrierte Server-Hardware gebunden verschlüsselt sowie ggf. als Key Derivation Keys ausgelegt.

Da Persistenz-Schlüssel nicht ohne Umschlüsselung persistierter Daten (mindestens datensatzspezifischer Schlüssel) getauscht werden können, sollen sie jeweils auf Daten eingeschränkt sein, die innerhalb eines anwendungsspezifisch festgelegten, begrenzten Zeitintervalls gespeichert werden. Die Rekonstruktion des jeweils benötigten Schlüssels im Verarbeitungskontext des HCC-Dienstes erfolgt auf der Basis von unverschlüsselt mit den Daten persistierten Zeitstempeln als Parameter für eine Schlüsselableitungsfunktion.

## **7.7 Ausschluss der Betreiber und anderer Angreifer**

Eine wesentliche Eigenschaft von Healthcare Confidential Computing besteht darin, nicht nur externe Angreifer, sondern auch alle beteiligten Betreiber vom Zugriff auf die verarbeiteten sensiblen Daten auszuschließen. Als Betreiber gelten in diesem Zusammenhang der Infrastrukturanbieter (Cloud Provider, HCC-Provider), der Diensteanbieter, die gematik sowie ggf. ein durch die gematik beauftragter HCC-Plattformanbieter, der den Vertrauensraum HCC-Provider-übergreifend administriert. Die Gesamtheit der technischen Mechanismen sowie der physischen und organisatorischen Rahmenbedingungen, die diese Eigenschaft gewährleisten, wird im folgenden dargestellt.

Die bisher dargestellten Mechanismen der Sicherheitsarchitektur von Healthcare Confidential Computing zielen primär darauf ab, dass die Trusted Computing Base der Laufzeitumgebung zu jedem Zeitpunkt aus wohlbekannten Komponenten aufgebaut ist, die aus einem Prozess mit unabhängiger und TI-übergreifender Governance hervorgehen.

Die sicherheitstechnische Abgrenzung dieser Komponenten von weiteren Komponenten in der Infrastruktur, insbesondere von den Cloud-Management-Komponenten des HCC-Providers, hängt jedoch zusätzlich davon ab, dass die eingesetzte Confidential Computing Technologie eine sichere Isolation der umgesetzten Prozesse gewährleistet.

Die Gesamtsicherheit der Trusted Computing Base der Laufzeitumgebung hängt darüber hinaus davon ab, dass diese Prozesse, d. h. die (fachlichen) Dienste selbst, sicher und spezifikationsgemäß umgesetzt sind.

### **7.7.1 Physische Sicherheit der Rechenzentrumsumgebung**

Die Sicherheitsleistung von kryptographischen Verfahren hängt davon ab, dass die eingesetzten (privaten oder symmetrischen) Schlüssel außerhalb der vorgesehenen Komponenten und Funktionen nicht bekannt werden oder genutzt werden können. Die Sicherheit von Confidential Computing hängt davon ab, dass der in der CPU instanziierte Verarbeitungskontext nicht „belauscht“ werden kann. Eine Extraktion von Schlüsselmaterial oder eine Beobachtung von Verarbeitungen (über physikalische Seitenkanäle) können nicht ausgeschlossen werden, wenn Unberechtigte physische Kontrolle über oder physischen Zugriff auf die verarbeitenden Systeme erlangen können.

„Klassische Rechenzentrumssicherheit“ spielt daher eine weiterhin grundlegende Rolle auch beim Einsatz von Confidential Computing Technologien. Wenn es beim Cloud Computing gängige Auffassung ist, dass es gleichgültig ist, wo eine Verarbeitung stattfindet, dann ist es für Confidential Computing entscheidend, dass die physische Rechenzentrumssicherheit überall sichergestellt ist, wo Verarbeitungen stattfinden können. Dies gilt insbesondere vor dem Hintergrund der Anforderung des Betreiberausschlusses.

Neben der Erfüllung der grundsätzlichen Zertifizierungsanforderungen (siehe Kapitel 9-Zulassungen und Bestätigungen) müssen HCC-Provider daher insbesondere sicherstellen und nachweisen, dass ihre Prozesse zur Einrichtung und Wartung der Infrastruktur ihren damit betrauten Mitarbeitern keine Möglichkeiten für physische Angriffe auf die Vertraulichkeit der Verarbeitungen bieten, die nicht zuverlässig und kurzfristig erkannt und mitigiert werden.

Ähnlich zum Gebot der Minimierung der TCB gilt hier das Gebot der Minimierung von physischer Präsenz in der Rechenzentrumsumgebung. Darüber hinaus müssen alle Aktivitäten in der physischen Rechenzentrumsumgebung aufgabenbezogen organisiert und organisatorisch unabhängig überwacht werden. Geeignete Schleusen müssen verhindern, dass unzulässige Mittel durch Mitarbeiter in die Rechenzentrumsumgebung eingebracht werden können.

## **7.7.2 Isolation von Mandanten im Netz**

Ein wesentlicher Faktor der Sicherheit von Cloud-Infrastrukturen ist die Isolation der Dienste verschiedener Mandanten auf der Ebene des Netzwerks. Jeder Mandant existiert zunächst in einem eigenen Software Defined Network. Die grundlegende Einrichtung pro Mandanten ist automatisiert und kann im Anschluss durch den Mandanten selbst erweitert und konfiguriert werden, wobei die Einstellungsmöglichkeiten des Mandanten derart eingeschränkt sind, dass die Mandantenisolation für alle anderen Mandanten erhalten bleibt, selbst wenn der Mandant Dienste erreichbar macht.

Änderungen an der Netzwerkkonfiguration werden u. a. implizit ausgelöst, wenn der Mandant Services des Cloud-Anbieters hinzubucht. Hierbei sind sowohl die buchbaren Services als auch die Mechanismen zum Hinzubuchen so umgesetzt, dass die Mandantentrennung erhalten bleibt. Im Falle von Cloud-native Services ist dabei evtl. ein Übergang von der Trennung auf Netzwerkebene zur Trennung auf Anwendungsebene erforderlich.

Die Systeme und Mechanismen zur Mandantentrennung in der Infrastruktur eines HCC-Providers werden nicht unmittelbar zur Trusted Computing Base von HCC gerechnet. Die Sicherheit auf Netzwerkebene ist jedoch eine wichtige Voraussetzung dafür, dass die Verfügbarkeit der HCC-Dienste gewährleistet werden kann. Es wird daher vorausgesetzt, dass eine wirksame Mandantentrennung umgesetzt ist. Die Prüfung dieser Voraussetzung erfolgt im Rahmen der grundlegenden Zertifizierung des HCC-Providers (gemäß Kapitel 9-Zulassungen und Bestätigungen). Weitergehende Anforderung müssen im Rahmen der vorliegenden Spezifikation nicht gestellt werden.

## **7.7.3 Prozessisolation**

Confidential Computing Technologie wird als Mittel zur sicheren Auslagerung von Verarbeitungsprozessen an externe Infrastrukturbetreiber vermarktet, u. a., weil sie die Isolation von Daten im Arbeitsspeicher mittels Verschlüsselung garantiert. Insbesondere bei VM-basierten Varianten von Confidential Computing (z. B. Intel TDX oder AMD SEV-SNP) wird jeder VM ein eigener symmetrischer Schlüssel zur Verschlüsselung ihres Arbeitsspeichers zugeordnet, so dass Zugriffe außerhalb der vorgesehenen Speicherbereiche (Out of Bounds Access) durch andere Prozesse keine verwertbaren Daten der Confidential VM offenlegen. Der kryptographische Speicherschutz besteht zudem auch gegenüber privilegierten Prozessen, wie dem Betriebssystem oder dem Hypervisor.

Der auf diese Weise zu erreichende Isolationsgrad hat seine Grenzen darin, dass alle Prozesse auf einer CPU (oder GPU, etc.) auf gemeinsame Ressourcen zur Optimierung der Performance zurückgreifen, die sowohl in der zeitlichen Dimension als auch bzgl. ihrer

Speicheranforderungen charakteristische Muster offenbaren können, die von Prozessen außerhalb der Confidential VM beobachtet und zur Extraktion von Geheimnissen genutzt werden können. Solche Angriffsmöglichkeiten werden seitens der Prozessorhersteller als Schwachstellen behandelt und – meist unter Inkaufnahme von Performanceverlusten – mittels Firmware- oder Microcode-Updates geschlossen. Sie sind jedoch schwer prinzipiell auszuschließen, da Mechanismen zur Steigerung der Performance der Prozessoren ihren eigenen komplizierten Logiken folgen und meist auf der Einführung zusätzlicher prozessübergreifend geteilter Hardware-Ressourcen beruhen.

Vor diesem Hintergrund werden die Garantien hinsichtlich der Prozessisolation von Confidential Computing Technologien für HCC nur mit gewissen Einschränkungen als gegeben angesehen. Insbesondere der Betreiberausschluss erfordert, dass die Sicherheitsarchitektur auf hochprivilegierte potenzielle Angreifer ausgerichtet sein muss.

Es werden zwei Szenarien unterschieden:

- Angriffscode aus dem Anbieterkontext könnte versuchen Seitenkanäle auszunutzen, um Schlüsselmateriale oder sensible Nutzdaten aus der Confidential VM zu extrahieren. Insbesondere solcher Code kann auch privilegiert sein und z. B. Mechanismen zur Aufdeckung von Angriffen (die z. B. auf Behavioral Analyses basieren) unterlaufen.
- Angriffscode, der innerhalb anderer Confidential VMs (anderer Mandanten) läuft, könnte versuchen Seitenkanäle auszunutzen, um Schlüsselmateriale oder sensible Nutzdaten aus der Confidential VM zu extrahieren.

Die Ausnutzung von Seitenkanal-Schwachstellen ohne eine Ausführung von Angriffscode auf dem Zielsystem erscheint nahezu unmöglich, weil nur Code auf dem Prozessor die erforderlichen Beobachtungen machen oder den „Opferprozess“ gezielt stören kann. Ein entsprechender Angriff müsste Schwachstellen und sog. "Gadgets" in einer auf demselben Prozessor ausgeführten Software-Komponente ausnutzen, um seinen Angriffscode „on the fly“ zu generieren. Es wird angenommen, dass dies durch Härtung sowohl der HCC-Systemsoftware als auch der HCC-Dienstsoftware hinreichend abgewehrt wird.

Angesichts des sehr hohen Schutzbedarfs der in der TI verarbeiteten Daten ist es ein Ziel von HCC, die beiden genannten Angriffsszenarien über Seitenkanäle systematisch auszuschließen.

Angriffe aus Confidential VMs auf demselben Prozessor können zuverlässig dadurch ausgeschlossen werden, dass keine Kunden-Workloads geladen werden dürfen bzw. können, die nicht zum Vertrauensraum von HCC gehören. Für Workloads aus der HCC Trust Domain kann angenommen bzw. gefordert werden, dass sie hinreichend gründlich geprüft sind, um Angriffscode zur Ausnutzung von Seitenkanalangriffen auszuschließen. HCC-Hosts müssen daher so konfiguriert sein, dass sie kein Deployment von Nicht-HCC-Workloads zulassen.

Diese Anforderung schränkt den HCC-Provider in seiner Flexibilität bei der Verteilung von Workloads ein. HCC-Hosts sollen jedoch keine dauerhaft exklusiv bereitgestellten Server sein, sondern Server, die durch "Starten als HCC-Hosts" bei Bedarf zum Pool von HCC-Hosts hinzugefügt werden können und durch Neustart auch wieder aus dem Pool entfernt werden können. Darüber hinaus kann ein HCC-Host HCC-Workloads verschiedener HCC-Mandanten ausführen und damit als geteilte Ressource innerhalb der HCC-Trust-Domain verwendet werden. Der HCC-Provider muss sein Cloud-Management mit der Fähigkeit ausstatten, HCC-Hosts als HCC-exklusive aber HCC-Mandanten-übergreifend nutzbare Ressourcen zu konfigurieren und zu provisionieren. Er muss ein Abrechnungsmodell für ihre Nutzung anbieten, das der gemeinsamen Nutzung der Ressourcen durch seine Mandanten und der bedarfsgesteuerten Provisionierung der HCC-Hosts in den Vertrauensraum Rechnung trägt.

Für den Ausschluss von Angriffscodes des HCC-Providers kommen verschiedene Möglichkeiten infrage:

- Der HCC-Provider kann seinen CC-Stack offenlegen und damit einer Begutachtung durch beliebige unabhängige Dritte zugänglich machen. Gerade in Verbindung mit der Attestation kann hierdurch weitgehende Transparenz geschaffen und die Vertrauenswürdigkeit gesteigert werden.
- Der HCC-Provider kann seinen CC-Stack durch einen akkreditierten Gutachter prüfen lassen und das Gutachten der gematik zu Prüfung vorlegen.
- Der HCC-Provider kann seine Cloud-Management-Funktionen auf eine vom Workload-Prozessor unabhängige Komponente auslagern. Solche Komponenten werden z. B. als „Infrastructure Processing Units“ (IPU) bezeichnet. Sie verfügen über einen eigenen Prozessor und ggf. weitere Komponenten zur Beschleunigung von Netzwerkfunktionen und können anstelle von SmartNICs eingesetzt werden. Auf dem Workload-Prozessor verbleibt dann z. B. lediglich ein Hypervisor, d. h. eine besonders kleine, gut gehärtete und ggf. Open Source Komponente.

Jede der dargestellten Möglichkeiten bringt ihre eigenen Trade-offs mit sich.

Die Auslagerung der Cloud-Management-Funktionen auf eine IPU erhöht die Hardware-Kosten pro HCC-Host und erfordert angepasste Betriebssoftware, stellt aber ein von der Art des Workload-Prozessors unabhängiges Isolationsmuster dar, das daher auch für zukünftig relevante Prozessortypen, z. B. für die Verarbeitung von KI-Workloads, nutzbar bleibt und lässt dem HCC-Provider die größte Freiheit in der Gestaltung, Pflege und Geheimhaltung seines Cloud-Management-Systems. Die Nutzung von IPU ist derzeit (jenseits der Hyperscaler) nicht sehr verbreitet. Sie bietet sich jedoch längerfristiger als Standard für HCC an.

#### **7.7.4 Sichere Hardware-Komponenten der Runtime TCB**

Jede Komponente der Trusted Computing Base von HCC hat das Potenzial, bei fehlerhafter Umsetzung die Garantien von HCC zu kompromittieren. Die TCB von HCC muss daher mit großer Sorgfalt entwickelt werden.

Für die Hardware-Komponenten der TCB inkl. ihrer Firmware ist eine geeignete Wahl sowohl des Herstellers als auch der spezifischen Komponenten zu treffen. Aufgrund der geringen Zahl von Herstellern von Server-CPU mit Confidential Computing Funktionen und der gleichzeitig großen Verbreitung der Komponenten dieser Hersteller ist ein gewisses Vertrauen gerechtfertigt, dass diese Hersteller keine dedizierten Backdoors in ihre Systeme integrieren. Dieses Vertrauen erstreckt sich auch auf die Firmware der Systeme.

Damit können und sollen die für Confidential Computing bereitstehenden Online-Services der Hersteller zur Bestätigung der Authentizität der Komponenten (insb. Attestation der CPUs) genutzt werden, um den lokalen Vertrauensanker der HCC-Hosts abzusichern. Hierbei ist ein Verfahren zu wählen, dass zur Laufzeit keine direkte Verbindung der Attestation Services der CPU-Hersteller zu den attestierten HCC-Hosts benötigt, d. h. ein Verfahren zur Attestation über einen in der Verantwortung des HCC-Providers betriebenen Proxy Service. Die Attestation der CPUs der HCC-Hosts muss nach jedem CPU-Firmware-Update neu durchlaufen werden. Als Ergebnis liegt eine vom CPU-Hersteller signierte Bestätigung für die beim Booten ermittelten Messwerte über die Firmware vor, die als Ausgangspunkt für die lokale Vertrauenskette auf dem jeweiligen Host genutzt wird und dem TI Policy Administration Point bekannt gemacht wird.

Für die Lieferkette muss ausgeschlossen werden können, dass die Komponenten, insbesondere auch ihre Firmware, auf ihrem Weg vom Herstellungsort zum Einsatzort manipuliert werden. Beim Aufbau der Lieferkette sind auch Angriffsmöglichkeiten

feindlich gesinnter Staaten zu berücksichtigen, die aufgrund der Internationalität der Hardware-Märkte gegeben sein können.

Die Attestation mit dem CPU-Hersteller stellt für die Absicherung der Lieferkette von HCC-Hosts eine nur teilweise Lösung dar, weil auch andere Komponenten innerhalb von HCC-Hosts für Angriffe genutzt werden könnten. Technologien zur Attestation aller on-board Systemkomponenten sind derzeit in der Entwicklung, jedoch noch nicht der Regelfall. Die Lieferketten müssen daher noch mit organisatorischen Maßnahmen abgesichert werden, aufbauend auf der Wahl von Systemherstellern mit guter Reputation und eigenem detaillierten Management ihrer Zulieferer sowie ausreichendem Integration Testing.

Lange Lieferketten sind zu vermeiden. Als Mindestanforderungen kommen die für die allgemeine Zertifizierung der HCC-Provider zur Anwendung (siehe 9- Zulassungen und Bestätigungen).

Informationen zur Lieferkette der HCC-Hosts werden im Zuge der Registrierung der HCC-Hosts miterfasst und einer Prüfung und ggf. Beanstandung seitens der gematik zugänglich gemacht.

HCC-Hosts müssen zudem insoweit physisch geschlossene Systeme sein, dass in Verbindung mit den organisatorischen Sicherheitsanforderungen zur Zutrittskontrolle der Rechenzentrumsumgebung ausgeschlossen werden kann, dass HCC-Hosts unbemerkt physisch manipuliert werden können.

### **7.7.5 Sichere Software-Komponenten der Runtime TCB**

HCC-Dienste müssen wirksam gegen Angriffe über ihre bestimmungsgemäßen Schnittstellen gehärtet werden. Der HCC-Workload-Hersteller, sein Gutachter, oder – im Falle von Open Source Software – auch die Allgemeinheit, müssen daher zunächst einmal in der Lage sein, die Widerstandsfähigkeit des Dienstes gegen Angriffe zu beurteilen. Eine solche Beurteilung ist nur möglich, wenn die Komplexität der Workload begrenzt ist. Die erste Regel für die Entwicklung sicherer Software für die TCB von HCC lautet daher, nichts in die Software einzubauen oder darin zu belassen, was nicht benötigt wird.

Insbesondere für VM-basierte Workloads bedeutet dies, ein auf ein Minimum reduziertes Betriebssystem zu verwenden und sämtliche Werkzeuge zu entfernen, die für administrative Zugriffe normalerweise Teil von Betriebssystemen sind. Die Virtualisierung der Netzwerkschnittstelle, mit der die VM-Verbindungen nach außen aufbaut, ermöglicht ggf. die Verwendung eines vereinfachten Treibers. Die statische Natur der attestierbaren Workload-Images kann die Verwendung von Komponenten zur Absicherung von Veränderungen an der Software erübrigen. Eine Nutzung der Linux Integrity Measurement Architecture innerhalb der cVM kann je nach Art der Workload und ihres Lifecycles sinnvoll sein.

Die Cloud ermöglicht Lösungsdesigns, in denen Dienste jeweils nur eine Aufgabe erfüllen. Im Falle von HCC gehören dazu immer die Terminierung des VAU-Protokolls (TLS mit oder ohne ASL-Kanal) und die Verarbeitung von User Credentials zur Prüfung der Berechtigung zur Ausführung eines Requests. Hierfür strebt die gematik im Rahmen der Einführung der Zero Trust Architektur eine Standardisierung an. Für einen Großteil der fachlichen Aufrufe sind Schnittstellenstandards wie JSON/FHIR vorgesehen, so dass auch für das Parsing von Requests gehärtete Open Source Standardkomponenten denkbar sind.

Für die Umsetzung der fachlichen Verarbeitung stehen sichere Programmiersprachen wie Rust zur Verfügung, deren Compiler bereits ganze Klassen von Fehlern vermeidbar machen und damit auch die Begutachtung vereinfachen. Gleichzeitig ist z. B. Rust systemnah, d. h. für speichereffiziente und performante Implementierungen geeignet. Sprachen, die Speichersicherheit mittels eigener Laufzeitumgebungen mit Garbage Collection realisieren, sollten vermieden werden, da hierdurch eine zusätzliche Ebene von



Komplexität mit Auswirkungen auf die sicherheitstechnische Evaluierung und das Laufzeitverhalten eingeführt wird.

Bei der Entwicklung von Virtualisierung bzw. Container Runtime, von VM-Templates und Standardkomponenten sowie von fachlichen Verarbeitungskomponenten sind alle genannten Möglichkeiten zur Vereinfachung und Härtung der Code-Basis zu nutzen.

HCC-Provider müssen für die TCB eine zu jedem Zeitpunkt aktuell gehaltene und änderungsverfolgte Software Bill of Materials führen, die der gematik zugänglich ist.

### **7.7.6 Validierung des Mandantenkontextes**

In der Cloud stellt der Mandantenkontext einen „äußeren“ Security Perimeter dar, der die Dienste des Mandanten von den Diensten anderer Mandanten in derselben Rechenzentrumsumgebung isoliert und der die Gesamtheit der Konfigurationseinstellungen beherbergt. Der Mandantenkontext spielt damit eine entscheidende Rolle für die Verfügbarkeit der Dienste.

Während Verfügbarkeit nicht das führende Kriterium im Kontext von Confidential Computing darstellt, so ist sie für die TI entscheidend. Aufgrund der Härtung der TCB von Confidential Computing entstehen zusätzliche kryptographische Bindungen, die zusätzliche Quellen für Störungen der Verfügbarkeit darstellen können. Daher sollen HCC-Provider ihren Mandanten Werkzeuge zur Validierung ihrer HCC-Dienstkonfigurationen auf der Ebene des Mandantenkontextes anbieten, die prüfen, ob für die konfigurierten Workloads alle Abhängigkeiten erfüllt werden.

In der vorliegenden Spezifikation wird diese Anforderung derzeit nicht weiter qualifiziert. Eine Umsetzung muss im Kontext des jeweiligen HCC-Providers konzipiert werden.

## **7.8 Service Runtime**

Cloud-Infrastrukturen können eine ganze Reihe verschiedener Ebenen für die Einbringung von Diensten bereitstellen (z. B. Bare Metal, Virtual Machine, Container, Serverless). Während die Minimierung der TCB in Richtung Bare Metal weist, zeigen die Anforderungen nach High Availability, Elastizität und Resource Sharing (auf der Basis von z. B. Managed Kubernetes) in Richtung höherer Ebenen des Deployments. Als Standard für das Deployment normaler Cloud-Dienste werden derzeit containerisierte Workloads angesehen. Gleichzeitig definiert Confidential Computing virtuelle Maschinen als Standard (siehe 3.4- Standardisierung des Confidential Computing Ansatzes).

Zur Vermeidung divergierender Bewertungen der Sicherheitsleistungen unterschiedlich konstruierter Service Runtimes, zur Vereinheitlichung der Änderungsanforderungen gegenüber den HCC-Providern im Zuge der konzeptionellen Weiterentwicklung von HCC sowie zur Minimierung von Änderungsbedarfen beim Wechsel des HCC-Providers legt die vorliegende Spezifikation folgendes fest:

1. HCC-Workloads werden in Confidential Virtual Machines ausgeführt, die je eine containerisierte Workload des Dienstanbieters enthält, wobei hierzu mehrere Container gehören können, die auch miteinander zusammenarbeiten können, z. B. im Sidecar-Muster. Verschiedene fachliche Dienste der TI werden grundsätzlich in getrennten cVMs implementiert.
2. Die Sicherheitsleistung, insb. hinsichtlich des Betreiberausschlusses, wird auf der Grundlage von Host-Attestation in Kombination mit cVM-Attestation transparent und durchsetzbar gemacht. Der Host-Attestation kommt dabei in Verbindung mit der Speicherverschlüsselung durch die cVMs die Rolle der primären Absicherung

gegenüber dem Infrastrukturanbieter zu. Die cVM-Attestation setzt, darauf aufbauend, die Trennung der Dienste und damit auch der Mandanten durch.

Eine Klasse der Bereitstellung von Funktionalitäten in der Cloud sind die Cloud-Native Services. Diese sind typischerweise so aufgebaut, dass sie Kontexttrennung für Mandanten dienstintern implementieren. Die Nutzung von Cloud-native Services in HCC ist im Regelfall darauf beschränkt, diesen Diensten verschlüsselte und gegen De-Anonymisierung bzw. Profilbildung geschützte Daten zu übermitteln. Cloud-native Services könnten in Zukunft auch als Confidential Services bereitgestellt werden. Hierfür ist je Service eine Analyse der Vertraulichkeit bzw. des Betreiberausschlusses einerseits und der Isolationseigenschaften andererseits erforderlich. Die Garantien von Confidential Computing können bei derartigen Services nicht ohne Weiteres „von außen“, d. h. durch „Enklaven“ in der Laufzeitumgebung dargestellt werden.

## **7.9 Integration mit den Zero Trust Services der TI**

Die HCC-Plattform ist eine Ausprägung von Rechenzentrums Umgebung für Dienste der TI, die – wie alle anderen Ausprägungen – in die Gesamtarchitektur der TI 2.0 eingebettet sein soll. Damit werden auch die Ressourcen des HCC von der Zero Trust Architektur der TI 2.0 geschützt. Dies gilt bereits für die dargestellten Core Services und bedeutet, dass jedem Core Service ein Policy Enforcement Point zur Durchsetzung der Zugriffsregeln und ein Policy Decision Point zur Auswertung der Zugriffsattribute von Requests gegen die für den jeweiligen Dienst definierten Zugriffskontrollregeln (Access Policies) zugeordnet sind.

Die für HCC definierten Policies werden innerhalb des TI 2.0-weit gültigen Policy Administration Points verwaltet. Die von den PDP der HCC Core Services verarbeiteten Zugriffsregeln werden von dort bezogen. Der Policy Administration Point muss daher alle für die sichere Verarbeitung der HCC-Policies erforderlichen Funktionen bereitstellen.

In der Überblicksdarstellung Abbildung 7 sind PEP / PDP als dem Fachdienst bzw. Core Service zugeordnete Komponenten enthalten.

Gleichzeitig stellt HCC auch eine Umsetzung von Zero Trust dar. Identitäten von HCC-Diensten werden durch die Attestation auf die Grundlage von Evidence über das den Dienst ausführende System gestellt.

Die normativen Festlegungen zur Zero Trust Architektur der TI werden in gemSpec\_ZETA getroffen.

## **7.10 Erreichbarkeit aus dem Internet**

Die TI 2.0 Strategie der gematik sieht vor, dass in Zukunft alle Fachdienste über das Internet erreichbar sein werden. Dies gilt für die Versicherten und ihren Zugriff auf die ePA und das E-Rezept bereits heute. Für die Seite der Leistungserbringer ist ein schrittweiser Wandel vorgezeichnet. Im Kontext der vorliegenden Spezifikation wird bereits kein Zugang über das Netz der TI mehr vorgesehen. Falls ein solcher Zugang doch noch erforderlich werden sollte, wird er als auf Basis von bestehenden Konzepten weiterhin realisierbar angesehen.

Für die Protokolle für den Zugriff auf die Anwendungen der TI über das Internet ist von einer schrittweisen Entwicklung auszugehen. Die Einführung der wesentlichen TI-Dienste (ePA, E-Rezept, KIM, TIM, VZD) hat mit zeitlichem Versatz stattgefunden und etliche parallele Entwicklungsstränge hervorgebracht, die erst dann konvergieren können, wenn



auch die Zero Trust Architektur der TI 2.0 generell einsatzbereit ist. Daher ist es im Interesse auch der HCC-Provider, potenziell alle Zugriffsprotokolle der Fachanwendungen zu unterstützen und den Weg zur anwendungsübergreifenden Konvergenz mitzugehen.

Generell folgt die für HCC benötigte Erreichbarkeit aus dem Internet den Vorgaben gemäß gemSpec\_ZETA.

## **7.11 Abwehr von Überlastungsangriffen aus dem Internet**

HCC-Provider müssen grundsätzlich Überlastungsangriffe aus dem Internet abwehren können und damit die in ihren Infrastrukturen betriebenen HCC-Dienste schützen. Dies schließt nicht aus, dass einzelne Dienstanbieter einen vom HCC-Provider unabhängigen DDoS-Schutzanbieter wählen und ihre Außenschnittstellen entsprechend konfigurieren.

Aufgrund der starken Bündelung von Internet-Verkehr mit anwendungsübergreifendem Charakter beim HCC-Provider ist dieser möglicherweise besonders gut positioniert, um Profilbildung zu betreiben, d. h. Endnutzer aufgrund ihrer Zugriffsmuster zu erkennen und zu beobachten. Profilbildung muss jedoch aus Gründen des Datenschutzes ausgeschlossen werden.

Hier bietet es sich an, die Zusammenarbeit des HCC-Providers mit einem unabhängigen DDoS-Schutzanbieter zu nutzen. Während es nicht ausgeschlossen werden kann, dass der DDoS-Schutzanbieter aus den Quellnetzen genug Informationen erhält, um Nutzer zu identifizieren, kann er solche Informationen beim Durchleiten des Verkehrs an den HCC-Provider auf allen Ebenen unterhalb des Application Layers verschleiern. Der DDoS-Schutzanbieter „sieht“ dann möglicherweise noch die Aktivitäten von Nutzern, weiß jedoch nicht, auf welchen Anwendungskontext sie sich beziehen, während der HCC-Provider keine Möglichkeit zur Identifizierung von Endnutzern mehr hat, da deren Verbindungen in der VAU terminieren.

In einem solchen Szenario ist es dann erforderlich, den DDoS-Schutzanbieter mit Informationen darüber zu versorgen, welche Nutzerverbindungen als legitim angesehen werden können, um ihn in die Lage zu versetzen, andere Requests einfach herauszufiltern. Daher ist der Einsatz eines Protokolls zur Rückmeldung von erfolgreich authentisierten Sessions an den DDoS-Schutzanbieter zu empfehlen. Dieses Protokoll muss auf pseudonymen Session-Identities aufbauen.

Derzeit bleiben derzeit sowohl der Einsatz eines solchen Aufbaus als auch die Ausgestaltung offen.

## 8 Organisatorische Sicherheit

Die technischen Sicherheitsmechanismen von HCC müssen eingerichtet und gewartet werden. Dies führt zu Prozessen der organisatorischen Sicherheit als Voraussetzung für die Wirksamkeit der technischen Sicherheitsmechanismen. Erweiterungen der Infrastruktur, die Aufnahme und Zulassung von Diensteanbietern als Mandanten, aber auch ihr Ausscheiden, sowie die Aufnahme von (Fach-) Diensten als TI-Dienste stellen weitere Prozesse dar, die notwendigerweise organisatorischer Natur sind. Insgesamt sind die technischen Sicherheitsmaßnahmen von organisatorischen Strukturen und Maßnahmen eingerahmt.

Insbesondere für den HCC-Provider stellen sich die spezifischen Anforderungen zur organisatorischen Sicherheit als Erweiterungen, Spezialisierungen, teilweise auch Umsetzungen seines allgemeinen System- und Prozess-Frameworks zur Erreichung der erforderlichen Zertifizierungen gemäß entsprechender Prüfkataloge und Normen dar (siehe Kapitel 9. Zulassungen und Bestätigungen). Soweit anwendbar sollten die im Folgenden geforderten Prozesse und Maßnahmen in die bestehenden Frameworks der HCC-Provider integriert implementiert werden.

### 8.1 Rollen und Verantwortlichkeiten

Die folgende Tabelle liefert eine Übersicht über die mit den Rollen der bei HCC beteiligten Akteure verbundenen Aufgaben.

**Tabelle 1 : Akteure und ihre Aufgaben**

Akteur/Aufgabe	Beschreibung
<b>gematik - Trust Domain Provider</b>	
Spezifikation	Entwicklung und Pflege der Spezifikation: <ul style="list-style-type: none"> <li>• Marktoffenheit</li> <li>• organisatorische Sicherheitsanforderungen</li> <li>• technische Sicherheitsanforderungen</li> <li>• sicherheitsfunktionalen Eigenschaften</li> <li>• Governance-Schnittstellen</li> </ul>
Zulassung HCC-Provider	Prüfung von: <ul style="list-style-type: none"> <li>• Zulassungsantrag</li> <li>• Zertifizierungen</li> <li>• Produktgutachten</li> <li>• Sicherheitsgutachten</li> <li>• Herstellererklärungen</li> </ul> Registrierung HCC-Provider, Verantwortliche, Identitäten Einrichtung der Schnittstellen

	<p>Veröffentlichung</p> <p>Durchführung Zeremonie zur Einrichtung des Root of Trust, TDCAS, auch bei Änderungen (z. B. Key Roll), Prüfung des Handbuchs für die Zeremonie</p>
Zulassung HCC-Dienstanbieter	<p>Prüfung von:</p> <ul style="list-style-type: none"> <li>• Zulassungsantrag</li> <li>• Zertifizierungen (Prozesse)</li> <li>• Anbietererklärungen</li> </ul> <p>Registrierung HCC-Dienstanbieter, Verantwortliche, Identitäten</p> <p>Einrichtung der Schnittstellen</p> <p>Veröffentlichung</p>
Zulassung HCC-Diensthersteller	<p>Prüfung von:</p> <ul style="list-style-type: none"> <li>• Zulassungsantrag</li> <li>• Zertifizierung Entwicklungsprozess</li> <li>• Herstellererklärungen</li> </ul> <p>Registrierung HCC-Diensthersteller, Verantwortliche, Identitäten</p> <p>Einrichtung der Schnittstellen</p> <p>Veröffentlichung</p>
Zulassung HCC-Dienst	<p>Prüfung von:</p> <ul style="list-style-type: none"> <li>• Zulassungsantrag</li> <li>• Produktgutachten</li> <li>• Herstellererklärungen</li> </ul> <p>Registrierung HCC-Dienst (als Workload) im TI Design &amp; Configuration Repository, Einrichtung im TI Verification &amp; Build Service</p>
Zulassung Erneuerung, Delta, Terminierung	<p>Prüfung von:</p> <ul style="list-style-type: none"> <li>• Änderungsantrag</li> <li>• Delta-Gutachten</li> </ul> <p>Aktualisierung der Registrierungseinträge</p>
HCC-Governance Repository	<p>Bereitstellung TI Design &amp; Configuration Repository</p> <ul style="list-style-type: none"> <li>• Entwicklung (Beauftragung), Betrieb, Weiterentwicklung</li> <li>• Versionierung, Manipulationsschutz, Mehr-Augen-Prinzip, Abläufe</li> </ul>

HCC-Governance Build-Service	<p>Bereitstellung TI Verification &amp; Build Service Entwicklung</p> <ul style="list-style-type: none"> <li>• Betrieb (als HCC-Dienst), Weiterentwicklung</li> <li>• Co-Entwicklung mit TI Design &amp; Configuration Repository</li> <li>• Integration von spezifischen HCC-Provider Schnittstellen</li> </ul>
HCC-Governance Identitäten	<p>Bereitstellung von Identitäten für HCC-Governance</p> <ul style="list-style-type: none"> <li>• Entwicklung der Vorgaben für starke Authentisierung und für das Signieren von Policies und anderen Artefakten</li> <li>• Definition von Herausgabeprozessen</li> </ul>
HCC-Governance Prozesse	<p>Ausgestaltung der Prozesse für HCC-Governance</p> <ul style="list-style-type: none"> <li>• Definition und Besetzung der organisatorischen Rollen für die Administration der Elemente im TI Design &amp; Configuration Repository</li> </ul>
Begutachtung	<p>Beauftragung einer unabhängigen Begutachtung der HCC-Governance (Prozesse und Systeme)</p>
Audit	<p>Planung und Durchführung von Audits bei HCC-Providern</p> <ul style="list-style-type: none"> <li>• Prüfung der Konformität mit den vorgelegten Zertifizierungen insb. hinsichtlich der TCB</li> <li>• Durchführung von Penetration Tests</li> </ul>
Issue Tracking & Management	<p>Kontinuierliche Überwachung</p> <ul style="list-style-type: none"> <li>• Betrieb</li> <li>• Sicherheit</li> </ul> <p>Management von Incidents, etc. Monitoring des Threat Environments, SIEM</p>
<b>Gutachter (der gematik)</b>	
Bestätigung	<p>Prüfung der Governance-Prozesse und Systeme Prüfung des Ausschlusses von Manipulationen (durch einzelne Täter) Ausstellung Bestätigung, Erneuerung</p>
<b>HCC-Provider</b>	
Sicheres Datacenter Design	<p>Bestätigt durch Zertifizierung:</p> <ul style="list-style-type: none"> <li>• Physische Sicherheit</li> <li>• Isolation der Datenverarbeitungsbereiche</li> </ul>
Sichere Datacenter Operations	<p>Bestätigt durch Zertifizierung:</p> <ul style="list-style-type: none"> <li>• Zutrittsschutz, Zutrittskontrolle, Zutrittsprozesssteuerung</li> </ul>

	<ul style="list-style-type: none"> <li>• Einsatz sicherheitsüberprüftes Personal</li> <li>• Trennung betrieblicher Verantwortlichkeiten gegen Manipulationsmöglichkeiten</li> </ul>
Sicherer TCB Setup	<p>Bereitstellung HSM-Cluster Bereitstellung Server-Hardware aus sicherer Lieferkette (dokumentiert) Bereitstellung und Pflege HCC-Services (begutachtet) Bereitstellung und Pflege Plattform-Software für HCC-Hosts (begutachtet)</p>
Sichere TCB Operations	<p>Umsetzung des Bootstrappings der TCB (Zeremonien) Dokumentierte, standortspezifische Registrierung von HCC-Servern (inkl. Hersteller-Attestation) und HSMs Anbindung an Designtime-Systeme der gematik Trennung HCC- und Nicht-HCC Verarbeitungsressourcen (begutachtet) Abbildung von HCC im Cloud-Management (begutachtet) Provisionierung von HCC-Verarbeitungskapazitäten nur an zugelassene Mandanten (begutachtet, dokumentiert) Mandantentrennung auf Netzwerkkonfigurationsebene (begutachtet, dokumentiert) Beauftragung der HCC-spezifischen Begutachtungen Einreichen geforderter Nachweise bei der gematik TI SIEM Integration und Unterstützung</p>
Zertifizierung	<p>Aufbau und Dokumentation der Prozesse Beauftragung und Unterstützung der Begutachtung Einreichen geforderter Nachweise bei der gematik</p>
<b>Gutachter (des HCC-Providers)</b>	
Zertifizierung (C5 etc., EUCS)	<p>Durchführung der Prüfungen, Dokumentation, Delta-Prüfungen Beachtung des angestrebten Schutzniveaus (insb. in Zweifelsfällen) Ausstellung Zertifikate, Erneuerung Zertifikate</p>
Begutachtung HCC	<p>Fundierte Analyse der TCB (Plattform-Ebene)</p> <ul style="list-style-type: none"> <li>• Source Code Analyse, Pen-Tests, Fuzzing, automatisierte Prüf-Tools, etc.</li> <li>• Prüfung der korrekten Umsetzung der spezifizierten Zugriffs-Policies</li> <li>• Insb. Nicht-Verletzung des Betreiberausschlusses (auf allen Ebenen)</li> </ul> <p>Spezielle Beachtung des Betreiberausschlusses als Schutzziel angesichts des Angriffspotenzials des Betreibers Erstellung und Bereitstellung Gutachten</p>
<b>HCC-Dienstanbieter</b>	

Legitimation des Dienstes	Nachweis der Legitimation für die Aufnahme des Dienstes in den Vertrauensraum von HCC (rechtlich, fachlich)
Bereitstellung Dienst	Beauftragung HCC-Workload-Hersteller Integration in den eigenen Mandantenkontext, Konfiguration Integration in die Betriebs- und Monitoring-Prozesse der TI (ggf. über von HCC-Provider bereitgestellte APIs) Ggf. Bereitstellung von Client-Software
Endnutzer Dokumentation	Dokumentation von Zugang, Bedingungen, Handhabung Support-Dokumentation
Endnutzer Support	Aufbau der Support-Prozesse, Kontaktpunkte Dokumentation der Support-Vorgänge
Anbieterzulassung	Nachweis der Nutzung eines HCC-Providers
<b>HCC-Workload-Hersteller</b>	
Bereitstellung HCC-Workload-Image	Entwicklung, Test, Dokumentation Issue Tracking Registrierung (je Release) im TI Design & Configuration Repository Durchlaufen der TI Verification & Build Service, Ermittlung der Referenzwerte
Zertifizierung	Sicherer Entwicklungsprozess Sichere Programmiersprache
Begutachtung	Beauftragung und Unterstützung der Begutachtung
Produktzulassung HCC-Dienst	Zulassung beantragen Bereitstellung Nachweise
<b>Gutachter (Workload)</b>	
Begutachtung HCC-Workload	Prüfungen: <ul style="list-style-type: none"> <li>• Source Code Analyse, Pen-Tests, Fuzzing, automatisierte Prüf-Tools, etc.</li> <li>• Prüfung der korrekten Umsetzung der spezifizierten Zugriffs-Policies</li> <li>• Insb. Nicht-Verletzung des Betreiberausschlusses (auf allen Ebenen)</li> <li>• Insb. Ausschluss von Angriffs-Code gegen andere HCC-Dienste auf demselben HCC-Host oder auf anderen Hosts</li> </ul> Bereitstellung Gutachten

Die hier aufgeführten Rollen und Verantwortlichkeiten müssen im Rahmen der Schaffung der organisatorischen Voraussetzungen für eine Zulassung der Anbieter und Hersteller

1898  
1899

1900 konkretisiert und ausgearbeitet werden. Hierfür werden die bestehenden  
1901 Zulassungsprozesse und Verantwortlichkeiten bei der gematik entsprechend erweitert.



---

## **9 Zulassungen und Bestätigungen**

---

Die Darstellungen in diesem Abschnitt orientieren sich an den Zulassungs- und Bestätigungsprozessen der gematik für Produkte und Anbieter.

Die gematik erteilt Zulassungen für Produkte. Dies können Komponenten oder Dienste sein – insbesondere auch solche, die aufgrund der Verarbeitung schutzwürdiger Daten eine VAU umfassen.

Die Zulassung eines Produkts umfasst dabei das Produkt im Umfang der Spezifikation der gematik und den sicheren Softwareentwicklungsprozess des Herstellers. Im Produktumfang ist insbesondere auch das VAU-Image enthalten.

Falls der Hersteller des Produkts die VAU selbst umsetzt, muss das Produkt auch die Anforderungen an die VAU erfüllen. Den Nachweis über die Erfüllung der Anforderungen muss der Hersteller gemäß den im Produkttypsteckbrief vermerkten Prüfverfahren erbringen. Der Anbieter bzw. Betreiber des zugelassenen Produkts muss in diesem Fall die Erfüllung der Anforderungen an den VAU-Betreiber nachweisen.

Anderenfalls muss der Anbieter bzw. Betreiber des Produkts einen bei der gematik gelisteten HCC-Provider auswählen. Die gelisteten HCC-Provider erfüllen die Anforderungen an VAU-Betreiber und haben dies in einem Assessment der gematik und durch die Vorlage folgender Dokumente nachgewiesen:

- Erklärung über die Erfüllung der Anforderungen in diesem Dokument,
- Erklärung zur DSGVO-Konformität,
- Testat des HCC-Providers über die Zertifizierung nach geeigneten Standards (siehe folgende Ausführungen).

Als geeigneter Standard für die Zertifizierung des HCC-Providers wird in Zukunft EUCS zur Anwendung kommen. Dieser Standard ist derzeit noch in der Erarbeitung durch die entsprechenden EU-Gremien. Seine Anwendung ist erst möglich, wenn der Standard normativ geworden ist. Ab dem Zeitpunkt seiner normativen Geltung ersetzt er bisher geltende Normen, insbesondere den Kriterienkatalog C5 des BSI. EUCS baut auf einer Vielzahl von ISO/IEC-Normen auf, die dadurch implizit normativ geltend werden.

EUCS ist in seinem an einer Liste von „Controls“ ausgerichteten Aufbau mit dem Kriterienkatalog C5 des BSI vergleichbar, definiert im Gegensatz zu C5 jedoch Zertifizierungslevels.

EUCS wird voraussichtlich drei Zertifizierungslevels definieren CS-EL1, CS-EL2 und CS-EL3. Sie unterscheiden sich durch eine deutliche Konkretisierung der geforderten Nachweise zu vielen der Controls, insbesondere beim Übergang von CS-EL1 (basic) zu CS-EL2 (substantial). Es ist davon auszugehen, dass durch EUCS für die Verarbeitung von personenbezogenen medizinischen Daten die Anwendung des Level CS-EL3 vorgeschrieben sein wird.

EUCS ist darauf ausgerichtet, möglichst viele Zertifikate auf der Grundlage von z. B. C5 oder auf der Grundlage verschiedener ISO/IEC-Normen nachnutzbar zu machen. Die Anhebung des Zertifizierungsniveaus auf EUCS sollte daher bei den Anbietern nicht zu völlig anders strukturierten Prozessen führen.

Eine Zertifizierung gemäß EUCS hat stets Bezug zu einem definierten Service. In diesem Sinne kann HCC als Zertifizierungsgegenstand aufgefasst werden. Die Umsetzung von HCC gemäß der vorliegenden Spezifikation sollte für den HCC-Provider die Erfüllung vieler EUCS-Anforderungen auf Level CS-EL3 abdecken oder mindestens vereinfachen.

Bis zum Zeitpunkt, einer normativen Geltung von EUCS in der EU werden HCC-Provider auf der Grundlage der folgenden Testate und Zertifizierungen zugelassen:

- Testat über die Erfüllung der Anforderungen aus dem Kriterienkatalog C5 (Typ 2) des BSI in der jeweils gültigen Version,
- ISO 27001 Zertifizierung (Information security, cybersecurity and privacy protection – Information security management systems - Requirements),
- ISO 27017 Zertifizierung (Information Technology - Security Techniques - Code of practice for Information Security Controls based on ISO/IEC 27002 for Cloud Services Standard),
- ISO 27018 Zertifizierung (Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors),
- ISO 27701 Zertifizierung (Security techniques - Extension to ISO/IEC 27001 and ISO 27002 for privacy information management - requirements and guidelines Standard).

Die folgende Tabelle fasst die Zulassungsgrundlagen für HCC-Provider zusammen:

**Tabelle 2: Zulassung von HCC-Providern**

Aspekt / Umsetzung	HCC
Zulassung/Bestätigung	Produktzulassung + Anbieterzulassung
Prüfung	Produktgutachten + Sicherheitsgutachten + Zertifizierungen
Anforderungsgrundlage Datenschutz und Informationssicherheit	gemSpec_HCC + weitere

---

## **10 Interoperabilität**

---

Die folgenden Schnittstellen der HCC-Provider für die Nutzung durch Dienste der gematik müssen anbieterübergreifend interoperabel ausgeführt sein, damit die HCC-Plattform für die TI handhabbar funktioniert:

1. Web-API des Trust Domain Deployment Repository für die Aufnahme der signierten HCC Workload Images, Konfigurationen, Policies und zugehöriger Metadaten aus dem TI Verification & Build Service,
2. Web-API des Trust Domain Build Service zur Entgegennahme von Workload Images und Rückgabe konvertierter Workload-Images mit den dazu ermittelten Referenzwerten aus dem TI Verification & Build Service (die manuelle Alternative muss nicht interoperabel gestaltet sein),
3. Web-API des Trust Domain Configuration & Attestation Service zur Befüllung der Konfigurationsdatenbank mit signierten Einträgen aus dem TI Verification & Build Service,
4. Web-API zur Steuerung und Konfiguration von Trust Domain Deployment Repository und Trust Domain Configuration & Attestation Service im Mandantenkontext der gematik – soweit nicht abgedeckt durch die vorstehenden Schnittstellen für die Verteilung von deren Inhalten,
5. Schnittstelle für das Einbringen von Workload-Images in ggf. Provider-neutraler Form in das TI Design & Configuration Repository. Hierbei geht es um die Standardisierung der für ein Einbringen geeigneten Formate der Images (Container- oder VM-Images) sowie ggf. um Metadaten und Konfigurationsdaten. (Diese Schnittstelle wird erst im Zuge des Aufbaus des Service bei der gematik spezifiziert.)

Die Web-APIs 1 bis 4 sollen als Ergebnis der Konsultationen mit der Industrie spezifiziert werden. Die gematik bittet hierzu um Input und Hinweise auf geeignete Standards oder bereits implementierte Lösungen. Für diese WebAPIs ist es für eine Übergangszeit denkbar, dass auch spezifische (nicht interoperable) Schnittstellen von HCC-Providern unterstützt werden, die es erfordern, dass Artefakte zunächst (z. B. per Skript) konvertiert werden müssen, bevor sie übermittelt werden können.

1992

---

## 11 Integration in das SIEM der TI

---

1993

*Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet.*

1994

## 12 Integration in das Testing Framework der TI

1995 Die Integration von Healthcare Confidential Computing (HCC) in das Testing Framework  
1996 der TI dient dazu, Qualität, Stabilität und Evolvierbarkeit der HCC-Plattform und der  
1997 darauf betriebenen HCC-Dienste in allen Lebenszyklusphasen systematisch zu prüfen. Im  
1998 Vordergrund steht dabei eine testgetriebene Nutzung von Cloud- und  
1999 CI/CD-Mechanismen, die es ermöglicht, funktionale und nicht-funktionale Eigenschaften  
2000 iterativ zu verifizieren, die Weiterentwicklung zu unterstützen und Regressionen  
2001 frühzeitig zu erkennen. Ziel ist es, die Vertrauenswürdigkeit, Reproduzierbarkeit und  
2002 Auditierbarkeit der Plattform nachweisbar zu machen.

2003

### 12.1 Tests der HCC Cloud Plattform

2004 Für die HCC Cloud Plattform kommt ein fachlich neutraler Testcontainer zum Einsatz, der  
2005 als Referenz-Workload die grundlegenden Plattform-Funktionen aus Sicht eines  
2006 HCC-Dienstes nutzt. Der Testcontainer ist als einfaches, OCI-konformes Container-Image  
2007 ausgelegt, das die für HCC erforderlichen Mechanismen implementiert und dadurch eine  
2008 neutrale, reproduzierbare Basis für Plattfortmtests schafft. Der fachlich neutrale Ansatz  
2009 ermöglicht provider- und umgebungsübergreifende Vergleichbarkeit und reduziert  
2010 Abhängigkeiten von domänenspezifischer Logik; die Entscheidungsbegründung ist damit  
2011 dokumentiert.

2012 Der Referenz-Workload des Testcontainers bildet eine definierte Menge an  
2013 grundlegenden Plattformfunktionen ab, die ein HCC-Dienst typischerweise nutzen muss.  
2014 Dazu zählen insbesondere die Bereitstellung standardisierter HTTP(S)-Schnittstellen zur  
2015 Entgegennahme und Verarbeitung von Test-Requests und die Nutzung der vorgesehenen  
2016 Routing Mechanismen. Der Container interagiert in minimaler, fachlich neutraler Weise  
2017 mit ausgewählten HCC-Basisdiensten, um deren Erreichbarkeit und korrektes  
2018 Zusammenspiel zu validieren, ohne dabei domänenspezifische Logik abzubilden. Darüber  
2019 hinaus ist der Referenz-Workload so ausgelegt, dass sein Verhalten deterministisch und  
2020 reproduzierbar ist, um konsistente Testergebnisse über verschiedene Umgebungen und  
2021 Provider hinweg zu gewährleisten. Ergänzend kann der Container gezielt einfache Fehler-  
2022 und Grenzfallszenarien auslösen, um das Verhalten der Plattform unter definierten  
2023 Störbedingungen überprüfbar zu machen.

2024 Der Build- und Deploy-Prozess des Testcontainers ist vollständig CI/CD-gestützt:  
2025 Änderungen an Quellcode oder Basis-Images werden automatisiert zu einem neuen  
2026 Container-Artefakt gebaut, versioniert und in ein Repository eingestellt. In einer  
2027 nachgelagerten Pipeline-Stufe wird das Container-Image über den Trust Domain Build  
2028 Service in ein für die HCC-Plattform ausführbares cVM-Workload-Image überführt, sodass  
2029 dieselbe Workload konsistent in verschiedenen Umgebungen – verstanden als technisch  
2030 getrennte Ausführungs- und Testkontexte entlang definierter Test- und Freigabephasen –  
2031 sowie bei unterschiedlichen HCC-Providern ausgeführt werden kann. Eine weitere  
2032 Pipeline-Stufe instanziiert den Workload in einer solchen Testumgebung und führt  
2033 automatisierte Funktionstests durch, die u. a. Konnektivität, Erreichbarkeit über HTTPS,  
2034 die Verarbeitung von Test-Requests sowie die Interaktion mit den HCC-Basisdiensten  
2035 prüfen, ohne dabei sicherheitsrelevante Eigenschaften selbst zu bewerten.

2036 Die so gestalteten Tests verstehen den Referenz-Workload als Durchstich durch die  
2037 Schichten der Cloud-Plattform: Sie decken den technischen Weg von der Bereitstellung  
2038 eines OCI-Images über die Build-Verarbeitung bis hin zum Lauf eines HCC-Dienstes im  
2039 produktionsnahen Mandantenkontext ab. Im Mittelpunkt stehen dabei Aspekte wie

korrekte Orchestrierung, konsistente Nutzung von Mandanten-Ressourcen, funktionierendes Routing und Logging sowie das Zusammenspiel der CI/CD-Pipelines mit den Plattformkomponenten. Negative und Grenzfall-Szenarien können anhand abgeleiteter Varianten desselben Testworkloads (z. B. bewusst fehlerhafte Konfigurationen, nicht erreichbare Abhängigkeiten) geprüft werden, um Plattformverhalten unter Störungssituationen zu beobachten.

Durch die konsequente Nutzung dieser einfachen Referenz-Workloads wird die HCC-Plattform selbst testbar, ohne dass fachliche Dienste oder sensible Daten erforderlich sind. Der Testcontainer dient zudem als Beispiel für HCC-Dienste, wie ein cloud-nativer, CI/CD-integrierter Entwicklungs- und Testprozess in HCC auszusehen hat, und schafft eine gemeinsame Grundlage für Provider-übergreifende Qualitätssicherung.

Darüber hinaus wird der Referenz-Workload genutzt, um die Konfiguration und Trennung von Mandantenkontexten zu validieren: Tests prüfen, ob gematik-Mandanten und HCC-Dienstanbieter-Mandanten über die vorgesehenen APIs vollständig konfigurierbar sind, ob Mandantentrennung und TI-Policy-Durchsetzung im SDN und an den relevanten Gateways greifen und ob nur die vorgesehenen Verbindungen zwischen Diensten und Basisdiensten der Plattform hergestellt werden können.

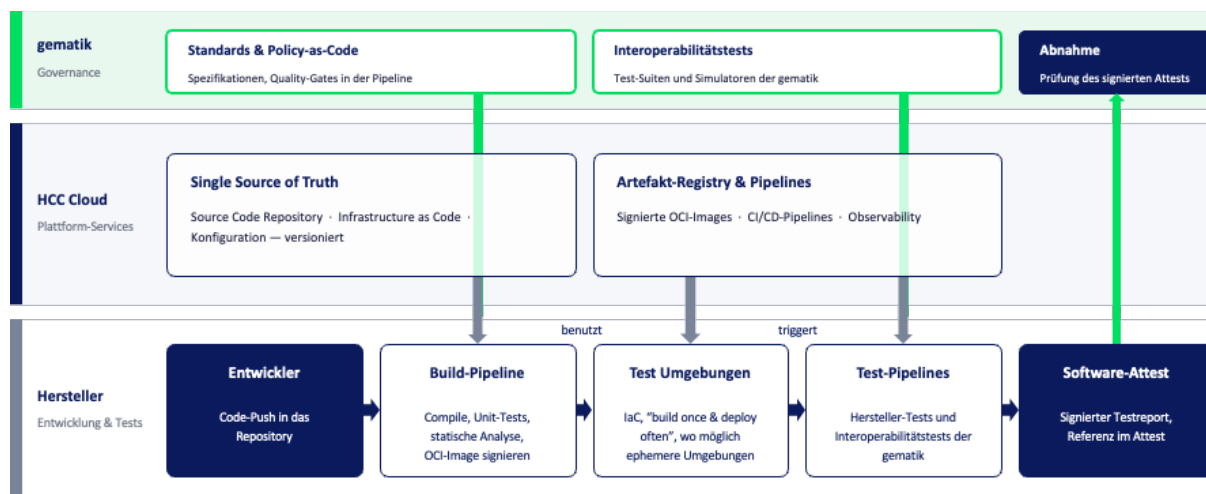
Ergänzend adressiert die Teststrategie nichtfunktionale Plattformaspekte: Mit Hilfe des Testcontainers und geeigneter Fault-Injection-Mechanismen werden Standortausfälle, HSM-Cluster-Verhalten sowie Scale-out/Scale-in von Pods und cVM-Nodes überprüft, um die geforderte Verfügbarkeit und elastische Skalierung der HCC-Plattform nachzuweisen.

## **12.2 Tests mit der HCC Cloud Plattform**

Kernbestandteile der Cloud-basierten Teststrategie sind:

- Continuous Testing und Continuous Delivery: Durch die Integration automatisierter Tests in die von der Cloud-Plattform bereitgestellten CI/CD-Pipelines – ergänzt durch konfigurierbare Zugriffskontrollen sowie HCC-basierte Build- und Deployment-Prozesse auf allen Umgebungen – wird Continuous Testing systematisch ermöglicht und die Softwarequalität kontinuierlich sowie nachvollziehbar sichergestellt.
- Förderung einer CI/CD-nativen Entwicklung: Einsatz von Infrastructure as Code, containerbasierten Deployments sowie vollständig automatisierten Test-Pipelines.

Diese Ausrichtung folgt Test Prinzipien, nach denen Tests fokussiert, zeitnah, häufig ausgeführt, aussagekräftig und zuverlässig sein müssen; genau dies wird durch automatisierte Pipelines auf konsistent bereitgestellten Umgebungen erreicht.



**Abbildung 8: Überblicksdarstellung Tests auf der HCC-Plattform**

Die HCC Cloud Plattform muss dafür CI/CD Pipelines mit konfigurierbarer Rechtevergabe bereitstellen. Für die Nutzungs- und Zugriffskontrolle muss eine Mandantentrennung mit klaren Verantwortlichkeiten unterstützt werden. Das gilt für CI/CD Pipelines wie auch für Artefakte und Testumgebungen. Eine klar geregelte Mandantentrennung und Rollenvergabe reduziert dabei Koordinationsaufwand und Wartezeiten zwischen den am Test beteiligten Akteuren und verhindert typische Engpässe, die entstehen, wenn Testen als getrennte Phase organisiert wird.

Die HCC Cloud Plattform muss eine Speicherlösung bereitstellen, in der signierte Testreports abgelegt werden können. Auf diese Reports wird im Software-Attest referenziert. Zusätzlich muss sichergestellt sein, dass die Testreports eindeutig auf die jeweils getesteten, kryptografisch identifizierten Workload-Images als System under Test (SuT) verweisen, sodass eine nachvollziehbare und reproduzierbare Zuordnung zwischen Attest, Report und dem getesteten Workload hergestellt wird. Ziel ist die Integrität (Unveränderbarkeit) der Testreports und ihre eindeutige Verknüpfung mit dem kryptografisch identifizierten SuT-Image. Eine solche eindeutige Nachvollziehbarkeit entspricht einem „Tests als First-Class-Citizen“ Gedanken: Testartefakte werden wie Produktcode behandelt, versioniert und auditierbar gehalten, um regulatorische Anforderungen mit möglichst wenig Prozess-Overhead erfüllen zu können.

Tests auf der HCC-Plattform müssen in ephemeren Testumgebungen durchgeführt werden können, die on-demand aufgebaut und nach Nutzung automatisiert wieder abgebaut werden. Grundlage ist eine „Single Source of Truth“ aus Source Code, Infrastructure as Code (IaC) und Konfiguration, die versioniert vorliegt und alle Stages – von Entwicklungs- über Integrations- bis zu produktionsnahen Umgebungen und Produktion selber – konsistent beschreibt. Damit werden Konfigurationsdrift und manuelle Sonderwege vermieden und die Nachvollziehbarkeit von Testergebnissen über Releases und Provider-Instanzen hinweg erleichtert.

Das Prinzip „build once, deploy often“ ist für alle Teststufen verbindlich: identische Artefakte werden in verschiedenen Umgebungen ausgerollt, sodass Unterschiede im Verhalten auf Umgebungsfaktoren und nicht auf Artefaktvarianten zurückzuführen sind. Deployments erfolgen vollautomatisiert über CI/CD-Pipelines, die durch Commits, Pull Requests oder zeitgesteuert angestoßen werden und sowohl Infrastruktur- als auch Applikationsanteile abdecken. Infrastruktur und Applikation sind strikt getrennt konfigurierbar; Infrastrukturänderungen erfolgen ausschließlich über IaC-Änderungen, während dienstspezifische Konfigurationen in klar abgegrenzten Parametern oder Konfigurationsdateien gehalten werden. Umgebung ist in diesem Sinne eine logische Zuordnung und keine statische Infrastruktur. Durch die in der CI/CD-Pipeline ausgeführten



2111 Tests kann für eine bestimmte Version der Software under Test – im Sinne einer  
2112 Testinstanz – eine schrittweise steigende Betriebsreife nachgewiesen werden. Unter  
2113 ‘Umgebung’ verstehen wir also die Kombination aus Deployment- und  
2114 Qualifizierungsstufen sowie den jeweils zugehörigen Anforderungen an Verfügbarkeit und  
2115 Skalierung, ergänzt um ihre Einbettung in eine spezifische Trust-Domain (z. B. eine  
2116 TI-Föderation) und eine zugehörige Network-Domain (z. B. Cloud VPC).

2117 Ephemere Testumgebungen müssen zu jedem Zeitpunkt reproduzierbar sein;  
2118 Versionierung von IaC, Artefakten und Konfiguration erlaubt es, jeden früheren Teststand  
2119 gezielt wiederherzustellen, z. B. für Fehleranalysen oder Regressionstests. Die Plattform  
2120 unterstützt schnelles Re-Deployment, damit Rollback-Szenarien, Blue-Green- oder  
2121 Canary-Deployment-Strategien sowie komplexe Integrationsfälle unter realistischen  
2122 Bedingungen getestet werden können. Durch eine horizontale Skalierung der Container-  
2123 Instanzen in Testumgebungen lassen sich umfangreiche Testreihen (z. B. Last-,  
2124 Skalierungs- oder Kompatibilitätstests) effizient durchführen, ohne dass sich Tests  
2125 gegenseitig beeinflussen.

2126 Alle relevanten Infrastrukturkomponenten (Compute, Netzwerk, Storage,  
2127 Security-Funktionen und Orchestrierung) sind deklarativ als IaC beschrieben, und  
2128 Änderungen werden ausschließlich über diesen Weg vorgenommen; manuelle Eingriffe in  
2129 laufende Instanzen sind nicht vorgesehen („Immutable Infrastructure“). Fachdienste  
2130 werden in Form dynamischer Produktketten aus containerisierten Services betrieben, die  
2131 sich flexibel zu Testketten zusammensetzen lassen – inklusive Mischszenarien aus neuen  
2132 Versionen als Testobjekten und freigegebenen Referenzversionen. Ephemere  
2133 Infrastruktur ermöglicht es, Testumgebungen schnell und reproduzierbar bereitzustellen,  
2134 Kosten zu senken und Seiteneffekte zwischen Tests zu minimieren, da jede Umgebung  
2135 neu aufgebaut und nach der Nutzung wieder entfernt werden kann. Dadurch sinkt die  
2136 Abhängigkeit von lange laufenden, gemeinsam genutzten Testumgebungen, die schwer  
2137 konsistent zu halten sind und häufig zu Wartezeiten, Fehlkonfigurationen und damit zu  
2138 nicht aussagekräftigen Testergebnissen führen. Die Cloud Plattform muss also  
2139 dynamisches Routing unterstützen. Dynamisches Routing unterstützt Ansätze wie  
2140 Contract-Testing und das Aufsetzen kurzlebiger Produktketten, die das Testen lose  
2141 gekoppelter Systeme deutlich erleichtern.

2142 Observability ist integraler Bestandteil jeder Testumgebung: Logs werden zentral  
2143 aggregiert, und Monitoring-Funktionen stehen bereits in den Testumgebungen zur  
2144 Verfügung. Observability ist wichtig, um Tests nicht nur binär „pass/fail“ zu bewerten,  
2145 sondern deren Ergebnisse hinsichtlich Stabilität, Performance und Ressourcennutzung  
2146 auszuwerten und gezielt Verbesserungsmaßnahmen abzuleiten. Dadurch lassen sich  
2147 funktionale und nicht-funktionale Testergebnisse (z. B. Antwortzeiten, Fehlerraten,  
2148 Ressourcennutzung) automatisiert auswerten und mit den Anforderungen an HCC-Dienste  
2149 und Plattformbetrieb verknüpfen. Die so gewonnenen Daten können über die  
2150 bestehenden Mechanismen zur betrieblichen Überwachung in die Systeme der TI  
2151 eingebracht und für Qualitätssicherung, Kapazitätsplanung und kontinuierliche  
2152 Verbesserung der HCC-Plattform genutzt werden.

2153 Die folgende beispielhafte Darstellung verdeutlicht den Aufbau der Build Pipelines für das  
2154 Staging von Diensten durch die Testumgebungen:

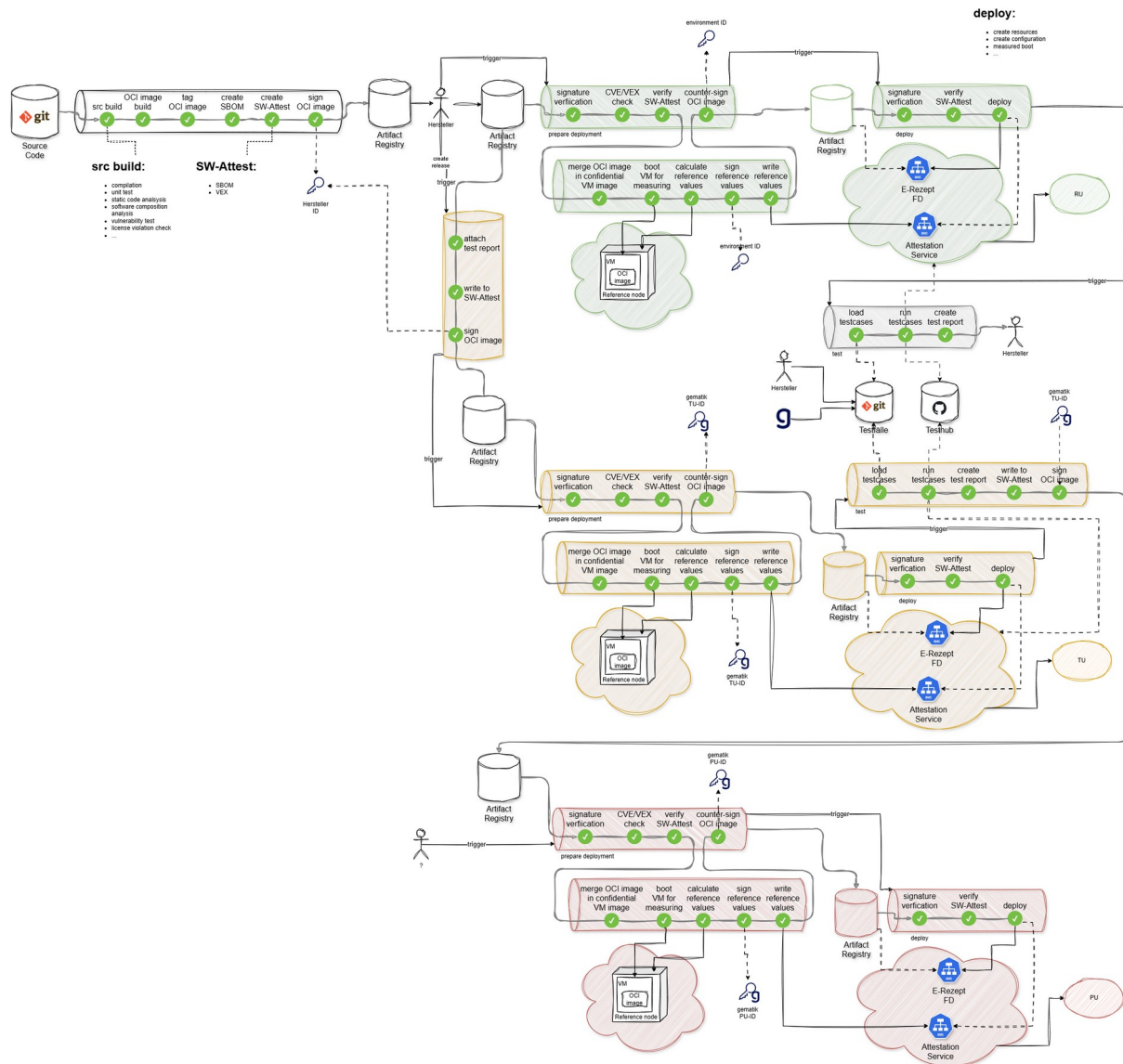


Abbildung 9: Staging von Diensten auf der HCC-Plattform

## 13 Integration in die betriebliche Steuerung der TI

*Die konkrete Anforderungslage für die betriebliche Organisation und Performance wird zu einem späteren Entwicklungsstand dieses Dokuments erweitert und konkretisiert. Die hier skizzierten Ideen und Prozesse sollen einen Rahmen setzen, zum Diskurs anregen und im Verlauf der weiteren Abstimmungen konkretisiert werden. Es ist angedacht, dass die für HCC spezialisierten Anforderungen in diesem Dokument geführt und diese mit den übergreifenden, normativen Regelungen aus [gemRL\_Betr\_TI], [gemSpec\_Perf] und [gemKPT\_Betr] harmonisiert werden.*

In der Telematikinfrastruktur liegen Anwendungs- und Infrastrukturbetrieb bisher stets in einer integrierten Betriebsverantwortung: Ein zugelassener Anbieter verantwortete beide Schichten vom Rechenzentrum bis zur fachlichen Verarbeitungslogik. Das Health-Confidential-Computing-Modell (HCC) verändert dieses Grundprinzip strukturell. Infrastruktur und Anwendung werden künftig durch separate, rechtlich eigenständige Akteure betrieben. Dieser Wesensunterschied ist nicht das Ergebnis einer organisatorischen Präferenz, sondern die technische Konsequenz des Confidential-Computing-Architekturprinzips: Infrastruktur und Anwendung operieren in getrennten Vertrauenssphären und können im laufenden Betrieb nicht unilateral aufeinander zugreifen.

Diese strukturelle Neuordnung birgt erhebliche Qualitätsgewinne. Cloud-Infrastrukturen gewährleisten kryptographisch erzwungene Integritätsgarantien, die im klassischen Rechenzentrumsbetrieb nur auf prozessualer Basis sichergestellt werden konnten. Skalierbarkeit, Ausfallsicherheit und Konfigurationsüberwachung erreichen ein strukturell höheres Niveau. Zugleich entstehen neue Anforderungen an Steuerung, Prozessgestaltung und vertragliche Absicherung, weil bisher intern gelöste Koordinationsaufgaben nunmehr explizit zwischen mehreren, rechtlich eigenständigen Akteuren geregelt werden müssen.

### 13.1 Verfügbarkeit und Performance

Die Verfügbarkeitsverantwortung und Verantwortung für die Einhaltung der Performance-Vorgaben ist folgendermaßen aufgeteilt:

- Der HCC-Provider ist verantwortlich für die Zuleitung aller Requests an den HCC-Dienst bzw. die Rückleitung aller Responses sowie für die bedarfsgerechte Instanziierung des HCC-Dienstes gemäß seiner Konfigurationseinstellungen.
- Der HCC-Dienstanbieter ist verantwortlich für die fachliche Verarbeitung, aber auch für die Performance im Zusammenspiel mit den genutzten Services des HCC-Providers (z.B. Datenbank-Service).
- Die Verantwortung gegenüber den Endnutzern des HCC-Dienstes liegt, wie bisher in der TI, beim HCC-Dienstanbieter (Anbieter TI-Fachdienst).

## 13.2 Logging- und Monitoringsysteme

Der HCC-Provider ist dafür verantwortlich, geeignete und robuste Logging- und Monitoringsysteme bereitzustellen, die sich leicht in die Anwendungen der HCC-Dienstanbieter integrieren lassen. So können beispielsweise maschinennahe Lösungen wie Softwarebibliotheken mit standardisierten Logging-Zielen des HCC-Providers integriert oder auf Ebene der Laufzeitumgebung mittels Logging-Agent die Ausleitung von Textdaten umgesetzt werden. Ziel ist es, zu jeder Zeit genügend Informationen über den Zustand und die Funktionsfähigkeit des eingesetzten Cloud-Ressourcen zu erhalten und damit jederzeit Aussagen zum Gesundheitszustand der Laufzeitumgebung treffen zu können. Diese Anforderung gilt auch für die Netzwerkinfrastruktur vor der Anwendung, Managed-Services des HCC-Providers und die HCC-spezifischen Dienste.

Der HCC-Dienstanbieter ist dafür verantwortlich, Telemetrie- und Performancedaten in seiner Anwendung zu erheben und als Betriebsdaten an die gematik zu senden. Für Ressourcen, für die der HCC-Provider keine Performancedaten bereitstellt, muss die Anwendung des HCC-Dienstanbieters Verfügbarkeit und Performance messen und der gematik zugänglich machen, u.a. damit die gematik eine SLA-Verletzung eindeutig dem HCC-Dienstanbieter oder HCC-Provider zuordnen kann.

Folgende Anstriche führen die hier gezeigten Lösungsideen weiter:

- Wie Loggingdaten des HCC-Providers zur gematik transportiert werden und wer für eine ggf. notwendige Konvertierung verantwortlich ist.
- Der HCC-Provider stellt durch interne Kategorisierung sicher, dass Loggingdaten eindeutig einem Quellsystem zugeordnet werden können. Dies betrifft vorrangig Metadaten wie Umgebungstyp (DEV/PU/RU), den Dienst- und Mandantenkontext.

Die gematik aggregiert die Monitoring- und Observability-Daten beider Dienstleister zu einer systemisch konsolidierten E2E-Sicht. Diese Sicht bildet die operative Grundlage für alle übergreifenden Steuerungsentscheidungen. Die gematik konsolidiert eingehende Betriebsdaten zu einem plattformübergreifenden Lagebild und leitet daraus erforderliche Maßnahmen ab. Sicherheitsrelevante Ereignisse sind von allen Dienstleistern unverzüglich zu melden.

## 13.3 Betriebliche Rollen und Verantwortung

Das HCC-Betriebsmodell gründet auf zwei abgegrenzten Akteuren, HCC-Cloud-Provider und HCC-Anwendungsbetreiber, mit eigenständigen Verantwortungssphären.

**Der HCC-Provider** betreibt eine mandantenfähige Cloud-Infrastruktur mit von der gematik definierten Vertrauensräumen. Seine Leistung umfasst Rechenkapazität, Speicher, Netzwerktransport sowie Cloud-Services. Mandanten in einem gematik Vertrauensraum sind ausschließlich HCC-Dienstanbieter. Der HCC-Provider verantwortet den Nachweis der Infrastruktursicherheit durch anerkannte Zertifizierungen.

**Der HCC-Dienstanbieter** verantwortet als Anwendungsbetreiber den Betrieb des jeweiligen Dienstes im Mandantenkontext des HCC-Providers. Zu seinen Aufgaben zählen die Herstellung und Testung des Dienstes, Bereitstellung umgebungsabhängiger Konfiguration, Deployment in Referenz- und Testumgebungen, Begutachtung und Zulassung des Workload-Images, Überwachung und Steuerung des produktiven Dienstes, Nutzer-Rollout und Support.

**Die gematik** übernimmt als alleiniger Vertragshalter und SIAM-Integrator (Service Integration and Management) folgende zentrale Aufgabenbereiche:

- 2241 • Erstens die Steuerung von Verträgen und Vergütung: aktive Überwachung der  
2242 Leistungserbringung aller Lose (HCC-Provider & HCC-Diensteanbieter), Durchsetzung  
2243 vertraglicher Verpflichtungen und Einhaltung des Schnittstellendesigns.
- 2244 • Zweitens das Multi-Provider-Management: Koordination der Dienstleister über  
2245 Losgrenzen, Abstimmung übergreifender Roadmaps und Funktion als zentrale  
2246 Eskalationsinstanz bei loskoordinierten Abhängigkeiten.
- 2247 • Drittens die Ende-zu-Ende-Verantwortung für Leistungsfähigkeit und Verfügbarkeit der  
2248 Gesamtplattform sowie Koordination bei plattformübergreifenden Vorfällen.

## 2249 **13.4 Betriebliche Schnittstellen**

2250 Zur effizienten Verwaltung der HCC-Umgebung sind klar definierte organisatorische und  
2251 technische Strukturen erforderlich. Dies umfasst insbesondere die Provisionierung und  
2252 Administration von Ressourcen, die Mandantenverwaltung, eine konsistente Rechte- und  
2253 Rollenverwaltung sowie die kontinuierliche Betriebsüberwachung.

2254 Um einen sicheren, stabilen und revisionsfähigen Betrieb zu gewährleisten, sind  
2255 Schnittstellen zwischen dem HCC-Provider, der gematik sowie der  
2256 HCC-Mandanten-Administration notwendig. Darüber hinaus muss die Vergabe und  
2257 Verwaltung von Berechtigungen strikt nach dem Prinzip der minimalen Privilegien  
2258 erfolgen, um Sicherheitsrisiken zu minimieren und die Verantwortlichkeiten transparent  
2259 abzubilden.

## 2260 **13.5 Provisionierung und Service-Fulfillment**

2261 HCC Anbieter ist Laufzeit Umgebung für Dritte. Zusammenspiel, Aufsicht der gematik,  
2262 muss einen Registrierungsprozess bei der gematik durchlaufen, in diesem Prozess  
2263 werden Informationen über provisionierte Ressourcen/Komponenten/Dienste/Services  
2264 bereitgestellt, um eine sichere komm mit anderen Diensten der TI und Integration in die  
2265 Föderation zu ermöglichen.

## 2266 **13.6 Anwendbarkeit betrieblicher Prozesse (TI-ITSM)**

2267 Die nachfolgenden Ausführungen betrachten die IT Service Management Prozesse auf  
2268 Basis des ITIL-Rahmenwerks und des aktuellen TI-Betriebsmodells. Die beschriebenen  
2269 Prozesse sind dabei so gestaltet, dass sie mit dem bestehenden TI-ITSM-Rahmen der TI  
2270 kompatibel sind und diesen erweitern, nicht ersetzen. Der aktuelle Fokus liegt auf Change  
2271 Management und Incident Management, da diese Prozesse im Übergang zu einem Cloud-  
2272 Betriebsmodell den größten konzeptionellen Anpassungsbedarf aufweisen. Die konkreten  
2273 Anpassungsbedarfes für diese Prozesse sowie die übrigen ITSM-Prozesse werden im  
2274 weiteren zeitlichen Verlauf detailliert ausgearbeitet.

### 2275 **13.6.1 Change Management**

2276 Das Change Management ist die prozessuale Schlüsselschnittstelle des Betriebsmodells.  
2277 Die Trennung von Infrastruktur und Anwendung erzeugt zwei strukturell eigenständige  
2278 Change-Pfade, die sich in ihren Freigabemechanismen, Vorlaufzeiten und  
2279 Verantwortlichkeiten grundlegend unterscheiden. Eine Aufgabe mit besonderem Fokus ist  
2280 die Ausdefinition der Change Management Prozesse über alle Change Auslöser hinweg



2281 mit unterschiedlichen Ausprägungen („Change Arten“), unter der Berücksichtigung der  
2282 veränderten Rahmenbedingungen.

2283 Der HCC-Provider ist Initiator und Durchführungsverantwortlicher für Infrastruktur-  
2284 Changes. Dies umfasst Firmware, Hypervisor und Plattform-Software sowie alle weiteren  
2285 TCB-relevanten Komponenten. Jeder Change-Antrag (RFC) enthält eine verpflichtende  
2286 TCB-Relevanzprüfung. Bei positiver Bewertung ist ein Delta-Gutachten durch einen  
2287 unabhängigen Gutachter obligatorisch.

2288 Der HCC-Dienstleister verantwortet Workload-Changes vollständig im eigenen  
2289 Mandantenkontext. Er plant und führt Deployments eigenständig durch, einschließlich der  
2290 Wahl der Deployment-Strategie (Blue/Green oder Canary Release) und des Rollback-  
2291 Mechanismus. Gegenüber der aktuellen TI-Architektur entsteht eine neue Pflicht: Die  
2292 Kompatibilität des eigenen Workload-Images mit einer veränderten Infrastruktur ist bei  
2293 jedem Infrastruktur-Change des HCC-Providers zu prüfen und zu bestätigen.

2294 Infrastruktur-Changes des HCC-Providers erzwingen beim HCC-Dienstleister damit eine  
2295 unmittelbare operative Reaktion. Der HCC-Provider ist daher zur rechtzeitigen  
2296 Ankündigung von Maintenance Windows verpflichtet. Der HCC-Dienstleister hat in einer  
2297 zu definierenden Frist die Workload-Kompatibilität im Rahmen der dafür vorgesehenen  
2298 Staging-Instanz zu prüfen und zwischen Bestätigung und Rollback zu entscheiden. Durch  
2299 Instanziierung/ Staging kann das höchste Verfügbarkeitsniveau an der Schnittstelle der  
2300 Dienstleister im Public Cloud Modell umgesetzt werden.

2301 Die gematik kann im Change-Prozess je nach Change Art unterschiedlich ausgeprägt sein.  
2302 Die Rolle im Prozess kann zwischen Beobachter- und Unterstützer-Rolle sowie der Gate-  
2303 Keeper-Rolle (Freigabe) variieren. Unter welchen Bedingungen welches Modell gilt, ist im  
2304 weiteren zeitlichen Verlauf intensiv zu bearbeiten. Bei Root-of-Trust-relevanten  
2305 Änderungen ist eine formale Zeremonie erforderlich. Changes, welche die Trusted  
2306 Computing Base berühren, gehen nicht ohne erfolgreiche Attestation durch den TDCAS  
2307 (Trust Domain Configuration and Attestation Service) in Betrieb, unabhängig von  
2308 prozessualer Compliance. Zusätzlich verantwortet die gematik die Freigabe aller  
2309 Workload-Images über den TI-Verification- und Build-Service sowie deren Registrierung im  
2310 D&C Repository. Gleichzeitig kann auch hier der Betrieb durch Instanziierung und Staging  
2311 in unverändert hoher Qualität aufrecht erhalten werden. Diese Kombination aus  
2312 regulatorischem und technisch erzwungenem Durchgriff ist eine Weiterentwicklung des  
2313 aktuell gelebten VAU-Konstrukts im bisherigen E-Rezept-Fachdienst.

## 2314 **13.6.2 Incident Management**

2315 Incident Management im HCC-Betriebsmodell folgt derselben strukturellen Logik wie das  
2316 Change Management: Die Trennung der Betriebssphären erzeugt eigenständige  
2317 Zuständigkeitsbereiche mit einer systemisch kritischen Schnittstelle. Die entscheidende  
2318 neue Herausforderung liegt nicht in den eindeutig zuordenbaren Incidents, sondern in  
2319 jenen, deren Ursache an der Grenze zwischen Infrastruktur- und Anwendungssphäre liegt.  
2320 Diese Schnittstelle muss in den Anforderungen und der Prozessgestaltung antizipiert  
2321 werden.

2322 Der HCC-Provider trägt die Lösungsverantwortung für alle Infrastruktur-Incidents. Dazu  
2323 zählen Attestation-Fehler, Ausfälle von TCB-Komponenten und Rechenzentrum-  
2324 Sicherheitsvorfälle. Der HCC-Cloud-Provider betreibt eigene First- und Second-Level-  
2325 Prozesse innerhalb seiner Infrastruktursphäre und ist zur unverzüglichen Information des  
2326 HCC-Dienstleister und der gematik bei betriebsrelevanten Ereignissen verpflichtet.

2327 Der HCC-Dienstleister trägt die vollständige Lösungsverantwortung für Anwendungs-  
2328 Incidents. Er ist Empfänger von Infrastruktur-Incident-Informationen und muss auf diese  
2329 reaktiv antworten können, durch Failover oder strukturierten Dienst-Wiederaufbau, ohne  
2330 dabei in die Ursachenbehebung auf Infrastrukturebene einzugreifen. Meldepflichten bei

2331 sicherheitsrelevanten Vorfällen gegenüber der gematik bleiben dem HCC-  
2332 Dienstanbieter unverändert zugeordnet.

2333 Die strukturell neue und höchste Prozessanforderung liegt bei Incidents, deren Ursache  
2334 nicht unmittelbar einer Sphäre zuzuordnen sind. Eine Anwendungsstörung kann Symptom  
2335 eines Infrastruktur-Incidents sein, der sich bspw. über fehlerhafte Attestation oder  
2336 gesperrtes Schlüsselmaterial manifestiert. Ohne definierte Abgrenzungskriterien und  
2337 Eskalationspfade entsteht an dieser Schnittstelle das operativ kritische „Ping-Pong-Risiko“  
2338 zwischen HCC-Provider und HCC-Dienstanbieter, mit direkten Auswirkungen auf  
2339 Verfügbarkeit und SLA-Erfüllung. Die Abgrenzung ist daher vertraglich, in den  
2340 Anforderungen und der Prozessgestaltung zu hinterlegen. Voraussetzung ist die Definition  
2341 klar messbarer Messpunkte an der Infrastruktur-Workload-Grenze als Grundlage für die  
2342 Ursachenzuordnung.

2343 Die gematik übernimmt im Incident Management eine Rolle als losübergreifender  
2344 Eskalationsautorität und überbrückt damit die Verantwortungsgrenzen zwischen HCC-  
2345 Provider und HCC-Dienstanbieter. Da beide Dienstleister jeweils nur ihre eigene Sphäre  
2346 vollständig überblicken, erwächst der gematik daraus eine aktive Betriebsaufgabe.  
2347 Incident-Informationen des HCC-Providers werden zwar bereitgestellt, müssen jedoch von  
2348 der gematik, insbesondere an der Schnittstelle zwischen den Dienstleistern, im  
2349 Bedarfsfall aktiv überwacht, konsolidiert, ausgewertet und nachgesteuert werden. Erst  
2350 durch diese aktive Auswertung, auf Basis Betriebsdaten, entsteht der notwendige  
2351 Informationsumfang, um als neutrale und informierte Schiedsinstanz auftreten zu können.

### 2352 **13.6.3 ITSM-Toolanbindung**

2353 Der HCC-Provider sowie der HCC-Dienstanbieter betreiben jeweils ein eigenständiges  
2354 ITSM-Tool, das über eine standardisierte Schnittstelle bidirektional an das zentrale ITSM-  
2355 System der gematik angebunden wird, so dass eine übergreifende Bearbeitung von  
2356 Changes, Incidents, Problems und anderem erfolgen kann.



---

## 14 Anforderungen an HCC

---

### 14.1 HCC-Provider - marktoffenes Angebot

Die Anforderungen in diesem Abschnitt sollen sicherstellen, dass Healthcare Confidential Computing von unabhängigen Dienst- und Anwendungsanbietern genutzt werden kann.

#### **A\_26830 -HCC-Provider - Angebot am Markt**

Der HCC-Provider MUSS Healthcare Confidential Computing am Markt, d. h. für Dritte nutzbar, anbieten und dazu mindestens:

- einen generischen Vertrag über seine Leistungen für HCC-Dienstanbieter anbieten, der nicht im Widerspruch zu den Anforderungen der vorliegenden Spezifikation steht und diese abdeckt,
- öffentlich auf die Verfügbarkeit des Angebots aufmerksam machen,
- für interessierte Dienstanbieter darstellen, auf welchem Weg das Angebot genutzt werden kann,
- für interessierte Dienstanbieter aussagekräftige Preisinformationen zur Abschätzung ihrer zu erwartenden Betriebskosten bereitstellen.

[<=]

[Herstellererklärung]

*Hinweis: Die tatsächliche Nutzung von HCC durch einen Dienstanbieter für einen HCC-Dienst in der TI steht unter dem Vorbehalt der Zulassung des Dienstanbieters und des Dienstes durch die gematik.*

#### **A\_26834 -HCC-Provider - Eigennutzung**

Der HCC-Provider KANN selbst als HCC-Dienstanbieter auftreten und für seine HCC-Dienste die eigene HCC-Plattform nutzen.[<=]

[Herstellererklärung]

#### **A\_26835 -HCC-Provider - organisatorische Trennung von Dienst- und Plattformbetrieb**

Der HCC-Provider MUSS, wenn er die eigene HCC-Plattform für die Bereitstellung eigener HCC-Dienste nutzt, nachweisen, dass der Betrieb der HCC-Plattform organisatorisch getrennt ist vom Betrieb der HCC-Dienste.[<=]

[Herstellererklärung]

*Hinweis: A\_26835 stellt keine Sicherheitsanforderung dar, sondern eine Anforderung zur Realisierung eines marktoffenen Angebots.*

#### **A\_26836 -HCC-Provider - Nutzung von Mandantenkontexten für eigene Dienste**

Der HCC-Provider MUSS, wenn er die eigene HCC-Plattform für die Bereitstellung eigener HCC-Dienste nutzt, die auch Dritten angebotenen HCC-Mandantenkontexte als Betriebs- bzw. Verwaltungsumgebung für die eigenen HCC-Dienste nutzen.[<=]

[Herstellererklärung]

#### **A\_26837 -HCC-Provider - nutzungsbezogene Preismodelle**

Der HCC-Provider MUSS für die Nutzung seiner HCC-Plattform Preismodelle am Markt anbieten, die seinen Kunden (HCC-Mandanten) nur Kosten für tatsächlich genutzte HCC-

2397 Ressourcen auferlegen. Die Granularität der Abrechnung entspricht dabei dem Modell für  
2398 die Zuteilung von Ressourcen der HCC-Plattform (Host-based, VM-based, etc.). Eine  
2399 Berechnung angemessener, fester Sockelkosten für die Bereitstellung des  
2400 Mandantenkontextes und damit verbundener administrativer Aufwände ist statthaft. [≤]

2401 [Herstellererklärung]

## 2402 14.2 HCC-Provider - Bereitstellung HCC-Infrastruktur

2403 Die Anforderungen in diesem Abschnitt dienen der Darstellung des grundlegenden HCC-  
2404 Provider Angebots sowie der Abgrenzung zwischen HCC-Providern und anderen Anbietern  
2405 innerhalb der TI.

### 2406 14.2.1 Cloud-Infrastruktur

#### 2407 A\_29048 -HCC-Provider - Cloud-Infrastruktur hohe Verfügbarkeit

2408 Der [#\\_msocom\\_1](#) HCC-Provider MUSS geeignete Rechenzentrumsinfrastruktur  
2409 bereitstellen, die auf hohe Verfügbarkeit nach [RZ-Standortkriterien] ausgelegt ist. [≤]

2410 [Anbietererklärung]

#### 2411 A\_29049 -HCC-Provider - Cloud-Infrastruktur Standort

2412 Der HCC-Provider MUSS sicherstellen, dass die bereitgestellte  
2413 Rechenzentrumsinfrastruktur im Inland, in einem Mitgliedstaat der EU bzw. des EWR oder  
2414 der Schweiz lokalisiert sind. [≤]

2415 [Sicherheitsgutachten]

#### 2416 A\_29050 -HCC-Provider - Cloud-Infrastruktur Georedundanz

2417 Der HCC-Provider MUSS sicherstellen, dass die bereitgestellte  
2418 Rechenzentrumsinfrastruktur die Vorgaben des BSI zur Georedundanz gemäß [RZ-  
2419 Standortkriterien] erfüllt. [≤]

2420 [Sicherheitsgutachten]

#### 2421 A\_29051 -HCC-Provider - Cloud-Infrastruktur redundante Versorgung

2422 Der HCC-Provider MUSS sicherstellen, dass die bereitgestellte  
2423 Rechenzentrumsinfrastruktur je Standort redundant an das Internet angeschlossen ist  
2424 sowie je Standort redundant aufgebaute Stromversorgung, Kühlung und  
2425 Netzwerkstrukturen aufweist, so dass Single Points of Failure vermieden werden. [≤]

2426 [Sicherheitsgutachten]

#### 2427 A\_29052 -HCC-Provider - Cloud-Infrastruktur Vernetzung

2428 Der HCC-Provider MUSS sicherstellen, dass die bereitgestellte  
2429 Rechenzentrumsinfrastruktur standortübergreifend mit niedriger Latenz und mit  
2430 ausreichender Kapazität vernetzt ist. [≤]

2431 [Anbietererklärung]

2432 **Offen: Anforderung in gemSpec\_Perf präzisieren**

#### 2433 A\_29053 -HCC-Provider - Cloud-Infrastruktur Verfügbarkeit

2434 Der HCC-Provider MUSS sicherstellen, dass die bereitgestellte  
2435 Rechenzentrumsinfrastruktur über nachgewiesene wirksame Mechanismen zur  
2436 Kompensation von Ausfällen auf der Ebene von Netzen, Komponenten, Diensten,  
2437 Systemen und Standorten die durchgehende Verfügbarkeit der HCC-Dienste aus Sicht  
2438 ihrer Endnutzer gewährleistet. [≤]

2439 [Sicherheitsgutachten]

2440 **A\_29054 -HCC-Provider - Cloud-Infrastruktur Kapazitäten**

2441 Der HCC-Provider MUSS sicherstellen, dass die bereitgestellte  
2442 Rechenzentrumsinfrastruktur immer die gemäß Anforderungen der deployten Dienste  
2443 ausreichende Kapazitäten bereitstellt

- 2444 • für die Ausführung containerisierter Dienst-Software (Container Runtime und/oder VM  
2445 Runtime) auf registrierten Servern mit Unterstützung für Confidential Computing  
2446 (HCC-Hosts),
- 2447 • für die Speicherung von Daten (mindestens Block Storage),
- 2448 • für den Transport von Daten (Ingress, Egress Internet, internes SDN) sowie
- 2449 • für die sichere Handhabung von Schlüsselmaterial (in HSM-Clustern).

2450 [ $\leq$ ]

2451 [Anbietererklärung]

2452 *Offen: Schema für die initial kalkulierte und später aus Betriebsdaten abgeschätzte*  
2453 *Maximallast entwickeln*

2454 **A\_29055 -HCC-Provider - Cloud-Infrastruktur Mandantenisolation**

2455 Der HCC-Provider MUSS sicherstellen, dass die bereitgestellte  
2456 Rechenzentrumsinfrastruktur Mandantenkontexte auf der Ebene aller zugeteilten  
2457 Ressourcen isoliert und Datenverkehr mandantenbezogen routet. [ $\leq$ ]

2458 [Produktgutachten]

2459 **A\_29056 -HCC-Provider - Cloud-Infrastruktur Autoscaling**

2460 Der HCC-Provider MUSS sicherstellen, dass die bereitgestellte  
2461 Rechenzentrumsinfrastruktur über (mindestens) ein automatisiertes Verfahren zur  
2462 bedarfsabhängigen (lastgesteuerten) Erhöhung bzw. Verringerung der je Mandant und je  
2463 Dienst zugeteilten Ressourcen verfügt. [ $\leq$ ]

2464 [Sicherheitsgutachten, Produktgutachten]

2465 *Hinweis: Autoscaling kann z. B. als Funktion von Managed Kubernetes umgesetzt sein.*

2466 **A\_29057 -HCC-Provider - Cloud-Infrastruktur Schutz**

2467 Der HCC-Provider MUSS sicherstellen, dass die bereitgestellte  
2468 Rechenzentrumsinfrastruktur physisch und gegen unberechtigten Zugriff geschützt ist.  
2469 [ $\leq$ ]

2470 [Sicherheitsgutachten, Produktgutachten]

2471 **14.2.2 DDoS-Abwehr**

2472 **A\_26839 -HCC-Provider - DDoS-Schutz**

2473 Der HCC-Provider MUSS die Schnittstellen der in seinen Rechenzentren betriebenen HCC-  
2474 Dienste mittels eigener vorgelagerter Systeme oder in Zusammenarbeit mit einem darauf  
2475 spezialisierten und durch das BSI zugelassenen Anbieter gemäß [DDoS-Anbieter] wirksam  
2476 gegen Überlastungsangriffe auch hohen Volumens aus dem Internet schützen. [ $\leq$ ]

2477 [Sicherheitsgutachten]

2478 **A\_29058 -HCC-Provider - DDoS-Schutz, DDoS-Abwehrsystem**

2479 Das [#\\_msocom\\_4](#)genutzte DDoS-Abwehrsystem DARF

- 2480 • TLS-Terminierung und Authentisierung von Requests NICHT auf der Grundlage von  
2481 Nutzer-Credentials durchführen, und

- legitime Client-Verbindungen bzw. Requests NICHT mit Attributen mit Nutzerbezug „markieren“.

[<=]

[Produktgutachten]

*Hinweis: Die Anforderung besteht sowohl beim Einsatz eigener Systeme zur DDoS-Abwehr als auch bei der Zusammenarbeit mit einem spezialisierten Anbieter.*

#### **A\_29059 -HCC-Provider - DDoS-Schutz, De-Anonymisierung von Requests**

Der HCC-Provider MUSS sicherstellen, dass eine [#\\_msocom\\_11](#) De-Anonymisierung von Requests nicht außerhalb der Verarbeitungskontexte der HCC-Dienste erfolgen kann.

[<=]

[Produktgutachten]

#### **A\_26841 -HCC-Provider - DDoS-Schutz, organisatorische Trennung**

Der HCC-Provider MUSS im Falle eines Einsatzes eigener Systeme zur Abwehr von DDoS-Angriffen den für den Betrieb dieser Systeme verantwortlichen Teil seines Unternehmens auf solche Weise organisatorisch von dem für den Betrieb der HCC-Systeme verantwortlichen Teil seines Unternehmens trennen, dass eine Zusammenarbeit zwischen Personen aus beiden Unternehmensteilen zur De-Anonymisierung von Endnutterzugriffen auf HCC-Dienste ausgeschlossen ist.[<=]

[Sicherheitsgutachten]

### **14.3 HCC-Provider - Integration mit gematik**

Die Anforderungen in diesem Abschnitt definieren die in der Laufzeitumgebung des HCC-Providers implementierte Beziehung zwischen der gematik als Trust Domain Provider für HCC und dem HCC-Provider als Betreiber seiner Infrastruktur. Die Beziehungen zwischen den HCC-Diensteanbietern und der gematik bauen auf dieser Beziehung auf.

#### **A\_26847 -HCC-Provider - Mandantenkontext für gematik**

Der HCC-Provider MUSS der gematik einen Mandantenkontext (Account, Zugriffsberechtigungen) zur Verfügung stellen, mittels dessen die gematik ihre Rolle und Funktion als Trust Domain Provider für HCC innerhalb der Infrastruktur des HCC-Providers ausfüllen kann.[<=]

[Herstellererklärung, Test durch gematik]

#### **A\_29060 -HCC-Provider - Zugriff auf Mandantenkontext für gematik**

Der HCC-Provider MUSS einen Zugriff auf den gematik-Mandanten über eine TLS- oder VPN-gesicherte Web-API ermöglichen.[<=]

[Produktgutachten]

#### **A\_26848 -HCC-Provider - Dienste im gematik-Mandanten**

Der HCC-Provider MUSS der gematik innerhalb ihres Mandantenkontextes folgende Dienste zur Verfügung stellen:

- Zugriff auf den Vertrauensanker für HCC und weiteres Schlüsselmaterial im HSM-Cluster,
- den Trust Domain Configuration & Attestation Service (TDCAS) sowie

- 2525 • das Trust Domain Deployment Repository.

2526 Die für andere HCC-Dienste relevanten Schnittstellen dieser Dienste müssen über das  
2527 SDN des jeweiligen Standortes des HCC-Providers nutzbar sein. [≤]

2528 *[Herstellererklärung, Test durch gematik]*

2529 *Hinweis: Das Trust Domain Deployment Repository kann als „Partition“ im Cloud*  
2530 *Management System des HCC-Providers umgesetzt sein, d. h. es wird nicht zwingend ein*  
2531 *eigenes System oder eine eigene Dienstinstanz gefordert.*

2532 *Hinweis: Der Vertrauensanker kann in einer „Partition“ eines auch für andere Zwecke*  
2533 *eingesetzten HSM-Clusters verwaltet werden.*

#### 2534 **A\_29061 -HCC-Provider - Schnittstellen Trust Domain Dienste**

2535 Der HCC-Provider MUSS sicherstellen, dass die für andere HCC-Dienste relevanten  
2536 Schnittstellen der in A\_26848 definierten Dienste über das SDN des jeweiligen Standortes  
2537 des HCC-Providers nutzbar sind. [≤]

2538 *[Produktgutachten]*

#### 2539 **A\_26849 -HCC-Provider - Funktionen des gematik-Mandanten (Administration)**

2540 Der HCC-Provider MUSS der gematik innerhalb ihres Mandantenkontextes API-Funktionen  
2541 zur Ausführung folgender Anwendungsfälle API bereitstellen:

- 2542 • Registrierung administrativer Nutzer mit jeweils eigenen, auf Multi-Factor-  
2543 Authentication auf Sicherheitsniveau hoch basierenden User Credentials (ggf. über  
2544 Web-Portal anstelle einer API),
- 2545 • Zuordnung von Nutzern zu Rollen für die im Mandantenkontext abgebildeten  
2546 Verwaltungsfunktionen sowie
- 2547 • Einsicht bzw. Überwachung der Konfiguration des gematik Mandantenkontextes inkl.  
2548 aller Zugriffsberechtigungen und im Kontext verfügbarer Funktionen.

2549 [≤]

2550 *[Herstellererklärung, Test durch gematik]*

#### 2551 **A\_29062 -HCC-Provider - Funktionen des gematik-Mandanten (Abruf von Daten)**

2552 Der HCC-Provider MUSS der gematik innerhalb ihres Mandantenkontextes API-Funktionen  
2553 zur Ausführung folgender Anwendungsfälle zum Abruf von Daten bereitstellen:

- 2554 • Abruf der Attestation Logs über alle Attestationsvorgänge für HCC-Dienste sowie
- 2555 • Abruf aller für die Governance relevanten Metadaten inkl. Hash-Werten und  
2556 Signaturen für alle im Runtime Deployment Repository des HCC-Providers für HCC  
2557 verfügbaren Artefakte

2558 [≤]

2559 *[Herstellererklärung, Test durch gematik]*

#### 2560 **A\_29063 -HCC-Provider - Funktionen des gematik-Mandanten (Einbringen von Daten)**

2561 Der HCC-Provider MUSS der gematik innerhalb ihres Mandantenkontextes API-Funktionen  
2562 zur Ausführung folgender Anwendungsfälle zum Einbringen von Daten bereitstellen:

- 2564 • *Einbringen von gültig signierten Deployment-Artefakten in das Runtime Deployment*  
2565 *Repository,*
- 2566 • *Sicheres Einbringen und Aktualisieren des für die Prüfung der Signaturen von*  
2567 *Deployment-Artefakten genutzten Zertifikats im Vier-Augen-Prinzip mit dem HCC-*  
2568 *Provider sowie*

- sicheres Einbringen signierter Policy-Statements und Referenzwerte in die Konfigurationsdatenbank des Trust Domain Configuration & Attestation Service.

[<=]

[Herstellererklärung, Test durch gematik]

#### **A\_29064 -HCC-Provider - Signaturprüfung Deployment-Artefakte**

Der HCC-Provider MUSS sicherstellen, dass beim Einbringen eines signierten Deployment-Artefaktes in das Runtime Deployment Repository durch die gematik (s. A\_29063) das Trust Domain Deployment Repository eine Signaturprüfung durchführt. Bei einer gescheiterten Signaturprüfung MUSS das jeweilige Artefakt abgelehnt werden.[<=]

[Produktgutachten]

#### **A\_29065 -HCC-Provider - Funktionen des gematik-Mandanten (Zeremonien)**

Der HCC-Provider MUSS der gematik innerhalb ihres Mandantenkontextes API-Funktionen zur Teilnahme (nach der Initialisierungszeremonie auch remote) an den Zeremonien zur Verwaltung des Vertrauensankers bereitstellen.[<=]

[Herstellererklärung, Test durch gematik]

#### **A\_28998 -HCC-Provider - Implementierung der TI-Policy**

Der HCC-Provider MUSS die übergreifende TI-Policy implementieren und dazu ggf. seine Cloud-Management Systeme entsprechend gestalten oder konfigurieren, um automatisiert zu gewährleisten, dass die in der TI-Policy definierten, erforderlichen Verbindungen - und nur diese - zwischen den HCC-Diensten in der Cloud-Plattform, in der Trust Domain sowie in sowie zu den Mandanten-Diensten hergestellt werden können (betrifft u. a. SDN-Konfigurationen, Access Policies, Ingress, Egress).[<=]

[Herstellererklärung, Produktgutachten]

*Hinweis: Für diese Ebene der TI-Policy ist derzeit keine formale Darstellung verfügbar. Die Anforderung ist so zu interpretieren, dass der in dieser Spezifikation dargestellte Funktionsaufbau für HCC im Sinne einer Policy interpretiert und funktionsfähig gemacht wird.*

## **14.4 HCC-Provider - Mandanten für HCC-Dienstanbieter**

Als Cloud-Provider stellt der HCC-Provider jedem seiner Kunden, den Anbietern von HCC-Diensten, einen individuellen Zugang in Form eines Mandantenkontextes zur Verfügung.

#### **A\_26850 -HCC-Provider - Mandantenkontext für HCC-Dienstanbieter**

Der HCC-Provider MUSS einem HCC-Dienstanbieter, als seinem Kunden, einen Mandantenkontext zur Verfügung stellen, den der HCC-Dienstanbieter über eine Web-Oberfläche bzw. eine Web-API eigenständig konfigurieren kann und mittels dessen der HCC-Dienstanbieter seine HCC-Dienste im HCC-Vertrauensraum der TI für seine Nutzer verfügbar machen kann.[<=]

[Herstellererklärung, Produktgutachten]

#### **A\_29066 -HCC-Provider - Funktionen des HCC-Dienstanbietermandanten (administrativ)**

Der [#\\_msocom\\_1](#) HCC-Provider MUSS es HCC-Dienstanbietern im Mandantenkontext ermöglichen:

- administrative Nutzer des HCC-Dienstanbieters mit jeweils eigenen, starken User Credentials zu registrieren,
- die für die Verwaltung der Cloud-Ressourcen im Mandantenkontext vorhandenen Rollen mit registrierten Nutzern zu besetzen sowie



- 2614 • Cloud-Ressourcen einzurichten, zu verwalten und zu überwachen.

2615 [**<=**]

2616 [Herstellererklärung]

2617 **A\_29067 -HCC-Provider - Funktionen des HCC-Dienstanbietermandanten**  
2618 **(Einrichten von Diensten)**

2619 Der HCC-Provider MUSS es HCC-Dienst Anbietern im Mandantenkontext ermöglichen:

- 2620 • eigene Dienstinstanzen aus VM-Images bzw. Container Images im TD Deployment  
2621 Repository ausführbar zu machen,
- 2622 • eigene Dienstinstanzen für die beim Starten von Instanzen automatisch durchgeführte  
2623 Attestation durch den TDCAS und den anschließend gewährten Zugriff auf die TLS-  
2624 Identität des HCC-Dienstes und anderes Schlüsselmaterial einzurichten sowie
- 2625 • die Betriebsdatenlieferung an die gematik (inkl. konformer Labels) über eine von HCC-  
2626 Diensten einzubindende API einzurichten.

2627 [**<=**]

2628 [Herstellererklärung]

2629 **A\_29068 -HCC-Provider - Funktionen des HCC-Dienstanbietermandanten**  
2630 **(Einbinden von Diensten)**

2631 Der HCC-Provider MUSS es HCC-Dienst Anbietern im Mandantenkontext ermöglichen:

- 2632 • Standardkomponenten der TI und die dem HCC-Dienst zugeordneten Policies in  
2633 Ausführungskontexte von HCC-Diensten einzubinden sowie
- 2634 • Plattform-Dienste des HCC-Providers (z. B. Datenbanken, Caching) einzubinden,  
2635 insoweit diese HCC-konform genutzt werden können.

2636 [**<=**]

2637 [Herstellererklärung]

2638 *Hinweis: Unter einem HCC-Dienst zugeordnete Policies fallen beispielsweise die Access*  
2639 *Control Policies von Zero Trust Komponenten.*

2640 *Hinweis: Das Einbinden von Standardkomponenten der TI und dem HCC-Dienst*  
2641 *zugeordneten Policies kann beispielsweise über Sidecar-Muster oder Service Mesh*  
2642 *Konfiguration erfolgen.*

2643 **A\_29069 -HCC-Provider - Funktionen des HCC-Dienstanbietermandanten**  
2644 **(Konfiguration)**

2645 Der HCC-Provider MUSS es HCC-Dienst Anbietern im Mandantenkontext ermöglichen:

- 2646 • die Ressourcenallokation je HCC-Dienst zu konfigurieren (lastabhängige automatische  
2647 Skalierung, Limits und Warnungen bei Erreichung bestimmter Schwellwerte für  
2648 Compute-, Storage-, Netzwerk-, HSM-Nutzung auf Dienst- und Mandantenebene)  
2649 sowie
- 2650 • die DNS-Records für die im Internet erreichbaren Web-Schnittstellen und APIs je HCC-  
2651 Dienst im Rahmen eines übergreifenden Namensschemas für HCC-Dienste zu  
2652 konfigurieren.

2653 [**<=**]

2654 [Produktgutachten]

2655 **A\_29000 -HCC-Provider - Unterstützung von Microservice-Architekturen**

2656 Der HCC-Provider MUSS seinen Mandanten den Aufbau von HCC-Diensten als Service  
2657 Meshs aus verschiedenen Diensten mit jeweils eigener (automatischer) Skalierung  
2658 ermöglichen und dazu geeignete Werkzeuge (z. B. gängige Kubernetes-

Konfigurationsmöglichkeiten und Orchestrierung) im Mandantenkontext bereitstellen.  
[<=]

*[Herstellererklärung, Produktgutachten, Test durch gematik]*

#### **A\_29001 -HCC-Provider - Bereitstellung Template**

Der [#\\_msocom\\_1](#) HCC-Provider MUSS mindestens ein cVM-Template bereitstellen, in das OCI-konform paketierte Workloads (Container-Images, die die HCC-Dienstfunktionalität und ZETA implementieren) integriert werden können, so dass diese automatisch mit der cVM gestartet werden oder auf andere Weise automatisch gestartet werden können. [<=]

*[Herstellererklärung]*

#### **A\_29070 -HCC-Provider - Build Pipeline Tools**

Der HCC-Provider MUSS für die Umwandlung von Workload-Container-Images und cVM-Template(s) in cVM-Images, die in der HCC-Umgebung ausführbar und attestierbar sind, geeignete Tools bzw. Scripte für den Build-Prozess bereitstellen und aktuell halten. [<=]

*[Produktgutachten]*

#### **A\_29071 -HCC-Provider - Integration von ZETA-Komponenten**

Der HCC-Provider MUSS die Integration der als OCI-Container-Images vorliegenden ZETA-Komponenten mit gleichfalls als OCI-Container-Images vorliegenden fachlichen Dienstkomponenten im Rahmen der Umwandlung unterstützen. [<=]

*[Herstellererklärung]*

#### **A\_29072 -HCC-Provider - Übertragung von Images**

Der HCC-Provider MUSS die automatisierte Übertragung der fertigen cVM-Images in sein Deployment Repository unterstützen. [<=]

*[Produktgutachten]*

#### **A\_29002 -HCC-Provider - Unterstützung ZETA-Integration**

Der HCC-Provider MUSS für ZETA (als Komponente für die Implementierung von HCC-Diensten) die Integration in die Laufzeitumgebung und deren Konfiguration, inkl. der Anbindung der erforderlichen Ressourcen (z. B. der Datenbank) unterstützen. [<=]

*[Herstellererklärung, Produktgutachten, Test durch gematik]*

#### **A\_26852 -HCC-Provider - HCC-Dienste mit anderen Diensten integrieren**

Der HCC-Provider MUSS mit Werkzeugen, die im Mandantenkontext für HCC-Dienstleister verfügbar sind, die Integration von HCC-Diensten seiner HCC-Mandanten mit anderen Diensten ermöglichen. Bei den Integrationsmöglichkeiten handelt es sich

- um die Integration mit über das Internet oder über das Netz der TI erreichbaren Web-API-Schnittstellen anderer Systeme oder
- um die Bereitstellung von Web-API-Schnittstellen der HCC-Dienste für den Zugriff durch die anderen Dienste.

[<=]

*[Herstellererklärung]*

*Hinweis: Bei den zu integrierenden Diensten kann es sich um HCC-Dienste in seiner Infrastruktur oder in der Infrastruktur eines anderen HCC-Providers oder um Nicht-HCC-Dienste handeln.*

#### **A\_29073 -HCC-Provider - Integration mit anderen Diensten: Gateways**

Der HCC-Provider MUSS die Einrichtung von Gateways ermöglichen, über die alle Verbindungen bei der Integration mit anderen Diensten nach A\_26852 realisiert werden und die neben der Datenverkehrssteuerung auch eine erste Stufe des Ausschlusses von

2704 unbekannten externen Verbindungspartnern umsetzen, d. h. Verbindungen auf  
2705 registrierte Partner einschränken. [≤]

2706 [Produktgutachten]

2707 **Offen: Anwendung der Policy Administration der gematik auf die Gateways**

2708 **A\_29074 -HCC-Provider - Integration mit anderen Diensten: Konfiguration**

2709 Der HCC-Provider MUSS für die Integration mit anderen Diensten nach A\_26852 in  
2710 geeigneter und kontrollierter Weise Änderungen an SDN-Konfigurationen, an Gateways,  
2711 an Policies sowie ggf. an anderen Komponenten seiner Infrastruktur ermöglichen. [≤]

2712 [Herstellereklärung]

## 2713 14.5 HCC-Provider - HCC-Sicherheitsfunktionalität

2714 Neben den betrieblichen und fachlichen Funktionalitäten, die der HCC-Provider für die  
2715 gematik und für HCC-Dienstanbieter bereitstellt, um HCC-Dienste zur Ausführung bringen  
2716 zu können, und neben den Sicherheitsanforderungen, die seine betrieblichen  
2717 Umgebungen (Rechenzentrumsstandorte) sowie seine Systeme, Software und Prozesse  
2718 erfüllen, um die in Kapitel9- Zulassungen und Bestätigungengeforderten Zertifizierungen  
2719 zu erhalten, müssen HCC-Provider Sicherheitsfunktionalitäten implementieren, die zur  
2720 Erreichung des besonders hohen Sicherheitsstandards von HCC erforderlich sind.

2721 **A\_28999 -HCC-Provider - Ende-zu-Ende Schutz der Datenverarbeitung**

2722 Der HCC-Provider MUSS seine HCC-Umgebung so aufbauen, dass die Ende-zu-Ende  
2723 sichere Datenverarbeitung, inkl. Ausschlusses des HCC-Providers und des  
2724 Dienstanbieters, durch geeignet implementierte HCC-Dienste umgesetzt wird, d. h. dass  
2725 das übergreifende Sicherheitsziel von HCC (gemäß Kapitel4- Sicherheitsziel) erreicht wird.  
2726 [≤]

2727 [Produktgutachten]

2728 *Hinweis: Die Anforderung gilt nur für die vom HCC-Provider verantworteten Teile des*  
2729 *Gesamtsystems. Dieses muss jedoch in jedem Fall eine Erreichung des Sicherheitsziel*  
2730 *ermöglichen, wenn alle anderen Akteure ihre Anteile am Gesamtsystem entsprechend*  
2731 *umsetzen.*

2732 **A\_26853 -HCC-Provider - Attestationsfähige Server**

2733 Der HCC-Provider MUSS für die Ausführung von HCC-Diensten Server-Hardware einsetzen,  
2734 die ein sicheres Verfahren zur Remote Attestation der Hardware und des gesamten CC-  
2735 Stacks (inkl. CPU-Firmware, Bootloader, Hypervisor, VMs und HCC-Dienste-Container)  
2736 mittels Measured Boot und den Confidential Computing Mechanismen unterstützt und  
2737 dafür einen vom HCC-Provider unabhängigen und in Hardware ausgeführten  
2738 Signaturschlüssel einsetzt (Root of Trust for Measurement) oder mehrere  
2739 Signaturschlüssel (z. B. CPU und TPM). [≤]

2740 [Produktgutachten]

2741 **A\_26854 -HCC-Provider - Confidential Computing Lösung**

2742 Der HCC-Provider MUSS eine Confidential Computing Lösung einsetzen bzw. umsetzen,  
2743 die die Anforderungen A\_26848, A\_29075, A\_29076, A\_29077, A\_29078, A\_29079,  
2744 A\_29080 und A\_29081 erfüllt. [≤]

2745 [Produktgutachten]

2746 **A\_29075 -HCC-Provider - Confidential Computing Server**

2747 Der HCC-Provider MUSS für die bei ihm betriebenen HCC-Dienste Server zur Verfügung  
2748 stellen, die

- 2749 • für HCC registriert sind,
- 2750 • für den „Confidential Mode“ konfiguriert sind (Ausschluss z. B. bei Betrieb im Debug
- 2751 Mode),
- 2752 • für Arbeitsspeicherverschlüsselung konfiguriert sind,
- 2753 • einen Measured Boot Prozess bzw. Confidential Computing Mechanismus
- 2754 unterstützen, der alle Aspekte des Systems erfasst, die für die Feststellung der
- 2755 Vertraulichkeit der Verarbeitung notwendig sind, sowie
- 2756 • eine Ausführung von nicht für HCC zulässiger Software verhindern (z. B. über
- 2757 Signaturprüfung von Software-Komponenten beim Laden).

2758 **[<=]**

2759 *[Produktgutachten]*

2760 **A\_29076 -HCC-Provider - Confidential Computing Dienst-Attestation**

2761 Der HCC-Provider MUSS sicherstellen, dass nur Dienste vom Trust Domain Configuration  
2762 & Attestation Service attestiert werden, welche auf Servern nach A\_29075 laufen und  
2763 mittels als zulässig registrierter Software umgesetzt sind (inkl. CPU-Firmware, Bootloader,  
2764 Hypervisor, VMs und HCC-Dienste-Container). **[<=]**

2765 *[Produktgutachten]*

2766 **A\_29077 -HCC-Provider - Confidential Computing HSM-Cluster**

2767 Der HCC-Provider MUSS die sichere Steuerung des Zugriffs auf das in HSMs gehaltene  
2768 oder aus HSMs bezogene Schlüsselmaterial für alle HCC-Dienste technisch über den  
2769 lokalen HSM-Cluster gewährleisten. **[<=]**

2770 *[Produktgutachten]*

2771 **A\_29078 -HCC-Provider - Confidential Computing Konfiguration**

2772 Der HCC-Provider MUSS sicherstellen, dass die von ihm bereitgestellte HCC-Infrastruktur

- 2773 • die Authentizität aller benötigten Konfigurationsdaten prüft,
- 2774 • die Integrität aller benötigten Konfigurationsdaten schützt, sowie
- 2775 • gegen Rollback-Angriffe auf die Konfiguration schützt.

2776 **[<=]**

2777 *[Produktgutachten]*

2778 **A\_29079 -HCC-Provider - Confidential Computing Programmiersprache**

2779 Der HCC-Provider MUSS sicherstellen, dass die von ihm bereitgestellte HCC-Infrastruktur  
2780 in einer sicheren Programmiersprache implementiert ist. **[<=]**

2781 *[Produktgutachten]*

2782 **A\_29080 -HCC-Provider - Confidential Computing Härtung**

2783 Der HCC-Provider MUSS sicherstellen, dass die von ihm bereitgestellte HCC-Infrastruktur  
2784 eine, falls vorhanden, nach dem Stand der Technik und unter Berücksichtigung des  
2785 Standes der Forschung gehärtete Ausführungsumgebung für Confidential Workloads  
2786 mitbringt. **[<=]**

2787 *[Produktgutachten]*

2788 **A\_29081 -HCC-Provider - Confidential Computing Isolation**

2789 Der HCC-Provider MUSS sicherstellen, dass die von ihm bereitgestellte HCC-Infrastruktur  
2790 die Möglichkeiten der Hardware-Plattform zur Isolation von Confidential Workloads auf  
2791 einem HCC-Host nutzt. **[<=]**

2792 *[Produktgutachten]*

**A\_26855 -HCC-Provider - Mandantenkontext Administrationsclients**

Der [#\\_msocom\\_1](#)HCC-Provider MUSS für alle Mandantenkontexte (der gematik und der HCC-Dienstanbieter) Administrations-Clients (Hardware und Software) mit lokalem Passwort-Schutz mit Nutzerbezug registrieren. Dabei MUSS der HCC-Provider sicherstellen, dass die Administrations-Clients vor lokaler Schadsoftware mit technischen Mitteln sowie mit restriktiven Policies für die Installation von Software und die Handhabung geschützt sind. [≤]

[Produktgutachten]

**A\_29082 -HCC-Provider - Sicherer Zugang zum Mandantenkontext**

Der HCC-Provider MUSS für alle Mandantenkontexte (der gematik und der HCC-Dienstanbieter) sichere Authentisierungsverfahren anbieten und erzwingen, die mindestens den Zugriff auf nach A\_26855 registrierte und durch einen Dienst des HCC-Providers attestierte Administrations-Clients beschränken sowie ein Hardware-Credential mit lokalem PIN-Schutz als Authentisierungsfaktor (z. B. Smartcard) voraussetzen. [≤]

[Produktgutachten]

**A\_29083 -HCC-Provider - Mandantenkontext TLS 1.3**

Der HCC-Provider MUSS für alle Mandantenkontexte (der gematik und der HCC-Dienstanbieter) sicherstellen, dass der Zugriff auf die Authentisierungsverfahren sowie auf den Mandantenkontext selbst über eine mit TLS 1.3 gesicherte Verbindung stattfindet. [≤]

[Produktgutachten]

**A\_29084 -HCC-Provider - Mandantenkontext Möglichkeit Beschränkung Geo-Locations**

Der HCC-Provider MUSS für alle Mandantenkontexte (der gematik und der HCC-Dienstanbieter) ermöglichen, dass der Zugriff auf den Mandantenkontext hinsichtlich des Ortes, von dem aus zugegriffen wird, konfigurativ durch den HCC-Provider selbst oder durch den Mandanten beschränkt werden kann. [≤]

[Produktgutachten]

*Hinweis: Die Beschränkung der Geo-Location kann dabei über eine Whitelist, eine Blacklist oder über eine Kombination von beidem umgesetzt werden, bei der je Mandantenkontext neu entschieden werden kann, ob eine Whitelist oder eine Blacklist genutzt wird. Die Granularität der Geo-Locations soll dabei auf dem Level von Staaten umgesetzt werden. Ist eine Konfiguration der Beschränkung der Geo-Locations durch den HCC-Provider vorgesehen, muss die Auswahl der plausiblen Geo-Locations, auf die der Zugriff eingeschränkt wird, in Absprache mit dem Mandanten (der gematik bzw. dem HCC-Dienstanbieter) geschehen.*

**A\_29085 -HCC-Provider -Zugang zum Mandantenkontext über Internet**

Der HCC-Provider MUSS für alle Mandantenkontexte (der gematik und der HCC-Dienstanbieter) sicherstellen, dass der Zugriff auf die Authentisierungsverfahren sowie auf den Mandantenkontext selbst über das Internet (ggf. unter zusätzlichem Einsatz von VPN) möglich sind. [≤]

[Herstellereklärung]

**A\_26856 -HCC-Provider - Validierung der Mandantenkontexte**

Der HCC-Provider MUSS für alle Mandantenkontexte der HCC-Dienstanbieter eine Validierungsfunktion implementieren, die bei jeder Konfigurationsänderung ausgeführt wird und sicherstellt, dass

- alle für den Betrieb der HCC-Dienste erforderlichen Abhängigkeiten (z. B. zu den Trust Domain Services) erfüllt sind,



- nur für HCC qualifizierte Dienste eingebunden sind (falls der HCC-Dienstanbieter weitere Dienste beim HCC-Provider betreiben lässt, so müssen diese über andere Mandantenkontexte abgebildet sein).

[<=]

[Produktgutachten]

## 14.6 HCC-Provider - Sicherheitsanforderungen

### 14.6.1 Bereitstellung geeigneter Hardware

#### A\_26857 -HCC-Provider - Qualifizierte Server-Hardware Hersteller

Der HCC-Provider MUSS sicherstellen, dass die für die Ausführung von HCC-Diensten vorgesehene Server-Hardware von einem Hersteller stammt, für den hinsichtlich Herstellung und über die gesamte Lieferkette ausgeschlossen werden kann, dass seine Server-Produkte hinsichtlich ihrer Sicherheitseigenschaften manipuliert wurden (z. B. durch Einbau kompromittierter oder qualitativ unzureichender Komponenten oder durch verdeckten Einbau von Vorrichtungen zur Ausleitung von Datenverkehr). [<=]

[Anbieterklärung]

#### A\_26858 -HCC-Provider - Einbringen qualifizierter Server ins RZ

Der [#\\_msocom\\_1](#) HCC-Provider MUSS sicherstellen, dass jeder für die Ausführung von HCC-Diensten vorgesehene Server im Zuge seiner Einbringung in die geschützte Rechenzentrumsumgebung (Onboarding) sicher überprüft und registriert wird, indem das Onboarding nach A\_29086, A\_29087, A\_29088, A\_29089, A\_29090, A\_29091 sowie A\_29092 umgesetzt wird. Dabei MUSS das Onboardings im Mehr-Augen-Prinzip durch sicherheitsüberprüftes Personal und auf der Grundlage eines auditfähigen Auftrags (Tickets) durchgeführt werden. [<=]

[Anbietererklärung, Audit durch gematik]

#### A\_29086 -HCC-Provider - Onboarding Server: Lieferkettenüberprüfung

Der HCC-Provider MUSS beim Onboarding eines Servers prüfen, dass die Hardware tatsächlich vom vorgesehenen Hersteller stammt, sowie eine Überprüfung der Lieferkette des Servers auf der Grundlage geeigneter Lieferpapiere oder elektronischer Datensätze, um Manipulationen am Server auf dem Weg zum Rechenzentrum auszuschließen, durchführen. [<=]

[Anbietererklärung, Sicherheitsgutachten]

#### A\_29087 -HCC-Provider - Onboarding Server: Unversehrtheit

Der HCC-Provider MUSS beim Onboarding eines Servers die Unversehrtheit des Servers, insbesondere die Unversehrtheit ggf. vorhandener Gehäuseversiegelungen, sowie die grundsätzliche Funktionsfähigkeit des Servers überprüfen und dokumentieren. [<=]

[Anbietererklärung]

#### A\_29088 -HCC-Provider - Onboarding Server: Attestation

Der HCC-Provider MUSS beim Onboarding eines Servers eine Attestation des Servers gegenüber dem Attestation Service des Hardware-Herstellers des Workload-Prozessors (z. B. Intel Attestation Service) durchführen und den dabei entstehenden Attestation Report dokumentieren. [<=]

[Anbietererklärung, Sicherheitsgutachten]

#### A\_29089 -HCC-Provider - Onboarding Server: Registrierung Schlüssel



2884 Der HCC-Provider MUSS beim Onboarding eines Servers die öffentlichen Schlüssel oder  
2885 Zertifikate der für die Signierung von Attestation Reports auf dem Server genutzten und  
2886 in der Server-Hardware (Workload-Prozessor, TPM) verankerten privaten Schlüssel  
2887 registrieren. [≤]

2888 [Sicherheitsgutachten]

#### 2889 **A\_29090 -HCC-Provider - Onboarding Server: Protokollierung**

2890 Der HCC-Provider MUSS das Onboarding eines Servers in einem  
2891 manipulationsgeschützten, auditfähigen Protokoll, das Auftragsreferenz (Ticket),  
2892 Zeitpunkt, Ort, beteiligte Personen, Lieferkettendaten, Attestation Report, die  
2893 registrierten Schlüssel und ggf. weitere Informationen umfasst, dokumentieren. [≤]

2894 [Sicherheitsgutachten]

#### 2895 **A\_29091 -HCC-Provider - Onboarding Server: Absicherung**

2896 Der HCC-Provider MUSS das Onboarding eines Servers gegen Inbetriebnahme von  
2897 registrierten Servern außerhalb der geschützten Rechenzentrumsumgebung absichern, z.  
2898 B. durch Absicherung der physischen Onboarding-Umgebung sowie der  
2899 Rechenzentrumsumgebung. [≤]

2900 [Sicherheitsgutachten]

#### 2901 **A\_29092 -HCC-Provider - Onboarding Server: Protokoll-Übertragung**

2902 Der HCC-Provider MUSS nach dem Onboarding eines Servers den Onboarding-  
2903 Protokolleintrag an das Trust Domain Design & Configuration Repository der gematik in  
2904 vom HCC-Provider signierter Form übertragen. [≤]

2905 [Herstellererklärung, Audit durch gematik]

2906 *Hinweis: Für die Signer-ID des HCC-Providers für den Onboarding-Protokolleintrag kann*  
2907 *der HCC-Provider im Zuge des Zulassungsverfahrens einen Vorschlag machen. Z. B.*  
2908 *könnte das Asset Management System des HCC-Providers selbst die Übertragung steuern*  
2909 *und zu diesem Zweck mit einer Signer-ID ausgestattet werden. Die Signer-ID und das sie*  
2910 *verwendende System müssen dafür entsprechenden Schutz gegen Verlust und*  
2911 *missbräuchliche Verwendung aufweisen.*

#### 2912 **A\_26859 -HCC-Provider - Betreiberausschluss für Cloud Management**

2913 Der HCC-Provider MUSS mit hoher Sicherheit gegenüber einer anerkannten,  
2914 unabhängigen Prüfstelle nachweisen, dass die zur Steuerung seiner Cloud erforderliche  
2915 Cloud Management Software auf den HCC-Hosts durch Angreifer innerhalb (Innentäter)  
2916 und außerhalb (Außentäter) seiner Organisation nicht dazu genutzt werden kann, den  
2917 Ausschluss des Betreibers vom Zugriff auf die durch HCC-Dienste verarbeiteten  
2918 schützenswerten Daten zu unterlaufen. [≤]

2919 [Produktgutachten]

2920 *Hinweis: Für die Machbarkeit dieses Nachweises kann die Architektur der Confidential*  
2921 *Computing Lösung entscheidend sein, z. B. wenn die Cloud Management Software im*  
2922 *Wesentlichen außerhalb der Trusted Computing Base ausgeführt wird.*

#### 2923 **A\_26860 -HCC-Provider - HCC-Sicherheitskonzept**

2924 Der HCC-Provider MUSS ein Sicherheitskonzept für die Umsetzung seiner spezifischen  
2925 Implementierung von HCC erstellen (HCC-Sicherheitskonzept) und auf Anfrage der  
2926 gematik zur Verfügung stellen, welches mindestens folgende Inhalte besitzt:

- 2927 • Beschreibung der Sicherheitsarchitektur,
- 2928 • Beschreibung der relevanten betrieblichen Prozesse und Rollen, insbesondere für
- 2929 Installation, Aktualisierung, Patches, Backups, Administration, Konfiguration,
- 2930 • Beschreibung der Bedrohungen und Risiken inkl. Schutzmaßnahmen vor
- 2931 physikalischen und vor Seitenkanalangriffen,

- Nachweis der kryptographisch geschlossenen Kette vom Vertrauensanker bis zu den HCC-Diensten

[<=]

[Sicherheitsgutachten]

#### **A\_26861 -HCC-Provider - Unabhängiger Root of Trust für Attestierung**

Die HCC-Provider MUSS nachweisen, dass die Root of Trust des für die Signatur der Hashwertrepräsentation einer gestarteten HCC-Workload genutzten Schlüsselmaterials nicht in der Hoheit des HCC-Providers liegt.[<=]

[Sicherheitsgutachten]

*Hinweis: Hierbei handelt es sich um den Signaturschlüssel für die Attestation Reports, der in die Hardware der HCC-Hosts vom Hersteller der CPU oder des TPM eingebracht ist (Root of Trust for Measurement).*

*Hinweis: Der Nachweis kann durch Nutzung eines Fremdherstellers geeigneter Reputation erbracht werden oder durch Zertifizierung eigener Root of Trust Komponenten auf hohem Evaluierungsniveau.*

#### **A\_26862 -HCC-Provider - Ausschluss von Manipulationen über physische Angriffe**

Der HCC-Provider MUSS mit technischen und organisatorischen Mitteln ausschließen, dass ein Angreifer aus seinem betrieblichen Umfeld physische Angriffsmittel zur Kompromittierung der HCC-Hosts innerhalb der Rechenzentrumsumgebung zum Einsatz bringen kann.[<=]

[Sicherheitsgutachten]

### **14.6.2 Schutz der Integrität der VAU**

Im Folgenden wird die beim HCC-Provider betriebene Umgebung für HCC als Vertrauenswürdige Ausführungsumgebung (VAU) bezeichnet. Dies entspricht der bisherigen Benennung in entsprechenden Spezifikationen der gematik und stellt eine für die Formulierung der Sicherheitsanforderungen weiterhin geeignete Abstraktion gegenüber der konkreten Architektur von HCC dar.

Die Anforderungen richten sich an den HCC-Provider, an den HCC-Dienstanbieter oder an die HCC-Workload (Dienst-Software), je nach Quelle des Gegenstands der jeweiligen Anforderung.

#### **A\_26863 -VAU - Ausschluss von Manipulationen an HCC-Hosts**

Die VAU MUSS die Integrität der Hardware der HCC-Hosts, der Hosts zur Ausführung der HCC Platform Services sowie der HSMs gegen Manipulationen an der Hardware durch den HCC-Provider schützen.[<=]

[Produktgutachten]

*Hinweis: Die Anforderung richtet sich an den HCC-Provider.*

*Hinweis: Für den geforderten Integritätsschutz der Hardware ist es ausreichend, wenn HCC-Server und Hosts zur Ausführung der HCC Platform Services durch Gehäuse geschützt sind, die eine Manipulation hinreichend erschweren, um Manipulationen für die Prozesse der Sicherheitsüberwachung im Rechenzentrum, die für die Zertifizierung des Anbieters nach C5 Typ 2 umgesetzt sind, zuverlässig erkennbar werden zu lassen. Die Sicherheitsüberwachung muss dabei durch Personen durchgeführt und verantwortet werden, die nicht selbst zum Kreis der Zutrittsberechtigten zu den Räumlichkeiten gehören, in denen die HCC-Hosts betrieben werden. Für die Gehäuse von HSMs gelten die Anforderungen der FIPS-Zertifizierung.*

**A\_26864 -VAU - Ausschluss des Starts ungültiger Workload-Images auf HCC-Hosts**

Die VAU MUSS beim Laden eines Workload-Images auf einem HCC-Host die Signatur des Workload-Images prüfen und den Start des VAU-Images verhindern, wenn es nicht gültig durch den Trust Domain Verification & Build Service signiert ist. [ $\leq$ ]

[Produktgutachten]

*Hinweis: Die Anforderung richtet sich an den HCC-Provider.*

*Hinweis: Die Umsetzung kann dadurch erfolgen, dass die Laufzeitumgebung auf den HCC-Hosts (z. B. Hypervisor, Container-Runtime) so konfiguriert ist, dass sie nur Workload-Images aus dem (authentifizierten) Trust Domain Deployment Repository ausführt und dass das Trust Domain Deployment Repository nachweislich nur entsprechend signierte und nicht zurückgezogene Workload-Images enthält.*

**A\_26865 -VAU - Attestation von Workload-Images beim Start eines Verarbeitungskontextes**

Die VAU MUSS die Aufnahme eines manipulierten Workload-Images in den Vertrauensraum von HCC verhindern, indem der TDCAS die ihm bekannt gemachte, gültige Hashwertrepräsentation des Workload-Images mit der beim Start des Verarbeitungskontextes gemessenen Hashwertrepräsentation des Workload-Images auf Übereinstimmung prüft und die Zugänglichmachung des Schlüsselmaterials verweigert, wenn keine Übereinstimmung festgestellt werden kann. [ $\leq$ ]

[Produktgutachten]

*Hinweis: Die Anforderung richtet sich an den HCC-Provider als Provider des TDCAS und der attestationsfähigen Server-Plattform und an das Workload-Image, das die Attestation initiieren muss.*

**A\_26866 -VAU - Attestation der Plattform**

Die VAU MUSS die Aufnahme eines HCC-Hosts in ungültigem Konfigurationszustand oder mit ungültiger Plattform-Software in den Vertrauensraum von HCC verhindern, indem der TDCAS die Werte aus dem Measured Boot für die Hardware und HCC-Stack insgesamt berücksichtigt und die Zugänglichmachung des Schlüsselmaterials verweigert, wenn keine Übereinstimmung festgestellt werden kann. [ $\leq$ ]

[Produktgutachten]

*Hinweis: Die Anforderung richtet sich an den HCC-Provider als Provider des TDCAS und der attestationsfähigen Server-Plattform und an das Workload-Image, das die Attestation initiieren muss.*

**A\_26867 -VAU - Integrität des HCC-Stacks**

Die VAU MUSS auf einem HCC-Stack aufbauen, der keine Veränderungen zur Laufzeit aus betrieblichen Gründen erfordert. [ $\leq$ ]

[Produktgutachten]

*Hinweis: Die Anforderungen stellt sicher, dass die attestierte Integrität der Betriebssystemumgebung über den gesamten Boot-Zyklus eines HCC-Hosts erhalten bleiben kann. Updates erfordern daher grundsätzlich einen Neustart des HCC-Hosts.*

**A\_26868 -VAU - Keine Konfigurationsänderungen zur Laufzeit**

Die VAU MUSS sicherstellen, dass die zum Zeitpunkt der Erstellung des Attestation Reports mitgemessene Konfiguration für eine Workload für die Laufzeit der Instanz unverändert bleibt. [ $\leq$ ]

[Produktgutachten]

*Hinweis: Die Anforderung richtet sich an den HCC-Provider.*

3025 *Hinweis: Die Umsetzung kann z. B. dadurch erfolgen, dass die Konfiguration nur bei der*  
3026 *Instanziierung der Workload ausgewertet wird, so dass spätere Änderungen an*  
3027 *Konfigurationsdateien keine Auswirkungen haben können.*

3028 **A\_29021 -VAU - Dynamische Skalierung**

3029 Die VAU MUSS ermöglichen bei Bedarf weitere HCC-Hosts der VAU hinzuzufügen und bei  
3030 Wegfall des Bedarfs HCC-Hosts wieder aus der VAU zu entfernen.[<=]

3031 *Hinweis: Die Anforderung richtet sich an den HCC-Provider.*

3032 **14.6.3 Schutz der Datenverarbeitung**

3033 **A\_26869 -VAU - Klartext-Daten ausschließlich im Verarbeitungskontext**

3034 Die VAU MUSS technisch sicherstellen, dass eine Klartext-Verarbeitung von  
3035 schützenswerten Daten ausschließlich innerhalb eines Verarbeitungskontextes erfolgt.  
3036 [<=]

3037 [Produktgutachten]

3038 *Hinweis: Die Anforderung richtet sich an den HCC-Provider, den HCC-Dienstanbieter und*  
3039 *an das Workload-Image.*

3040 **A\_26870 -VAU - Isolation der VAU von Datenverarbeitungsprozessen des**  
3041 **Betreibers**

3042 Die VAU MUSS die in ihren Verarbeitungskontexten ablaufenden  
3043 Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des  
3044 Betreibers trennen und damit gewährleisten, dass der Betreiber der VAU vom Zugriff auf  
3045 die in der VAU verarbeiteten schützenswerten Daten technisch ausgeschlossen ist.[<=]

3046 [Produktgutachten]

3047 *Hinweis: Die Anforderung richtet sich an den HCC-Provider.*

3048 **A\_26871 -VAU - Isolation zwischen Datenverarbeitungsprozessen mehrerer**  
3049 **Verarbeitungskontexte der VAU**

3050 Die VAU MUSS mit technischen Mitteln ausschließen, dass sich die Verarbeitungen eines  
3051 Verarbeitungskontextes schadhaft auf die Verarbeitungen eines anderen  
3052 Verarbeitungskontextes auswirken können.[<=]

3053 [Produktgutachten]

3054 *Hinweis: Die Anforderung richtet sich an den HCC-Provider, den HCC-Dienstanbieter und*  
3055 *an das Workload-Image.*

3056 *Hinweis: Diese Anforderung kann durch hinreichend tiefe Prüfung der Software des*  
3057 *Dienstes auch für Verarbeitungskontexte erfüllt werden, die auf Thread-Ebene*  
3058 *voneinander getrennt sind, wie z. B. bei regulären HTTP-Servern.*

3059 **A\_26872 -VAU - Schutz der Daten vor physischem Zugang zu Systemen der VAU**

3060 Die VAU MUSS mit technischen Mitteln sicherstellen, dass bei einem physischen Zugang  
3061 zu Hardware-Komponenten der VAU keine schützenswerten Daten aus den  
3062 Verarbeitungskontexten extrahiert oder schützenswerte Daten manipuliert werden  
3063 können.[<=]

3064 [Produktgutachten]

3065 *Hinweis: Die Anforderung richtet sich an den HCC-Provider.*

3066 **A\_26873 -VAU - Löschen aller Daten beim Beenden des Verarbeitungskontextes**

3067 Die VAU MUSS sicherstellen, dass beim Beenden eines Verarbeitungskontextes sämtliche  
3068 Klartextdaten dieses Verarbeitungskontextes aus flüchtigen Speichern sicher gelöscht  
3069 werden oder ein Zugriff auf diese Daten technisch ausgeschlossen ist.[<=]

3070 [Produktgutachten]

3071 *Hinweis: Die Anforderung richtet sich an den HCC-Provider und an das Workload-Image.*

3072 *Hinweis: Die Daten können in verschlüsselter Form in einem (ggf. verteilten) In-Memory-*  
3073 *Cache gehalten werden, um folgende Requests – ggf. in einer anderen Instanz des*  
3074 *Dienstes – performant beantworten zu können.*

#### 3075 **14.6.4 Schutz der Daten bei Speicherung**

##### 3076 **A\_26874 -VAU - Verschlüsselung von außerhalb des Verarbeitungskontextes** 3077 **gespeicherten Daten**

3078 Falls in einem Verarbeitungskontext verarbeitete schützenswerte Daten außerhalb des  
3079 Verarbeitungskontextes gespeichert werden sollen, MUSS die VAU sicherstellen, dass die  
3080 Daten den Verarbeitungskontext ausschließlich mit dem Persistenzschlüssel verschlüsselt  
3081 verlassen.[<=]

3082 [Produktgutachten]

3083 *Hinweis: Die Anforderung richtet sich an das Workload-Image.*

##### 3084 **A\_26875 -VAU - Ableitung der Persistenzschlüssel durch ein HSM**

3085 Die VAU MUSS Persistenzschlüssel für den Verarbeitungskontext von einem Schlüssel im  
3086 HSM-Cluster ableiten.[<=]

3087 [Produktgutachten]

3088 *Hinweis: Die Anforderung richtet sich an den HCC-Provider und an das Workload-Image.*

##### 3089 **A\_26876 -VAU - Nutzen des Persistenzschlüssels ausschließlich im** 3090 **Verarbeitungskontext**

3091 Die VAU MUSS sicherstellen, dass der Persistenzschlüssel ausschließlich in einem  
3092 Verarbeitungskontext des jeweiligen Dienstes genutzt wird.[<=]

3093 [Produktgutachten]

3094 *Hinweis: Die Anforderung richtet sich an den HCC-Provider und an das Workload-Image.*

#### 3095 **14.6.5 Schutz der Daten beim verteilten Caching**

##### 3096 **A\_26877 -VAU - Verschlüsselung von Daten in verteilten Caches**

3097 Falls für einen Verarbeitungskontext verarbeitete schützenswerte Daten in einem  
3098 verteilten Cache zwischengespeichert werden sollen, z. B., um den Dienst zustandslos  
3099 horizontal zu skalieren, MUSS die VAU sicherstellen, dass die Daten den  
3100 Verarbeitungskontext ausschließlich mit dem dienstspezifischen Cache-Schlüssel  
3101 verschlüsselt verlassen.[<=]

3102 [Produktgutachten]

3103 *Hinweis: Die Anforderung richtet sich an das Workload-Image.*

##### 3104 **A\_26878 -VAU - Erzeugung des dienstspezifischen Cache-Schlüssels durch ein** 3105 **HSM**

3106 Die VAU MUSS dienstspezifische Cache-Schlüssel für den Verarbeitungskontext im HSM-  
3107 Cluster erzeugen und ggf. von dort zur lokalen Verwendung abrufen.[<=]

3108 [Produktgutachten]

3109 *Hinweis: Die Anforderung richtet sich an das Workload-Image.*

##### 3110 **A\_26879 -VAU - Nutzen des Cache-Schlüssels ausschließlich im** 3111 **Verarbeitungskontext**



3112 Die VAU MUSS sicherstellen, dass Cache-Schlüssel ausschließlich in  
3113 Verarbeitungskontexten des jeweiligen Dienstes genutzt werden.【<=】

3114 [Produktgutachten]

3115 *Hinweis: Die Anforderung richtet sich an den HCC-Provider und an das Workload-Image.*

3116 **A\_26880 -VAU - Regelmäßiger Wechsel des Cache-Schlüssels**

3117 Die VAU MUSS sicherstellen, dass Cache-Schlüssel mindestens alle 24 Stunden  
3118 gewechselt werden.【<=】

3119 [Produktgutachten]

3120 *Hinweis: Die Anforderung richtet sich an den HCC-Provider und an das Workload-Image.*

3121 *Hinweis: Der Wechsel des Cache-Schlüssels muss so umgesetzt werden, dass dafür keine*  
3122 *Unterbrechung des Dienstes erforderlich wird und dass keine noch relevanten Cache-*  
3123 *Inhalte unbrauchbar werden.*

3124 **14.6.6 Schutz der Daten beim Transport**

3125 **A\_26881 -VAU - Geschützte Weitergabe von Daten an autorisierte Nutzer**

3126 Die VAU MUSS sicherstellen, dass schützenswerte Daten aus dem Verarbeitungskontext  
3127 ausschließlich über sichere Verbindungen an autorisierte Nutzer weitergegeben werden.  
3128 Bei den Nutzern kann es sich um andere Dienste handeln, die als zugelassene Dienste für  
3129 andere Verarbeitungen oder als Agenten von Nutzern schützenswerte Daten abfragen. In  
3130 diesem Fall müssen die abfragenden Dienste selbst ein vergleichbares Schutzniveau  
3131 erreichen oder im Rahmen der Selbstbestimmung des Eigentümers der schützenswerten  
3132 Daten (bzw. des datenschutzrechtlich Betroffenen) durch diesen prüfbar autorisiert  
3133 worden sein.【<=】

3134 [Produktgutachten]

3135 *Hinweis: Die Anforderung richtet sich an den HCC-Provider und an das Workload-Image.*

3136 **A\_26882 -VAU - Sicherer VAU-Kanal vom VAU-Client zum Verarbeitungskontext**

3137 Die VAU MUSS sicherstellen, dass schützenswerte Daten zwischen einem VAU-Client und  
3138 einem Verarbeitungskontext ausschließlich über einen vertraulichen und  
3139 integritätsgeschützten VAU-Kanal übermittelt werden.【<=】

3140 [Produktgutachten]

3141 *Hinweis: Die Anforderung richtet sich an den HCC-Provider und an das Workload-Image.*

3142 **A\_26883 -VAU - Sicherer Kanal vom Verarbeitungskontext zu Diensten**

3143 Die VAU MUSS sicherstellen, dass schützenswerte Daten zwischen einem  
3144 Verarbeitungskontext und einem Dienst ausschließlich über einen vertraulichen und  
3145 integritätsgeschützten und beidseitig authentisierten Kommunikationskanal übermittelt  
3146 werden.【<=】

3147 [Produktgutachten]

3148 *Hinweis: Die Anforderung richtet sich an den HCC-Provider und an das Workload-Image.*

3149 **A\_26884 -VAU - vertrauliche Kommunikation zwischen Komponenten**

3150 Die VAU MUSS sicherstellen, dass alle Komponenten der VAU ausschließlich  
3151 transportverschlüsselt mit anderen Komponenten (außerhalb oder innerhalb) der VAU  
3152 kommunizieren.【<=】

3153 [Produktgutachten]

3154 *Hinweis: Die Anforderung richtet sich an den HCC-Provider und an das Workload-Image.*

3155 **A\_26885 -VAU - Authentisierung gegenüber VAU-Clients**



Die VAU MUSS sicherstellen, dass sich der Verarbeitungskontext gegenüber Kommunikationspartnern mittels der dienstspezifischen Identität der VAU ausweist, die vom Trust Domain Configuration & Attestation Service bereitgestellt wird und aus der Komponenten-PKI der Telematikinfrastruktur abgeleitet ist. [≤]

[Produktgutachten]

#### **A\_26886 -VAU - Sichere Verbindung zwischen VAU-Image und HSM**

Die VAU MUSS technisch sicherstellen, dass zwischen einem Verarbeitungskontext der VAU und dem HSM-Cluster nur beidseitig authentifizierte und vertrauliche Verbindungen zustande kommen können, wobei die Authentizität der Workload über den Trust Domain Configuration & Attestation Service abgesichert ist. Die vertrauliche Verbindung muss auch gegen Zugriffe durch den Betreiber der VAU und den Betreiber des Dienstes schützen. [≤]

[Produktgutachten]

*Hinweis: Die Anforderung richtet sich an den HCC-Provider und an das Workload-Image.*

### **14.6.7 Konsistenz des Systemzustands, Logging und Monitoring**

#### **A\_26887 -VAU - Konsistenter Systemzustand des Verarbeitungskontextes**

Die VAU MUSS sicherstellen, dass ein konsistenter Zustand des Verarbeitungskontextes auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw. wiederhergestellt werden kann. [≤]

[Produktgutachten]

*Hinweis: Diese Anforderung ist insbesondere dann von Bedeutung, wenn in Verarbeitungskontexten mehrere gleichzeitig aktive Nutzer-Sessions auf einen gemeinsam genutzten Datenbestand zugreifen können und die transaktionale Integrität des Datenbestandes gewährleistet werden muss.*

#### **A\_26888 -VAU - Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes**

Die VAU MUSS die für den Betrieb eines Dienstes erforderlichen Logging- und Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass dem HCC-Provider sowie dem Anbieter des Dienstes schützenswerte vertrauliche oder zur unautorisierten Profilbildung geeignete Daten zur Kenntnis gelangen. [≤]

[Produktgutachten]

### **14.7 HCC-Provider - Trust Domain Services und Komponenten**

#### **A\_28996 -HCC-Provider - Bereitstellung HCC Runtime Services**

Der HCC-Provider MUSS pro Standort die folgenden Runtime Services für HCC ausfallsicher bereitstellen und über alle Standorte kontinuierlich synchronisiert halten:

- Trust Domain Configuration & Attestation Service (TDCAS),
- Trust Domain Deployment Repository (TDDR),
- HCC-Provider Deployment Repository (TDBS).

[≤]

[Herstellererklärung]

## 14.7.1 Trust Domain Deployment Repository

### A\_26889 -HCC-Provider - TDDR: Aufnahme von Artefakten

Das [#\\_msocom\\_1](#) Trust Domain Deployment Repository des HCC-Providers MUSS zur Aufnahme von signierten Artefakten aus dem TI Verification & Build Service über eine API bereitstellen. Dabei MUSS das TDDR sicherstellen, dass Artefakte für den HCC-Vertrauensraum nur vom TI Verification & Build Service eingebracht werden können. [ $\leq$ ]

[Produktgutachten]

*Hinweis: Bei den Artefakten handelt es sich um Workload-Images, für den Betrieb der Workload-Images relevante Konfigurationsdatensätze sowie Policy Sets.*

### A\_29094 -HCC-Provider - TDDR: Verwaltung von Artefakten

Das Trust Domain Deployment Repository des HCC-Providers MUSS alle Artefakte des HCC-Vertrauensraums von allen anderen Artefakten auf einfache Art unterscheidbar verwalten. [ $\leq$ ]

[Produktgutachten]

### A\_29095 -HCC-Provider - TDDR: Bereitstellung von Artefakten

Das Trust Domain Deployment Repository des HCC-Providers MUSS die signierten Artefakte für die Instanziierung von HCC-Diensten der HCC-Mandanten des HCC-Providers sowie der gematik bereitstellen und dabei Einschränkungen auf berechnigte Mandanten je Artefakt durchsetzen. [ $\leq$ ]

[Produktgutachten]

*Hinweis: Berechnigter HCC-Mandant ist im Regelfall der Dienstanbieter, der das Workload-Image bzw. die dazu gehörenden Konfigurations- und Policy-Datensätze eingebracht hat. In anderen Fällen, z. B. für durch die gematik bereitgestellte Zero Trust Komponenten, ist für diese Artefakte explizit festgelegt, dass sie z. B. für alle HCC-Mandanten nutzbar sind.*

### A\_29096 -HCC-Provider - TDDR: Notfall-Revokation und Redundanz

Das Trust Domain Deployment Repository des HCC-Providers MUSS die Notfall-Revocation von Artefakten unterstützen sowie stets aktuell gehaltene Repliken an allen Standorten haben. [ $\leq$ ]

[Produktgutachten]

## 14.7.2 Trust Domain Configuration & Attestation Service

### A\_26890 -HCC-Provider - TDCAS: Aufnahme von Artefakten

Der [#\\_msocom\\_1](#) Trust Domain Configuration & Attestation Service des HCC-Providers MUSS zur Aufnahme von signierten Artefakten (HCC-Policies und HCC-Referenzwerte) aus dem TI Verification & Build Service in seine Konfigurationsdatenbank eine API bereitstellen, und bei jeder Annahme von Artefakten sicherstellen, dass diese gültig signiert sind und andernfalls die Annahme verweigern und eine Fehlermeldung im Log erzeugen, die einen betrieblichen Alert zur Folge hat. [ $\leq$ ]

[Produktgutachten]

### A\_29097 -HCC-Provider - TDCAS: Konfiguration

Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS zur Prüfung der Signaturen der Artefakte mit der Signer-Identität des TI Verification & Build Service sicher konfiguriert werden können. [ $\leq$ ]

[Produktgutachten]

### A\_29098 -HCC-Provider - TDCAS: Attestation von Diensten

3241 Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS als  
3242 Attestation Verification Service für HCC-Dienstinstanzen der Mandanten des HCC-  
3243 Providers verfügbar und erreichbar sein und die Attestation von HCC-Diensten auf deren  
3244 Anforderung gegen die in der eigenen Konfigurationsdatenbank vorhandenen  
3245 Referenzwerte durchführen.[<=]

3246 [Produktgutachten]

3247 *Hinweis: Der TDCAS und Repliken seiner Konfigurationsdatenbank werden in alle*  
3248 *Rechenzentrumsstandorte des HCC-Providers verteilt. Der TDCAS in einer Location kann*  
3249 *nur HCC-Workloads in derselben Location attestieren.*

3250 **A\_29099 -HCC-Provider - TDCAS: Service für attestierte Dienste**

3251 Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS an  
3252 erfolgreich attestierte HCC-Dienstinstanzen Zugriffs-Credentials für die dem HCC-Dienst  
3253 zugeordneten Operationen auf den dem HCC-Dienst zugeordneten Schlüsseln im HSM-  
3254 Cluster übermitteln und

- 3255 • als Sub-CA der TI Komponenten-PKI, falls erforderlich, eine X.509-Identität der TI für  
3256 die HCC-Dienstinstanz im HSM-Cluster erzeugen, sowie
- 3257 • als Sub-CA einer Internet CA mit Extended Validation, falls erforderlich, eine Internet  
3258 X.509-Identität für die HCC-Dienstinstanz im HSM-Cluster erzeugen.

3259 [<=]

3260 [Produktgutachten]

3261 **A\_29100 -HCC-Provider - TDCAS: Log**

3262 Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS über  
3263 jeden Attestationsvorgang einen kryptographisch gegen Veränderungen geschützten Log-  
3264 Eintrag erzeugen.

3265 [<=]

3266 [Produktgutachten]

3267 **A\_29101 -HCC-Provider - TDCAS: Private Schlüssel**

3268 Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS für private  
3269 Schlüssel zu Sub-CA-Zertifikaten den lokalen HSM-Cluster nutzen.[<=]

3270 [Produktgutachten]

3271 **A\_29102 -HCC-Provider - TDCAS: Pairing mit Root of Trust**

3272 Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS das  
3273 Pairing mit dem HCC Root of Trust im HSM-Cluster in Zeremonien zu dessen Einrichtung  
3274 bzw. Erneuerung und mittels der vom HSM-Cluster bestimmten  
3275 Authentisierungsmechanismen unterstützen.[<=]

3276 [Herstellernerklärung]

3277 *Hinweis: (Auszug aus dem konzeptionellen Teil dieser Spezifikation) Das Pairing des*  
3278 *TDCAS mit dem Root of Trust basiert auf dem Einbringen eines*  
3279 *Authentisierungsschlüssels für den HSM-Zugriff auf dedizierten TDCAS-Hosts. Der TDCAS*  
3280 *wird als Confidential Service ausgeführt. Der Schlüssel wird als Sealed Key, d. h. mittels*  
3281 *eines in der Hardware verankerten Schlüssels verschlüsselt, lokal gespeichert, so dass er*  
3282 *nach einem Neustart des TDCAS-Hosts wieder verfügbar ist. Das Sealing berücksichtigt*  
3283 *die Werte aus dem Measured Boot Process, so dass der Authentisierungsschlüssel nur*  
3284 *dann wiederhergestellt werden kann, wenn dieselbe Software auf demselben Host*  
3285 *gestartet wurde. Key Rolling und Update der Software werden durch einen darauf*  
3286 *aufbauenden Mechanismus unterstützt.*

3287 **A\_29103 -HCC-Provider - TDCAS: Steuerung von Zugriffsberechtigungen**

3288 Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS die  
3289 Steuerung von Zugriffsberechtigungen für die Nutzung der jeweils benötigten  
3290 Schnittstellen und Schlüssel im HSM-Cluster umsetzen, soweit diese nicht in Zeremonien  
3291 erfolgt. [≤]

3292 [Produktgutachten]

3293 **A\_29104 -HCC-Provider - TDCAS: Confidential Service**

3294 Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS als HCC  
3295 Confidential Service betrieben werden und sicherheitstechnisch gehärtet sein. [≤]

3296 [Herstellererklärung]

3297 **A\_29105 -HCC-Provider - TDCAS: Sealing**

3298 Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS

- 3299 • die eigenen Zugriffs-Credentials für den HSM-Cluster mittels Sealing schützen und  
3300 nach einem Neustart wieder verfügbar haben,
- 3301 • Updates der eigenen Software mit Erhaltung der Sealed Secrets unterstützen, sowie
- 3302 • das Erneuern von Sealing Keys unterstützen.

3303 [≤]

3304 [Produktgutachten]

3305 *Hinweis: (Auszug aus dem konzeptionellen Teil dieser Spezifikation) Das Pairing des*  
3306 *TDCAS mit dem Root of Trust basiert auf dem Einbringen eines*  
3307 *Authentisierungsschlüssels für den HSM-Zugriff auf dedizierten TDCAS-Hosts. Der TDCAS*  
3308 *wird als Confidential Service ausgeführt. Der Schlüssel wird als Sealed Key, d. h. mittels*  
3309 *eines in der Hardware verankerten Schlüssels verschlüsselt, lokal gespeichert, so dass er*  
3310 *nach einem Neustart des TDCAS-Hosts wieder verfügbar ist. Das Sealing berücksichtigt*  
3311 *die Werte aus dem Measured Boot Process, so dass der Authentisierungsschlüssel nur*  
3312 *dann wiederhergestellt werden kann, wenn dieselbe Software auf demselben Host*  
3313 *gestartet wurde. Key Rolling und Update der Software werden durch einen darauf*  
3314 *aufbauenden Mechanismus unterstützt.*

3315 **A\_29106 -HCC-Provider - TDCAS: Konfigurationsdatenbank**

3316 Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS seine  
3317 lokale Konfigurationsdatenbank hinsichtlich Authentizität und Integrität schützen,  
3318 einschließlich Schutz vor Rollback-Attacken. [≤]

3319 [Produktgutachten]

3320 **A\_29107 -HCC-Provider - TDCAS: Attestations-Schnittstellen**

3321 Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS seine  
3322 Schnittstelle für die Attestation ausschließlich für HCC-Hosts innerhalb derselben  
3323 physischen Location verfügbar machen. [≤]

3324 [Herstellererklärung]

3325 *Hinweis: Der TDCAS und Repliken seiner Konfigurationsdatenbank werden in alle*  
3326 *Rechenzentrumsstandorte des HCC-Providers verteilt. Der TDCAS in einer Location kann*  
3327 *nur HCC-Workloads in derselben Location attestieren.*

3328 **A\_29108 -HCC-Provider - TDCAS: Inbetriebnahme**

3329 Der Trust Domain Configuration & Attestation Service des HCC-Providers MUSS in einer  
3330 gemeinsamen Zeremonie mit der gematik in Betrieb genommen und mit dem  
3331 Vertrauensanker verbunden werden. [≤]

3332 [Herstellererklärung]

### 14.7.3 Trust Domain Build Service

#### **A\_26891 -HCC-Provider - TDBS: Schnittstelle**

Der Trust Domain Build Service des HCC-Providers MUSS für den TI Verification & Build Service eine API und für User der HCC-Mandanten und der gematik eine Web-Schnittstelle bereitstellen zur gleichzeitigen

- Konvertierung generischer Workload-Images in Confidential Workload-Images und
- Ermittlung der Referenzwerte für die Attestation

[<=]

[Produktgutachten]

*Hinweis: Die Web-Schnittstelle zur manuellen Durchführung der Konvertierung soll Entwicklungs-, Test- und Deployment-Aktivitäten unterstützen.*

*Hinweis: Die generischen Workload-Images sollen einem weit verbreiteten Standard für Binaries oder Container entsprechen und mittels weit verbreiteten, offenen und bestenfalls lizenzfreien Entwicklungswerkzeugen hergestellt werden können.*

#### **A\_29109 -HCC-Provider - TDBS: Konvertierung**

Der Trust Domain Build Service des HCC-Providers MUSS für die Konvertierung geeignete Templates und Mechanismen zugrunde legen, die unterstützen, dass

- ausführbare Software-Komponenten mit fachlichem Fokus in ein minimales VM-Template mit Betriebssystem und Netzwerkunterstützung eingebracht werden,
- Zero Trust Komponenten für die Autorisierung zur Ausführung in gemeinsamen Speicherbereichen mit der fachlichen Funktionalität mit eingebracht werden (z. B. als Sidecars).

[<=]

[Herstellererklärung]

#### **A\_29110 -HCC-Provider - TDBS: Rückgabe**

Der Trust Domain Build Service des HCC-Providers MUSS das aus der Konvertierung resultierende Workload-Image zusammen mit den gemessenen Referenzwerten als vom Trust Domain Build Service signierte Artefakte zurückgeben.[<=]

[Produktgutachten]

#### **A\_29111 -HCC-Provider - TDBS: Confidential Service**

Der Trust Domain Build Service des HCC-Providers MUSS als HCC Confidential Service betrieben werden und sicherheitstechnisch gehärtet sowie als HCC Confidential Service durch den Trust Domain Configuration & Attestation Service attestiert und mit Identität ausgestattet sein.[<=]

[Herstellererklärung]

### 14.7.4 HSM-Cluster

#### **A\_26842 -HCC-Provider - HSM-Cluster**

Der HCC-Provider MUSS pro Standort mindestens ein HSM-Cluster bereitstellen.[<=]

[Anbietererklärung]

#### **A\_29112 -HCC-Provider - HSM-Cluster Kapazität**

Ein für die HCC-Infrastruktur vom HCC-Provider bereitgestellter HSM-Cluster MUSS immer über ausreichend Kapazität für das im Rahmen von HCC anfallende Volumen an HSM-



3375 pflichtigen kryptographischen Operationen verfügen und dies über ein geeignetes  
3376 Kapazitätsmanagement sicherstellen. [ $\leq$ ]

3377 [Anbietererklärung]

3378 **A\_29113 -HCC-Provider - HSM-Cluster Redundanz**

3379 Ein für die HCC-Infrastruktur vom HCC-Provider bereitgestellter HSM-Cluster MUSS mit der  
3380 zur Gewährleistung der Verfügbarkeit der HCC-Dienste notwendige Redundanz  
3381 ausgestattet sein. [ $\leq$ ]

3382 [Anbietererklärung]

3383 **A\_29114 -HCC-Provider - HSM-Cluster Synchronisation**

3384 Der HCC-Provider MUSS eine geräte- und standortübergreifender Synchronisation von  
3385 allen, für die HCC-Infrastruktur bereitgestellten HSM-Clustern implementieren. Dabei  
3386 müssen das persistente Schlüsselmaterial sowie die Zugriffsregeln (in durch die HSMs  
3387 gesteuerter, verschlüsselter Form) synchronisiert werden. [ $\leq$ ]

3388 [Produktgutachten]

3389 **A\_26892 -HCC-Provider - HSM-Cluster: Partition für Vertrauensraum**

3390 Der HSM-Cluster des HCC-Providers MUSS für den HCC-Vertrauensraum eine eigene  
3391 Partition bereitstellen. [ $\leq$ ]

3392 [Produktgutachten]

3393 **A\_29115 -HCC-Provider - HSM-Cluster: Requests nur aus derselben Location**

3394 Der HSM-Cluster des HCC-Providers MUSS für die HCC-Partition der HSMs in einer  
3395 physischen Location nur Requests von HCC-Hosts innerhalb derselben Location zulassen.  
3396 [ $\leq$ ]

3397 [Produktgutachten]

3398 **A\_29116 -HCC-Provider - HSM-Cluster: Synchronisierung**

3399 Der HSM-Cluster des HCC-Providers MUSS Schlüsselmaterial und die Konfigurationsdaten  
3400 für die Zugriffskontrolle über alle HSMs im Cluster innerhalb jeder Location und Location-  
3401 übergreifend synchron halten. [ $\leq$ ]

3402 [Produktgutachten]

3403 **A\_29117 -HCC-Provider - HSM-Cluster: Teilnahme an Zeremonien**

3404 Der [#\\_msocom\\_5](#) HSM-Cluster des HCC-Providers SOLL Key Attestation unterstützen sowie  
3405 die sichere Authentifizierung von Teilnehmern an Zeremonien über das Netz, um die  
3406 Durchführung von Zeremonien für Teilnehmer außerhalb der Rechenzentrumsumgebung  
3407 zu ermöglichen. [ $\leq$ ]

3408 [Produktgutachten]

3409 **A\_26996 -HCC-Provider - HSM-Cluster: Einsatz zertifizierter HSM**

3410 Der HCC-Provider MUSS HSMs verwenden, deren Eignung durch eine erfolgreiche  
3411 Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common  
3412 Criteria, ITSEC oder Federal Information Processing Standard (FIPS) in Frage.  
3413 Die Prüftiefe MUSS mindestens

- 3414 • FIPS 140-2 Level 3 oder
  - 3415 • Common Criteria EAL 4+ mit hohem Angriffspotenzial
- 3416 entsprechen. [ $\leq$ ]

3417 [Produktgutachten]

3418 **A\_26997 -HCC-Provider - HSM-Cluster: Erstellung und Pflege der Schlüssel nur  
3419 im Mehr-Augen-Prinzip**

3420 Der HCC-Provider MUSS HSMs einsetzen, die technisch sicherstellen, dass



- die Erstellung, Sicherung und Wiederherstellung von nicht kurzzeitig gültigen Schlüsseln und
  - die Administration des HSM-Clusters
- ausschließlich im Mehr-Augen-Prinzip erfolgen kann. [≤]

[Produktgutachten]

## 14.7.5 HCC-Hosts

### A\_26893 -HCC-Provider - HCC-Hosts: CPU

Jeder HCC-Host des HCC-Providers MUSS CPUs einsetzen, die eine Verschlüsselung des Arbeitsspeichers mit Hardware-Unterstützung ermöglichen. [≤]

[Herstellererklärung]

### A\_29118 -HCC-Provider - HCC-Hosts: Attestationsreports

Jeder HCC-Host des HCC-Providers MUSS Attestationsreports über den gesamten Hardware-, Firmware- und Software-Stack des Systems erzeugen können und diese Attestationsreports mit in der Hardware der CPU bzw. in einem TPM geschützten und durch den Hersteller attestierten Schlüssel signieren können. [≤]

[Produktgutachten]

### A\_29119 -HCC-Provider - HCC-Hosts: Abtrennung

Jeder HCC-Host des HCC-Providers MUSS eine gegen Seitenkanalangriffe mit lokalem Angriffsvektor geschützte Abtrennung der für den Cloud-Betrieb notwendigen Funktionen (Cloud Management Stack) von der Trusted Computing Base umsetzen. [≤]

[Produktgutachten]

## 14.7.6 HCC-Stack

### A\_26894 -HCC-Provider - HCC-Stack: Begutachtung

Der HCC-Stack des HCC-Providers, d. h. die Software, die als Ausführungsbasis für die HCC-Dienste dient, MUSS sicherheitstechnisch begutachtet sein, um insb. nachzuweisen, dass sie keine Angriffsmöglichkeiten auf die Isolation von Mandanten und Diensten bietet. [≤]

[Produktgutachten]

### A\_29120 -HCC-Provider - HCC-Stack: Stabilität

Der HCC-Stack des HCC-Providers, d. h. die Software, die als Ausführungsbasis für die HCC-Dienste dient, MUSS auf Stabilität, d. h. auf eine niedrige Änderungsrate ausgelegt sein, um zu vermeiden, dass entweder hohe wiederkehrende Begutachtungsaufwände entstehen oder die Qualität der Begutachtung sinkt. [≤]

[Herstellererklärung]

### A\_29121 -HCC-Provider - HCC-Stack: Minimale Code-Basis

Der HCC-Stack des HCC-Providers, d. h. die Software, die als Ausführungsbasis für die HCC-Dienste dient, MUSS auf minimalen Umfang der Code Base ausgelegt sein, um überhaupt eine ausreichend tiefe Begutachtung der Sicherheitseigenschaften zu ermöglichen. [≤]

[Produktgutachten]

### A\_29122 -HCC-Provider - HCC-Stack: Härtung

Der HCC-Stack des HCC-Providers, d. h. die Software, die als Ausführungsbasis für die HCC-Dienste dient, MUSS mit Unterstützung von automatisierten Verfahren nach Stand

der Technik und – wo möglich – nach Stand der Forschung sicherheitstechnisch gehärtet sein.【<=】

[Produktgutachten]

### 14.7.7 Key Management Service

#### **A\_26843 -HCC-Provider - Key Management Service**

Der HCC-Provider KANN einen Key Management Service zur Verwaltung und Verteilung von verschlüsseltem Schlüsselmaterial als standortübergreifend synchronisierten Cloud-native Service bereitstellen und diesen in die Abläufe zur Provisionierung von cVMs integrieren, so dass innerhalb der cVM das aus dem Key Management Service bezogene Schlüsselmaterial entschlüsselt werden kann, wenn die cVM erfolgreich attestiert werden konnte.【<=】

[Herstellererklärung, Produktgutachten]

#### **A\_26895 -HCC-Provider - KMS: Zugriff für HCC-Dienste**

Der Key Management Service des HCC-Providers MUSS für HCC-Dienste über eine API nutzbar sein, und dabei für alle Zugriffe sicherstellen, dass nur autorisierte Dienste (verschlüsseltes) Schlüsselmaterial abrufen können.【<=】

[Produktgutachten]

*Hinweis: Die Bereitstellung des KMS ist eine KANN-Anforderung und die Anforderung gilt nur dann, wenn auch ein KMS bereitgestellt wird.*

#### **A\_29123 -HCC-Provider - KMS: Verwaltung von Schlüsselmaterial**

Der Key Management Service des HCC-Providers MUSS Schlüsselmaterial je HCC-Dienst unterscheidbar (d. h. mit Dienstzuordnung) verwalten.【<=】

[Produktgutachten]

*Hinweis: Die Bereitstellung des KMS ist eine KANN-Anforderung und die Anforderung gilt nur dann, wenn auch ein KMS bereitgestellt wird.*

#### **A\_29124 -HCC-Provider - KMS: Verteilung des Schlüsselmaterials**

Der Key Management Service des HCC-Providers MUSS die Verteilung des Schlüsselmaterials über mehrere seiner Instanzen auf für HCC zugelassene Standorte beschränken.【<=】

[Produktgutachten]

*Hinweis: Die Bereitstellung des KMS ist eine KANN-Anforderung und die Anforderung gilt nur dann, wenn auch ein KMS bereitgestellt wird.*

#### **A\_29125 -HCC-Provider - KMS: Schlüsselmaterial nur in für HCC zugelassenen Kontexten**

Der Key Management Service des HCC-Providers MUSS sicherstellen, dass (verschlüsseltes) Schlüsselmaterial innerhalb des für HCC zugelassenen Rechenzentrums- bzw. Systemkontext verbleibt.【<=】

[Produktgutachten]

*Hinweis: Die Bereitstellung des KMS ist eine KANN-Anforderung und die Anforderung gilt nur dann, wenn auch ein KMS bereitgestellt wird.*

### 14.7.8 Weitere Dienste

#### **A\_26844 -HCC-Provider - RDBMS**

Der HCC-Provider KANN einen selbst skalierenden und standortübergreifend synchronisierten Relational Database Management Service zur Speicherung von vorab verschlüsselten relationalen Daten als Cloud-native Service bereitstellen, der durch die HCC-Dienste nutzbar ist. [≤]

[Herstellererklärung]

#### **A\_26845 -HCC-Provider - Key Value Store**

Der HCC-Provider KANN einen selbst skalierenden und standortübergreifend synchronisierten Key Value Store zur Speicherung vorab verschlüsselter Daten als Cloud-native Service bereitstellen, der durch die HCC-Dienste nutzbar ist. [≤]

[Herstellererklärung]

#### **A\_26846 -HCC-Provider - Confidential RDBMS**

Der HCC-Provider KANN einen selbst skalierenden und standortübergreifend synchronisierten RDBMS zur Speicherung unverschlüsselter Daten als Cloud-native Service bereitstellen, der durch die HCC-Dienste nutzbar ist. [≤]

[Herstellererklärung]

#### **A\_29093 -HCC-Provider - Confidential KV-Store**

Der HCC-Provider KANN einen selbst skalierenden und standortübergreifend synchronisierten Key Value Store zur Speicherung unverschlüsselter Daten als Cloud-native Service bereitstellen, der durch die HCC-Dienste nutzbar ist. [≤]

[Herstellererklärung]

*Hinweis: Aufgrund der in solchen Diensten stattfindenden Verarbeitung unverschlüsselter personenbezogener medizinischer Daten im Klartext müssen Dienste nach A\_26846 als HCC-Dienste zugelassen werden, wobei der HCC-Provider in dem Zulassungsprozess in einer dualen Rolle als HCC-Diensthersteller und HCC-Dienstanbieter fungiert. Es werden somit dieselben (hohen) Anforderung an die sicherheitstechnische Prüfung gestellt wie an andere HCC-Dienste.*

### **14.7.9 Sicherheitsgutachten**

Die in diesem Abschnitt verzeichneten Festlegungen sind Gegenstand der Prüfung der Sicherheitseignung gemäß [gemRL\_PruefSichEig\_DS]. Das entsprechende Sicherheitsgutachten ist der gematik vorzulegen.

**Tabelle3: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten"**

ID	Bezeichnung	Quelle (Referenz)
<a href="#">A_19147</a>	Sicherheitstestplan	gemSpec_DS_Hersteller
<a href="#">A_19148</a>	Sicherheits- und Datenschutzkonzept	gemSpec_DS_Hersteller
<a href="#">A_19150</a>	Umsetzung Sicherheitstestplan	gemSpec_DS_Hersteller
<a href="#">A_19151</a>	Implementierungsspezifische Sicherheitsanforderungen	gemSpec_DS_Hersteller
<a href="#">A_19152</a>	Verwendung eines sicheren Produktlebenszyklus	gemSpec_DS_Hersteller

<a href="#">A_19153</a>	Sicherheitsrelevanter Softwarearchitektur-Review	gemSpec_DS_Hersteller
<a href="#">A_19154</a>	Durchführung einer Bedrohungsanalyse	gemSpec_DS_Hersteller
<a href="#">A_19155</a>	Durchführung sicherheitsrelevanter Quellcode-Reviews	gemSpec_DS_Hersteller
<a href="#">A_19156</a>	Durchführung automatisierter Sicherheitstests	gemSpec_DS_Hersteller
<a href="#">A_19157</a>	Dokumentierter Plan zur Sicherheitsschulung für Entwickler	gemSpec_DS_Hersteller
<a href="#">A_19158</a>	Sicherheitsschulung für Entwickler	gemSpec_DS_Hersteller
<a href="#">A_19159</a>	Dokumentation des sicheren Produktlebenszyklus	gemSpec_DS_Hersteller
<a href="#">A_19160</a>	Änderungs- und Konfigurationsmanagementprozess	gemSpec_DS_Hersteller

### 14.7.10 Herstellererklärung funktionale Eignung

In diesem Abschnitt sind alle funktionalen und nichtfunktionalen Festlegungen an den technischen Teil des Produkttyps verzeichnet, deren durchgeführte bzw. geplante Umsetzung und Beachtung der Hersteller bzw. der Anbieter durch eine Herstellererklärung bestätigt bzw. zusagt.

**Tabelle4: Festlegungen zur funktionalen Eignung "Herstellererklärung"**

ID	Bezeichnung	Quelle (Referenz)
<a href="#">A_20060</a>	Versionierung der Konfiguration von Produktinstanzen	gemKPT_Test
<a href="#">A_20061</a>	Beschreibung Art und Umfang der Fehlerkorrektur	gemKPT_Test
<a href="#">A_20065</a>	Nutzung der Dokumententemplates der gematik	gemKPT_Test
<a href="#">A_25392-01</a>	Nutzung Testfallmatrix-Template der gematik	gemKPT_Test
<a href="#">A_27475</a>	Fehlerbehebungsplan	gemKPT_Test
<a href="#">A_27604</a>	Ausführung von gematik-Testfällen in der Testphase EvT	gemKPT_Test
<a href="#">A_27809</a>	Ausführung von gematik-Testfällen in der Testphase Zulassungstest	gemKPT_Test
<a href="#">A_27854</a>	Ausführung von gematik-Lasttests in der Testphase Zulassungstest	gemKPT_Test
<a href="#">TIP1-</a>	Nachstellen von PU-Fehlern in der TU	gemKPT_Test

<a href="#">A_2803-01</a>		
<a href="#">TIP1-A_4191</a>	Keine Echtdaten in RU und TU	gemKPT_Test
<a href="#">TIP1-A_4923-02</a>	Dauerhafte Verfügbarkeit RU und TU	gemKPT_Test
<a href="#">TIP1-A_6088</a>	Unterstützung bei Fehlernachstellung	gemKPT_Test
<a href="#">TIP1-A_6517-02</a>	Eigenverantwortlicher Test: Zulassungsnehmer	gemKPT_Test
<a href="#">TIP1-A_6524-01</a>	Testdokumentation gemäß Vorlagen	gemKPT_Test
<a href="#">TIP1-A_6526-02</a>	Produkttypen: Bereitstellung	gemKPT_Test
<a href="#">TIP1-A_6529</a>	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	gemKPT_Test
<a href="#">TIP1-A_6772</a>	Partnerprodukte bei Interoperabilitätstests	gemKPT_Test
<a href="#">TIP1-A_7334</a>	Risikoabschätzung bezüglich der Interoperabilität	gemKPT_Test
<a href="#">TIP1-A_7335</a>	Bereitstellung der Testdokumentation	gemKPT_Test
<a href="#">GS-A_3695</a>	Grundlegender Aufbau Versionsnummern	gemSpec_OM
<a href="#">GS-A_3696</a>	Zeitpunkt der Erzeugung neuer Versionsnummern	gemSpec_OM
<a href="#">GS-A_3697</a>	Anlass der Erhöhung von Versionsnummern	gemSpec_OM
<a href="#">GS-A_4541</a>	Nutzung der Produkttypversion zur Kompatibilitätsprüfung	gemSpec_OM
<a href="#">GS-A_5025</a>	Versionierung von Produkten auf Basis von zentralen Produkttypen der TI-Plattform und fachanwendungsspezifischen Diensten durch die Produktidentifikation	gemSpec_OM
<a href="#">GS-A_5038</a>	Festlegungen zur Vergabe einer Produktversion	gemSpec_OM
<a href="#">GS-A_5054</a>	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	gemSpec_OM

<a href="#">A_28782</a>	Performance - Telemetriedatenlieferung - Konfiguration Datenlieferung ZETA Guard	gemSpec_Perf
<a href="#">A_27818</a>	Unterstützung der Wartbarkeit des ZETA Guard- Dienstes	gemSpec_ZETA

### 14.7.11 Herstellererklärung sicherheitstechnische Eignung

Sofern in diesem Abschnitt Festlegungen verzeichnet sind, muss der Hersteller bzw. der Anbieter deren Umsetzung und Beachtung zum Nachweis der sicherheitstechnischen Eignung durch eine Herstellererklärung bestätigen bzw. zusagen.

**Tabelle5: Festlegungen zur sicherheitstechnischen Eignung "Herstellererklärung"**

ID	Bezeichnung	Quelle (Referenz)
<a href="#">A_17178</a>	Produktentwicklung: Basisschutz gegen OWASP Top 10 Risiken	gemSpec_DS_Hersteller
<a href="#">A_17179</a>	Auslieferung aktueller zusätzlicher Softwarekomponenten	gemSpec_DS_Hersteller
<a href="#">A_19147</a>	Sicherheitstestplan	gemSpec_DS_Hersteller
<a href="#">A_19148</a>	Sicherheits- und Datenschutzkonzept	gemSpec_DS_Hersteller
<a href="#">A_19150</a>	Umsetzung Sicherheitstestplan	gemSpec_DS_Hersteller
<a href="#">A_19151</a>	Implementierungsspezifische Sicherheitsanforderungen	gemSpec_DS_Hersteller
<a href="#">A_19152</a>	Verwendung eines sicheren Produktlebenszyklus	gemSpec_DS_Hersteller
<a href="#">A_19153</a>	Sicherheitsrelevanter Softwarearchitektur-Review	gemSpec_DS_Hersteller
<a href="#">A_19154</a>	Durchführung einer Bedrohungsanalyse	gemSpec_DS_Hersteller
<a href="#">A_19155</a>	Durchführung sicherheitsrelevanter Quellcode- Reviews	gemSpec_DS_Hersteller
<a href="#">A_19156</a>	Durchführung automatisierter Sicherheitstests	gemSpec_DS_Hersteller
<a href="#">A_19157</a>	Dokumentierter Plan zur Sicherheitsschulung für Entwickler	gemSpec_DS_Hersteller
<a href="#">A_19158</a>	Sicherheitsschulung für Entwickler	gemSpec_DS_Hersteller
<a href="#">A_19159</a>	Dokumentation des sicheren Produktlebenszyklus	gemSpec_DS_Hersteller
<a href="#">A_19160</a>	Änderungs- und	gemSpec_DS_Hersteller



	Konfigurationsmanagementprozess	
<a href="#">A_19163</a>	Rechte der gematik zur sicherheitstechnischen Prüfung des Produktes	gemSpec_DS_Hersteller
<a href="#">A_19164</a>	Mitwirkungspflicht bei Sicherheitsprüfung	gemSpec_DS_Hersteller
<a href="#">A_19165</a>	Auditrechte der gematik zur Prüfung der Herstellerbestätigung	gemSpec_DS_Hersteller
<a href="#">A_22984</a>	Unverzögliche Bewertung von Schwachstellen	gemSpec_DS_Hersteller
<a href="#">A_22985</a>	Bereitstellung der Bewertung von Schwachstellen gegenüber der gematik	gemSpec_DS_Hersteller
<a href="#">A_23029</a>	Bereitstellung von Updates abhängig von der Kritikalität der Schwachstellen	gemSpec_DS_Hersteller
<a href="#">A_23445</a>	Beteiligung der Hersteller am Coordinated Vulnerability Disclosure Programm	gemSpec_DS_Hersteller
<a href="#">GS-A_2330-02</a>	Hersteller: Schwachstellen-Management	gemSpec_DS_Hersteller
<a href="#">GS-A_2525-01</a>	Hersteller: Schließen von Schwachstellen	gemSpec_DS_Hersteller
<a href="#">GS-A_4944-01</a>	Produktentwicklung: Behebung von Sicherheitsmängeln	gemSpec_DS_Hersteller
<a href="#">GS-A_4945-01</a>	Produktentwicklung: Qualitätssicherung	gemSpec_DS_Hersteller
<a href="#">GS-A_4946-01</a>	Produktentwicklung: sichere Programmierung	gemSpec_DS_Hersteller
<a href="#">GS-A_4947-01</a>	Produktentwicklung: Schutz der Vertraulichkeit und Integrität	gemSpec_DS_Hersteller
<a href="#">A_28407</a>	ZETA Guard – Nachweisbarkeit verwendete Version des ZETA-Images	gemSpec_ZETA

## 14.8 Anforderungen an HCC-Dienstleister

*Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet.*

**A\_26995 -HCC-Dienstleister – Private und geheime Schlüssel der VAU im HSM**  
Der HCC-Dienstleister MUSS alle privaten und geheimen Schlüssel, die für den Betrieb des Dienstes und der VAU benötigt werden, in einem Hardware Security Module (HSM) erzeugen und anwenden, z.B. private bzw. geheime Schlüssel, die

- 3555 • zur Authentisierung der Verarbeitungskontexte gegenüber von VAU-Clients und  
3556 Diensten,  
3557 • zur Ver- und Entschlüsselung oder  
3558 • zur Signatur  
3559 genutzt werden.[<=]

3560 *[Sicherheitsgutachten]*

## 3561 **14.9 Anforderungen an die HCC-Dienste der gematik**

3562 *Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet.*

## 3563 **14.10 Anforderungen an HCC-Clients**

3564 Anforderungen an HCC-Clients wird in dieser Spezifikation nicht betrachtet, sondern in  
3565 den Spezifikationen zu ZeroTrust (ZETA)

3566 Die Vertraulichkeit auf Cloud-Seite wird erreicht, indem die Serverkomponente ZETA-  
3567 Guard als HCC-Workload innerhalb der VAU läuft.

## 15 Anhang A - Verzeichnisse

### 15.1 A1 - Abkürzungen

**Tabelle 6 : Im Dokument verwendete Abkürzungen**

Kürzel	Erläuterung
cVM	Confidential VM
FHIR-IG	FHIR Implementation Guide
FIPS	Federal Information Processing Standard
HCC	Healthcare Confidential Computing
HSM	Hardware Security Module
KMS	Key Management Service
RZ	Rechenzentrum
TDBS	HCC-Provider Deployment Repository
TDCAS	Trust Domain Configuration & Attestation Service
TDDR	Trust Domain Deployment Repository
TPM	Trusted Platform Module
VAU	Vertrauenswürdige Ausführungsumgebung
ZETA	ZeroTrust

### 15.2 A2 - Glossar

**Tabelle 7 : Glossar der explizit im Dokument verwendeten Begriffe**

Begriff	Erläuterung


Weitere Begriffserklärungen befinden sich in [gemGlossar].

## **15.3 A3 - Abbildungsverzeichnis**

Abbildung 1: Shared Responsibility - Verteilung der Aufgaben.....	23
Abbildung 2: Governance - Deployment View.....	24
Abbildung 3: Integration von HCC-Diensten mit TI-Diensten und externen Diensten.....	25
Abbildung 4: gematik als Garant für HCC.....	26
Abbildung 5: Designtime- und Runtime-Umgebung.....	28
Abbildung 6: Attestation beispielhaft, vereinfacht.....	31
Abbildung 7: HCC-Services in Designtime- und Runtime-Umgebung.....	34
Abbildung 8: Überblicksdarstellung Tests auf der HCC-Plattform.....	63
Abbildung 9: Staging von Diensten auf der HCC-Plattform.....	65

## **15.4 A4 - Tabellenverzeichnis**

Tabelle 1 : Akteure und ihre Aufgaben.....	51
Tabelle 2: Zulassung von HCC-Providern.....	58
Tabelle3: Festlegungen zur sicherheitstechnischen Eignung "Sicherheitsgutachten".....	98
Tabelle4: Festlegungen zur funktionalen Eignung "Herstellereerklärung".....	99
Tabelle5: Festlegungen zur sicherheitstechnischen Eignung "Herstellereklärung".....	101
Tabelle 6 : Im Dokument verwendete Abkürzungen.....	104
Tabelle 7 : Glossar der explizit im Dokument verwendeten Begriffe.....	104
Tabelle 8 : Referenzierte Dokumente der gematik.....	106
Tabelle 9 : Weitere Referenzen.....	107

## **15.5 A5 - Referenzierte Dokumente**

### **15.5.1 Dokumente der gematik**

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

3600

**Tabelle 8 : Referenzierte Dokumente der gematik**

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemSpec_DS_Anbieter]	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter <a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_DS_Anbieter/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_DS_Anbieter/latest/</a>
[gemRL_PruefSichEig_DS]	gematik: Richtlinie zur Prüfung der Sicherheitseignung <a href="https://gemspec.gematik.de/docs/gemRL/gemRL_PruefSichEig_DS/latest/">https://gemspec.gematik.de/docs/gemRL/gemRL_PruefSichEig_DS/latest/</a>
[gemSpec_DS_Hersteller]	Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Hersteller <a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_DS_Hersteller/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_DS_Hersteller/latest/</a>
[gemSpec_Net]	Übergreifende Spezifikation Netzwerk <a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_Net/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_Net/latest/</a>
[gemSpec_Krypt]	Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur <a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_Krypt/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_Krypt/latest/</a>
[gemSpec_Perf]	Übergreifende Spezifikation Performance und Mengengerüst TI-Plattform <a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_Perf/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_Perf/latest/</a>
[gemSpec_ZETA]	Spezifikation Zero Trust Access (ZETA) <a href="https://gemspec.gematik.de/docs/gemSpec/gemSpec_ZETA/latest/">https://gemspec.gematik.de/docs/gemSpec/gemSpec_ZETA/latest/</a>
[gemKPT_Betr]	Betriebskonzept Online-Produktivbetrieb <a href="https://gemspec.gematik.de/docs/gemKPT/gemKPT_Betr/latest/">https://gemspec.gematik.de/docs/gemKPT/gemKPT_Betr/latest/</a>
[gemRL_Betr_TI]	Übergreifende Richtlinien zum Betrieb der TI <a href="https://gemspec.gematik.de/docs/gemRL/gemRL_Betr_TI/latest/">https://gemspec.gematik.de/docs/gemRL/gemRL_Betr_TI/latest/</a>

3601

## 15.5.2 Weitere Dokumente

3602

**Tabelle 9 : Weitere Referenzen**

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
----------	--

[DDoS-Anbieter]	BSI (15.05.2026) Qualifizierte DDoS-Mitigation Dienstleister <a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.pdf?__blob=publicationFile&amp;v=23">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.pdf?__blob=publicationFile&amp;v=23</a> BSI (01.12.2016) Kriterien für qualifizierte Dienstleister - DDoS-Mitigation Dienstleister <a href="https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation.pdf?__blob=publicationFile&amp;v=1">https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation.pdf?__blob=publicationFile&amp;v=1</a>

3603

3604

3605

3606

3607

3608

3609