

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Healthcare Confidential Computing

Version: 0.9.0_20241118
Revision: 1047926
Stand: 18.11.2024
Status: in Bearbeitung
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_HCC

Dokumentinformationen

Bei dieser Version des Dokumentes handelt es sich um eine Grundlage für den Austausch mit interessierten Anbietern zur weiteren Ausgestaltung der Spezifikation. Eine Folgeversion, die den Prozess der Kommentierung für die Freigabe zur normativen Veröffentlichung durchläuft, wird auf der Basis der Ergebnisse dieses Austauschs erstellt und zu einem späteren Zeitpunkt bereitgestellt.

Änderungen zur Vorversion

Es handelt sich um eine Erstveröffentlichung.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.9.0	18.11.2024		Erstentwurf / Diskussionsgrundlage	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments.....	6
1.1 Zielsetzung.....	6
1.2 Zielgruppe.....	6
1.3 Geltungsbereich.....	6
1.4 Abgrenzung des Dokuments.....	6
1.5 Methodik.....	7
2 Einleitung.....	8
2.1 Inhaltlicher Aufbau dieser Spezifikation.....	9
2.2 Formaler Aufbau dieser Spezifikation.....	9
2.3 Fortschreibung dieser Spezifikation.....	10
3 Sicherheitsziel.....	12
4 Begriffsdefinitionen.....	13
5 Konzepte, Systemkontext und Akteure.....	18
5.1 Confidential Computing.....	18
5.2 Cloud Computing.....	19
5.3 Shared Responsibility.....	20
5.4 Governance.....	21
5.5 Integration mit Diensten außerhalb von HCC.....	22
6 Sicherheitsarchitektur von HCC.....	23
6.1 Trennung zwischen Designtime- und Runtime-Services.....	24
6.2 Attestation des Sicherheitszustands.....	25
6.3 Bootstrapping der technischen Sicherheitsarchitektur.....	29
6.4 Umfang und Grenzen der Initialisierungszeremonie.....	30
6.5 HCC Platform Services.....	30
6.5.1 HSM-Cluster (Runtime).....	31
6.5.2 Trust Domain Configuration & Attestation Service (Runtime).....	31
6.5.3 Key Management Service (Runtime).....	33
6.5.4 Trust Domain Deployment Repository (Runtime).....	33
6.5.5 HCC-Provider Deployment Repository (Runtime).....	34
6.5.6 Trust Domain Build Service (Runtime).....	34
6.5.7 TI Policy Administration Point (Designtime).....	34
6.5.8 TI Design & Configuration Repository (Designtime).....	35
6.5.9 TI Verification & Build Service (Designtime).....	35
6.6 Schlüsselmanagement.....	36

6.6.1 Öffentliche HCC-Service-Identität.....	36
6.6.2 TI-Identität von HCC-Services.....	37
6.6.3 Session-Cache-Schlüssel.....	37
6.6.4 Persistenz-Schlüssel.....	37
6.7 Ausschluss des Betreibers und anderer Angreifer.....	38
6.7.1 Physische Sicherheit der Rechenzentrums Umgebung.....	38
6.7.2 Isolation von Mandanten im Netz.....	39
6.7.3 Prozessisolation.....	39
6.7.4 Sichere Hardware-Komponenten der Runtime TCB.....	41
6.7.5 Sichere Software-Komponenten der Runtime TCB.....	42
6.7.6 Validierung des Mandantenkontextes.....	43
6.8 Service Runtime.....	43
6.9 Integration mit den Zero Trust Services der TI.....	45
6.10 Erreichbarkeit aus dem Internet und aus dem Netz der TI.....	45
6.11 Abwehr von Überlastungsangriffen aus dem Internet.....	46
7 Organisatorische Sicherheit.....	48
7.1 Rollen und Verantwortlichkeiten.....	48
8 Zulassungen und Bestätigungen.....	54
9 Interoperabilität.....	56
10 Integration in das SIEM der TI.....	57
11 Integration in das Testing Framework der TI.....	58
12 Integration in die betriebliche Steuerung der TI.....	59
12.1 Verfügbarkeit und Performance.....	59
12.2 Logging- und Monitoringsysteme.....	59
12.3 Betriebliche Rollen und Verantwortung.....	60
12.4 Anwendbarkeit betrieblicher Prozesse (TI-ITSM).....	60
12.5 Weitere Funktionalität.....	60
13 Sicherheitsanalyse.....	61
13.1 Angreifer.....	61
13.2 Bedrohungen.....	63
14 Anforderungen an HCC.....	64
14.1 HCC-Provider - marktoffenes Angebot.....	64
14.2 HCC-Provider - Bereitstellung HCC-Infrastruktur.....	65
14.3 HCC-Provider - Integration mit gematik.....	67
14.4 HCC-Provider - Mandanten für HCC-Dienstleister.....	69
14.5 HCC-Provider - HCC-Sicherheitsfunktionalität.....	70

14.6 HCC-Provider - Sicherheitsanforderungen.....	72
14.6.1 Bereitstellung geeigneter Hardware.....	72
14.6.2 Schutz der Integrität der VAU.....	74
14.6.3 Schutz der Datenverarbeitung.....	76
14.6.4 Schutz der Daten bei Speicherung.....	77
14.6.5 Schutz der Daten beim verteilten Caching.....	77
14.6.6 Schutz der Daten beim Transport.....	78
14.6.7 Konsistenz des Systemzustands, Logging und Monitoring.....	79
14.7 HCC-Provider - Trust Domain Services und Komponenten.....	79
14.8 HCC-Provider -Verfügbarkeitsanforderungen.....	84
14.9 Anforderungen an HCC-Diensthersteller.....	84
14.10 Anforderungen an HCC-Dienstanbieter.....	84
14.11 Anforderungen an die HCC-Dienste der gematik.....	85
14.12 Anforderungen an HCC-Clients.....	85
15 Anhang A - Verzeichnisse.....	86
15.1 A1 - Abkürzungen.....	86
15.2 A2 - Abbildungsverzeichnis.....	86
15.3 A4 - Tabellenverzeichnis.....	86
15.4 A5 - Referenzierte Dokumente.....	86
15.4.1 Dokumente der gematik.....	86
15.4.2 Weitere Dokumente.....	87

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 Vertrauenswürdigem 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

Anforderungen 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 werden im Dokument wie folgt dargestellt:

<AFO-ID> - <Titel der Afo>

Text / Beschreibung

[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und Textmarke [<=] angeführten Inhalte.

2 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 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.

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.

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.

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 substanziell zu vereinfachen.

2.1 Inhaltlicher Aufbau dieser Spezifikation

Healthcare Confidential Computing definiert eine Plattform für die vertrauenswürdige Ausführung von Diensten der TI, jedoch keine im eigentlichen Sinne fachliche Funktionalität. Die fachliche Funktionalität 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 Produktspezifikation.

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 Nachweispflichten und 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 anwendungsübergreifende 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 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.

2.2 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.

2.3 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 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.

- Die Isolationsgarantien von Enklaven oder Confidential VMs werden regelmäßig durch neu entdeckte Schwachstellen, insbesondere durch Seitenkanäle, infrage gestellt.
- Die Möglichkeiten zur Abbildung einer anbieterunabhängigen Governance-Rolle befinden sich noch in der Entstehung. Das vorliegende Dokument stellt gerade hierzu einen Entwurf dar.
- Standards z. B. für die Formate, Inhalte und Protokolle für Remote Attestation befinden sich noch im Entstehungsprozess.
- 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 konnten. 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.
- Ein integriertes und formales Modell für die Plattformsicherheit fehlt bisher.

Die vorliegende Spezifikation versucht 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 (insbesondere zu Schwachstellen) 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.

Gleichzeitig sollten und können HCC-Provider damit rechnen, dass Weiterentwicklungen der Technik in Zukunft auch Vereinfachungen bzw. Entlastungen ermöglichen werden.

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 und Trust und Provisioning Models.
- 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.
- die Erweiterung von Steuerungsmöglichkeiten, die der HCC-Provider seinen Kunden zur Verfügung stellen soll. Dies betrifft 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), die betrieblich jedem Fachdienst zugeordnet werden müssen.

- die Erweiterungen der Service Portfolios der HCC-Anbieter.
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 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 Telematikinfrasturktur 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 (siehe Abschnitt 13.1- Angreifer) 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 eingehender 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.

4 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 bereit, der dazu dient, den kryptographischen Vertrauensraum der TI für HCC (**HCC-Trust-Domain**) in seiner Infrastruktur verfügbar zu machen.

HCC-Dienst: 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 aus dem Netz der TI an den HCC-Dienst und der Responses zurück an Clients, wenn solche Komponenten dem Betreiber oder Angreifern Einblick in individuelles Nutzerverhalten ermöglichen könnten. 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 auf der Basis von Measured Boot eine eindeutige **Workload Identity** (in Form von 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 prüfen und im Erfolgsfall 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 (ggf. 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 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 im Bedarfsfall 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 (siehe [gemSpec_Krypt]). Insbesondere die Möglichkeit zur Verwendung von reinem TLS wirkt sich auf die dem Verarbeitungskontext vorgelagerten Infrastrukturkomponenten sowie auf die Definition des anwendungsübergreifend interoperablen Client-Zugriffsprotokolls aus, da in diesem Fall DDoS-Schutzkomponenten, Firewalls, Load Balancer, API- und Ingress-Gateways keine Entschlüsselung der Payload 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-Runtime-Management: Gesamtheit der Komponenten für das betriebliche Management der Laufzeitumgebung einer HCC-Infrastruktur, u.a. für das Deployment von HCC-Hosts und Workload-Images, für das Monitoring und für die betriebliche Protokollierung.

Das HCC-Runtime-Management umfasst ebenfalls das Management von Schlüsseln, z. B. in einem HSM-Cluster. Es wird davon ausgegangen, dass das HCC-Runtime-Management weitgehend automatisiert ist.

HCC-Design & Configuration (HCC-D&C): Gesamtheit der Komponenten für Erstellung, Konfiguration, Autorisierung und Verwaltung der Komponenten von HCC. Es umfasst Repositories, Build-Pipelines, Policy Administration und Prozesse zur Freigabe der Releases von Workload-Images, Plattformkomponenten etc. HCC-D&C sichert die Integrität und Authentizität aller HCC-Komponenten, Policies und Konfigurationseinträge kryptographisch ab.

HCC-Workload-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.

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. Kunde bzw. Mandant des HCC-Providers sind HCC-Dienstanbieter. Wenn ein Anbieter 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-Platform-Instance (HCC-PI): Eine an einem Standort eines HCC-Providers aufgebaute und betriebene HCC-Infrastruktur inkl. Services, Komponenten und Prozessen.

HCC-Tenant: 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-Tenants 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 mehrerer (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.

HCC-Attestation: Eine Kombination aus Services und (Konfigurations-) Daten, die in jeder HCC-PI vorhanden ist und die HCC-TD am jeweiligen Standort etabliert, d. h. für alle HCC-Tenants die Workload Attestation für ihre HCC-Dienste übernimmt und die kryptographischen Dienstidentitäten bereitstellt.

Die Verwaltung der HCC-Attestation liegt in der Verantwortlichkeit der gematik unter Einbeziehung weiterer Stakeholder. Die zentrale Komponente der HCC-Attestation ist der **Trust Domain Configuration & Attestation Service (TDCAS)**.

HCC-Policy: Regelwerk für die Steuerung des Systems inkl. seiner Konfiguration.

Die HCC-Policy ist als Teil der TI-Policy für die TI 2.0 anzusehen. Sie dient insbesondere dazu, HCC-Laufzeitumgebungen möglichst weitgehend automatisiert betreiben zu können. Die HCC-Policy umfasst alle Daten zur Konfiguration der Laufzeitumgebung in menschen- und maschinenlesbarer Form sowie alle Referenzwerte für die Attestation. Sie ist ein Kernelement von HCC-D&C und muss innerhalb eines kryptographisch geschützten Policy-Managements verwaltet werden, das die für die Vertrauenswürdigkeit von HCC notwendigen organisatorischen Zuweisungen, Freigabeprozesse und organisatorischen Trennungsgebote umfasst und absichert.

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

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

- Verschlüsselung des Arbeitsspeichers zur Abwehr von Angriffen auf Daten im Arbeitsspeicher mittels Entnahme des Arbeitsspeichers und Auslesens außerhalb des Schutzes durch den Server sowie
- Fähigkeit zur Attestation des Systems inkl. Hardware, Firmware, Hypervisor, Betriebssystem, Plattformkomponenten und Anwendungskomponenten auf der Basis eines Hardware-geschützten Vertrauensankers.

Im weiteren Sinne ist der CC-Stack durch die Gesamtheit der Anforderungen in der vorliegenden Spezifikation definiert.

5 Konzepte, Systemkontext und Akteure

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

5.1 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.
- Die Auswertung nutzer- bzw. institutionsbezogenen Verhaltens durch den Anbieter ist im Confidential Computing weitgehend systematisch durch die Systemarchitektur 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.
- Die Software der Dienste und an der Verarbeitung der Nutzdaten beteiligter Komponenten wird mittels sicherer Prozesse entwickelt, durch anerkannte Prüfstellen begutachtet und integritätsgeschützt in die Betriebsumgebung eingebracht.
- Die Hardware von an der Verarbeitung der Nutzdaten beteiligten Systeme ist hinsichtlich ihrer Eignung für das erforderliche Vertrauensniveau geprüft und wird über sichere Prozesse beschafft und verwaltet.

- Die Wirksamkeit der technischen Mittel wird durch die gematik, als unabhängige Institution und Governance-Verantwortliche für die TI, möglichst öffentlich, kontinuierlich und prüfbar dargestellt.
- Die gematik basiert ihre Datenschutzgarantien auf einer Produktzulassung für die HCC-Infrastruktur, auf geeigneten weiteren Zulassungs-, Begutachtungs- und Zertifizierungsprozessen, die den Anbietern auferlegt sind, sowie auf der Attestation der laufenden Dienste.

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 aus dem Internet (und derzeit noch aus dem zentralen Netz der TI) und Verfügbarkeit der Transport-, Verarbeitungs- und Speicherkapazitäten. Seine administrativen Eingriffsmöglichkeiten enden an den Grenzen der Trusted Computing Base.

5.2 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-Computings zu ermöglichen.

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

Ein TI-Diensteanbieter 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 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.

Der Diensteanbieter kann für seinen Dienst damit die vom HCC-Provider bereitgestellten Systemressourcen nutzen und darauf verzichten 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 Diensteanbieter konfiguriert werden, und muss solche Funktionalitäten nicht selbst entwickeln. Der Diensteanbieter 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.

5.3 Shared Responsibility

Für die Bereitstellung von Fachdiensten resultiert beim Confidential Computing in der Cloud ein Modell von „Shared Responsibility“ in dem der Fachdienstanbieter 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 der HCC-Plattform anbietet.

Die geteilte Verantwortlichkeit zwischen Fachdienstanbieter und HCC-Provider wird durch die Verantwortung der gematik als Garant für den Vertrauensraum der TI erweitert.

Bei der Verarbeitung von Daten mit hohem bzw. sehr hohem Schutzbedarf außerhalb der Hoheit anderer autorisierter Akteure in der TI und für Anwendungen mit hohen Anforderungen an ihre durchgängige Verfügbarkeit bildet sich die Verantwortlichkeit der gematik 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.

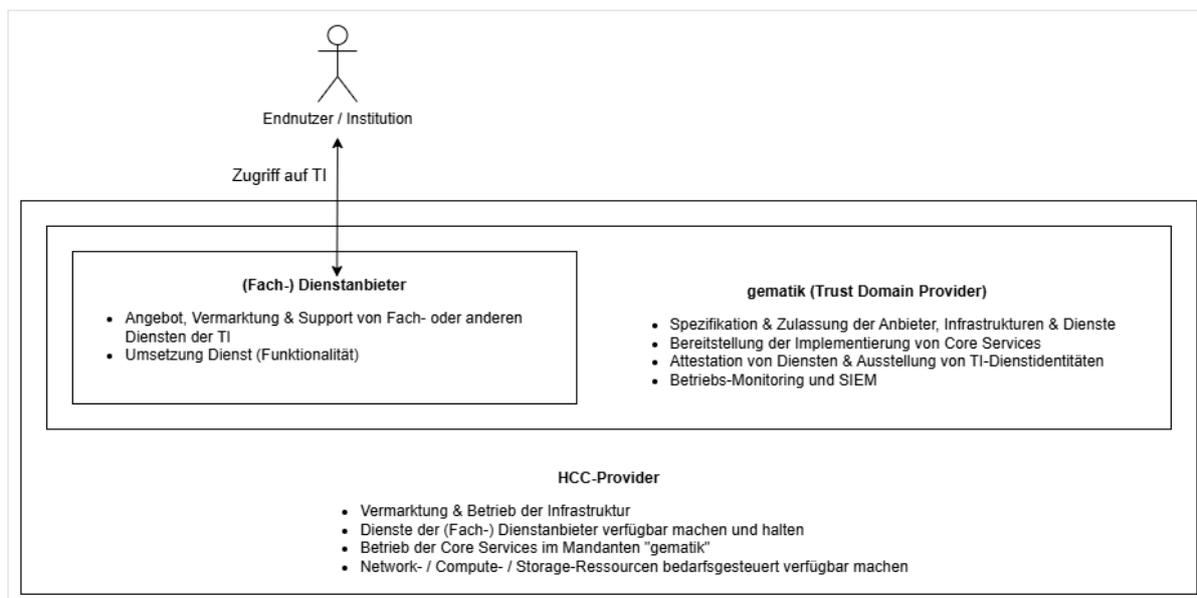


Abbildung 1: Shared Responsibility - Verteilung der Aufgaben

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

5.4 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 Basisdienste der

TI, die sowohl den HCC-Dienst als auch die HCC-Infrastruktur zur Laufzeit den Governance-Prozessen der gematik unterstellen.

Die Basisdienste müssen direkt in der Infrastruktur der HCC-Provider bereitgestellt werden, damit die hohen Schutzbedarfe für die verarbeiteten Daten erfüllt und gleichzeitig eine hohe Verfügbarkeit aller Schnittstellen innerhalb der Betriebsverantwortung des HCC-Providers erreicht werden können. Basisdienste sind Image- und Konfigurations-Repositories bzw. Registries, ein Attestation-Service, betriebliche Monitoring Schnittstellen, etc. Ein wichtiger Basisdienst ist der in jedem Rechenzentrum eines HCC-Providers vor Ort in einer Zeremonie unter Mitwirkung der gematik initialisierte Hardware-Vertrauensanker für den lokalen HCC-Vertrauensraum der TI in einem HSM-Cluster.

Um die Basisdienste hoheitlich steuern zu können, stellt der HCC-Provider der gematik einen spezifischen Mandantenkontext zur Verfügung in dem Basisdienste der TI verwaltet und betrieben werden. Die funktionalen Schnittstellen der Basisdienste müssen aus den Mandantenkontexten der Dienstanbieter 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.

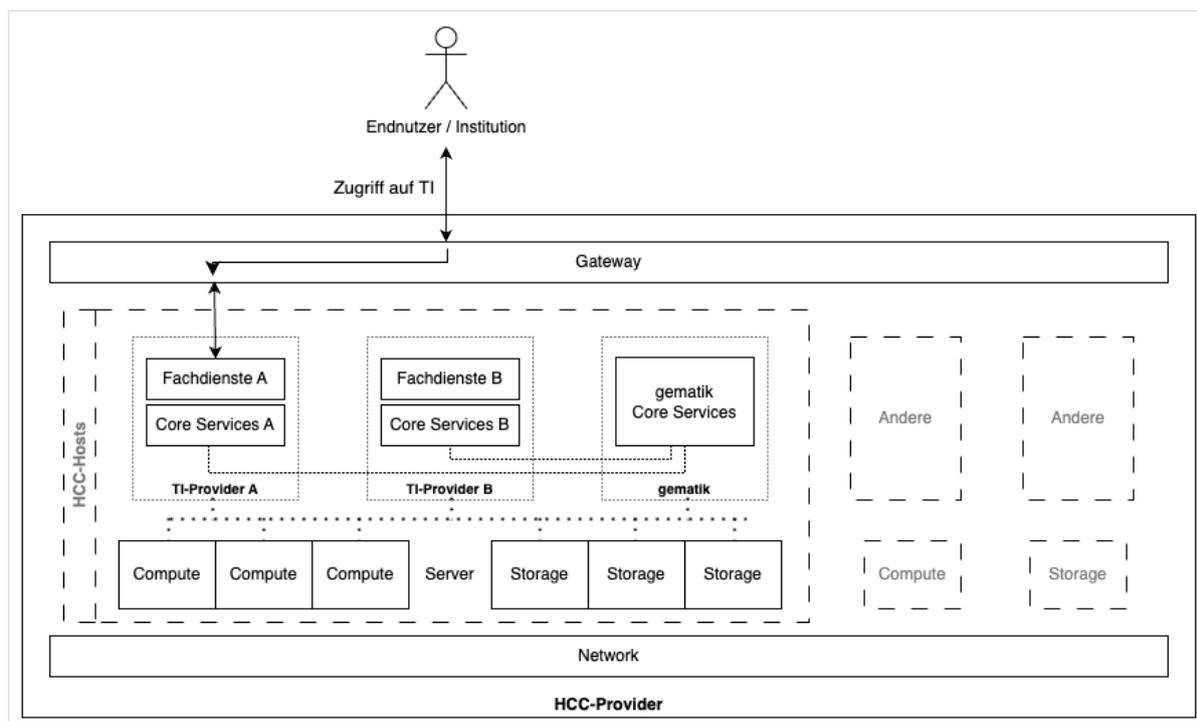


Abbildung 2: Governance - Deployment View

5.5 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.

Beispiele sind Entwicklungs- und Testplattformen, Verwaltungswerkzeuge, Primärsysteme 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 anderen Diensten erfolgt über Gateway-Funktionen beim HCC-Provider, die neben der Datenverkehrssteuerung auch eine erste Stufe des Ausschlusses von unbekanntem externen Verbindungspartnern umsetzen. Die Verwendung solcher Gateways im Kontext eines HCC-Dienstes setzt damit Konfigurationseinstellungen auf Policy- und Netzwerkebene voraus. Die Konfigurationseinstellungen sollen im Mandantenkontext angesiedelt sein.

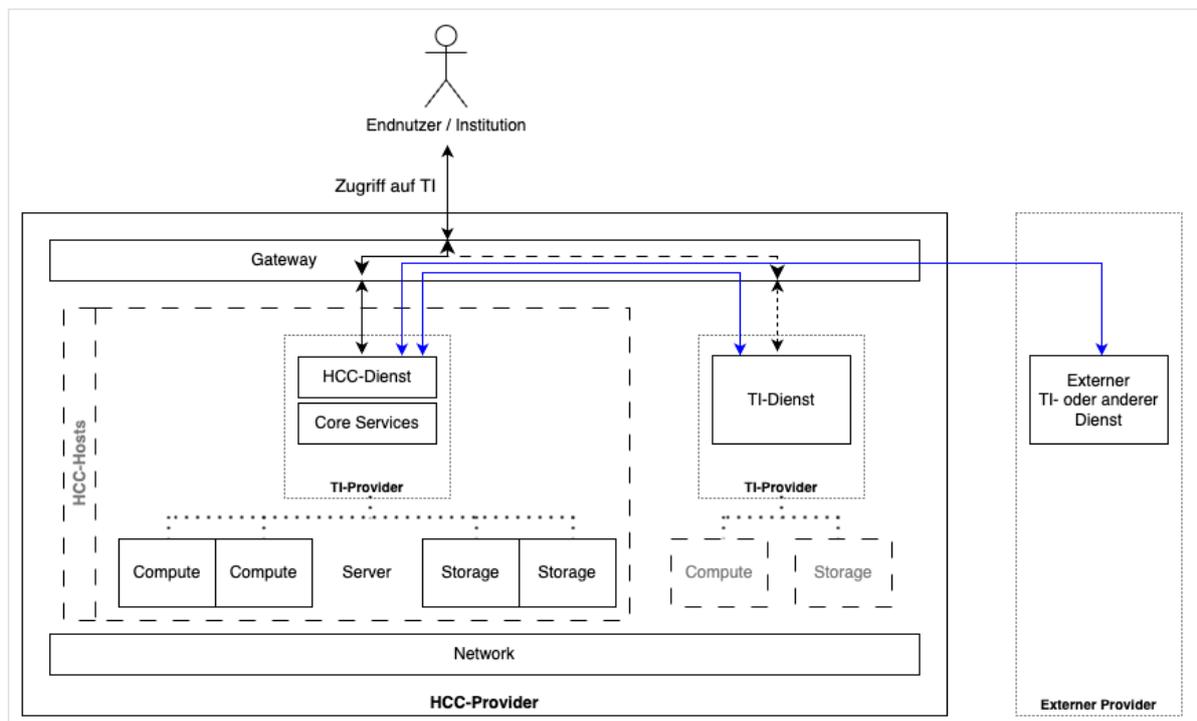


Abbildung 3: Integration mit HCC- und TI-externen Diensten

6 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 systematisch vom Zugriff auf die Datenverarbeitung auszuschließen.

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 Normen wie ISO 27001 und viele weitere abgesichert sind. Ein entsprechendes betriebliches Umfeld wird vorausgesetzt (siehe Kapitel 8- Zulassungen und Bestätigungen).

Die Sicherheitsarchitektur von HCC beschreibt daher primär den Aufbau und die Komponenten, die innerhalb der Rechenzentrums Umgebung das substanziiell 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 insofern einen Sonderfall von Confidential Computing in der Cloud dar, als Cloud Computing i. A. keinen unabhängigen Dritten, wie die gematik, als technisch integrierten Garanten für die Sicherheits- und Privacy-Eigenschaften vorsieht. Vergleichbare Konstellationen könnten jedoch auch für andere Anwendungsbereiche mit staatlicher Aufsicht und hohem Schutzbedarf entstehen.

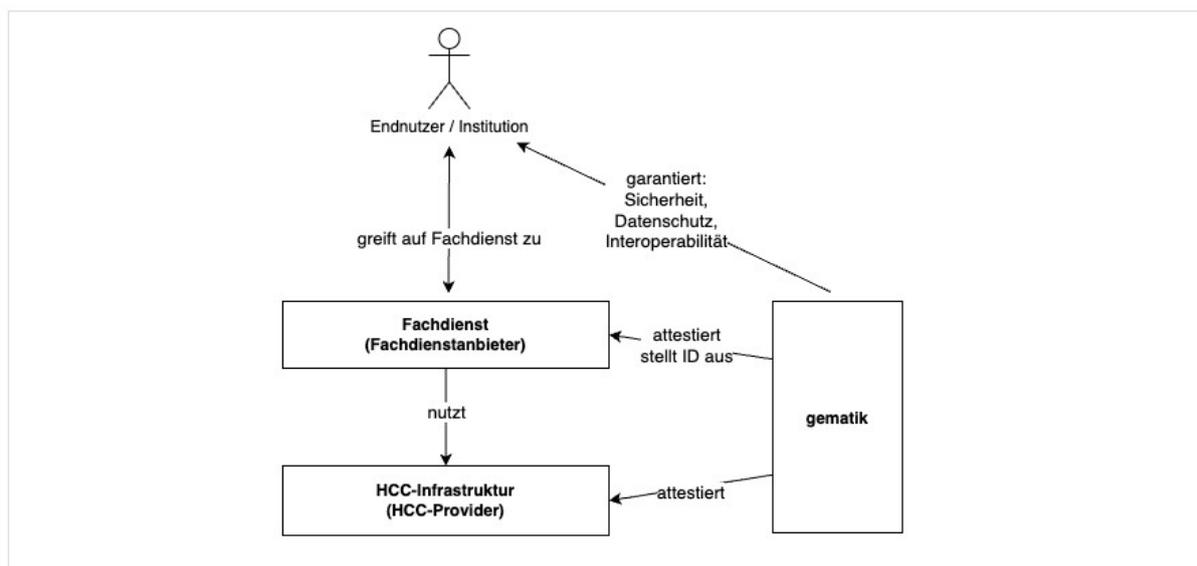


Abbildung 4: gematik als Garant für HCC

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

6.1 Trennung zwischen Designtime- und Runtime-Services

Der Aufbau des Systems trennt die zur Laufzeit der Plattform- und Anwendungsdienste erforderlichen Artefakte von den Designtime-Systemen zur Bereitstellung dieser Artefakte. Die Trennung wird mittels Signierung der zur Laufzeit benötigten Artefakte in der Designtime erreicht.

Ein TI Design & Configuration Repository in dem ggf. komplexe organisatorische Abläufe umgesetzt sein 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, der die Umwandlung durchführt, die umgewandelten Artefakte zurückliefert (und ggf. signiert) und gleichzeitig die Referenzwerte für die Attestation ermittelt. Der Vorgang soll sowohl automatisiert als auch manuell durchgeführt werden können.

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

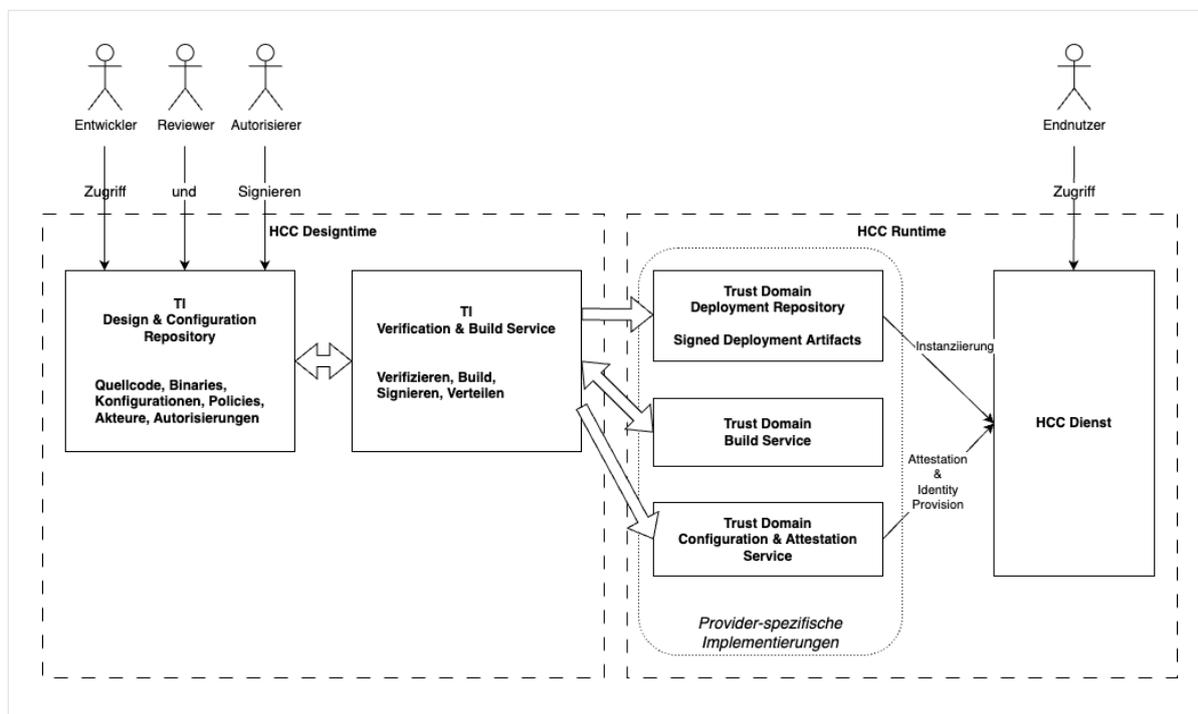


Abbildung 5: Designtime- und Runtime-Umgebung

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.

6.2 Attestation des Sicherheitszustands

Basis für die Erreichung der Sicherheitsziele von HCC ist ein wohldefinierter Sollzustand und eine stets aktuelle und gegen den Sollzustand validierte Erfassung des Istzustands aller Systeme in der Trusted Computing Base.

Die Definition des Sollzustands 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 Istzustandes, zum Abgleich mit dem Sollzustand 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 verwendeten Komponenten abhängen, ist der TDCAS anbieterspezifisch umgesetzt. HCC-Provider können ihre HCC-Stacks auf der Basis verschiedener Technologien, wie Intel SGX, Intel TDX, AMD SEV-SNP, ARM CCA, etc. aufbauen, wenn diese Technologien sowohl die Speicherverschlüsselung als auch die Attestation des HCC-Stacks (inkl. Workloads)

unterstützen, ggf. in Kombination mit einem TPM. Der TDCAS muss eine unabhängig begutachtete Software sein (inkl. Source Code Review) und das Gutachten der gematik vorgelegt werden. 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, die aktuell zugelassenen Versionen aller zur TCB gehörenden Software-Komponenten und Konfigurationen sowie weitere Daten registriert. Die Konfigurationsdatenbank bildet den Sollzustand ab und wird über administrative Prozesse gefüllt, die in der Designtime-Umgebung liegen.

Für jede HCC-Dienstinstanz wird das Speicherabbild gemessen, während sie als Enklave oder Confidential VM gestartet wird. Anschließend ruft sie einen Attestation Report ab, der von der Hardware und Firmware der CPU bzw. vom TPM des registrierten HCC-Hosts geschützt und mit einem Root of Trust (for Measurement) signiert ist. Der Report enthält auch die für Confidential Computing notwendigen Angaben zu aller Software und zur Konfiguration des Hosts.

Der Root of Trust (for Measurement) muss von einem vom HCC-Provider unabhängigen Hardware-Hersteller kommen, um ihn jedem Einfluss seitens des HCC-Providers zu entziehen. Alternativ kann ein begutachtetes (ggf. zertifiziertes) Verfahren des HCC-Providers zur Einbringung und Nutzung eines Root of Trust (for Measurement) eingesetzt werden das Manipulationen seitens des HCC-Providers ausschließt. Letztere Möglichkeit könnte insbesondere für Cloud-Provider interessant sein, die eigene Hardware-Komponenten einsetzen und auf diesen ihre Sicherheitsarchitektur aufbauen, ist jedoch vermutlich aufwändig.

Der Attestation Report 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 HCC registrierten Server. Damit kann der TDCAS die Signaturen der Attestation Reports prüfen. Attestation Reports enthalten die Ergebnisse der Messungen in der Form von kryptographischen Hash-Werten. In dieser Form sind daher auch die Referenzwerte für die zugelassenen Komponenten in der Konfigurationsdatenbank des TDCAS registriert.

Die Datenbank umfasst darüber hinaus 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 Designtime- in die Runtime-Umgebungen automatisiert.

Erst im Anschluss an eine erfolgreiche Verifikation des Attestation Reports durch den TCCAS 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.

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

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

- Dienstzertifikate mit kurzer Laufzeit
- Das Setzen eines erweiterten Attributs im Dienstzertifikat, das eine Referenz auf den Log-Eintrag des spezifischen Attestationsvorgangs darstellt. Clients können eine

Funktion zur Interpretation der Referenz als URL und 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 mittels monotoner Versionszähler gegen Rollback geschützt.

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. Auch der private Schlüssel zum Sub-CA-Zertifikat des TDCAS wird im HSM-Cluster verwaltet.

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 Attestation kann in die CPU integriert sein, oder auch in ein TPM. Auch Kombinationen sind möglich (bzw. notwendig, um bei der Nutzung bestimmter Confidential Computing Technologien die Anforderung zur Erfassung des gesamten CC-Stacks umzusetzen).

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

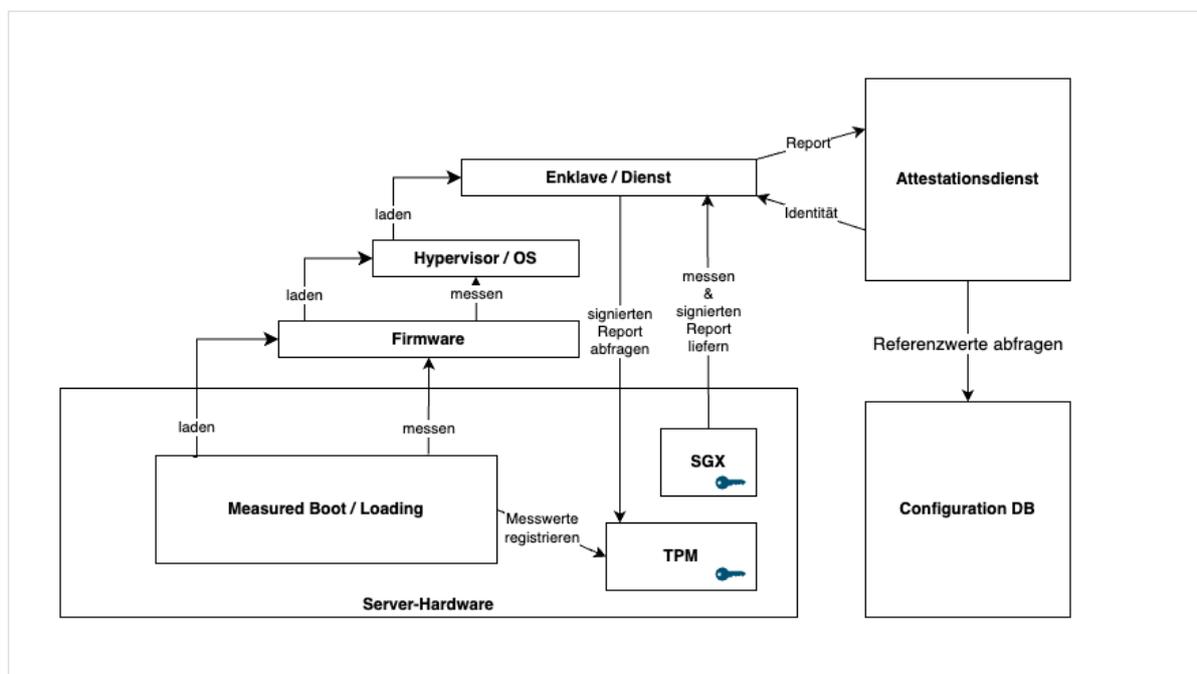


Abbildung 6: Attestation beispielhaft, vereinfacht

Die notwendigerweise system- und technologiespezifische Ausgestaltung der HCC-Umgebung inkl. der Attestation durch die HCC-Provider steht einer Standardisierung im Rahmen der vorliegenden Spezifikation entgegen. 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 hier derzeit 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 benötigt. Solche Mechanismen vergrößern im Normalfall die TCB, können damit selbst zur Angriffsfläche beitragen und sollten bei konsequenter Trennung zwischen statisch integritätsgeschützten und zur Laufzeit veränderbaren Speicherinhalten by Design entbehrlich sein.

Für alle außerhalb der Enklaven oder Confidential VMs laufenden Software-Komponenten der HCC-Host-Plattform – wie Firmware, Hypervisor, Betriebssystem und Provisionierungskomponenten – müssen Attestationsreferenzwerte im TI Design & Configuration Repository hinterlegt sein.

Die Attestation der Host-Plattform außerhalb der Enklaven oder VMs dient primär dem Integritätsschutz der HCC-Hosts. Dieser ist erforderlich, da Enklaven oder VMs 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 Enklaven oder VMs laufenden Verarbeitungen über Seitenkanäle angreift. Der TPM-basierte Attestationsreport wird in die Attestation der Enklaven oder VMs eingebettet.

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. Updates erfordern daher grundsätzlich einen Neustart des Hosts.

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. 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.

6.3 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. 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.

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 in Abschnitt 5.2 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 mit dem Signer-Zertifikat des TI Verification & Build Service konfiguriert.

6.4 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-Dienstanbietern 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.

6.5 HCC Platform 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-Tenants 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:

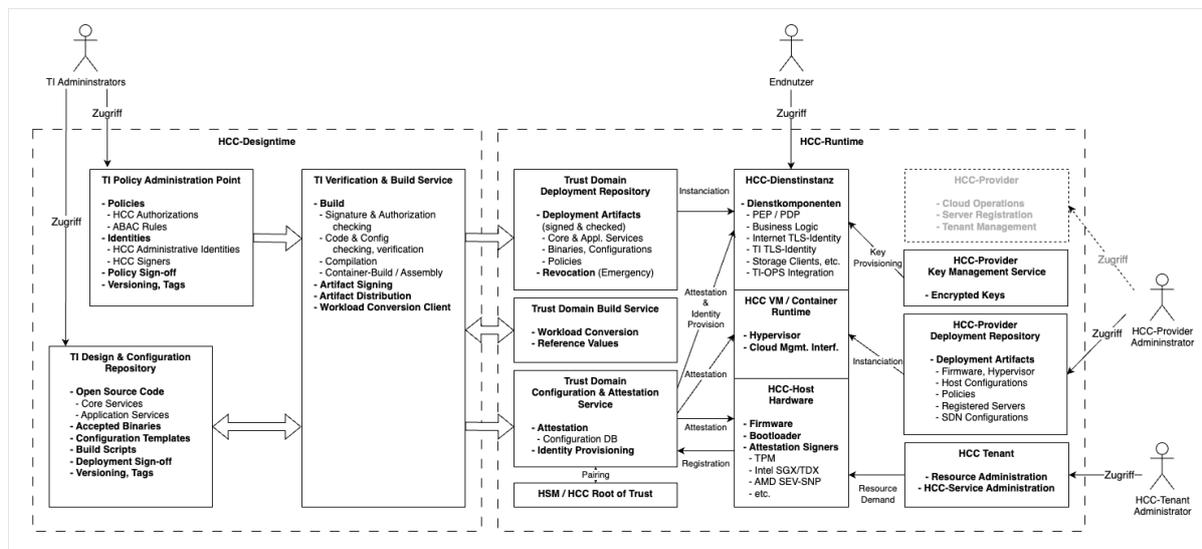


Abbildung 7: HCC-Services in Designtime- und Runtime-Umgebung

6.5.1 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-Workload-Hersteller müssen solche Libraries in ihre Workloads integrieren können (operativ und rechtlich).

6.5.2 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 der Plattform.

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

Zu den für den Attestationsdienst notwendigen Konfigurationsdaten gehören das Sub-CA-Zertifikat für die Ausstellung der HCC-Dienstidentitäten sowie die Identität des Signers der vom TDCAS benötigten Referenzdaten zur Prüfung der Authentizität dieser Daten. Das Schlüsselpaar des 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 SGX in Kombination mit einem TPM werden folgende Schritte durchlaufen:

- Der TDCAS wird von allen Hosts 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), um festzustellen, ob der Host mit zulässiger Firmware und einem zulässigen Boot Image inkl. aller für den Betrieb als Container Runtime erforderlichen Software-Komponenten gestartet wurde.
- Wenn das der Fall ist, wird angenommen, dass weiteres Laden von Software-Komponenten, z. B. das Laden der Container Images der Enklaven, von einer bekannten und vertrauenswürdigen Software-Komponente auf dem Host ausgeführt wird, so dass nur korrekt signierte Container 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 SGX-Signer-Key des Hosts der Enklave signierten Attestation Reports gegen Referenzwerte für die Enklave prüfen zu lassen. Im Erfolgsfall provisioniert der TDCAS die Service Identitäten für die Enklave. 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.

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

6.5.3 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 zum Kern der TCB. Es muss trotzdem sichergestellt sein, dass (verschlüsseltes) Schlüsselmaterial nur innerhalb der für HCC qualifizierten Rechenzentrumsumgebungen verwaltet wird und diese nicht verlässt.

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

6.5.4 Trust Domain Deployment Repository (Runtime)

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

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

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

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

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

6.5.5 HCC-Provider Deployment Repository (Runtime)

Das HCC-Provider Deployment Repository ist der (logische) Teil des betrieblichen Steuerungssystems des HCC-Providers, der die Software-Komponenten und Konfigurationen zur Bereitstellung der HCC-Laufzeitumgebungen sowie die Registrierungsdaten für alle beim HCC-Provider eingesetzten HCC-Hosts umfasst. Es kann

durch verschiedene Systeme des HCC-Providers realisiert sein, wird von ihm verwaltet und gehört nicht zur TCB.

6.5.6 Trust Domain Build Service (Runtime)

Der Trust Domain Build Service ist ein mit der Laufzeitumgebung 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. In seiner Nutzung ist der Service eher der Designtime zuzurechnen. Er wird via API durch den TI Verification & Build Service verwendet, kann jedoch von der gematik, von HCC-Diensteanbietern oder von HCC-Workload Herstellern zu Testzwecken auch manuell genutzt werden.

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.

6.5.7 TI Policy Administration Point (Designtime)

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

Der TI Policy Administration Point stellt alle Funktionalitäten zur Administration der Policy 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 für menschliche oder institutionelle Akteure oder Dienste, die an der Verwaltung der HCC Trust Domain beteiligt sind. Er enthält keine Endnutzeridentitäten der TI und keine an den fachlichen Prozessen der TI beteiligten Institutions- oder Organisationsidentitäten. Er 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.

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 der Sicherheitsarchitektur von HCC und daher hier dargestellt.

6.5.8 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 wurde.

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 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 in der Verantwortung der gematik. Es wird von der gematik verantwortet, entwickelt und weiterentwickelt. Er ist daher nicht Gegenstand der Zulassung von HCC-Providern, jedoch notwendig für das Verständnis 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.

6.5.9 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.

Referenzwerte für Binaries und Konfigurationen werden durch den Build Service 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-Enklave und Erzeugung des Attestation Reports 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 bereits während der Zeremonie erstellt wird. Der TI Verification & Build Service ist nicht Gegenstand der Zulassung von HCC-Providern, jedoch notwendig für das Verständnis der Sicherheitsarchitektur von HCC und daher hier dargestellt.

6.6 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.

6.6.1 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 bereitgestellter 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 erhöhten Lasten 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 im Rahmen der Attestierung 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.

6.6.2 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.

6.6.3 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.

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-Identifizierer als Parameter für die Schlüsselableitung verwendet werden.

6.6.4 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. 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 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 als Key Derivation Keys ausgelegt.

Da Persistenz-Schlüssel nicht ohne Umschlüsselung persistierter Daten 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.

6.7 Ausschluss des Betreibers und anderer Angreifer

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 mittels der Komponenten 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.

6.7.1 Physische Sicherheit der Rechenzentrums Umgebung

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 [8... 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 Rechenzentrums Umgebung. Darüber hinaus müssen alle Aktivitäten in der physischen Rechenzentrums Umgebung aufgabenbezogen organisiert und organisatorisch unabhängig überwacht werden. Geeignete Schleusen müssen verhindern, dass unzulässige Mittel durch Mitarbeiter in die Rechenzentrums Umgebung eingebracht werden können.

6.7.2 Isolation von Mandanten im Netz

Ein wesentlicher Faktor der Sicherheit von Cloud-Infrastrukturen ist die Isolation der Dienste von 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 erhalten bleibt.

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 gegeben. Dabei haben Cloud-native Services Netzwerkadressen, die aus verschiedenen Mandantenkontexten erreicht werden können. Sie stellen über diese Adressen APIs bereit, die eine auf Mandanten bezogene Zugriffskontrolle umsetzen.

Obwohl die Systeme und Mechanismen zur Mandantentrennung in der Infrastruktur eines HCC-Providers nicht unmittelbar zur Trusted Computing Base von HCC gerechnet werden,

ist die Sicherheit auf Netzwerkebene 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. Weitergehende Anforderung müssen im Rahmen der vorliegenden Spezifikation nicht gestellt werden.

6.7.3 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 Accesses) 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 gefixt. Sie sind jedoch schwer prinzipiell auszuschließen, da Mechanismen zur Steigerung der Performance der Prozessoren ihrer eigenen komplizierten Logik 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:

- Angriffscodes des Anbieters könnten Seitenkanäle auszunutzen versuchen, um Schlüsselmaterial oder sensible Nutzdaten aus der Confidential VM oder Enklave 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.
- Angriffscodes, die innerhalb anderer Confidential VMs oder Enklaven läuft, könnten Seitenkanäle auszunutzen versuchen, um Schlüsselmaterial oder sensible Nutzdaten aus der Confidential VM oder Enklave zu extrahieren.

Die Ausnutzung von Seitenkanal-Schwachstellen ohne eine Ausführung von Angriffscodes auf dem Zielsystem erscheint 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 Angriffscodes „on the fly“ zu generieren. Es wird angenommen, dass dies durch Härtung sowohl der Systemsoftware als auch der Anwendungssoftware hinreichend abgewehrt wird.

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

Angriffe aus Confidential VMs oder Enklaven 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. Dabei kann ein HCC-Host jedoch HCC-Workloads verschiedener HCC-Tenants ausführen. Diese Anforderung schränkt den HCC-Provider in seiner Flexibilität bei der Verteilung von Workloads ein, ermöglicht jedoch weiterhin HCC-Hosts als geteilte Ressourcen innerhalb der HCC-Trust-Domain zu verwenden. Der HCC-Provider muss sein Cloud-Management mit der Fähigkeit ausstatten, HCC-Hosts als HCC-exklusive aber HCC-Tenant-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 Rechnung trägt.

Für den Ausschluss von Angriffscode 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 stellen können anstelle von SmartNICs eingesetzt werden. Auf dem Workload-Prozessor verbleibt dann z. B. lediglich ein Hypervisor, d. h. eine besonders kleine, gut zu härtende 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 nicht sehr verbreitet. Sie bietet sich jedoch längerfristiger als Standard für HCC an.

6.7.4 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.

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. Hierzu gehört, dass HCC-Hosts keine offenen Ports haben dürfen, über die ein Angriff mittels eingesteckter Hardware (z. B. USB-Stick) erfolgen kann.

6.7.5 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 die Verwendung eines vereinfachten Treibers. Die statische Natur der attestierbaren Workload-Images erübrigt die Verwendung von Komponenten zur Absicherung von Veränderungen an der Software (wie Viren-Scanner o. Ä.).

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 VAU-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, sollen 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.

6.7.6 Validierung des Mandantenkontextes

In der Cloud stellt der Mandantenkontext einen „äußeren“ Security Perimeter dar, den die Dienste des Mandanten von den Diensten anderer Mandanten in derselben Rechenzentrumsumgebung isoliert und 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. Es wird erwartet, dass sich konkretere Anforderungen aus einem zukünftigen Austausch mit der Industrie zu diesem Thema ergeben.

6.8 Service Runtime

Cloud-Infrastrukturen können eine ganze Reihe verschiedener Ebenen für die Einbringung von Diensten bereitstellen (Bare Metal, Virtual Machine, Container, Serverless). Während die Minimierung der TCB in Richtung Bare Metal weist, zeigen die Anforderungen nach High Availability und Elastizität in Richtung höherer Ebenen des Deployments. Als Standard werden derzeit containerisierte Workloads angesehen. Diese Form des Deployments müssen HCC-Provider daher mindestens anbieten.

Auch die vom HCC-Provider eingesetzte Confidential Computing Technologie kann auf verschiedenen Ebenen ansetzen, wobei nicht alle Ebenen dieselben Sicherheitsgarantien

realisieren. Unter der Annahme einer Container-Runtime sind die folgenden Umsetzungen denkbar:

Tabelle 1: Mapping Provisioning- und CC-Modelle

Provisioning-Modell	CC-Modell	Sicherheitsleistungen
Bare Metal Container Runtime on BM	Intel TME TPM	Arbeitsspeicherverschlüsselung Attestation Gesamtsystem
Virtual Machine Container Runtime in VM	Intel TDX AMD SEV-SNP ARM CCA (+ TPM)	Arbeitsspeicherverschlüsselung (pro VM) Attestation HW/FW + VM (+ Attestation Gesamtsystem)
Container Runtime	Intel SGX (+ TPM)	Arbeitsspeicherverschlüsselung (alle Enklaven) Attestation HW/FW + Enklave (Prozess) (+ Attestation Gesamtsystem)
Serverless	Alle CC-Modelle als Basis denkbar	Sicherheitsleistungen des Basis-CC-Modells (Arbeitsspeicherverschlüsselung, Attestation der Serverless Runtime) Sicherheitseigenschaften der Serverless Runtime

Intel TDX lässt sich in Kombination mit Intel SGX einsetzen, d. h., innerhalb einer attestierten VM können separat attestierte SGX-Enklaven gestartet werden.

ARM CCA ist kein Produkt im gleichen Sinne wie Intel SGX/TDX oder AMD SEV-SNP, sondern eine Spezifikation, die von den Lizenznehmern von ARM umgesetzt werden kann.

Für die Umsetzung des Serverless Provisioning-Modells gibt es derzeit keinen der gematik bekannten, direkten Confidential Computing Mechanismus mit angepasster Hardware-Unterstützung. Da solche Funktionen on-Demand gestartet und anschließend sofort wieder terminiert werden, ist der Overhead zur Integration mit Attestationsmechanismen der Hardware sowie mit zugehörigen Isolationsmechanismen vermutlich prohibitiv.

Eine weitere 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.

Aufgrund der sich derzeit ständig weiterentwickelnden Modelle für Confidential Computing und aufgrund der sich gleichzeitig weiterentwickelnden Modelle für die Bereitstellung von Compute-Leistungen und Native Services in der Cloud ist es derzeit nicht ohne starke Einschränkungen der Gestaltungsmöglichkeiten der Anbieter möglich,

einen singulären Standard für die Kombination aus Provisionierungsmodell und Confidential Computing Technologie zu definieren. Die vorliegende Spezifikation verzichtet daher zum aktuellen Zeitpunkt darauf. Eine Erweiterung als Ergebnis der Konsultationen mit der Industrie ist denkbar. Unabhängig davon ist es ein Ziel der gematik, für Dienstanbieter in der TI die Aufwände im Zusammenhang mit einem Anbieterwechsel zu begrenzen und zu diesem Zweck Interoperabilitätsstandards zu setzen.

Während es also dem HCC-Provider überlassen bleibt, seine spezifische Umsetzung von Confidential Computing für HCC zu realisieren, empfiehlt die gematik insbesondere im Sinne der Zukunftsfähigkeit die Beachtung einiger Leitlinien:

- Minimierung der TCB,
- Evaluierung von Technologien im Hinblick auf die Übereinstimmung ihrer ursprünglichen Zielsetzungen mit den Einsatzbedingungen von Confidential Computing,
- Einsatz sicherer Programmiersprachen,
- Einsatz automatisierter Prüfverfahren für spezifische Fehlerklassen,
- Einsatz von Modellbildung für Sicherheitseigenschaften,
- Einsatz formaler Methoden,
- Schaffung von Transparenz bzgl. Hardware und Software,
- Entkopplung von Infrastrukturmanagement von den Verarbeitungsprozessen sowie
- Verteilung von organisatorischen Sicherheitsmaßnahmen auf unabhängige Organisationseinheiten.

6.9 Integration mit den Zero Trust Services der TI

Die HCC-Plattform ist eine Ausprägung von Rechenzentrumsumgebung 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.

6.10 Erreichbarkeit aus dem Internet und aus dem Netz der TI

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, der aktuell mit Produkten wie dem TI-Gateway bereits die Obsoleszenz des Konnektors vor Ort vorbereitet.

Gleichwohl müssen die wichtigsten Anwendungen der TI weiterhin über das Netz der TI erreichbar sein. Ein HCC-Provider muss daher bis auf Weiteres über einen Anschluss an dieses Netz verfügen und diesen mandantenfähig für HCC-Dienste nutzbar machen. Hierfür ist eine Erweiterung der Netzwerkspezifikation [gemSpec_Net] um eine mandantenfähige Cloud-Variante des SZZP-Light vorgesehen. Demnach stellt der Anbieter des zentralen Netzes der TI (auf Antrag des Cloud-Providers) in einem Mandantenkontext des Cloud-Providers einen Anschluss an das Netz der TI als Dienst bereit, der von Diensteanbietern in derselben Cloud nachgenutzt werden kann. Die vorgesehene Lösung ist nicht spezifisch für HCC, kann jedoch für HCC genutzt werden.

Auch hinsichtlich der 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.

Aufgrund von zum Zeitpunkt der Veröffentlichung noch nicht abschließend festgelegten Details zum Zugriff auf Dienste der TI mit Zero Trust Protokollen, verzichtet die vorliegende Spezifikation auf detailliertere Anforderungen bzgl. des Zugriffs auf die Dienste und überlässt es den HCC-Providern, in ihren Infrastrukturen betriebene Dienste bedarfsgerecht und konform mit den Anforderungen der Dienste verfügbar zu machen.

Es ist jedoch vorgesehen, mindestens bestimmte Zugriffsprotokolle als Standard für die Zukunft vorzugeben. Schon heute ist http/2 verpflichtend, in Zukunft wird http/3 hinzukommen.

Die Betrachtung der Zugriffsprotokolle ist insofern von Bedeutung, als sich der Aufbau der Infrastrukturen teilweise daran ausrichten kann. Für HCC sind zwei Möglichkeiten des Verbindungsaufbaus zum Verarbeitungskontext vorgesehen:

1. Die Verbindung basiert auf TLS, das direkt im Verarbeitungskontext terminiert. Dies erfordert eine gehärtete Implementierung von TLS und schließt eine Terminierung vor dem Verarbeitungskontext und den Einsatz spezieller Komponenten hierfür aus.
2. Die Verbindung basiert auf dem VAU-Protokoll. Damit kann TLS an einer dem Verarbeitungskontext vorgelagerten Schnittstelle terminieren.

Im Übergang von http/2 zu http/3 ist damit zu rechnen, dass sich die Gateway-Infrastrukturen anpassen müssen, weil hier das TCP-Protokoll eine Rolle als fallback-Lösung einnimmt, während das QUIC-Protokoll den Standard definiert. Das QUIC-Protokoll stellt andere Anforderungen an die Gateway-Infrastruktur aufgrund seines anderen Zustandsmodells, des Wegfalls der Source TCP Ports als Filterkriterium und aufgrund der tiefen Integration mit TLS.

Die Abwehr von Angriffen aus dem Internet muss daher insgesamt anders aufgebaut werden. Insbesondere Überlastungsangriffe sind hier von Bedeutung.

6.11 Abwehr von Überlastungsangriffen aus dem Internet

HCC-Provider müssen grundsätzlich die Abwehr von Überlastungsangriffen 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. Es wird jedoch angenommen, dass diese Möglichkeit nur in Sonderfällen in Betracht kommt.

Aufgrund der starken Bündelung von Internet-Verkehr mit anwendungsübergreifendem Charakter beim HCC-Provider ist dieser möglicherweise in 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.

Hierzu können im Zuge der Einführung von http/3 konkrete Anforderungen eingeführt werden. Derzeit bleiben derzeit sowohl der Einsatz eines solchen Aufbaus als auch die Ausgestaltung offen.

7 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 Dienst Anbietern 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 8- Zulassungen und Bestätigungen). Soweit anwendbar sollten die im Folgenden geforderten Prozesse und Maßnahmen in die bestehenden Frameworks der HCC-Provider integriert implementiert werden.

7.1 Rollen und Verantwortlichkeiten

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

Tabelle 2 : Akteure und ihre Aufgaben

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

	<p>Veröffentlichung 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"> • Zulassungsantrag • Zertifizierungen (Prozesse) • Anbietererklärungen <p>Registrierung HCC-Dienstanbieter, Verantwortliche, Identitäten Einrichtung der Schnittstellen Veröffentlichung</p>
Zulassung HCC-Workload-Hersteller	<p>Prüfung von:</p> <ul style="list-style-type: none"> • Zulassungsantrag • Zertifizierung Entwicklungsprozess • Herstellererklärungen <p>Registrierung HCC-Workload-Hersteller, Verantwortliche, Identitäten Einrichtung der Schnittstellen Veröffentlichung</p>
Zulassung HCC-Workload	<p>Prüfung von:</p> <ul style="list-style-type: none"> • Zulassungsantrag • Produktgutachten • Herstellererklärungen <p>Registrierung HCC-Workload im TI Design & Configuration Repository, Einrichtung im TI Verification & Build Service</p>
Zulassung Erneuerung, Delta, Terminierung	<p>Prüfung von:</p> <ul style="list-style-type: none"> • Änderungsantrag • Delta-Gutachten <p>Aktualisierung der Registrierungseinträge</p>
HCC-Governance Repository	<p>Bereitstellung TI Design & Configuration Repository</p> <ul style="list-style-type: none"> • Entwicklung (Beauftragung), Betrieb, Weiterentwicklung • Versionierung, Manipulationsschutz, Mehr-Augen-Prinzip, Abläufe
HCC-Governance Build-Service	<p>Bereitstellung TI Verification & Build Service Entwicklung</p> <ul style="list-style-type: none"> • Betrieb (als HCC-Dienst), Weiterentwicklung • Co-Entwicklung mit TI Design & Configuration Repository

	<ul style="list-style-type: none"> Integration von spezifischen HCC-Provider Schnittstellen
HCC-Governance Identitäten	<p>Bereitstellung von Identitäten für HCC-Governance</p> <ul style="list-style-type: none"> Entwicklung der Vorgaben für starke Authentisierung und für das Signieren von Policies und anderen Artefakten Definition von Herausgabeprozessen
HCC-Governance Prozesse	<p>Ausgestaltung der Prozesse für HCC-Governance</p> <ul style="list-style-type: none"> Definition und Besetzung der organisatorischen Rollen für die Administration der Elemente im TI Design & Configuration Repository
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"> Prüfung der Konformität mit den vorgelegten Zertifizierungen insb. hinsichtlich der TCB Durchführung von Penetration Tests
Issue Tracking & Management	<p>Kontinuierliche Überwachung</p> <ul style="list-style-type: none"> Betrieb Sicherheit <p>Management von Incidents, etc. Monitoring des Threat Environments, SIEM</p>
Gutachter (der gematik)	
Bestätigung	<p>Prüfung der Governance-Prozesse und Systeme Prüfung des Ausschlusses von Manipulationen (durch einzelne Täter) Ausstellung Bestätigung, Erneuerung</p>
HCC-Provider	
Sicheres Datacenter Design	<p>Bestätigt durch Zertifizierung:</p> <ul style="list-style-type: none"> Physische Sicherheit Isolation der Datenverarbeitungsbereiche
Sichere Datacenter Operations	<p>Bestätigt durch Zertifizierung:</p> <ul style="list-style-type: none"> Zutrittsschutz, Zutrittskontrolle, Zutrittsprozesssteuerung Einsatz sicherheitsüberprüftes Personal Trennung betrieblicher Verantwortlichkeiten gegen Manipulationsmöglichkeiten

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>
Gutachter (des HCC-Providers)	
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"> • Source Code Analyse, Pen-Tests, Fuzzing, automatisierte Prüf-Tools, etc. • Prüfung der korrekten Umsetzung der spezifizierten Zugriffs-Policies • Insb. Nicht-Verletzung des Betreiberausschlusses (auf allen Ebenen) <p>Spezielle Beachtung des Betreiberausschlusses als Schutzziel angesichts des Angriffspotenzials des Betreibers Erstellung und Bereitstellung Gutachten</p>
HCC-Dienstanbieter	
Legitimation des Dienstes	<p>Nachweis der Legitimation für die Aufnahme des Dienstes in den Vertrauensraum von HCC (rechtlich, fachlich)</p>

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
HCC-Workload-Hersteller	
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
Gutachter (Workload)	
Begutachtung HCC-Workload	Prüfungen: <ul style="list-style-type: none"> • Source Code Analyse, Pen-Tests, Fuzzing, automatisierte Prüf-Tools, etc. • Prüfung der korrekten Umsetzung der spezifizierten Zugriffs-Policies • Insb. Nicht-Verletzung des Betreiberausschlusses (auf allen Ebenen) • Insb. Ausschluss von Angriffs-Code gegen andere HCC-Dienste auf demselben HCC-Host oder auf anderen Hosts Bereitstellung Gutachten

Die hier aufgeführten Rollen und Verantwortlichkeiten müssen im Rahmen der Schaffung der organisatorischen Voraussetzungen für eine Zulassung der Anbieter und Hersteller konkretisiert und ausgearbeitet werden. Hierfür werden die bestehenden Zulassungsprozesse und Verantwortlichkeiten bei der gematik entsprechend erweitert.

8 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/Cloud-Anbieter auswählen. Die gelisteten HCC/Cloud-Anbieter erfüllen die Anforderungen an VAU-Betreiber in diesem Dokument 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 des BSI,
- 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 3: Zulassung von HCC-Providern

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

9 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 Web-APIs 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.

10 Integration in das SIEM der TI

Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet.

11 Integration in das Testing Framework der TI

Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet.

12 Integration in die betriebliche Steuerung der TI

Die Anforderungslage für die betriebliche Organisation und Performance wird zu einem späteren Entwicklungsstand dieses Dokuments hinzugefügt. 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.

12.1 Verfügbarkeit und Performance

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

- Der HCC-Provider ist verantwortlich für die Zu- und Rückleitung aller Requests an den bzw. Reponses vom HCC-Dienst.
- Der HCC-Dienstanbieter ist verantwortlich für die fachliche Verarbeitung, aber auch für die Performance im Zusammenspiel mit den Services des HCC-Providers, die der HCC-Dienst nutzt (z.B. Datenbank-Service).
- Die Verantwortung gegenüber den Endnutzern des HCC-Dienstes liegt, wie bisher in der TI, beim HCC-Dienstanbieter (Anbieter TI-Fachdienst).

12.2 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 HCC-Dienstes zu erhalten und damit jederzeit Aussagen zum Gesundheitszustand des Dienstes treffen zu können. Dies soll ebenfalls für die Managed-Services des HCC-Providers umgesetzt werden.

Folgende Anstriche führen die hier gezeigten Lösungsideen weiter:

- Daten für die betriebliche Überwachung werden dienstbezogen benötigt, d. h. die Anforderungen dazu betreffen die HCC-Dienstanbieter spezifisch für den jeweiligen HCC-Dienst.
- Der HCC-Provider stellt eine Konvertierungslösung zur Gewinnung der seitens gematik benötigten Betriebsdaten aus der Workload-API-Nutzung / Betriebsumgebung bereit. Dies kann als eigenständige Workloads (Agents) umgesetzt sein, oder "Cloud-native".
- Der HCC-Provider stellt die Übermittlungsmöglichkeit an die gematik für alle seine HCC-Tenants bereit. Dabei werden die Daten anbieter- und dienstspezifisch gebündelt, so dass sie in den Systemen der gematik korrekt zugeordnet sind.

- Der HCC-Diensteanbieter muss sich nicht um die Integration mit den Datenliefersystemen der gematik kümmern. Er muss jedoch gewährleisten, dass die von der gematik benötigten Daten dem Loggingsystem für die Übertragung zur Verfügung gestellt werden.
- Der HCC-Provider stellt Möglichkeiten zur Überwachung der "Gesundheit" der HCC-Dienste bereit (Health-Checks), die vom HCC-Diensteanbieter genutzt und ggf. an die gematik berichtet werden können.
- Der HCC-Provider stellt durch interne Kategorisierung sicher, dass erhaltene Loggingdaten eindeutig einem Quellsystem zugeordnet werden können. Dies betrifft vorrangig Metadaten wie Umgebungstyp (DEV/PU/RU), den Dienst- und Mandantenkontext.

12.3 Betriebliche Rollen und Verantwortung

Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet. Hier sollen, in Abstimmung mit der Industrie, insbesondere die Abgrenzungen der Verantwortlichkeit für die Verfügbarkeit festgelegt werden. Dies erfordert die Präzisierung der Grenze zwischen Infrastruktur und Workload sowie die Definition entsprechender Messpunkte.

12.4 Anwendbarkeit betrieblicher Prozesse (TI-ITSM)

Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet. Hier sollen, in Abstimmung mit der Industrie, insbesondere Fragen der Haftung im Zusammenhang mit der neuen "Shared Responsibility" behandelt werden.

12.5 Weitere Funktionalität

Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet. Themen sind:

- Betriebliche Überwachung des eingesetzten DDoS-Schutzes
- Implementation und Anwendbarkeit von Loadbalancing
- Implementation und Anwendbarkeit von Deployment Strategien (Red/Blue; Canary; etc.)

13 Sicherheitsanalyse

Dieses Kapitel umfasst das Angreifermodell und die sich daraus und aus der Sicherheitsarchitektur ableitende Bedrohungsanalyse.

13.1 Angreifer

Die folgende Tabelle zeigt die Typen von Angreifern.

Tabelle 4: Typen von Angreifern

Angreifertyp	Erläuterung
Außentäter	<p>Außentäter sind Personen oder Gruppen von Personen, die keinen berechtigten Zugriff auf den Dienst haben, nicht zum Personal eines Betreibers des Dienstes bzw. der HCC-Infrastruktur gehören und nicht an der Entwicklung des Dienstes oder der HCC-Infrastruktur beteiligt sind. Hierzu gehören auch die organisierte Kriminalität, Terroristen oder feindlich gesinnte Drittstaaten ohne direkten staatlichen Einfluss auf Beteiligte an der Bereitstellung der HCC-Infrastruktur.</p> <p>Es wird angenommen, dass Außentäter versuchen, Schaden zu verursachen, sich zu bereichern, Aufsehen zu erregen oder etwas zu vertuschen.</p>
berechtigter Nutzer einer Anwendung als Angreifer	<p>Nutzer einer Anwendung können auf den Dienst zugreifen, um berechtigterweise auf ihre im Dienst verarbeiteten Daten zuzugreifen.</p> <p>Es wird davon ausgegangen, dass einzelne Nutzer versuchen könnten, darüber hinaus bewusst unberechtigte Aktionen durchzuführen bzw. durch einen unsachgemäßen Umgang mit der Anwendung unabsichtlich Schaden herbeiführen.</p>
Mitarbeiter des HCC-Providers als Innentäter	<p>Mitarbeiter des HCC-Providers haben im Rahmen ihrer regulären Tätigkeit Zugriff auf die Systeme der VAU. Mitarbeiter des Betreibers können privilegierte Rechte besitzen (z.B. Administratoren).</p> <p>Es wird angenommen, dass Innentäter versuchen, Schaden zu verursachen, sich zu bereichern oder etwas zu vertuschen.</p>
HCC-Provider als Organisation als Angreifer	<p>Der HCC-Provider als Organisation könnte ein Interesse an einer Kenntnisnahme von verarbeiteten Daten haben.</p> <p>Es wird angenommen, dass der Betreiber versuchen könnte, sich zu bereichern.</p>
Mitarbeiter des HCC-Diensteanbieters als Innentäter	<p>Mitarbeiter des Anbieters des HCC-Dienstes haben im Rahmen ihrer regulären Tätigkeit Zugriff auf Funktionen des Mandantenkontextes, in dem der HCC-Dienst beim HCC-</p>

	<p>Provider ausgeführt wird. Mitarbeiter des Anbieters des HCC-Dienstes können privilegierte Rechte besitzen (z.B. Administratoren).</p> <p>Es wird angenommen, dass Innentäter versuchen, Schaden zu verursachen, sich zu bereichern oder etwas zu vertuschen.</p>
HCC-Diensteanbieter als Organisation als Angreifer	<p>Der HCC-Diensteanbieter als Organisation könnte ein Interesse an einer Kenntnisnahme von verarbeiteten Daten haben.</p> <p>Es wird angenommen, dass der Anbieter versuchen könnte, sich zu bereichern.</p>
Entwickler der HCC-Infrastruktur als Innentäter	<p>Entwickler der HCC-Infrastruktur kennen ihre Schwachstellen und könnten diese auszunutzen oder gezielt Schwachstellen in die HCC-Infrastruktur einzubauen versuchen.</p> <p>Es wird angenommen, dass Innentäter versuchen, sich zu bereichern oder etwas zu vertuschen.</p>
Entwickler des HCC-Dienstes als Innentäter	<p>Entwickler des HCC-Dienstes kennen seine Schwachstellen und könnten diese auszunutzen oder gezielt Schwachstellen in den Dienst einzubauen versuchen.</p> <p>Es wird angenommen, dass Innentäter versuchen, sich zu bereichern oder etwas zu vertuschen.</p>
Andere Mandanten eines HCC-Providers als Angreifer	<p>Andere Mandanten eines HCC-Providers betreiben ihre Dienste auf einer gemeinsamen Infrastruktur mit der VAU und könnten versuchen ihre Privilegien auszuweiten oder Seitenkanäle auszunutzen.</p> <p>Es wird angenommen, dass andere Mandanten versuchen könnten, Schaden zu verursachen, einen Beteiligten am Betrieb der HCC-Infrastruktur zu diskreditieren oder sich zu bereichern.</p>
Staatliche Organe als Angreifer	<p>Staatliche Organe der Exekutive könnten auf den HCC-Diensteanbieter, den HCC-Provider als Organisation oder den Hersteller einer verwendeten Soft- oder Hardware-Komponente einzuwirken versuchen, damit dieser auf die im HCC-Dienst verarbeiteten Daten zugreift und Daten weitergibt oder ihnen Zugriff ermöglicht.</p> <p>Es wird angenommen, dass staatliche Organe als Angreifer illegitime politische Ziele verfolgen könnten oder gesetzliche Beschränkungen hinsichtlich der Überwachung von Personen zu umgehen versuchen könnten.</p>
Fremde Staaten als Angreifer	<p>Fremde Staaten könnten internationale Lieferketten anzugreifen versuchen.</p> <p>Es wird angenommen, dass fremde Staaten versuchen könnten, geheimdienstliche Interessen zu verfolgen oder politischen Schaden anzurichten.</p>
gematik	<p>Die gematik könnte in ihrer Spezifikations-, Zulassungs- oder Betriebsrolle Schaden erzeugen.</p>

HCC muss Angriffe mit einem Potential von „high“ abwehren.

13.2 Bedrohungen

Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet.

14 Anforderungen an HCC

14.1 HCC-Provider - marktoffenes Angebot

Die Anforderungen in diesem Abschnitt sollen die Entwicklung eines Marktes für Healthcare Confidential Computing fördern.

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

[Herstellererklärung]

14.2 HCC-Provider - Bereitstellung HCC-Infrastruktur

Die Anforderungen in diesem Abschnitt dienen primär der Abgrenzung zwischen HCC-Providern und anderen Anbietern innerhalb der TI.

A_26838 - HCC-Provider - Bereitstellung Cloud-Infrastrukturbasis

Der HCC-Provider MUSS geeignete Rechenzentrumsinfrastruktur bereitstellen, die

- auf hohe Verfügbarkeit ausgelegt ist und dazu
 - über mindestens zwei Standorte in Deutschland oder in einem an Deutschland angrenzenden Mitgliedstaat der EU verteilt ist und dabei die Vorgaben des BSI zur Georedundanz gemäß [BSI-Georedundanz] erfüllt,
 - je Standort redundant an das Internet angeschlossen ist,
 - je Standort redundant aufgebaute Stromversorgung, Kühlung und Netzwerkstrukturen aufweist, so dass Single Points of Failure vermieden werden,
 - standortübergreifend performant, mit niedriger Latenz und mit ausreichender Kapazität vernetzt ist sowie
 - über nachgewiesene wirksame Mechanismen zur Kompensation von Ausfällen auf der Ebene von Netzen, Komponenten, Diensten, Systemen und Standorten die durchgehende Verfügbarkeit der HCC-Dienste aus Sicht ihrer Endnutzer gewährleistet,
- immer ausreichende Kapazitäten bereitstellt
 - für die Ausführung containerisierter Dienst-Software (Container Runtime und/oder VM Runtime) auf registrierten Servern mit Unterstützung für Confidential Computing (HCC-Hosts),
 - für die Speicherung von Daten (mindestens Block Storage),
 - für den Transport von Daten (Ingress, Egress Internet, internes SDN) sowie
 - für die sichere Handhabung von Schlüsselmaterial (in HSM-Clustern),
- mandantenbezogen provisioniert werden kann und dazu
 - Mandantenkontexte auf der Ebene aller zugewiesenen Ressourcen isoliert,
 - Datenverkehr mandantenbezogen routet,
 - (mindestens) ein automatisiertes Verfahren zur bedarfsabhängigen (lastgesteuerten) Erhöhung bzw. Verringerung der je Mandant und je Dienst zugewiesenen Ressourcen implementiert (z. B. Managed Kubernetes mit Autoscaling),
- physisch und gegen unberechtigten Zugriff geschützt ist sowie
- professionell betrieben und dokumentiert ist.

[<=]

[Herstellererklärung, Produktgutachten]

A_26839 - HCC-Provider - DDoS-Schutz

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

[Herstellererklärung, Produktgutachten, Sicherheitsgutachten]

A_26840 - HCC-Provider - DDoS-Abwehr mit Ausschluss von Profilbildung

Der HCC-Provider SOLL zwischen den vorgelagerten Systemen zur DDoS-Abwehr und den HCC-Umgebungen innerhalb seiner HCC-Rechenzentren ein für die DDoS-Abwehrsysteme die Anonymität der Endnutzer erhaltendes Protokoll zur Steuerung der DDoS-Abwehr implementieren, welches

- einen Bandbreiten-limitierten und mittels DDoS-Abwehr-Heuristik geschützten Zugangspunkt für unbekannte Geräte (Device Registration mit Nutzerzuordnung) ermöglicht und
- an HCC-Dienstinstanzen adressierte Requests unbekannter Geräte vollständig bei den DDoS-Abwehrsystemen blockiert.

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

Die Erhaltung der Anonymität bedeutet insbesondere,

- dass bei den DDoS-Abwehrsystemen keine TLS-Terminierung und keine Authentisierung von Requests auf der Grundlage von Nutzer-Credentials erfolgt,
- dass das Protokoll ggf. bei den DDoS-Abwehrsystemen jeden auf Grundlage der Quelladresse oder anderer Request-Attribute erkennbaren Nutzerbezug gegenüber denjenigen Systemen des HCC-Providers maskiert, die den HCC-Diensten vorgelagert sind,
- dass eine De-Anonymisierung der Requests erst innerhalb der Verarbeitungskontexte der HCC-Dienste erfolgt und
- dass die „Markierung“ von legitimen Client-Verbindungen bzw. Requests mit Attributen ohne Nutzerbezug erfolgt.

[<=]

[Herstellererklärung, Produktgutachten, Sicherheitsgutachten]

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 Endnutzerzugriffen auf HCC-Dienste ausgeschlossen ist. **[<=]**

[Herstellererklärung, Produktgutachten, Sicherheitsgutachten]

A_26842 - HCC-Provider - HSM-Cluster

Der HCC-Provider MUSS pro Standort mindestens ein HSM-Cluster bereitstellen

- mit ausreichender Kapazität für das im Rahmen von HCC anfallende Volumen an gemäß dieser Spezifikation oder gemäß Spezifikationen der gehosteten HCC-Dienste HSM-pflichtigen kryptographischen Operationen,

- mit ausreichender Redundanz zur Gewährleistung der Verfügbarkeit sowie
- mit geräte- und standortübergreifender Synchronisation des persistenten Schlüsselmaterials und der Zugriffsregeln (in durch die HSMs gesteuerter, verschlüsselter Form).

[<=]

[Herstellererklärung, Produktgutachten]

A_26843 - HCC-Provider - Key Management Service

Der HCC-Provider SOLL einen Key Management Service zur Verwaltung und Verteilung von verschlüsseltem Schlüsselmaterial als standortübergreifend synchronisierten Cloud-native Service bereitstellen, der in die Abläufe zur Provisionierung von Workloads eingebunden ist und zusätzlich durch die HCC-Dienste nutzbar ist. [<=]

[Herstellererklärung, Produktgutachten]

A_26844 - HCC-Provider - RDBMS

Der HCC-Provider SOLL einen selbst skalierenden und standortübergreifend synchronisierten Relational Database Management Service zur Speicherung vorab verschlüsselter relationaler Daten als Cloud-native Service bereitstellen, der durch die HCC-Dienste nutzbar ist. [<=]

[Herstellererklärung]

A_26845 - HCC-Provider - Key Value Store

Der HCC-Provider SOLL 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 Database Services

Der HCC-Provider KANN einen selbst skalierenden und standortübergreifend synchronisierten RDBMS und/oder einen selbst skalierenden Key Value Store zur Speicherung unverschlüsselter Daten als (Confidential) Cloud-native Service bereitstellen, der durch die HCC-Dienste nutzbar ist. Aufgrund der in solchen Diensten stattfindenden Verarbeitung unverschlüsselter personenbezogener medizinischer Daten im Klartext, sind für die Zulassung der Dienste dieselben (hohen) Anforderung an die sicherheitstechnische Prüfung gestellt, wie an andere HCC-Dienste. [<=]

[Herstellererklärung, Produktgutachten]

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 über eine gesicherte Web-API ausfüllen kann. [<=]

[Herstellererklärung, Produktgutachten, Test durch gematik]

A_26848 - HCC-Provider - Dienste im gematik-Mandanten

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

- den Vertrauensanker für HCC und weiteres Schlüsselmaterial im HSM-Cluster,
- den Trust Domain Configuration & Attestation Service mit der Fähigkeit zur Attestation aller validen HCC-Workloads (paired mit dem Vertrauensanker),
- den Trust Domain Build Service zur Vorbereitung von Workloads für den Betrieb als Confidential Services beim HCC-Provider sowie
- das Trust Domain Deployment Repository mit der Fähigkeit zur Aufnahme aller für HCC benötigten Artefakte (Binaries, Konfigurationen, Policies).

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

[Herstellererklärung, Produktgutachten, Dokumentenprüfung, Test durch gematik]

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

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

A_26849 - HCC-Provider - Funktionen des gematik-Mandanten

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

- Registrierung administrativer Nutzer mit jeweils eigenen, starken User Credentials (ggf. über Web-Portal anstelle einer API),
- Zuordnung von Nutzern zu Rollen für die im Mandantenkontext abgebildeten Verwaltungsfunktionen,
- Einsicht bzw. Überwachung der Konfiguration des gematik Mandantenkontextes inkl. aller Zugriffsberechtigungen und im Kontext verfügbarer Funktionen,
- Abruf der Attestation Logs über alle Attestationsvorgänge für HCC-Dienste,
- Abruf aller für die Governance relevanten Metadaten inkl. Hash-Werten und Signaturen für alle im Runtime Deployment Repository des HCC-Providers für HCC verfügbaren Artefakte,
- Einbringen von gültig signierten Deployment-Artefakten in das Runtime Deployment Repository, wobei durch das Trust Domain Deployment Repository eine Signaturprüfung als Voraussetzung für die Annahme des jeweiligen Artefakts erfolgt,
- Sicheres Einbringen und Aktualisieren des für die Prüfung der Signaturen von Deployment-Artefakten genutzten Zertifikats im Vier-Augen-Prinzip mit dem HCC-Provider,
- sicheres Einbringen signierter Policy-Statements und Referenzwerte in die Konfigurationsdatenbank des Trust Domain Configuration & Attestation Service,
- Teilnahme (nach der Initialisierungszeremonie auch remote) an den Zeremonien zur Verwaltung des Vertrauensankers.

[≤]

[Herstellererklärung, Produktgutachten, Test durch gematik]

14.4 HCC-Provider - Mandanten für HCC-Diensteanbieter

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-Diensteanbieter

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

[Herstellererklärung, Produktgutachten]

A_26851 - HCC-Provider - Funktionen des HCC-Diensteanbietermandanten

Der HCC-Provider MUSS es HCC-Diensteanbietern im Mandantenkontext ermöglichen:

- administrative Nutzer des HCC-Diensteanbieters mit jeweils eigenen, starken User Credentials zu registrieren,
- die für die Verwaltung der Cloud-Ressourcen im Mandantenkontext vorhandenen Rollen mit registrierten Nutzern zu besetzen,
- Cloud-Ressourcen einzurichten, zu verwalten und zu überwachen,
- eigene Dienstinstanzen aus VM-Images bzw. Container Images im TD Deployment Repository ausführbar zu machen,
- eigene Dienstinstanzen für die beim Starten von Instanzen automatisch durchgeführte Attestation durch den TDCAS und den anschließend gewährten Zugriff auf die TLS-Identität des HCC-Dienstes und anderes Schlüsselmaterial einzurichten,
- die Betriebsdatenlieferung an die gematik (inkl. konformer Labels) über eine von HCC-Diensten einzubindende API einzurichten,
- Standardkomponenten der TI und die dem HCC-Dienst zugeordneten Policies (z. B. Zero Trust Komponenten mit ihren Access Control Policies) in Ausführungskontexte von HCC-Diensten (z. B. mittels Sidecar-Muster oder Service Mesh Konfiguration) einzubinden,
- Plattform-Dienste des HCC-Providers (z. B. Datenbanken, Caching) einzubinden insoweit diese HCC-konform genutzt werden können,
- die Ressourcenallokation je HCC-Dienst zu konfigurieren (lastabhängige automatische Skalierung, Limits und Warnungen bei Erreichung bestimmter Schwellwerte für Compute-, Storage-, Netzwerk-, HSM-Nutzung auf Dienst- und Mandantenebene),
- Konfiguration der DNS-Records für die im Internet erreichbaren Web-Schnittstellen und APIs je HCC-Dienst im Rahmen eines übergreifenden Namensschemas für HCC-Dienste.

[**<=**]

[Herstellererklärung, Produktgutachten]

A_26852 - HCC-Provider - HCC-Dienste mit anderen Diensten integrieren

Der HCC-Provider MUSS mit Werkzeugen, die im Mandantenkontext für HCC-Diensteanbieter verfügbar sind, die Integration von HCC-Diensten seiner HCC-Tenants mit anderen Diensten ermöglichen. 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.

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.

Alle Verbindungen MÜSSEN über Gateways realisiert werden, die neben der Datenverkehrssteuerung auch eine erste Stufe des Ausschlusses von unbekanntem externen Verbindungspartnern umsetzen, d. h. Verbindungen auf registrierte Partner einschränken.

Der HCC-Provider MUSS dazu in geeigneter und kontrollierter Weise Änderungen an SDN-Konfigurationen, an Gateways, an Policies sowie ggf. an anderen Komponenten seiner Infrastruktur ermöglichen.【<=】

[Herstellererklärung, Produktgutachten]

14.5 HCC-Provider - HCC-Sicherheitsfunktionalität

Neben den betrieblichen und fachlichen Funktionalitäten, die der HCC-Provider für die gematik und für HCC-Dienstleister bereitstellt, um HCC-Dienste zur Ausführung bringen zu können, und neben den Sicherheitsanforderungen, die seine betrieblichen Umgebungen (Rechenzentrumsstandorte) sowie seine Systeme, Software und Prozesse erfüllen, um die in Kapitel 8- Zulassungen und Bestätigungen geforderten Zertifizierungen zu erhalten, müssen HCC-Provider Sicherheitsfunktionalitäten implementieren, die zur Erreichung des besonders hohen Sicherheitsstandards von HCC erforderlich sind.

A_26853 - HCC-Provider - Attestationsfähige Server

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

[Herstellererklärung, Produktgutachten]

A_26854 - HCC-Provider - Confidential Computing Lösung

Der HCC-Provider MUSS eine Confidential Computing Lösung einsetzen bzw. umsetzen, die

- einen Trust Domain Configuration & Attestation Service umfasst,
- sicherstellt, dass nur Dienste attestiert werden können, die
 - auf Servern laufen, die
 - für HCC registriert sind,
 - für den „Confidential Mode“ konfiguriert sind (Ausschluss z. B. bei Betrieb im Debug Mode),
 - für Arbeitsspeicherverschlüsselung konfiguriert sind,
 - einen Measured Boot Prozess bzw. Confidential Computing Mechanismus unterstützen, der alle Aspekte des Systems erfasst, die für die Feststellung der Vertraulichkeit der Verarbeitung notwendig sind,
 - eine Ausführung von nicht für HCC zulässiger Software verhindern (z. B. über Signaturprüfung von Software-Komponenten beim Laden),

- nur mittels als zulässig registrierter Software umgesetzt sind (inkl. CPU-Firmware, Bootloader, Hypervisor, VMs und HCC-Dienste-Container).
- im Zusammenspiel mit dem lokalen HSM-Cluster die sichere Steuerung des Zugriffs auf das in HSMs gehaltene oder aus HSMs bezogene Schlüsselmaterial für alle HCC-Dienste gewährleistet,
- die Authentizität aller benötigten Konfigurationsdaten prüft,
- die Integrität aller benötigten Konfigurationsdaten schützt,
- gegen Rollback-Angriffe auf die Konfiguration schützt,
- in einer sicheren Programmiersprache implementiert ist,
- eine, falls vorhanden, nach dem Stand der Technik und unter Berücksichtigung des Standes der Forschung gehärtete Ausführungsumgebung für Confidential Workloads mitbringt sowie
- die die Möglichkeiten der Hardware-Plattform zur Isolation von Confidential Workloads auf einem HCC-Host nutzt.

[<=]

[Herstellererklärung, Produktgutachten]

A_26855 - 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

- mit Nutzerbezug registrierte und durch einen Dienst des HCC-Providers attestierte Administrations-Clients (Hardware und Software) mit lokalem Passwort-Schutz,
- auf geeignete Client-Gerätetypen (vor lokaler Schadsoftware geschützt mit technischen Mitteln sowie mit restriktiven Policies für die Installation von Software und die Handhabung) eingeschränkten Zugriff,
- ein Hardware-Credential mit lokalem PIN-Schutz als Authentisierungsfaktor (z. B. Smartcard),
- TLS 1.3 gesicherten Verbindungsaufbau und Transport zur Authentisierung und zur Web-Schnittstelle bzw. API des Mandantenkontextes sowie
- Beschränkungen hinsichtlich des Ortes, von dem aus zugegriffen wird, auf plausible Geo-Locations (z. B. nur Verbindungen aus Deutschland)

voraussetzen und über das Internet (ggf. unter zusätzlichem Einsatz von Wireguard-VPN) nutzbar sind.[<=]

[Herstellererklärung, Produktgutachten]

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).

[<=]

[Herstellererklärung, 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). [**<=**]

[Herstellererklärung, Produktgutachten]

A_26858 - HCC-Provider - Einbringen qualifizierter Server ins RZ

Der 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. Dies umfasst:

- die Durchführung des Onboardings im Mehr-Augen-Prinzip durch sicherheitsüberprüftes Personal und auf der Grundlage eines auditfähigen Auftrags (Tickets),
- die Prüfung, dass die Hardware tatsächlich vom vorgesehenen Hersteller stammt,
- die Überprüfung der Lieferkette des Servers auf der Grundlage geeigneter Lieferpapiere oder elektronischer Datensätze, um Manipulationen am Server auf dem Weg zum Rechenzentrum auszuschließen,
- Überprüfung der Unversehrtheit des Servers, insbesondere die Unversehrtheit ggf. vorhandener Gehäuseversiegelungen,
- Überprüfung der grundsätzlichen Funktionsfähigkeit des Servers,
- Durchführung der Attestation des Servers gegenüber dem Attestation Service des Hardware-Herstellers des Workload-Prozessors (z. B. Intel Attestation Service) und Dokumentation des dabei entstehenden Attestation Reports,
- Registrierung der öffentlichen Schlüssel oder Zertifikate der für die Signierung von Attestation Reports auf dem Server genutzten und in der Server-Hardware (Workload-Prozessor, TPM) verankerten privaten Schlüssel,
- Dokumentation des Server-Onboardings in einem manipulationsgeschützten, auditfähigen Protokoll, das Auftragsreferenz (Ticket), Zeitpunkt, Ort, beteiligte Personen, Lieferkettendaten, Attestation Report, die registrierten Schlüssel und ggf. weitere Informationen umfasst,
- Absicherung des Onboardings, z. B. durch Absicherung der physischen Onboarding-Umgebung sowie der Rechenzentrumsumgebung, gegen Inbetriebnahme von registrierten Servern außerhalb der geschützten Rechenzentrumsumgebung,
- Übertragung des Onboarding-Protokolleintrags an das Trust Domain Design & Configuration Repository der gematik in vom HCC-Provider signierter Form.

[<=]

[Herstellererklärung, Produktgutachten, Audit durch gematik]

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

A_26859 - HCC-Provider - Betreiberausschluss für Cloud Management

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

[Herstellererklärung, Produktgutachten]

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

A_26860 - HCC-Provider - HCC-Sicherheitskonzept

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

- Beschreibung der Sicherheitsarchitektur,
- Beschreibung der relevanten betrieblichen Prozesse und Rollen, insbesondere für Installation, Aktualisierung, Patches, Backups, Administration, Konfiguration,
- Beschreibung der Bedrohungen und Risiken inkl. Schutzmaßnahmen vor 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/oder 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 Betreiber 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 EUCS CS-EL3 bzw. nach den vor der Nutzbarkeit von EUCS geltenden Zertifizierungsanforderungen 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. [≤]

[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. [≤]

[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. [**<=**]

[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 - Attestation der Plattform

Die VAU MUSS auf einem HCC-Stack aufbauen, der keine Veränderungen zur Laufzeit aus betrieblichen Gründen erfordert. [**<=**]

[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 der Attestation Reports mitgemessene Konfiguration für eine Workload für die Laufzeit der Instanz unverändert bleibt. [**<=**]

[Produktgutachten]

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

14.6.3 Schutz der Datenverarbeitung

A_26869 - VAU - Klartext-Daten ausschließlich im Verarbeitungskontext

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

[Produktgutachten]

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

A_26870 - VAU - Isolation der VAU von Datenverarbeitungsprozessen des Betreibers

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

[Produktgutachten]

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

A_26871 - VAU - Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU

Die VAU MUSS mit technischen Mitteln ausschließen, dass sich die Verarbeitungen eines Verarbeitungskontextes schadhafte auf die Verarbeitungen eines anderen Verarbeitungskontextes auswirken können. [≤]

[Produktgutachten]

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

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

A_26872 - VAU - Schutz der Daten vor physischem Zugang zu Systemen der VAU

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

[Produktgutachten]

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

A_26873 - VAU - Löschen aller Daten beim Beenden des Verarbeitungskontextes

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

[Produktgutachten]

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

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

14.6.4 Schutz der Daten bei Speicherung

A_26874 - VAU - Verschlüsselung von außerhalb des Verarbeitungskontextes gespeicherten Daten

Falls in einem Verarbeitungskontext verarbeitete schützenswerte Daten außerhalb des Verarbeitungskontextes gespeichert werden sollen, MUSS der Verarbeitungskontext sicherstellen, dass die Daten den Verarbeitungskontext ausschließlich mit dem Persistenzschlüssel verschlüsselt verlassen. [≤]

[Produktgutachten]

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

A_26875 - VAU - Ableitung der Persistenzschlüssel durch ein HSM

Der Verarbeitungskontext MUSS Persistenzschlüssel von einem Schlüssel im HSM-Cluster ableiten. [≤]

[Produktgutachten]

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

A_26876 - VAU - Nutzen des Persistenzschlüssels ausschließlich im Verarbeitungskontext

Die VAU MUSS sicherstellen, dass der Persistenzschlüssel ausschließlich in einem Verarbeitungskontext des jeweiligen Dienstes genutzt wird. [\leq]

[Produktgutachten]

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

14.6.5 Schutz der Daten beim verteilten Caching

A_26877 - VAU - Verschlüsselung von Daten in verteilten Caches

Falls für einen Verarbeitungskontext verarbeitete schützenswerte Daten in einem verteilten Cache zwischengespeichert werden sollen, z. B., um den Dienst zustandslos horizontal zu skalieren, MUSS der Verarbeitungskontext sicherstellen, dass die Daten den Verarbeitungskontext ausschließlich mit dem dienstspezifischen Cache-Schlüssel verschlüsselt verlassen. [\leq]

[Produktgutachten]

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

A_26878 - VAU - Erzeugung des dienstspezifischen Cache-Schlüssels durch ein HSM

Der Verarbeitungskontext MUSS dienstspezifische Cache-Schlüssel im HSM-Cluster erzeugen und ggf. von dort zur lokalen Verwendung abrufen. [\leq]

[Produktgutachten]

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

A_26879 - VAU - Nutzen des Cache-Schlüssels ausschließlich im Verarbeitungskontext

Die VAU MUSS sicherstellen, dass Cache-Schlüssel ausschließlich in Verarbeitungskontexten des jeweiligen Dienstes genutzt werden. [\leq]

[Produktgutachten]

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

A_26880 - VAU - Regelmäßiger Wechsel des Cache-Schlüssels

Die VAU MUSS sicherstellen, dass Cache-Schlüssel mindestens alle 24 Stunden gewechselt werden. [\leq]

[Produktgutachten]

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

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

14.6.6 Schutz der Daten beim Transport

A_26881 - VAU - Geschützte Weitergabe von Daten an autorisierte Nutzer

Der Verarbeitungskontext MUSS sicherstellen, dass schützenswerte Daten aus dem Verarbeitungskontext ausschließlich über sichere Verbindungen an autorisierte Nutzer weitergegeben werden. Bei den Nutzern kann es sich um andere Dienste handeln, die als zugelassene Dienste für andere Verarbeitungen oder als Agenten von Nutzern schützenswerte Daten abfragen. In diesem Fall müssen die abfragenden Dienste selbst ein vergleichbares Schutzniveau erreichen oder im Rahmen der Selbstbestimmung des Eigentümers der schützenswerten Daten (bzw. des datenschutzrechtlich Betroffenen) durch diesen prüfbar autorisiert worden sein. [\leq]

[Produktgutachten]

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

A_26882 - VAU - Sicherer VAU-Kanal vom VAU-Client zum Verarbeitungskontext

Die VAU MUSS sicherstellen, dass schützenswerte Daten zwischen einem VAU-Client und einem Verarbeitungskontext ausschließlich über einen vertraulichen und integritätsgeschützten VAU-Kanal übermittelt werden. [<=]

[Produktgutachten]

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

A_26883 - VAU - Sicherer Kanal vom Verarbeitungskontext zu Diensten

Die VAU MUSS sicherstellen, dass schützenswerte Daten zwischen einem Verarbeitungskontext und einem Dienst ausschließlich über einen vertraulichen und integritätsgeschützten und beidseitig authentisierten Kommunikationskanal übermittelt werden. [<=]

[Produktgutachten]

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

A_26884 - VAU - vertrauliche Kommunikation zwischen Komponenten

Die VAU MUSS sicherstellen, dass alle Komponenten der VAU ausschließlich transportverschlüsselt mit anderen Komponenten (außerhalb oder innerhalb) der VAU kommunizieren. [<=]

[Produktgutachten]

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

A_26885 - VAU - Authentisierung gegenüber VAU-Clients

Der Verarbeitungskontext MUSS sich gegenüber Kommunikationspartnern mittels der dienstspezifischen Identität der VAU ausweisen, 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_26889 - HCC-Provider - Trust Domain Deployment Repository

Das Trust Domain Deployment Repository des HCC-Providers MUSS

- zur Aufnahme von signierten Artefakten aus dem TI Verification & Build Service über eine API bereitstehen. Bei den Artefakten handelt es sich um
 - Workload-Images,
 - für den Betrieb der Workload-Images relevante Konfigurationsdatensätze sowie
 - Policy Sets.
- alle Artefakte des HCC-Vertrauensraums von allen anderen Artefakten auf einfache Art unterscheidbar verwalten,
- sicherstellen, dass Artefakte für den HCC-Vertrauensraum nur vom TI Verification & Build Service eingebracht werden können,
- die signierten Artefakte für die Instanziierung von HCC-Diensten der HCC-Tenants des HCC-Providers sowie der gematik bereitstellen und dabei Einschränkungen auf berechnete Tenants je Artefakt durchsetzen,
- die Notfall-Revocation von Artefakten unterstützen sowie
- stets aktuell gehaltene Repliken an allen Standorten haben.

【<=】

[Herstellererklärung, Produktgutachten]

Hinweis: Berechtigter HCC-Tenant ist im Regelfall der Diensteanbieter, 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-Tenants nutzbar sind.

A_26890 - HCC-Provider - Trust Domain Configuration & Attestation Service

Der 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,
- 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,
- zur Prüfung der Signaturen der Artefakte mit der Signer-Identität des TI Verification & Build Service sicher konfiguriert werden können,

- als Attestation Verification Service für HCC-Dienstinstanzen der Mandanten des HCC-Providers verfügbar und erreichbar sein,
- die Attestation von HCC-Diensten auf deren Anforderung gegen die in der eigenen Konfigurationsdatenbank vorhandenen Referenzwerte durchführen,
- an erfolgreich attestierte HCC-Dienstinstanzen
 - Zugriffs-Credentials für die dem HCC-Dienst zugeordneten Operationen auf den dem HCC-Dienst zugeordneten Schlüsseln im HSM-Cluster übermitteln,
 - als Sub-CA der TI Komponenten-PKI falls erforderlich eine X.509-Identität der TI für die HCC-Dienstinstanz im HSM-Cluster erzeugen,
 - als Sub-CA einer Internet CA mit Extended Validation falls erforderlich eine Internet X.509-Identität für die HCC-Dienstinstanz im HSM-Cluster erzeugen,
- über jeden Attestationsvorgang einen kryptographisch gegen Veränderungen geschützten Log-Eintrag erzeugen,
- für private Schlüssel zu Sub-CA-Zertifikaten den lokalen HSM-Cluster nutzen,
- das Pairing mit dem HCC Root of Trust im HSM-Cluster in Zeremonien zu dessen Einrichtung bzw. Erneuerung und mittels der vom HSM-Cluster bestimmten Authentisierungsmechanismen unterstützen,
- die Steuerung von Zugriffsberechtigungen für die Nutzung der jeweils benötigten Schnittstellen und Schlüssel im HSM-Cluster umsetzen, soweit diese nicht in Zeremonien erfolgt,
- als HCC Confidential Service betrieben werden, sicherheitstechnisch gehärtet und inkl. Source Code Review begutachtet sein (Gutachten zur Vorlage bei der gematik),
- die eigenen Zugriffs-Credentials für den HSM-Cluster mittels Sealing schützen und nach einem Neustart wieder verfügbar haben,
- Updates der eigenen Software mit Erhaltung der Sealed Secrets unterstützen,
- das Erneuern von Sealing Keys unterstützen,
- seine lokale Konfigurationsdatenbank hinsichtlich Authentizität und Integrität schützen, einschließlich Schutz vor Rollback-Attacken,
- seine Schnittstelle für die Attestation ausschließlich für HCC-Hosts innerhalb derselben physischen Location verfügbar machen sowie
- in einer gemeinsamen Zeremonie mit der gematik in Betrieb genommen und mit dem Vertrauensanker verbunden werden.

[<=]

[Herstellererklärung, Produktgutachten]

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

Hinweis: 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.

A_26891 - HCC-Provider - Trust Domain Build Service

Der Trust Domain Build Service des HCC-Providers MUSS

- für den TI Verification & Build Service eine API und für User der HCC-Tenants und der gematik eine Web-Schnittstelle bereitstellen zur gleichzeitigen
 - Konvertierung generischer Workload-Images in Confidential Workload-Images und
 - Ermittlung der Referenzwerte für die Attestation,
- für die Konvertierung geeignete Templates und Mechanismen zugrunde legen, die unterstützen, dass
 - im Falle von VM-basierter Confidential Computing Technologie ausführbare Software-Komponenten mit fachlichem Fokus in ein minimales VM-Template mit Betriebssystem und Netzwerkunterstützung eingebracht werden,
 - im Falle von Container-basierter Confidential Computing Technologie ein Standard Container-Format für die fachliche Funktionalität eingebracht wird,
 - in beiden Fällen Zero Trust Komponenten für die Autorisierung zur Ausführung in gemeinsamen Speicherbereichen mit der fachlichen Funktionalität mit eingebracht werden (z. B. als Sidecars),
- das resultierende Workload-Image zusammen mit den gemessenen Referenzwerten als vom Trust Domain Build Service signierte Artefakte zurückgeben,
- als HCC Confidential Service betrieben werden, sicherheitstechnisch gehärtet und inkl. Source Code Review begutachtet sein sowie
- als HCC Confidential Service durch den Trust Domain Configuration & Attestation Service attestiert und mit Identität ausgestattet sein.

[<=]

[Herstellererklärung, 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_26892 - HCC-Provider - HSM-Cluster Funktionen

Der HSM-Cluster des HCC-Providers MUSS

- für den HCC-Vertrauensraum eine eigene Partition bereitstellen,
- für die HCC-Partition der HSMs in einer physischen Location nur Requests von HCC-Hosts innerhalb derselben Location zulassen sowie
- Schlüsselmaterial und die Konfigurationsdaten für die Zugriffskontrolle über alle HSMs im Cluster innerhalb jeder Location und Location-übergreifend synchron halten.

[<=]

[Herstellererklärung, Produktgutachten]

Hinweis: Die HSMs sollten Key Attestation unterstützen sowie die sichere Authentifizierung von Teilnehmern an Zeremonien über das Netz, um die Durchführung

von Zeremonien für Teilnehmer außerhalb der Rechenzentrumsumgebung zu ermöglichen.

A_26996 - HCC-Provider - Einsatz zertifizierter HSM

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

Die Prüftiefe MUSS mindestens

- FIPS 140-2 Level 3 oder
- Common Criteria EAL 4+ mit hohem Angriffspotenzial

entsprechen. [\leq]

[Produktgutachten]

A_26997 - VAU - Erstellung und Pflege der VAU-Schlüssel nur im Mehr-Augen-Prinzip möglich

Der Dienst-Anbieter MUSS ein HSM einsetzen, das technisch sicherstellt, dass

- die Erstellung, Sicherung und Wiederherstellung von nicht kurzzeitig gültigen Schlüsseln und
- die Administration des/der HSM

ausschließlich im Mehr-Augen-Prinzip erfolgen kann.

[\leq]

[Produktgutachten]

A_26893 - HCC-Provider - HCC-Hosts

Jeder HCC-Host des HCC-Providers MUSS

- CPUs einsetzen, die eine Verschlüsselung des Arbeitsspeichers mit Hardware-Unterstützung ermöglichen,
- Attestationsreports über den gesamten Hardware-, Firmware- und Software-Stack des Systems erzeugen können,
- Attestationsreports mit einem oder mehreren in der Hardware der CPU oder eines TPM geschützten und durch den Hersteller attestierten Schlüsseln signieren können sowie
- eine gegen Seitenkanalangriffe mit lokalem Angriffsvektor geschützte Abtrennung der für den Cloud-Betrieb notwendigen Funktionen (Cloud Management Stack) von der Trusted Computing Base umsetzen.

[\leq]

[Herstellererklärung, Produktgutachten]

A_26894 - HCC-Provider - HCC-Stack

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,
- 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,
- auf minimalen Umfang der Code Base ausgelegt sein, um überhaupt eine ausreichend tiefe Begutachtung der Sicherheitseigenschaften zu ermöglichen sowie

- mit Unterstützung von automatisierten Verfahren nach Stand der Technik und – wo möglich – nach Stand der Forschung sicherheitstechnisch gehärtet sein.

[<=]

[Herstellererklärung, Produktgutachten]

A_26895 - HCC-Provider - Sicherheit des Key Management Service

Der Key Management Service des HCC-Providers MUSS

- für HCC-Dienste über eine API nutzbar sein,
- Schlüsselmaterial je HCC-Dienst unterscheidbar (d. h. mit Dienstzuordnung) verwalten,
- für alle Zugriffe sicherstellen, dass nur autorisierte Dienste (verschlüsseltes) Schlüsselmaterial abrufen können,
- die Verteilung des Schlüsselmaterials über mehrere seiner Instanzen auf für HCC zugelassene Standorte beschränken sowie
- sicherstellen, dass (verschlüsseltes) Schlüsselmaterial innerhalb des für HCC zugelassenen Rechenzentrums- bzw. Systemkontext verbleibt.

[<=]

[Herstellererklärung, Produktgutachten]

Hinweis: Die Bereitstellung des KMS ist eine SOLL-Anforderung und die Anforderung gilt nur dann, wenn auch ein KMS bereitgestellt wird.

14.8 HCC-Provider -Verfügbarkeitsanforderungen

Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet. Es ist eine Zielsetzung, dass HCC-Provider das höchste in der TI bisher geforderte Niveau an Verfügbarkeit abbilden können.

14.9 Anforderungen an HCC-Diensthersteller

Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet.

14.10 Anforderungen an HCC-Dienstanbieter

Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet.

A_26995 - HCC-Dienstanbieter - Private und geheime Schlüssel der VAU im HSM

Der HCC-Dienstanbieter 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

- zur Authentisierung der Verarbeitungskontexte gegenüber von VAU-Clients und Diensten,
- zur Ver- und Entschlüsselung oder
- zur Signatur

genutzt werden.

[<=]

[Sicherheitsgutachten]

14.11 Anforderungen an die HCC-Dienste der gematik

Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet.

14.12 Anforderungen an HCC-Clients

Dieser Abschnitt wird in einer zukünftigen Version der Spezifikation ausgearbeitet.

15 Anhang A - Verzeichnisse

15.1 A1 - Abkürzungen

Kürzel	Erläuterung

Weitere Begriffserklärungen befinden sich in [gemGlossar].

15.2 A2 - Abbildungsverzeichnis

Abbildung 1: Shared Responsibility - Verteilung der Aufgaben.....	20
Abbildung 2: Governance - Deployment View.....	21
Abbildung 3: Integration mit HCC- und TI-externen Diensten.....	22
Abbildung 4: gematik als Garant für HCC.....	23
Abbildung 5: Designtime- und Runtime-Umgebung.....	25
Abbildung 6: Attestation beispielhaft, vereinfacht.....	28
Abbildung 7: HCC-Services in Designtime- und Runtime-Umgebung.....	31

15.3 A4 - Tabellenverzeichnis

Tabelle 1: Mapping Provisioning- und CC-Modelle.....	43
Tabelle 2 : Akteure und ihre Aufgaben.....	48
Tabelle 3: Zulassung von HCC-Providern.....	55
Tabelle 4: Typen von Angreifern.....	61

15.4 A5 - Referenzierte Dokumente

15.4.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

15.4.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel