

genua.

# VPN in der Cloud: Vertrauen dank Confidential Computing

Vertrauen für Ihr VPN in öffentlichen und geteilten Infrastrukturen schaffen

SecurITy made in Germany

# Executive Summary

Wer VPN-Endpunkte in Cloud- oder anderweitig geteilten Infrastrukturen betreibt, muss einer wachsenden Zahl von Beteiligten vertrauen, vom Infrastrukturbetreiber über dessen Dienstleister bis hin zum Personal des Rechenzentrums. Je mehr Schichten und Akteure zwischen der eigenen Anwendung und der physischen Hardware liegen, desto größer wird die Angriffsfläche und die nötige Vertrauensbasis. Gerade im Umfeld vertraulicher Behördenkommunikation ist diese Vertrauensbasis besonders kritisch zu hinterfragen: Hier reicht es nicht, sich auf vertragliche Zusicherungen oder Zertifizierungen des Betreibers zu verlassen, die tatsächliche technische Absicherung muss nachweisbar sein.

Confidential Computing bietet hierfür einen entsprechenden Lösungsweg. Es reduziert die notwendige Vertrauensbasis auf den CPU-Hersteller und den eigenen Software-Stack: Alle übrigen Eigenschaften der Ausführungsumgebung – Firmware, Hypervisor, Betriebssystem-Image – werden kryptografisch attestiert statt diesen schlicht vertrauen zu müssen. Damit lässt sich eine vertrauenswürdige Ausführungsumgebung („Enklave“) für die sichere Verarbeitung (data-in-use) von eingestuften Daten auch dann etablieren, wenn die umgebende Infrastruktur selbst nicht für VS-NfD freigegeben ist und nicht vollständig unter eigener Kontrolle steht.

Dieses Whitepaper überträgt dieses Prinzip konkret auf genuscreen Virtual, eine zugelassene Firewall- und VPN-Lösung von genua, und zeigt, wie sich damit ein auf VS-NfD-Niveau abgesicherter Betrieb realisieren lässt. Grundlage dafür sind drei Vertrauensanker: die CPU selbst sowie ein Attestation Server und ein Smartcard Server, die beide idealerweise On-Prem betrieben und über die Central Management Station genucenter verwaltet werden.

# 1. Einleitung

Die Verlagerung von IT-Infrastruktur in die Cloud oder in gemeinsam genutzte Rechenzentren ist heute für die meisten Organisationen – auch im öffentlichen Sektor – wirtschaftlich kaum mehr zu umgehen. Gleichzeitig steigen die Anforderungen an die Vertraulichkeit, insbesondere dort, wo Verschlusssachen verarbeitet werden. Diese beiden Entwicklungen scheinen zunächst im Widerspruch zueinander zu stehen: Geteilte Infrastruktur bedeutet grundsätzlich mehr Beteiligte und damit mehr potenzielle Angriffsflächen, während VS-NfD-Anforderungen eine möglichst kleine, gut kontrollierbare Vertrauensbasis verlangen.

Dieses Whitepaper zeigt, dass sich dieser scheinbare Widerspruch technisch auflösen lässt. Der Schlüssel liegt darin, die Frage „Wem muss ich vertrauen?“ so präzise und reduziert wie möglich zu beantworten. Confidential Computing liefert dafür die technische Grundlage, indem es Vertrauen durch kryptografisch nachprüfbare Verifikation ersetzt, wo immer dies möglich ist.

# 2. Vertrauen in Cloud-Umgebungen

Von der physischen Infrastruktur bis zur Anwendung enthalten Cloud-Umgebungen viele Schichten mit jeweils eigenen Verantwortlichen und Beteiligten: Rechenzentrumsbetreiber, Hardware- und Firmware-Hersteller, Virtualisierungs-Hersteller und Cloud-Anbieter, Betreiber von Plattformdiensten, Systemintegratoren und schließlich die Anwendungsverantwortlichen selbst. Jede zusätzliche Schicht und jeder zusätzliche Akteur erweitert die Fläche, auf der Vertrauen aufgebaut oder eben in Frage gestellt werden muss. Für jede Organisation, die Vertraulichkeit ernst nimmt, ist es daher hilfreich, diese Schichten explizit zu benennen und für jede einzelne zu klären, welches Vertrauen sie tatsächlich erfordert.

## 2.1 Ressourcen teilen: eine betriebswirtschaftliche Notwendigkeit

Das Teilen von Ressourcen ergibt auf praktisch jeder Schicht Sinn und ist wirtschaftlich kaum zu umgehen. Auf der Infrastrukturebene führt gemeinsam genutzte Hardware zu mehr Standardisierung sowie niedrigeren Investitions- und Betriebskosten (Capex/Opex), weil sich Anschaffung, Wartung und Betrieb auf viele Nutzer verteilen. Bei Virtualisierungs- und Cloud-Diensten profitieren Organisationen zusätzlich von der Expertise spezialisierter Anbieter, ohne diese Fähigkeiten selbst kostenintensiv aufbauen und vorhalten zu müssen – das senkt insbesondere die

Personalkosten für hochspezialisierte Tätigkeiten. Auch geteilter Speicher folgt dieser Logik: Durch Mandantenfähigkeit lassen sich Kapazitäten flexibel und kosteneffizient nutzen, statt für jede Organisation isolierte Silos vorzuhalten.

Diesen wirtschaftlichen Vorteilen stehen jedoch Risiken gegenüber, die untrennbar mit dem Teilen von Ressourcen verbunden sind. Werden Hardware, Virtualisierungsschicht oder Speicher gemeinsam genutzt, erhalten zwangsläufig weitere Akteure eine potenzielle Nähe zu den eigenen Daten und Systemen: der Betreiber der Infrastruktur selbst, dessen Personal und Dienstleister sowie – bei Cloud- und Virtualisierungsumgebungen – andere Kunden, die dieselbe physische Hardware nutzen. Anders als beim On-Prem-Betrieb lassen sich diese Akteure in der Regel weder vertraglich im Detail steuern noch organisatorisch kontrollieren. Die Angriffsfläche und die erforderliche Vertrauensbasis wächst damit genau in dem Maße, in dem Ressourcen geteilt werden – und muss gezielt wieder reduziert werden.

## 2.2 Risiko minimieren

Um die mit geteilter Infrastruktur verbundenen Risiken und Abhängigkeiten zu beherrschen, sind zwei Stellschrauben zentral. Erstens klare, idealerweise standardisierte Schnittstellen zwischen den Schichten: Diese sorgen dafür, dass Verantwortlichkeiten eindeutig zugeordnet werden können und Abhängigkeiten von einzelnen Anbietern durch Wechselfähigkeit reduziert werden. Zweitens, das ist der zentrale Hebel dieses Whitepapers, die konsequente Reduktion der notwendigen Vertrauensbasis: Je weniger Akteuren und Komponenten ungeprüft vertraut werden muss, desto kleiner wird die tatsächliche Angriffsfläche, unabhängig davon, wie viele Schichten formal existieren.

Verschlüsselung ist dabei durchgängig über alle drei relevanten Zustände von Daten hinweg umzusetzen:

### DATA AT REST

Die Daten werden auf Datenträgern verschlüsselt abgelegt, sodass ein Zugriff auf die Datenträger allein nicht zur Kenntnisnahme führt.

### DATA IN TRANSIT

Die Daten werden auf dem Übertragungsweg verschlüsselt, etwa mittels VPN/IPSec oder TLS, um Abhören und Manipulation zu verhindern.

### DATA IN USE

Die Daten werden auch während der Verarbeitung im Arbeitsspeicher verschlüsselt und in der CPU isoliert – dies ist genau der Bereich, den klassische Verschlüsselungskonzepte nicht abdecken und den Confidential Computing adressiert.

Erst die Kombination aller drei Zustände schließt die Lücke, die entsteht, wenn Daten zwar auf dem Datenträger und auf dem Transportweg geschützt sind, während der eigentlichen Verarbeitung im Speicher jedoch für den Host-Betreiber oder andere Mandanten auf derselben Hardware potenziell einsehbar wären. Besonderes Augenmerk muss hier auf das Handling der verwendeten kryptografischen Schlüssel gelegt werden: Die Verschlüsselung allein reicht nicht aus, wenn die Schlüssel vom Anbieter der Cloud-Infrastruktur verwaltet werden. “Bring your own key” ist hier das Stichwort, das dem Nutzer der Infrastruktur die Hoheit über die eigenen Daten sichert.

## 3. Vertrauen neu bewerten im VS-NfD-Umfeld

Im Bereich vertraulicher Behördenkommunikation gilt ein besonders strenger Maßstab. Nach der einschlägigen Definition ist eine Information als Verschlusssache einzustufen, „wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.“ (VSA §2 Abs 2.4)

Diese Definition ist bewusst weit gefasst und stellt nicht auf einzelne Technologien, sondern auf das Ergebnis ab: die Möglichkeit unbefugter Kenntnisnahme. Für den Betrieb von IT-Systemen bedeutet dies, dass alle Personen und Systeme, die potenziell Kenntnis entsprechender Daten erlangen könnten, explizit in die Vertrauensbetrachtung einzubeziehen sind, unabhängig davon, ob ein Zugriff im Regelbetrieb vorgesehen ist oder nur theoretisch möglich wäre.

Für den tatsächlichen Betrieb ergeben sich daraus im Kern zwei grundsätzliche Ansätze – der On-Prem-Betrieb und der Betrieb auf geteilter Infrastruktur – die mit jeweils eigenen Herausforderungen und Anforderungen an die Vertrauensbasis einhergehen. Der folgende Vergleich zeigt, an welchen Stellen sich diese Anforderungen unterscheiden.

### 3.1 On-Prem vs. geteilte Infrastruktur

Der Vergleich zwischen dem klassischen On-Prem-Betrieb und dem Betrieb auf geteilter Infrastruktur macht deutlich, an welchen Stellen sich die Vertrauensbasis vergrößert:

| Aspekt | On-Prem | Geteilte Infrastruktur |
|---|---|---|
| Dienstleister | Eigene, vertraglich gebundene Dienstleister | Dienstleister des Infrastrukturbetreibers, oft ohne direkten Vertragsbezug zum Nutzer |
| Personal | Eigenes, vertrauenswürdiges Personal | Personal und Dienstleister des Betreibers |
| Physische Absicherung | Vollständig selbst kontrolliert | Abhängig vom Betreiber; ggf. besondere RZ-Zertifizierung, aber fremde Kontrolle |
| Weitere Faktoren | – | Nationalität/Jurisdiktion und Standort des Betreibers; andere Kunden auf derselben Infrastruktur |

Besonders die Nationalität und Jurisdiktion des Betreibers sowie der physische Standort der Infrastruktur sind im VS-NfD-Kontext relevant, da sie bestimmen, welchem Rechtsraum – und damit welchen staatlichen Zugriffsrechten – die Infrastruktur unterliegt. Hinzu kommt, dass auf geteilter Infrastruktur grundsätzlich andere Kunden dieselbe Hardware nutzen, was zusätzliche Isolationsanforderungen mit sich bringt.

### 3.2 Abhängigkeiten und Wechselfähigkeit

Neben der reinen Vertrauensbasis gegenüber dem Betreiber stellt sich bei geteilter Infrastruktur eine zweite, eng verwandte Frage: die Abhängigkeit von genau diesem einen Anbieter. Genau wie die Vertrauensbasis selbst sollte auch diese Abhängigkeit so weit wie möglich reduziert werden – nicht zuletzt, weil ein späterer Wechsel des Anbieters aus wirtschaftlichen, rechtlichen oder sicherheitspolitischen Gründen notwendig werden kann. Der wirksamste Hebel dafür sind klare, möglichst offene Standards: Sie ermöglichen es, Workloads, Konfigurationen und Daten grundsätzlich auch zu einem anderen Anbieter zu portieren, statt an proprietäre Schnittstellen gebunden zu sein.

Wie stark diese Abhängigkeit in der Praxis tatsächlich ausgeprägt ist, hängt jedoch maßgeblich davon ab, auf welcher Ebene eine Organisation die Cloud oder geteilte Infrastruktur nutzt. Mit zunehmender Abstraktion – von der reinen Infrastruktur über eine Container-Plattform bis hin zu fertiger Software – steigt tendenziell auch die Abhängigkeit von den spezifischen Fähigkeiten und Standards des jeweiligen Anbieters:

| Nutzungsszenario | Charakteristik | Wechselfähigkeit |
|---|---|---|
| IaaS (Infrastructure as a Service) | Viel Eigenleistung bzw. Einsatz eines eigenen Dienstleisters; geringste Abstraktion, nahezu vollständige Kontrolle über den eigenen Software-Stack | Vergleichsweise einfach wechselbar, da im Wesentlichen nur Standard-Rechenleistung, Netzwerk und Storage genutzt werden |
| KaaS (Kubernetes as a Service) | Mehr Abstraktion, weniger Eigenleistung; Anwendungen laufen auf einer vom Anbieter betriebenen Container-Plattform | Bei konsequenter Nutzung offener, standardkonformer Schnittstellen (z. B. Kubernetes-API) grundsätzlich gut wechselbar; die Praxis hängt jedoch stark von anbieterspezifischen Erweiterungen ab |
| SaaS (Software as a Service) | Vollständige Abhängigkeit vom Anbieter für Betrieb und Funktionsumfang der Anwendung selbst | Gering; entscheidend ist die Kommunikation von VS-NfD-Anforderungen an den Anbieter sowie vertraglich gesicherter Datenexport und -zugriff |

Bei SaaS-Lösungen ist die Abhängigkeit vom Anbieter also ohnehin hoch und lässt sich über Standards allein kaum auflösen. Entscheidend ist hier, dass VS-NfD-Anforderungen dem Anbieter aktiv und frühzeitig kommuniziert werden – insbesondere dann, wenn die Software ein Fachverfahren der Verwaltung abbildet und der Anbieter faktisch im Auftrag des Staates tätig ist. Genau diese Zielgruppe – Betreiber und Nutzer von Fachverfahren mit VS-NfD-Bezug – adressiert dieses Whitepaper mit dem Confidential-Computing-Ansatz, der im Folgenden vorgestellt wird.

# 4. Confidential Computing: Funktionsweise im Überblick

Confidential Computing verfolgt einen einfachen, aber wirkungsvollen Grundgedanken: Statt vielen Akteuren entlang des gesamten Betriebs zu vertrauen, wird die Vertrauensbasis auf ein Minimum reduziert: im Idealfall auf den Hersteller der eingesetzten CPU und den eigenen Software-Stack. Technisch wird dies über ein sogenanntes Trusted Execution Environment (TEE) realisiert: einen durch die CPU-Hardware isolierten, verschlüsselten Speicherbereich, dessen Inhalt selbst für den Hypervisor, das Host-Betriebssystem oder durch physischen Zugriff auf den Server nicht einsehbar ist. Ergänzt wird dies durch eine passende Isolation der Prozesse insbesondere beim Kontextwechsel in der CPU, die absichtliches und unabsichtliches “Übersprechen” der vertraulichen Informationen verhindert.

Damit Vertrauen nicht blind vorausgesetzt, sondern echte Vertrauenswürdigkeit nachgewiesen werden kann, kommt das Prinzip der Remote Attestation zum Einsatz: Bei Inbetriebnahme der virtuellen Maschine – und bei Bedarf auch danach – weist die Ausführungsumgebung kryptografisch nach, welche CPU mit welchen CPU-Flags, welche Firmware-Version und welches Software-Image tatsächlich geladen sind. Erst wenn diese Prüfung erfolgreich ist, werden Geheimnisse wie Schlüsselmaterial oder Konfigurationsdaten in die Umgebung eingebracht. Wird eine Manipulation festgestellt – etwa ein verändertes Image oder eine nicht vertrauenswürdige Firmware – bleibt der Zugriff auf diese Geheimnisse verwehrt.

# 5. VPN sicher betreiben mit Confidential Computing

Überträgt man dieses Prinzip auf den Betrieb von genuscreen Virtual, ergibt sich eine Architektur mit drei Vertrauensankern, die zusammen die technische Basis für einen VS-NfD-konformen Betrieb auf geteilter Infrastruktur bilden.

## 5.1 Drei Vertrauensanker

**01** **CPU als Anker:**
Das Vertrauen beschränkt sich auf den CPU-Hersteller, dessen Confidential-Computing-Erweiterungen die Isolation und Verschlüsselung im laufenden Betrieb technisch durchsetzen und über Measurements in der Laufzeitumgebung überprüfbar machen.

**02** **genuscreen Attestation Server:**
Der zentrale Vertrauensanker, welcher CPU, Firmware und Software-Image der Instanz von genuscreen Virtual verifiziert, bevor diese in Betrieb geht; wird On-Prem betrieben und bleibt damit unter eigener Kontrolle.

**03** **genuscreen Smartcard Server:**
Der zugelassene Betrieb von genuscreen Virtual benötigt eine physische Smartcard für kryptografisches Material. Der Zugriff auf diese Smartcard wird virtualisiert bzw. abstrahiert über einen extra Server bereitgestellt, dessen physische Smartcard weiterhin On-Prem verbleibt.



**Die Betriebsmodi genuscreen Attestation Server und genuscreen Smartcard Server dienen als Vertrauensanker bei Confidential-Computing-Anwendungen.**

Der Betrieb des Attestation Server unter eigener Kontrolle ist hier ein zentraler Sicherheitsbaustein. Während bei klassischem “Bring your own key” das Schlüsselmaterial in die geteilte Infrastruktur übertragen wird, bleibt es bei diesem Ansatz vollständig in der Infrastruktur der Nutzer und wird zu einem “Use your own key”, wobei diese Keys auch physisch den eigenen Einflussbereich nie verlassen.

Confidential Computing sorgt dafür, dass die Inhalte der virtuellen Maschine – Konfiguration, Schlüsselmaterial und verarbeitete Daten – für den Host-Betreiber, für andere Gäste auf derselben Hardware sowie für potenzielle Angreifer unsichtbar bleiben. Das schließt grundsätzlich auch Administratoren ein: Zwar können Administratoren theoretisch sowohl beim Betreiber als auch beim Nutzer beschäftigt sein, in der Praxis sollte eine solche Konstellation jedoch über strikt getrennte Nutzerkonten bzw. ein föderiertes Identitäts- und Zugriffsmanagement (IAM) und streng getrennte Administrationsumgebungen abgebildet werden, damit keine faktische Umgehung der technischen Isolation entsteht.

## 5.2 Szenario A: VPN-Knoten auf geteilter Infrastruktur

In diesem Szenario soll skizziert werden, wie eine Kundenumgebung in einer geteilten Infrastruktur an die kundeneigene Infrastruktur sicher angebunden werden kann. „Geteilt“ meint hier eine Public Cloud Umgebung oder einen gemeinsam genutzten Dienstleister.

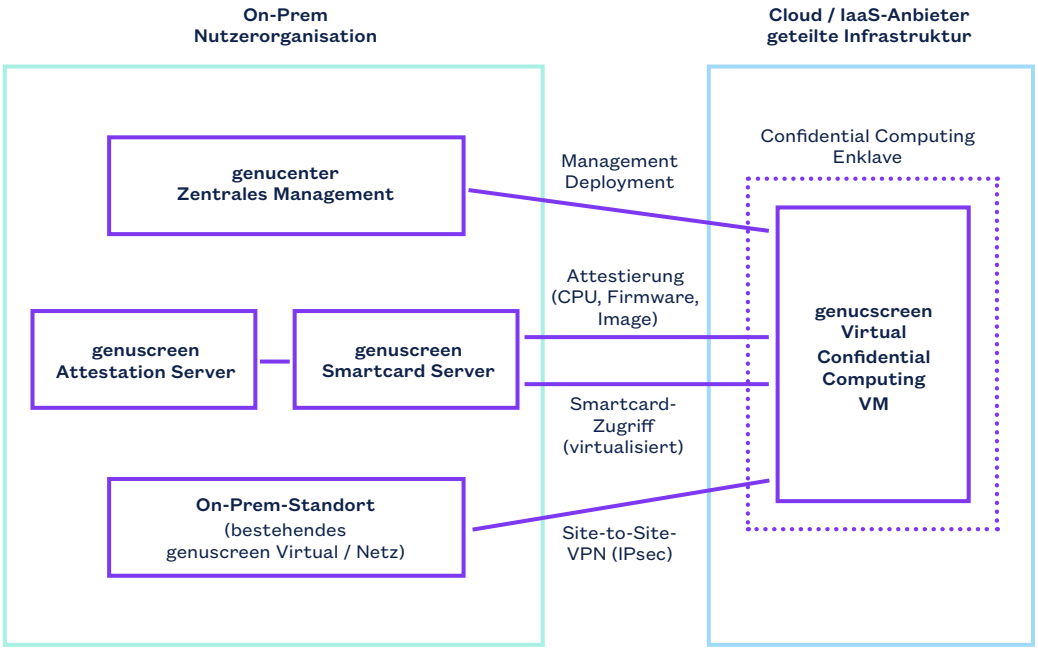
Architektonisch entspricht dies einem klassischen Site-to-Site-VPN, bei dem ein oder mehrere Standorte als Tenant in der Cloud bzw. beim Dienstleister liegen, statt – wie bislang üblich – ausschließlich in physisch kontrollierten eigenen Rechenzentren.

Der Aufbau der Cloud-seitigen genuscreen Virtual mit Confidential Computing gliedert sich in drei Schritte: Zunächst wird die virtuelle Maschine auf Basis von IaaS aufgesetzt. Anschließend prüft der genuscreen Attestation Server die initiale Konfiguration, stellt über die beschriebene Attestierung das notwendige Vertrauen in CPU, Firmware und Image her und übergibt die nötige Konfiguration für den Betrieb und den Kontakt zur zentralen Administration per genucenter und zum Smartcard Server. Schließlich sorgt der genuscreen Smartcard Server für das physische Vertrauen in die VPN-Infrastruktur, indem er den Zugriff auf die On-Prem-verbleibende Smartcard bereitstellt.

Die On-Prem-verbleibende Vertrauensbasis besteht aus drei Komponenten: der zentralen Management-Lösung genucenter, dem genuscreen Attestation Server und dem genuscreen Smartcard Server. Das zentrale Management verwaltet dabei die an dem VPN-Verbund beteiligten Instanzen von genuscreen und genuscreen Virtual und überdies auch den in Hardware ausgeführten genuscreen Attestation

Server und genuscreen Smartcard Server. Diese Bündelung stellt sicher, dass die eigentlichen Vertrauensanker jederzeit unter eigener, physischer Kontrolle bleiben, auch wenn die eigentliche Verarbeitung in fremder Infrastruktur stattfindet.

Im laufenden Betrieb erfolgt das Management zentral über genucenter, einschließlich der Steuerung von VPN-Verbünden bzw. eines VPN-Mesh über mehrere Instanzen von genuscreen Virtual hinweg. Updates werden bewusst nicht als persistente Änderungen am laufenden Image eingespielt, sondern wie in modernen Cloud-Deployments üblich über ein (paralleles) Neu-Deployment des neuen Images. Dieses Vorgehen ist durch die Attestierung ohnehin erforderlich, hat aber einen wichtigen positiven Nebeneffekt für die Sicherheit: Auch ein Angreifer, dem es gelingen sollte, sich in einer laufenden Instanz festzusetzen, verliert diesen Zugriff mit dem nächsten Deployment-Zyklus, da keine persistenten Änderungen am Image erhalten bleiben.




**VPN-Knoten auf geteilter Infrastruktur:
Vertrauensanker (genucenter, genuscreen Attestation Server und genuscreen Smartcard Server) bleiben On-Prem, genuscreen Virtual läuft attestiert in der Cloud**

Nun werden solche VPN-Verbünde selten rein als Selbstzeck betrieben, im Regelfall sollen über das VPN eine oder mehrere Fachanwendungen erreicht und genutzt werden. Dabei stellen sich an den sicheren Betrieb der Fachanwendung die gleichen Anforderungen wie an den Betrieb von genuscreen Virtual.

Eine Lösung in Form des Betriebes der Fachanwendung in einem per Confidential Computing gesicherten Trusted Execution Environment bietet sich an. Im Sinne der Wechselfähigkeit, Universalität und auch der einfacheren Entwicklung der Fachsoftware wird dieses TEE für den Anwendungsbetrieb wieder eine standardisierte Schnittstelle, etwa Kubernetes, bereitstellen. Dann kann eine Fachanwendung ohne spezielle Anpassungen über das Deployment in einem derartigen VS-NfD-konformen Cluster als entsprechende Fachanwendung betrieben werden. Die Knoten eines solchen Clusters werden untereinander und zur genuscreen Virtual ein sicheres und zugelassenes VPN als Underlay aufspannen und auf die eingebundenen Festplatten mit einer zugelassenen Verschlüsselung zugreifen. Damit profitieren Fachverfahren von der reduzierten Vertrauensbasis, ohne selbst vollständig neu konzipiert werden zu müssen.

Das in diesem Whitepaper beschriebene Prinzip – Vertrauen durch Attestierung statt durch Annahme – lässt sich damit konsequent von der VPN-Ebene auf die gesamte Laufzeitumgebung des Fachverfahrens ausdehnen.

### 5.3 Szenario B: VPN-Einwahlknoten in geteilter Infrastruktur

Ein weiteres Szenario, bei dem eine Cloud bzw. eine gemeinsame Infrastruktur eines Anbieters auf mehrere Mandanten aufgeteilt ihre Vorteile ausspielen kann, ist der Betrieb von VPN-Einwahlknoten. Viele unterschiedliche VS-NfD-Informationsverbünde laufen hier auf einer gemeinsamen Infrastruktur – typischerweise bei einem Dienstleister, der sich auf VPN-Einwahl spezialisiert hat und mehrere Kunden gleichzeitig bedient. Anders als in Szenario A steht hier nicht ein einzelner Standort-zu-Standort-Tunnel im Vordergrund, sondern die Fähigkeit, viele Endnutzer verschiedener Organisationen sicher und getrennt voneinander anzubinden.

Da mehrere VS-NfD-Informationsverbünde dieselbe Hardware nutzen, ist eine Mandantentrennung auf VS-NfD-Niveau zwingend erforderlich – und zwar unabhängig davon, ob das Rechenzentrum selbst bereits über eine besondere physische Absicherung verfügt. Eine gute physische Absicherung des Standorts ersetzt nicht die technische Trennung der Mandanten auf Ebene der einzelnen Ausführungsumgebungen.

genuscreen Virtual mit Confidential Computing besteht in diesem Szenario aus mehreren VMs auf IaaS, die über Templates mit Automatisierung zügig ausgerollt

und bei Lastspitzen skaliert werden können. Jede dieser Instanzen ist in gleicher Weise wie in Szenario A an einen genuscreen Attestation Server und einen genuscreen Smartcard Server angebunden, sodass jede einzelne Instanz unabhängig attestiert und mit den notwendigen Zertifikaten versorgt wird.

Anders als in Szenario A, bei dem Attestation Server und Smartcard Server zentral für eine Organisation On-Prem betrieben werden, stellt sich hier für jeden einzelnen Mandanten erneut die Frage, wo diese beiden Vertrauensanker angesiedelt werden.

Zwei Varianten sind denkbar:

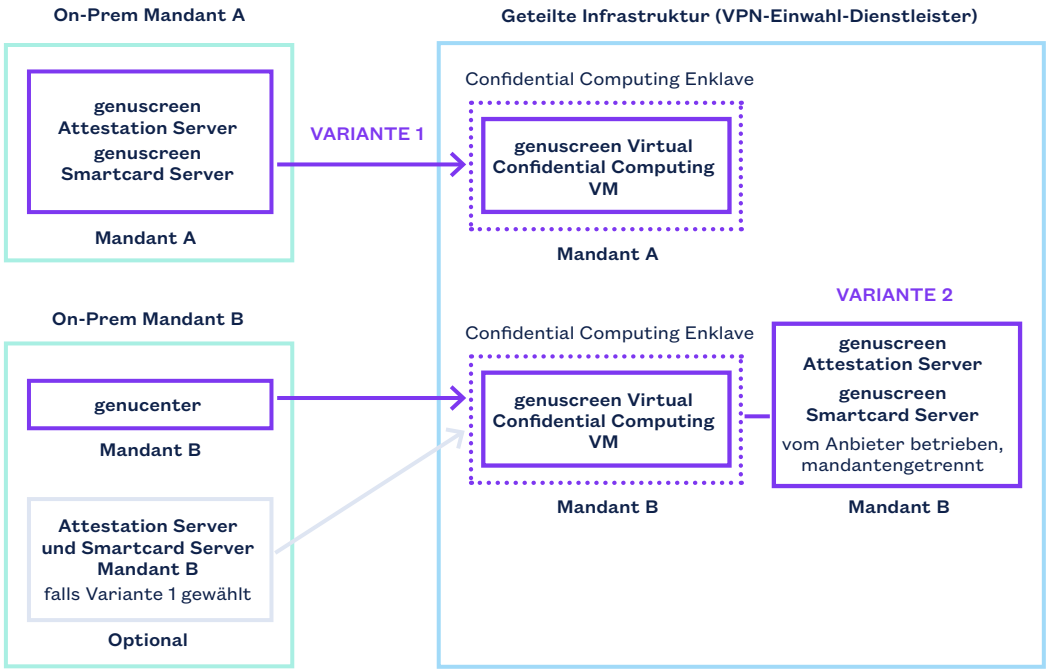
### VARIANTE 1

**genuscreen Attestation Server und genuscreen Smartcard Server On-Prem beim Mandanten:** Jeder Mandant betreibt seinen eigenen Attestation Server und Smartcard Server in seiner eigenen Organisation. Der Vorteil liegt darin, dass der Dienstleister selbst keine als Verschlusssache eingestufte Hardware handhaben muss – die kritischen Vertrauensanker verlassen zu keinem Zeitpunkt den Verantwortungsbereich des Mandanten. Der Dienstleister stellt lediglich die geteilte Infrastruktur für die eigentlichen VMs der genuscreen Virtual bereit.

### VARIANTE 2

**genuscreen Attestation Server und genuscreen Smartcard Server beim Anbieter, mandantengetrennt:** Alternativ betreibt der Dienstleister Attestation Server und Smartcard Server für jeden Mandanten getrennt selbst im eigenen Rechenzentrum. Dies kann sinnvoll sein, wenn Mandanten selbst keinen geeigneten On-Prem-Standort für diese Komponenten vorhalten wollen oder können. Voraussetzung ist dann allerdings, dass der Dienstleister als vertrauenswürdig genug eingestuft wird, um auch diese sensible Hardware mandantengetrennt und VS-NfD-konform zu betreiben.

Welche Variante im Einzelfall die Richtige ist, hängt von den organisatorischen Möglichkeiten des jeweiligen Mandanten sowie vom Vertrauen ab, das dem Dienstleister für den Betrieb sensibler Hardware entgegengebracht werden kann. Beide Varianten lassen sich technisch parallel innerhalb derselben Infrastruktur des Dienstleisters betreiben, da jede Instanz von genuscreen Virtual unabhängig von den anderen an ihre eigenen Attestation- und Smartcard-Services gebunden ist.




**VPN-Einwahlknoten mit mehreren Mandanten:
Mandant A nutzt Variante 1 (Vertrauensanker On-Prem),
Mandant B nutzt Variante 2 (Vertrauensanker mandantengetrennt beim Anbieter)**

Im Ergebnis entsteht eine Lösung, die Skalierung und gemeinsame Hardware-Nutzung miteinander vereinbart, ohne die notwendige Vertrauens- und Mandantentrennung aufzugeben: Jeder VS-NfD-Informationsverbund erhält eine eigene, kryptografisch isolierte und attestierte Ausführungsumgebung, unabhängig davon, wie viele andere Verbünde dieselbe physische Infrastruktur nutzen und unabhängig davon, für welche der beiden Varianten sich der jeweilige Mandant entscheidet.

# 6. Grenzen und Herausforderungen

Confidential Computing reduziert die notwendige Vertrauensbasis erheblich, hebt sie jedoch nicht vollständig auf. Ein Restvertrauen in den CPU-Hersteller bleibt erforderlich, da dieser die Hardware-Grundlage der Isolation und data-in-use-Verschlüsselung liefert und theoretisch in der Lage wäre, Schwachstellen einzubringen oder bestehende Schwachstellen auszunutzen. Dieses Restrisiko lässt sich nicht wegdiskutieren, ist aber deutlich geringer und besser eingrenzbar als das Vertrauen, das ein vollständig ungeschützter Cloud-Betrieb mit einer Vielzahl von Akteuren erfordern würde.

Darüber hinaus setzt der beschriebene Ansatz voraus, dass Attestation Server und Smartcard Server tatsächlich On-Prem und unter eigener Kontrolle betrieben werden – werden diese Anker ausgelagert, verschiebt sich auch ein Teil der reduzierten Vertrauensbasis wieder zurück auf einen externen Betreiber. Organisationen sollten daher bei der Umsetzung besonderes Augenmerk auf den Betrieb dieser beiden Komponenten legen.

Schließlich ist auch der organisatorische Aspekt nicht zu unterschätzen: Die in Kapitel 5.1 beschriebene Trennung von Rollen und Nutzerkonten zwischen Betreiber- und Nutzerorganisation muss in der Praxis konsequent umgesetzt und regelmäßig überprüft werden, damit die technische Isolation nicht durch organisatorische Nachlässigkeit unterlaufen wird.

# 7. Fazit und Ausblick

Confidential Computing liefert eine technische Lösung für belastbares Vertrauen in Cloud-Umgebungen, die über rein vertragliche oder organisatorische Zusicherungen hinausgeht: Statt sich auf Zertifikate und Selbstauskünfte des Betreibers zu verlassen, wird die tatsächliche Vertrauenswürdigkeit der Ausführungsumgebung kryptografisch nachgewiesen.

Auf dieser Grundlage werden Mandanten sowohl voneinander als auch vom Host-Betreiber klar getrennt. Dieses Sicherheitsniveau ist ausreichend für den Betrieb von VS-NfD und bildet damit eine belastbare technische Basis für Organisationen,

die VPN-Infrastruktur oder ganze Fachverfahren in geteilte oder Cloud-Umgebungen verlagern möchten, ohne die Vertraulichkeitsanforderungen von Verschlusssachen zu gefährden.

Verifizierte, attestierte Ausführungsumgebungen lassen sich dabei praktisch überall betreiben, solange die zentralen Vertrauensanker – Attestation Server und Smartcard Server – unter eigener Kontrolle bleiben, sei es On-Prem beim Nutzer selbst oder bei einem entsprechend vertrauenswürdigen Dienstleister. Im Ergebnis entsteht so eine VS-NfD-Enklave innerhalb einer fremden, nicht für VS-NfD freigegebenen Infrastruktur – und damit ein Weg, die wirtschaftlichen Vorteile geteilter Infrastruktur zu nutzen, ohne bei den Vertraulichkeitsanforderungen von Verschlusssachen Kompromisse einzugehen.

Für Organisationen, die vor der Entscheidung stehen, VPN-Infrastruktur oder ganze Fachverfahren in geteilte oder Cloud-Umgebungen zu verlagern, bietet der hier beschriebene Ansatz damit einen konkreten, technisch fundierten Weg, dies auch unter VS-NfD-Anforderungen verantwortbar umzusetzen – und, wie in Kapitel 5.2 skizziert, perspektivisch auch über die VPN-Ebene hinaus bis auf die Ebene der Fachverfahren selbst auszudehnen.

**Wie diese Erweiterung auf die Ebene der Fachverfahren im konkreten Anwendungsfall am besten ausgestaltet wird, lässt sich am besten im Dialog klären. Sprechen Sie uns gerne an, um gemeinsam die bestmögliche Umsetzung für Ihr Vorhaben zu erarbeiten.**

**Interessiert? Gerne informieren wir Sie persönlich. Kontaktieren Sie uns:**
+49 89 991950-902 oder vertrieb@genua.de

## ABKÜRZUNGSVERZEICHNIS

| | |
|---|---|
| **IaaS** | Infrastructure as a Service |
| **IAM** | Identity and Access Management |
| **KaaS** | Kubernetes as a Service |
| **PaaS** | Platform as a Service |
| **SaaS** | Software as a Service |
| **TEE** | Trusted Execution Environment – hardwareseitig isolierter, verschlüsselter Ausführungsbereich |
| **VS-NfD** | Verschlusssache – Nur für den Dienstgebrauch |

## Mehr zum Thema:

genua.de/confidential-computing

1026-01-DE

## Über genua

Mit ihren in Deutschland entwickelten und produzierten IT-Sicherheitslösungen ist die genua GmbH eine Wegbereiterin für digitale Souveränität. Behörden, geheimschutzbetreute Organisationen und KRITIS-Unternehmen vertrauen auf genua zum Schutz ihrer kritischen und hochsensiblen digitalen Infrastrukturen.

genuas Portfolio umfasst hochsichere, Backdoor-freie und skalierbare IT-Security-Produkte wie Firewalls, Gateways, quantenresiliente VPNs, Fernwartungssysteme und Komplettlösungen für VS-NfD-konformes mobiles Arbeiten. Viele Produkte sind auch als virtualisierte Variante für eine flexible Cloud-Integration verfügbar. Regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) belegen das hohe Sicherheits- und Qualitätsniveau.

Mit ihren rund 500 Mitarbeitenden ist die genua GmbH Teil der Bundesdruckerei-Gruppe. Das Unternehmen ist vom BSI als „Qualifizierter Hersteller“ eingestuft und mit seinen Produkten im Kaufhaus des Bundes gelistet. Zu den Kunden zählen u. a. BMW, die Bundeswehr, das THW und die Würth-Gruppe.

Teil der Bundesdruckerei-Gruppe

**genua GmbH**

Domagkstraße 7 | 85551 Kirchheim bei München
+49 89 991950-0 | info@genua.de | www.genua.de