Confidential Cloud

-

3D Encryption

Whitepaper

Fassung vom 02.06. 2023

1. Überblick

Spätestens seit dem Schrems-II Urteil wurde die Öffentlichkeit sensibilisiert, dass das ungeschützte Speichern von Daten in einer Cloud – insbesondere einer nicht-europäischen - die Vertraulichkeit und Integrität der Informationen gefährden kann. Dennoch möchte heutzutage kein Unternehmen mehr auf die enormen Vorteile einer Cloud-Lösung verzichten, die die Nutzung eines Cloud-Speicherdienstes bietet.

2. 3D Verschlüsselung

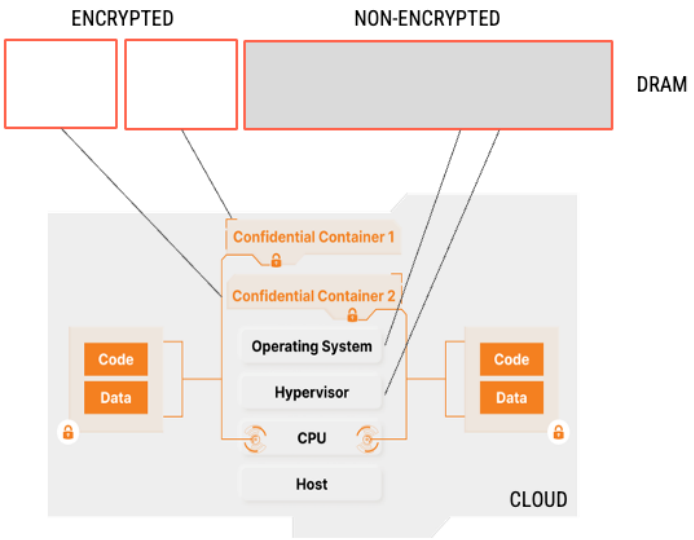
2.1 Überblick

Sämtliche, in der Confidential Nextcloud abgelegten Daten, werden mit der modernsten 3D Verschlüsselung abgesichert. Mit Hilfe von Confidential Cloud Computing, einem innovativen Sicherheitskonzept für Cloud-Lösungen, ermöglicht enclaive die automatische Verschlüsselung von Daten

- während des Nutzens („data in use encryption“)
- im Ruhenstand („data at rest encrytpion“)
- in Bewegung (“data in transit“)

Somit sind Daten auch während der Bearbeitung verschlüsselt. Sinnbildlich funktioniert die enclaive Technologie wie ein kryptographischer Tresor, in dem Daten gespeichert und prozessiert werden.

2.2 Verschlüsselung während des Nutzens



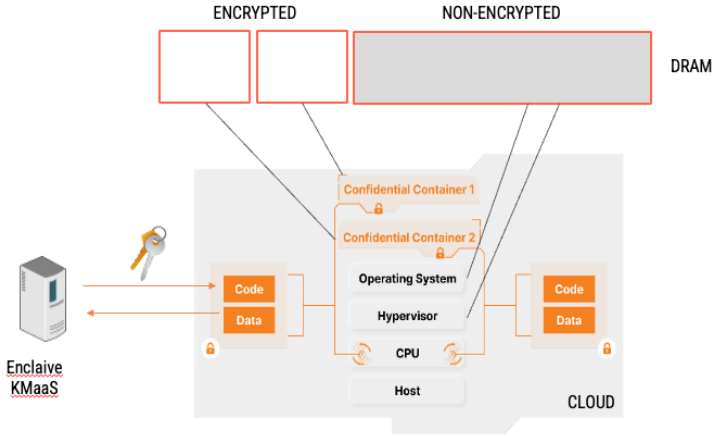
Moderne Prozessoren verfügen über ein Sicherheitsmodul (Intel SGX/TDX oder AMD SEV), welches den Prozessor (CPU) um Verschlüsselungsfähigkeiten des Speichers erweitert. Wenn ein Programm gestartet wird, dann passiert mittels enclaive Technologie folgendes:

1. Das Programm wird dekodiert und sogenannte Mikroinstruktionen werden in dem Hauptspeicher (DRAM) geladen.
2. Ein spezieller Speicherbereich wird adressiert, die so genannte Enklave, von der der Prozessor weiß, der Speicherbereich ist besonders geheim zu halten.
3. Die CPU generiert einen Schlüssel, der so genannte ephemeral enclave key (EEK), für jedes Programm und verschlüsselt die Mikroinstruktionen, bevor sie in den Speicher geschrieben werden.
4. Der Schlüssel wird einem speziell abgesicherten Register auf dem Prozessor gespeichert.
5. Soll die CPU nun das Programm ausführen, so lädt sie die verschlüsselten Mikroinstruktionen Schritt für Schritt aus dem Speicher, entschlüsselt sie mit dem ephemeral enclave key, führt sie aus, verschlüsselt das Ergebnis wieder mit dem ephemera enclave key, und schreibt das Chiffrat in den Speicher.

Vertrauensmodell

- Der ephemeral enclave key EEK wird für jede Enklave neu generiert
- Weder der Cloud Service Provider noch enclaive oder der Kunde haben Möglichkeiten auf den Schlüssel zuzugreifen
- Allein die CPU kann auf den Schlüssel zugreifen
- Sollte der Server neugestartet werden, so werden alle Enklaven als auch EEKs gelöscht

2.3 Verschlüsselung im Ruhezustand



Verschlüsselung im Ruhezustand ist eine komplementäre enclaive Technologie, um Daten dieses Mal nicht im Hauptspeicher, sondern auf einem persistenten Speicher wie der Festplatte zu verschlüsseln. Das Prinzip ist vergleichbar mit Festplattenverschlüsselung für Desktop-PCs, wobei enlaive als Dienstleistung das Schlüsselmanagment [1](KMaaS) übernimmt:

1. Nachdem das Programm in der Enklave ausgeführt wurde, wird es Zugriff auf die Festplatte

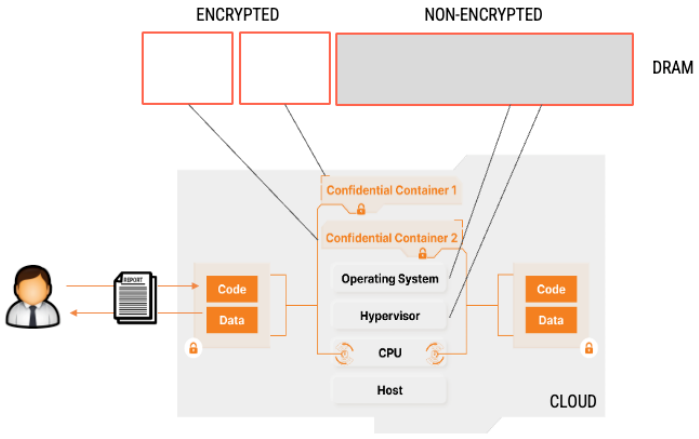
[1] Auch kann der Kunde das Schlüsselmanagement übernehmen

fordern.
2. Die Dateien sind mit einem Schlüssel, dem so genannten disc encryption key (DEK), verschlüsselt.
3. Die Enklave fragt beim enlaive Schlüsselmanagement Serives (KMaaS) an, ob sie berechtigt ist, auf den DEK zu zugreifen.
4. Über Remote Attestation TLS (RA-TLS), eine spezielle Erweiterung des TLS Protokolls, überprüft der KMaaS, ob die Enklave die Berechtigung kriegen kann. Dabei kontrolliert der KMaaS, ob (a) die Enklave tatsächlich verschlüsselt ist, und (b) ob es sich um das richtige und nicht modifizierte Programm handelt.
5. Sollte die Attestierung korrekt sein, so schickt der KMaaS über die verschlüsselte TLS Verbindung den DEK.
6. Die Enklave nutzt den DEK um die verschlüsselte Datei zu entschlüsseln bzw. zu verschlüsseln, nachdem die Datei modifiziert wurde.

Vertrauensmodell

- Innerhalb der Enklave oder des TLS Kanals ist der DEK zu keinem Zeitpunkt unverschlüsselt
- Der Cloud Service Provider kann die Daten nicht entschlüsseln, auch wenn er Zugriff auf die Festplatte hat, weil er keinen Zugriff zum DEK hat. Folglich sieht er nur randomisierte Chiffrate.
- Der KMaaS und somit enclaive können die Daten nicht entschlüsseln, weil enclaive keinen Zugang zur Cloud hat.

2.4 Verschlüsselung in Bewegung



Die Kommunikation zwischen dem Nutzer und der Enklave erfolgt über das TLS Protokoll. Eine verschlüsselte und authentische Verbindung wird mit der Enklave erstellt.

Vertrauensmodell:

- Der Enklaven Endpunkt wird durch die USERTRUST RSA Certification Authority authentifiziert, welche kontrolliert, ob der Nutzer der rechtmäßige Eigentümer der registrierten Domäne ist.

3. Kryptographie

3.1 Algorithmen

- Verschlüsselung in Bewegung: AES256-GCM
- Verschlüsslung im Ruhezustand: AES256-XTS
- Verschlüsselung in Bewegung: TLS 1.2

3.2 Kompatibilität mit BSI TR-021202

Die Algorithmen, Protokolle und Schlüssellängen entsprechen den aktuellen Empfehlungen des BSIs laut BSI TR-021202.[2]

	AES	TLS
BSI TR 02102-1	mindestens 128bit	mindestens 3000 bit (RSA-Verfahren)
enclaive	256 bit	4096 bit

3.3 Aktualisierung kryptographischer Verfahren

Über die Zeit könne sich die Anforderungen an die Sicherheit der verwendeten kryptographischen Verfahren ändern aufgrund neuer Erkenntnisse in der Kryptographieforschung oder dem Durchbruch von Quantencomputern. Generell stellt sich nicht die Frage, ob es zu einem Erkenntnissprung kommt, sondern lediglich, wann der Zeitpunkt wird. So überarbeitet das BSI seine Empfehlungen regelmäßig, wobei faktisch in einem 5 -10 Jahres Horizont Änderungen in der Wahl der Schlüssellänge zu erwarten sind.

Sollte das BSI Änderungen vorschlagen, so muss lediglich die Schlüssellänge oder der Algorithmus ausgetauscht werden. Die von enclaive benutzen Implementierungen orientieren sich an Open-Source Standards, so dass Aktualisierungen einfach umgesetzt werden können.

[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html