Zusammenfassung:

Teilgutachten zur Betriebsumgebung von fiskaly signCloud-TSE Instanzen Version 1.0

Seit 2020 ist der Einsatz von zertifizierten Technischen Sicherheitseinrichtungen (TSE) zur Absicherung von Aufzeichnungen in Registrierkassen in Deutschland gesetzlich vorgeschrieben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Sicherheitsanforderungen an Technischen Sicherheitseinrichtungen veröffentlicht und prüft die Einhaltung dieser zertifizierungsrelevanten Aspekte und Vorgaben durch die TSE-Hersteller. Die Einhaltung der Sicherheitsanforderungen werden durch anerkannte Prüfstellen des BSI bewertet. Bei positivem Prüfungsergebnis zertifiziert das BSI auf Grundlage des Prüfberichts die TSE eines Herstellers.

Nach erteilter Zertifizierung der TSE, muss für die Finanzbehörden zusätzlich nachgewiesen werden, dass der Betrieb einer TSE beim Steuerpflichtigen so erfolgt, dass der zertifizierte Zustand erhalten bleibt.

SRC hat als eine beim BSI anerkannte Prüfstelle das Produkt fiskaly sign Cloud TSE (Version 1.2.0 – 1.0.5) der fiskaly untersucht und das BSI hat hierfür die entsprechenden Zertifikate erteilt. Darüber hinaus hat SRC den Betrieb der fiskaly TSE näher beleuchtet. Die Anforderungen an den Betrieb wurden in intensiver gemeinsamer Zusammenarbeit mit fiskaly analysiert und geprüft. Die Überprüfung der Einhaltung zur Aufrechterhaltung des zertifizierten Zustands konnte für alle von fiskaly im Markt befindlichen o.g. TSE-Versionen durchgeführt werden.

Die Ergebnisse der Prüfung lassen sich in den nachfolgenden Punkten zusammenfassen:

1. Es wird nachgewiesen, dass die fiskaly SMAERS ausschließlich Anfragen von Systemen oder Komponenten entgegennehmen kann, welche aus derselben physischen operationellen Einsatzumgebung (vgl. “same physical operational environment”) kommen.

2. Die Kommunikation mit der fiskaly SMAERS ist integritätsgeschützt und verschlüsselt.

3. Es wird bestätigt, dass sowohl A.ProtComERS als auch OE.SecOEnv aus SMAERS PP konform umgesetzt sind.

4. Die Vorgaben aus dem von SRC betrachteten Umgebungsschutzkonzept von fiskaly werden eingehalten**.**

5. Die durch fiskaly betriebenen und von SRC betrachteten TSE-Instanzen erfüllen die Anforderungen an einen zertifizierten Betrieb.

Details sind dem nachfolgenden ausführlichen Untersuchungsbericht der SRC zu entnehmen.

Über fiskaly

fiskaly entwickelt innovative SaaS-Infrastruktur und bietet sichere Cloud-Lösungen rund um den Kassenbeleg für Kassenanbieter- und händler in Österreich und Deutschland. Im Bereich der Fiskalisierung betreibt das Unternehmen ein marktführendes Produkt im deutschen Markt, unsere zertifizierte TSE wird bundesweit in einer halben Million Registrierkassen eingesetzt. Mit dem digitalen Kassenbon wurde vor Kurzem ein neues Geschäftssegment eröffnet, die Erschließung neuer europäischer Märkte ist für Ende dieses Jahres geplant.

Gegründet wurde fiskaly 2019 in Wien. Mehr als 50 MitarbeiterInnen in den Büros in Wien, Frankfurt und Berlin tragen zum Erfolg des Unternehmens bei.

fiskaly.com

Auditierung der Betriebsumgebung aller durch fiskaly GmbH betriebenen fiskaly sign Cloud-TSE Instanzen (Version 1.2.0 – 1.0.5)

Teilgutachten

Version 1.0

Dr. Georg Mörsch

12.08.2022

Version	Datum	Genehmigt	Änderungen	Bemerkung
0.1	15.07.2022		-	Initiale Version
0.2	18.07.2022	smh	-	Interne QS
0.3	18.07.2022			Nach QS
0.4	12.08.2022			Aktualisierung nach Durchführung Tests
0.5	12.08.2022			Aktualisierung nach Kommentierung
0.6	12.08.2022	smh		QS Version
1.0	12.08.2022			Release Version

1 Einleitung

Die fiskaly GmbH entwickelt und betreibt Lösungen für die Fiskalisierung von Geschäftsfällen. Die für den deutschen Markt und die Kassensicherungsverordnung bestimmte TSE-Lösung, fiskaly sign Cloud-TSE, ist gemäß den Vorgaben der deutschen TR-03153 durch das BSI zertifiziert worden.

Es ist für den Betrieb notwendig nachzuweisen, dass durch fiskaly GmbH betriebene Instanzen der fiskaly sign Cloud-TSE alle Anforderungen an einen zertifizierten Betrieb erfüllen, insbesondere der im Konformitätsbescheid (siehe Seite 2, BSI-K-TR-0490-2021.pdf) genannten Nebenbestimmungen 1 und 2:

1. Der Betrieb des Prüfgegenstandes ist nur unter Verwendung der in Kapitel 7.1.1 – 7.1.7 des zugehörigen Konformitätsreports als System-Voraussetzungen genannten Umgebungen zulässig und durch die Zertifizierung abgedeckt. Für einen Betrieb unter anderen Systemvoraussetzungen besitzt das Zertifikat BSI-K-TR-0490-2021 keine Gültigkeit.
2. Für einen zertifizierten Betrieb des Prüfgegenstands müssen die Anweisungen des Dokuments [AdminT_Man] eingehalten werden

Für dieses Teilgutachten werden nur bestimmte Teile der Bestimmungen überprüft. Ein Gutachten, das die vollständige Prüfung sämtlicher oben genannter Nebenbestimmungenumfasst, wird zu einem späteren Zeitpunkt erstellt werden.

2 Prüfaspekte und Zusammenfassung der Ergebnisse

Die auditierte Betriebsumgebung der fiskaly SMAERS implementiert das in Kapitel 4.1 des fiskaly SMAERS Umgebungsschutzkonzepts (Version 1.3.5 vom 21.4.2021) [USK] beschriebene Szenario “Cloud Realization”. Das Gutachten betrachtet drei Prüfaspekte, die für die Gewährleistung des sicheren Betriebs der fiskaly sign Cloud-TSE erfüllt sein müssen:

1. Die Betriebsumgebung (“Operational Environment”) wird in der Google Cloud Platform, Region Frankfurt (europe-west3) umgesetzt (siehe Kapitel 4.1.2 “Google Cloud Platform” des Umgebungsschutzkonzepts).
2. Die Konfiguration der VPC (Virtual Private Cloud) Firewall in der auditierten Betriebsumgebung der fiskaly SMAERS gewährleistet, dass SMAERS ausschließlich Anfragen bzw. Befehle von Systemen oder Komponenten akzeptiert, welche sich in der gleichen physischen, operationellen Einsatzumgebung (physical operational environment) von SMAERS befinden (siehe A.ProtComERS aus [SMAERS-PP]). Des Weiteren stellt die VPC Firewall sicher, dass dafür ausschließlich der für verschlüsselte HTTPS Kommunikation notwendige Port verwendet werden kann.
3. In der Betriebsumgebung betriebene NGINX Reverse-Proxies forcieren eine mit TLS 1.2+ verschlüsselte und integritätsgeschützte Kommunikation mit SMAERS (siehe OE.SecOEnv aus [SMAERS-PP]).

Durch die im Folgenden beschriebenen Prüfungen konnte die Erfüllung aller drei Prüfaspekte bestätigt werden.

2.1 Cloud Realization

Prüfaspekt: Die Betriebsumgebung ("Operational Environment") wird in der Google Cloud Platform, Region Frankfurt (europe-west3) umgesetzt (siehe Kapitel 4.1.2 "Google Cloud Platform" des Umgebungsschutzkonzepts).

Als Ausgangsbasis für diese Prüfung gibt die fiskaly in ihrer API-Spezifikation an, dass sie abseits der auditierten Betriebsumgebung (GCP Frankfurt) keinerlei Produktiv-TSEs in anderen Umgebungen betreibt [API-Spec].

Über die gcloud CLI (siehe https://cloud.google.com/sdk/gcloud) hat sich der Gutachter mittels des Befehls

```
gcloud --project fiskaly-sign-de-prod compute instances list --fil-
ter="name~'live'" --format="table(name,networkInterfaces[0].accessCon-
figs[0].natIP,zone.basename(),status)" | tee smaers-vms.txt
```

alle im GCP-Projekt gehosteten SMAERS-VMs auflisten und für jede einzelne sowohl die Public-IP (NAT_IP) als auch die Cloud-Region (ZONE) anzeigen lassen und in einem Dokument gespeichert [List-VM]. Die Liste zeigt, dass jede einzelne VM Instanz in der Zone europe-west3-a (Region Frankfurt) liegt. Die ebenfalls ausgegebenen einzelnen IP-Adressen bestätigen dies.

Zur Konfiguration der Einsatzumgebung verwendet fiskaly zwei Tools, um Ressourcen in der GCP zu erzeugen und zu konfigurieren: terraform (siehe https://www.terraform.io) und ansible (siehe https://www.ansible.com). Dazu stellt fiskaly einen Auszug aus dem internen fiskaly SMAERS Infrastructure als Code Repository zur Verfügung [Config]. Die Verzeichnisstruktur des Code Repository ist in Abbildung 1 gezeigt.

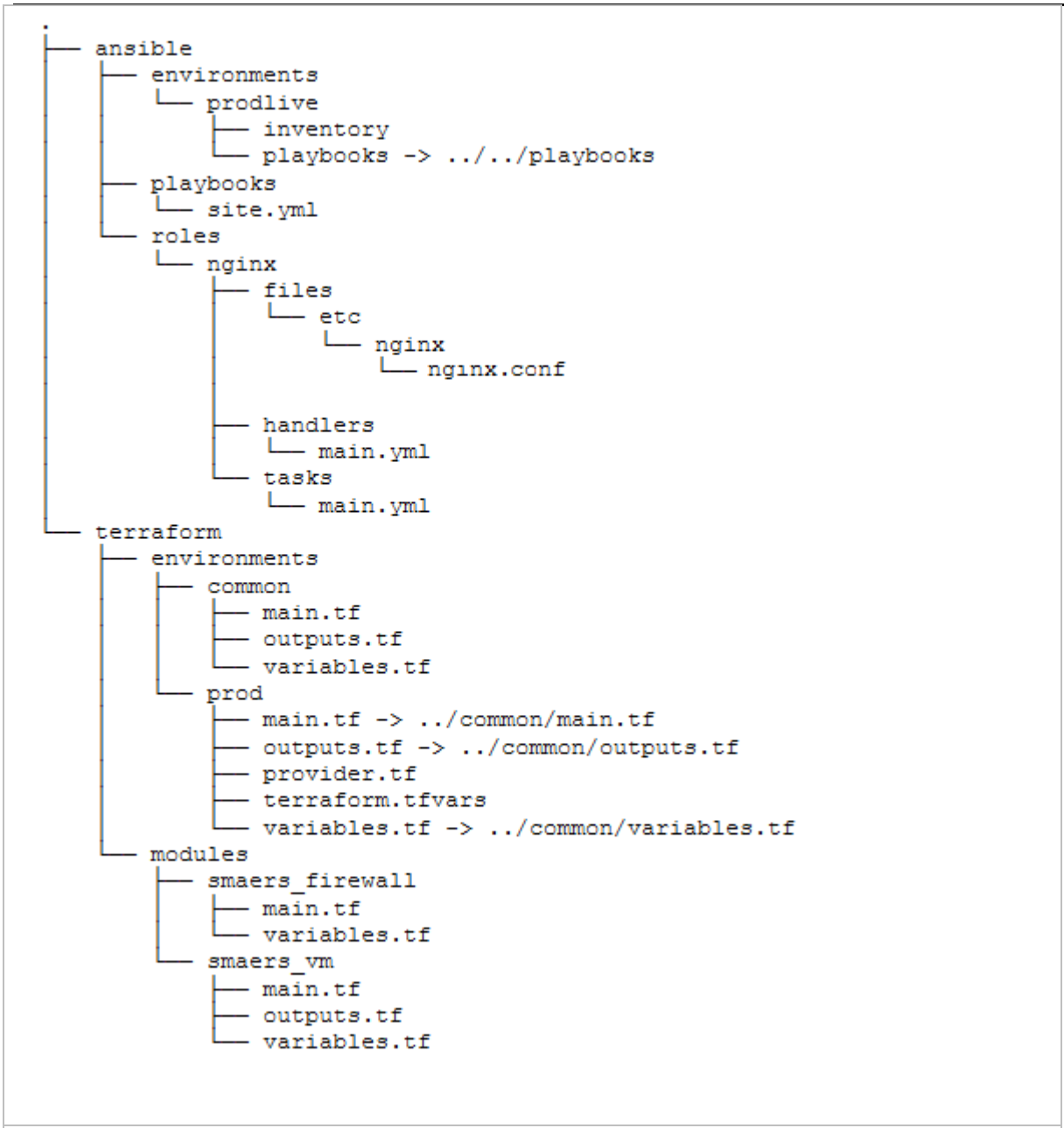

Abbildung 1: Verzeichnisstruktur der von fiskaly zur Verfügung gestellten Konfigurationsdateien

Die Gutachter haben die Konfigurationsdateien geprüft und finden die oben erläuterten Sachverhalte durch den Inhalt folgender Dateien bestätigt:

- `./terraform/environments/prod/main.tf`
- `./terraform/environments/prod/terraform.tfvars`
- `./terraform/modules/smaers_vm/main.tf`
- `./ansible/environments/prodlive/inventory`

Prüfergebnis: Es kann bestätigt werden, dass die Betriebsumgebung ("Operational Environment") in der Google Cloud Platform, Region Frankfurt (europe-west3) umgesetzt wird (siehe Kapitel 4.1.2 "Google Cloud Platform" des Umgebungsschutzkonzepts).

2.2 Firewall

Prüfaspekt: Die Konfiguration der VPC (Virtual Private Cloud) Firewall in der auditierten Betriebsumgebung der fiskaly SMAERS gewährleistet, dass SMAERS ausschließlich Anfragen bzw. Befehle von Systemen oder Komponenten akzeptiert, welche sich in der gleichen physischen, operationellen Einsatzumgebung (physical operational environment) von SMAERS befinden (siehe A.ProtComERS aus [SMAERS-PP]). Des Weiteren stellt die VPC Firewall sicher, dass dafür ausschließlich der für verschlüsselte HTTPS Kommunikation notwendige Port verwendet werden kann.

Der Gutachter hat sich über die gcloud CLI alle im GCP-Projekt fiskaly-sign-de-prod definierten VPC-Firewall-Regeln mit dem Befehl

```
gcloud --project fiskaly-sign-de-prod compute firewall-rules list --format=json
| tee smaers-firewall.json
```

auflisten lassen und in der Datei smaers-firewall.json abgespeichert [Firewall].

Die Regel mit dem Namen smaers-firewall-allow-https-same-region gewährleistet, dass SMAERS ausschließlich Anfragen bzw. Befehle von Systemen oder Komponenten akzeptiert (auf TCP Port 443 (HTTPS)), welche in der GCP Cloud-Region europe-west3 gehostet werden.

Sämtlicher eingehender Traffic, welcher nicht explizit durch Firewall-Regeln erlaubt wird, wird laut Dokumentation (siehe https://cloud.google.com/vpc/docs/firewalls#default_firewall_rules) geblockt.

Durch folgendes Skript wird bestätigt, dass die definierten sourceRanges der Regel smaers-firewall-allow-https-same-region mit den IP-Address-Ranges der GCP Cloud-Region europe-west3 übereinstimmen:

```
curl -s https://www.gstatic.com/ipranges/cloud.json | jq –r '.prefixes[] | se-
lect(.scope == "europe-west3" and .ipv4Prefix) | .ipv4Prefix'
```

Die Ausgabe des Skriptes ist in Abbildung 2 dargestellt.

```
➜  ~ curl -s https://www.gstatic.com/ipranges/cloud.json | jq -r
'.prefixes[] | select(.scope == "europe-west3" and .ipv4Prefix) |
.ipv4Prefix'

34.89.128.0/17
34.104.112.0/23
34.107.0.0/17
34.124.48.0/23
34.141.0.0/17
34.157.48.0/20
34.157.176.0/20
34.159.0.0/16
35.198.64.0/18
35.198.128.0/18
35.207.64.0/18
35.207.128.0/18
35.220.18.0/23
35.234.64.0/18
35.235.32.0/20
35.242.18.0/23
35.242.192.0/18
35.246.128.0/17
```

Abbildung 2: Ausgabe des Skriptes zur Ermittlung der IP-Ranges der GCP-Cloud Region europe-west3

Darüber hinaus haben die Gutachter die Konfigurationsdateien geprüft und finden die oben erläuterten Sachverhalte durch den Inhalt folgender Dateien bestätigt:

- `./terraform/environments/prod/main.tf`
- `./terraform/environments/prod/terraform.tfvars`
- `./terraform/modules/smaers_firewall/main.tf`
- `./terraform/modules/smaers_firewall/variables.tf`

Prüfergebnis: Es kann bestätigt werden, dass die Konfiguration der VPC (Virtual Private Cloud) Firewall in der auditierten Betriebsumgebung der fiskaly SMAERS gewährleistet, dass SMAERS ausschließlich Anfragen bzw. Befehle von Systemen oder Komponenten akzeptiert, welche sich in der gleichen physischen, operationellen Einsatzumgebung (physical operational environment) von SMAERS befinden (siehe A.ProtComERS aus [SMAERS-PP]). Desweiteren kann bestätigt werden, dass die VPC Firewall sicherstellt, dass dafür ausschließlich der für verschlüsselte HTTPS Kommunikation notwendige Port verwendet werden kann.

2.3 TLS 1.2+

Prüfaspekt: In der Betriebsumgebung betriebene NGINX Reverse-Proxies forcieren eine mit TLS 1.2+ verschlüsselte und integritätsgeschützte Kommunikation mit SMAERS (siehe OE.SecOEnv aus [SMAERS-PP]).

Das Tool ansible wird verwendet, um auf allen SMAERS-VMs (siehe `./ansible/environments/prodlive/inventory`) Konfigurations-Änderungen zu automatisieren. Dabei kommt das in `./ansible/environments/prodlive/playbooks/site.yml` definierte Playbook

zum Einsatz. Dieses installiert u.A. die Rolle nginx, welche in `./ansible/roles/nginx/tasks/main.yml` definiert ist, und u.A. die in `./ansible/roles/nginx/files/etc/nginx/nginx.conf` hinterlegte NGINX-Konfiguration auf der SMAERS-VM installiert [Config].

Die NGINX-Konfiguration forciert TLS1.2 mittels des Parameters `ssl_protocols TLSv1.2`; Zusätzlich erzwingt NGINX über den Parameter `ssl_ciphers` die Cipher-Suites `ECDHE-ECDSA-AES128-GCM-SHA256` oder `ECDHE-RSA-AES128-GCM-SHA256`, die vom BSI beim Einsatz von TLSv1.2 empfohlen werden. Auch bei der verwendeten ECDH-Kurve (secp256r1), des Signaturalgorithmus (RSA) und der RSA Schlüssellänge (2048 bit) folgt die Konfiguration den Empfehlungen des BSI.

Zur Überprüfung der tatsächlich auf den VM benutzten TLS-Konfiguration loggte der Gutachter sich mittels eines Skriptes [Skript] in alle in [List-VM] ermittelten SMAERS VM ein und verglich den Hash der tatsächlichen nginx-Konfiguration mit der in `./ansible/roles/nginx/files/etc/nginx/nginx.conf` hinterlegten NGINX-Konfiguration. So konnte der Nachweis erbracht werden, dass exakt diese NGINX-Konfiguration auf allen SMAERS-VMs installiert ist (siehe [List Hash_nginx]).

Schließlich prüfte der Gutachter mittels des Skriptes [Skript] den Zustand der nginx-Installation auf jeder SMAERS VM und konnte so nachweisen, dass nginx auf allen VM aktiv ist [List Active_nginx].

Darüber hinaus haben die Gutachter die Konfigurationsdateien geprüft und finden die oben erläuterten Sachverhalte durch den Inhalt folgender Dateien bestätigt:

- `./ansible/roles/nginx/tasks/main.yml`
- `./ansible/roles/nginx/handlers/main.yml`
- `./ansible/roles/nginx/files/etc/nginx/nginx.conf`
- `./ansible/environments/prodlive/playbooks/site.yml`
- `./ansible/environments/prodlive/inventory`

Prüfergebnis: Es kann bestätigt werden, dass der in der Betriebsumgebung betriebene NGINX Reverse-Proxy eine mit TLS 1.2+ verschlüsselte und integritätsgeschützte Kommunikation mit SMAERS forciert (siehe OE.SecOEnv aus [SMAERS-PP]).

3 Zusammenfassung

Die unter 2 aufgelisteten drei Prüfaspekte im Zusammenhang zur Prüfung der im Konformitätsbescheid (siehe Seite 2, BSI-K-TR-0490-2021.pdf) genannten Nebenbestimmungen wurden untersucht. Ihre Einhaltung wird mit diesem Gutachten bestätigt.

Es konnte nachgewiesen werden, dass die „fiskaly sign Cloud-TSE“ Instanzen (Version 1.2.0-1.0.5) und speziell die SMAERS Komponente, nur Anfragen von Nicht-TSE Komponenten entgegennehmen kann, welche sich in der gleichen physischen, operationellen Einsatzumgebung (“same physical operational environment”) befinden.

Es wird bestätigt, dass sowohl A.ProtComERS als auch OE.SecOEnv aus SMAERS PP konform umgesetzt sind.

4 Literaturverweise

Dokumetation

[USK] Umgebungsschutzkonzept fiskaly Security Module Application for Electronic Record-keeping Systems TOE Version 1.0.5, Version: 1.3.5, Date: 2021-04-21, fiskaly GmbH

[SMAERS-PP] Common Criteria Protection Profile Security Module Application for Electronic Recordkeeping Systems (SMAERS), BSI-CC-PP-0105-V2-2020, Version 1.0

Evidenzen

[API-Spec] Spezifikation fiskaly SIGN DE API (2.0.20), https://developer.fiskaly.com/api/kassensichv/v2

[List-VM] Auflistung aller SMAERS-VM mit Standort, 11.08.2022
Dateiname: smaers-vms.txt
SHA256:
5feb5ce26032aed536e58e5a4cd5f2127c4581c5337daf8ce4f65083608cbd5b

[Skript] Testskript zur Ermittlung der Evidenzen, 11.08.2022
Dateiname: smaers-audit-v2.sh
SHA256:
2c4e49ddbd3e508ed1ce4e674c40e6cab4ab72edfb5ee2d866e44102808c622e

[Config] Konfigurationsdateien zur SMAERS fiskaly Infrastructure, 04.07.2022
Dateiname: fiskaly-smaers-infrastructure-as-code.tar.gz"
SHA256:
154a2501900ef36f22ff06c4d94a307db4bfdec9e3c0e523b028f378a5c16ddf

[Firewall] Listing aller Firewall-Regeln im GCP-Projekt, 08.08.2022
Dateiname: smaers-firewall.json
SHA256:
63de26b5e787c0c0505209cf2461a89343655d6af7dc01bedc2c8c2ea403c6b4

[List Hash_nginx] Liste Prüfung nginx-Konfigurationen auf SMAERS-VMs, 08.08.2022
Dateiname: smaers-nginx-config-hash.txt
SHA256:
7492e97b0fee344202d53e32e88575402c0f19b3fe5a8750ce3e19f33792015a

[List Active_nginx] Liste Prüfung Aktivität nginx auf SMAERS-VMs, 08.08.2022
Dateiname: smaers-nginx-status.txt
SHA256:

e6940a0c9460d0633678c3738ca5e422ee3fd944a5e720c516a16b52e2488a2f