DATENBLATT

# Certificate Inventory Tool (CIT)

## Finden Sie alle SSL-Zertifikate in Ihren internen und öffentlichen Netzwerken, unabhängig von der ausstellenden CA

Wissen Sie genau, wo Sie SSL-Zertifikate installiert haben? Wann die einzelnen Zertifikate ablaufen und bei welcher CA Sie sie bestellt haben? Was ist mit dem Hash-Algorithmus oder den verwendeten Schlüssellängen? Die Antworten werden wahrscheinlich überwiegend „nein“ lauten, oder wenn „ja“, dass es schwierig ist, diese Informationen zusammenzusammeln.

Organisationen und Unternehmen bestellen Zertifikate oft bei unterschiedlichen Anbietern und installieren die Zertifikate sowohl in ihren internen als auch externen Netzwerken. Diese flexible Herangehensweise hat einige Vorteile, erschwert aber die Sache für denjenigen, der für die Verwaltung der Zertifikate und deren Erneuerung zuständig ist.

Unser neues Certificate Inventory Tool findet alle SSL-Zertifikate in Ihren Netzwerken, sowohl in internen als auch öffentlich zugänglichen, unabhängig von der ausstellenden Zertifizierungsstelle. Die daraus resultierende Inventarliste steht in einem benutzerfreundlichen Portal zur Verfügung. Dort können Sie Berichte über die Nutzung, anstehende Erneuerungen, bestehende Konfigurationen und ausstellende CAs generieren.

## VORTEILE

- Finden und überwachen Sie alle internen und öffentlichen SSL-Zertifikate an einem Ort, unabhängig von der ausstellenden CA
- Vermeiden Sie unerwartetes Ablaufen von Zertifikaten durch E-Mail-Erinnerungen an fällige Erneuerungen
- Problemloses Nachvollziehen der Quelle/ ausstellenden CA für alle Ihre Zertifikate
- Finden Sie sämtliche Zertifikate, die eventuell von anderen Personen oder Abteilungen ad hoc gekauft wurden
- Sparen Sie wertvolle Zeit und Ressourcen gegenüber manueller Überwachung
- Halten Sie Schritt mit Baseline Requirements und Best Practice Empfehlungen. Nutzen Sie die Möglichkeit, Berichte zu Schlüssellänge, Hash-Algorithmus und viele weitere Konfigurations-möglichkeiten zu erstellen

## Vermeiden Sie abgelaufene Zertifikate

Abgelaufene öffentliche SSL-Zertifikate können alarmierende Warnmeldungen in Browsern auslösen und damit den Ruf Ihres Unternehmens schädigen sowie die Besucherzahlen auf Ihrer Website verringern. Intern kann ein abgelaufenes Zertifikat - je nach Kommunikation - Prozesse unterbrechen. Glücklicherweise macht es das Certificate Inventory Tool besonders einfach, diese Probleme zu vermeiden. Nachdem Ihre Zertifikate inventarisiert wurden, erhalten Sie Warnmeldungen per E-Mail, wenn sie kurz vor dem Ablaufdatum stehen. Sobald Sie das Zertifikat erneuern und die Prüfung nochmals ausführen, wird der Status aktualisiert, und Sie erhalten keine weiteren Meldungen.

## Halten Sie mit SSL Best Practices Schritt

Best Practices für Schlüssellängen, Gültigkeitsdauer, Hash-Algorithmus und andere Zertifikatsoptionen werden ständig überarbeitet. Das Certificate Inventory Tool erleichtert es, sämtliche Zertifikate zu scannen, um sicherzustellen, dass sie auf dem neuesten Stand sind und aktuellen Empfehlungen entsprechen.

Sie können Ihr Konto anhand Ihrer Unternehmensrichtlinien zu Mindesteinstellungen für Schlüssellänge, Signier-Algorithmus, ausstellender CA, minimaler/maximaler Gültigkeitsdauer usw. konfigurieren. Alle eingesetzten Zertifikate werden gemäß dieser benutzerdefinierten Richtlinien überprüft und angezeigt. Sie können unterschiedliche Richtlinien für interne und externe Zertifikate oder auch für verschiedene Netzwerksegmente verwenden.

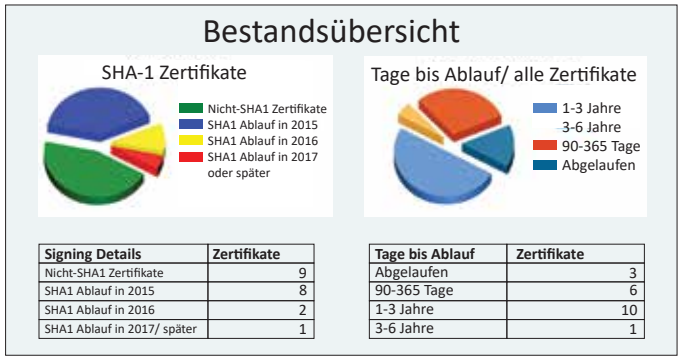
### So funktioniert's - Durchführung von Scans

Das Verfahren zum Scannen Ihrer Netzwerke unterscheidet sich leicht für öffentlich zugängliche und interne Netzwerke. Um interne Netzwerke zu scannen, müssen Sie zuerst einen Agenten herunterladen und lokal installieren. Danach wird alles über das Inventory-Portal abgewickelt.

- Erstellen Sie einen Auftrag im Portal (d.h. eine Reihe von IP-Adressen, eine Domain oder einen Host-Namen) und wählen Sie dann aus, ob der Auftrag vom Inventory-Tool-Server ausgeführt oder an einen lokalen Agenten gesendet werden soll.
- Führen Sie den Auftrag aus oder terminieren Sie ihn für einen späteren Zeitpunkt.
- Das Inventory Tool scannt die möglichen Locations nach SSL-Zertifikaten.
- Die Ergebnisse werden automatisch auf Ihr Portal hochgeladen, so dass Sie auf dieser Grundlage Reports und Analysen erstellen können.

### Ergebnisse anzeigen

Die Ergebnisse der Scans werden automatisch auf Ihr Portal hochgeladen, wo Sie ganz einfach Berichte erstellen und den Status von Zertifikaten überprüfen können, wie z.B. Ausstellungsdatum, ausstellende CA, Ablaufdatum und Gültigkeitsdauer.




| Signing Details | Zertifikate |
|---|---|
| Nicht-SHA1 Zertifikate | 9 |
| SHA1 Ablauf in 2015 | 8 |
| SHA1 Ablauf in 2016 | 2 |
| SHA1 Ablauf in 2017/ später | 1 |

| Tage bis Ablauf | Zertifikate |
|---|---|
| Abgelaufen | 3 |
| 90-365 Tage | 6 |
| 1-3 Jahre | 10 |
| 3-6 Jahre | 1 |

### Über GlobalSign

GlobalSign ist der führende Anbieter von vertrauenswürdigen Identitäts- und Sicherheitslösungen, die es Unternehmen, Großunternehmen, Cloud-Service-Anbietern und IoT-Innovatoren auf der ganzen Welt ermöglichen, Online-Kommunikation zu sichern, Millionen von verifizierten digitalen Identitäten zu verwalten und Authentifizierung und Verschlüsselung zu automatisieren. Mit Lösungen für hochskalierte Public Key Infrastructure (PKI) und Identitäten unterstützt das Unternehmen Milliarden von Geräten, Personen und Dingen innerhalb des Internet of Everything.

DE: +49 800 723 7980 verkauf@globalsign.com
EU: +32 16 89 19 00 www.globalsign.de

GlobalSign
GMO INTERNET GROUP

© Copyright 2017 GlobalSign