

Dokumentation



ALLRIS

Import eines Root-Zertifikats in Android

1.	EINFÜHRUNG	3
2.	IMPORT EINES ROOT-ZERTIFIKATS IN ANDROID	3

1. Einführung

Zum Schutz Ihrer Daten erfolgt der Zugriff auf ALLRIS net – auch aus der App heraus – über eine sichere HTTPS-Verbindung.

Android benötigt ein Root-Zertifikat, um die Vertrauenswürdigkeit von Websites und anderen Servern zu überprüfen, die HTTPS verwenden. Wenn Sie eine Website mit HTTPS besuchen, werden alle Daten zwischen Ihrem Gerät und dem Server verschlüsselt. Dies verhindert, dass Unbefugte die Daten mitlesen können.

Verschlüsselung erfordert Vertrauen: Um die Daten zu entschlüsseln, benötigt Ihr Gerät ein Zertifikat vom Server. Dieses TLS/SSL-Zertifikat bescheinigt, dass der Server derjenige ist, der er vorgibt zu sein.

Root-Zertifikate sind die Grundlage der Vertrauenskette: Root-Zertifikate werden von vertrauenswürdigen Zertifizierungsstellen (CAs) ausgestellt. Diese CAs überprüfen die Identität der Server, bevor sie ihnen ein Zertifikat ausstellen. Aus Sicherheitsgründen sind diese Zertifikate aber nur für eine begrenzte Zeit gültig. Danach müssen sie durch ein neues ersetzt werden.

Android vertraut nur Root-Zertifikaten, die in seinem vertrauenswürdigen Speicher integriert sind. Von Zeit zu Zeit stellen die CAs jedoch neue Root-Zertifikate bereit. Google kann diese über Android-Updates verteilen.

Wenn das neue Zertifikat des ALLRIS-Servers nun aber von einem Root-Zertifikat stammt, dass in Ihrer Android-Version noch nicht enthalten ist, müssen sie es manuell importieren.

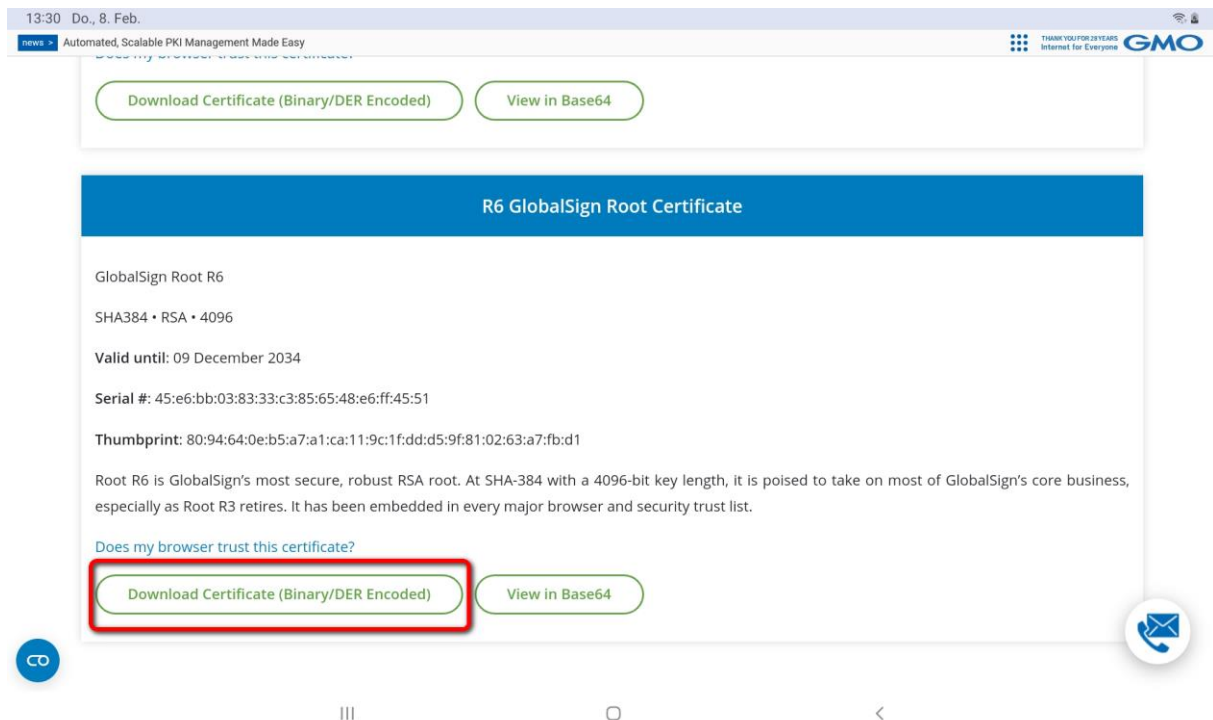
2. Import eines Root-Zertifikats in Android

Die folgende Anleitung bezieht sich auf ein spezielles Root-Zertifikat der GlobalSign CA. Die Vorgehensweise bei anderen Root-Zertifikaten von anderen CAs verläuft aber vergleichbar. Des Weiteren kann die Vorgehensweise bei Ihrem Gerät vom beschriebenen Ablauf abweichen, da es für die Darstellung und Gruppierung von Android-Einstellungen keine festen Vorgaben Seitens Google gibt und verschiedene Geräte-Hersteller dies unterschiedlich umsetzen.

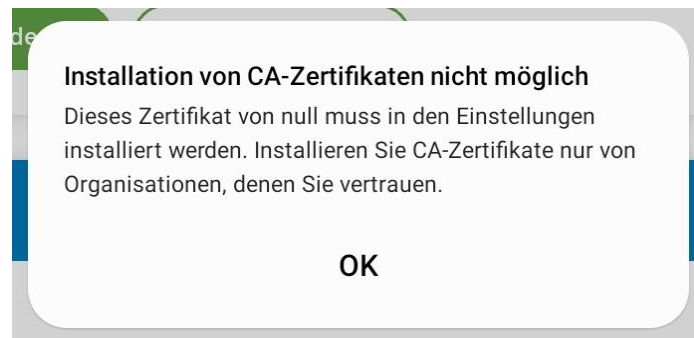
Laden Sie das Zertifikat von GlobalSign herunter. Rufen Sie dazu folgende Webseite im Browseri auf Ihrem Android-Gerät auf:

<https://support.globalsign.com/ca-certificates/root-certificates/globalsign-root-certificates>

Sie benötigen das „R6 GlobalSign Root Certificate“. Wählen Sie „Download Certificate (Binary/DER Encoded)“:

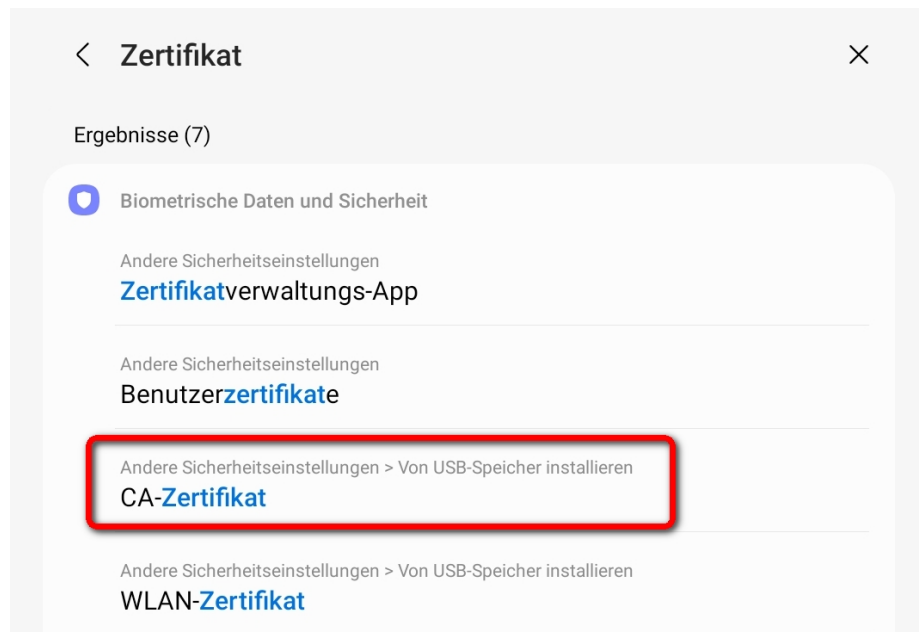


Ignorieren Sie die Meldung, dass eine Installation von CA-Zertifikaten nicht möglich ist, indem sie „OK“ klicken:

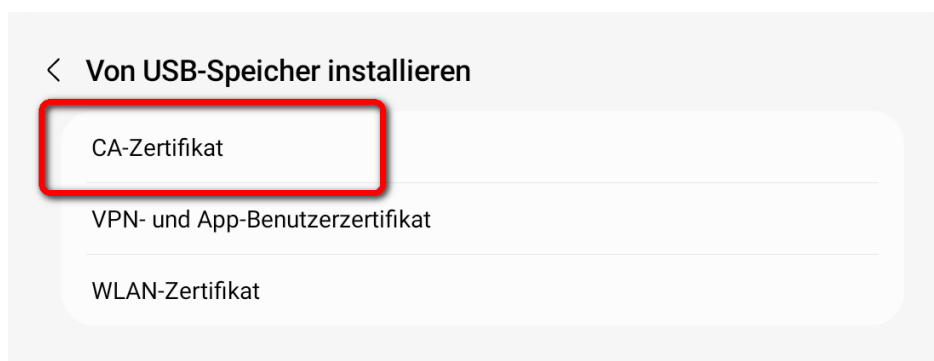


Es werden kurz die Meldungen angezeigt, dass die Datei heruntergeladen wurde und dass das Zertifikat **nicht** installiert wurde.

Öffnen sie die Android-Einstellungen und suchen Sie innerhalb der Einstellungen nach **Zertifikat**. Wählen Sie die Option, die eine Installation eines CA-Zertifikats (von USB) ermöglicht:



und im folgenden Dialog:



Bestätigen Sie den Warnhinweis zur Installation mit **Trotzdem installieren**:



Sie werden nun aufgefordert, den Vorgang mit der Geräte-PIN zu bestätigen, und Ihnen wird dann eine Elementauswahl angeboten, die nur die auf Ihrem Gerät gespeicherten Zertifikate anzeigt:

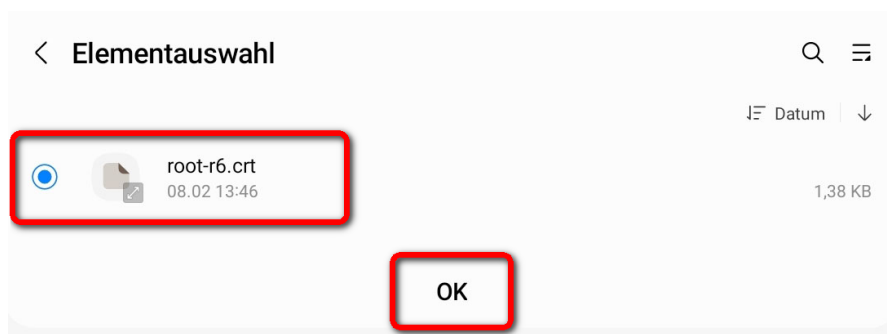
Schritt 1:



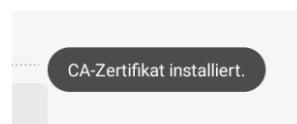
Schritt 2:



Markieren Sie die Zertifikatsdatei und bestätigen Sie Ihre Auswahl mit **OK**:



Es erscheint kurz eine Bestätigungsmeldung über die erfolgreiche Installation des Zertifikats:



Damit ist die Installation abgeschlossen und die ALLRIS-App und ALLRIS net können wie gewohnt genutzt werden.

DOKUMENTATION



Import eines Root-Zertifikats in Android

ED01 Februar 2024

CC e-gov GmbH

Gotenstraße 10

20097 Hamburg

Tel.: +49 (0)40 227199-0

E-Mail: info@cc-egov.de

Web: www.cc-egov.de