ZERTIFIKATE DER PILOT PUBLIC KEY INFRASTUKTUR (PKI)

Auf der Webseite https://19.test.mcg.escrypt.com/ sind die Zertifikate der Pilot Public Key Infrastuktur (PKI) zu finden, die für das Verifizieren der von den Absperrtafeln versendeten Nachrichten notwendig sind. Dazu gehören Zertifikat der ausstellenden Sub-CA Authorization Authority (AA) und das Zertifikat der Root CA (RCA) sowie die Revokationsliste (CRL).

Die Nachrichten, die von der IRS am Sperranhänger verschickt werden, werden mittels eines Authorization Tickets (AT) signiert. Einmal pro Sekunde wird hier das AT-Zertifikat mit an die verschickte Nachricht angehängt. Um die Nachricht als vertrauenswürdig einstufen zu können, muss der Empfänger die Signatur der IRS-Nachricht mit Hilfe des empfangenen AT-Zertifikats prüfen (verifizieren). Dieses, von der IRS versendete AT-Zertifikat, muss ebenfalls hinsichtlich der Gültigkeit geprüft werden. Dazu wird die Zertifikatskette bis zur Root CA validiert. Dies erfolgt in drei Schritten:

- Zur Überprüfung der Signatur des AT-Zertifikats wird das Zertifikat der ausstellenden Sub-CA Authorization Authority (AA) benötigt.
- Zur Verifikation des AA-Zertifikats das RCA-Zertifikat herangezogen.
- Zudem wird mit der von der RCA ausgestellten CRL überprüft, ob das AA-Zertifikat revoziert wurde.