Überprüfung der PDF-Integrität | Verification of PDF Integrity

> ***English version down below***

Inhaltsverzeichnis

Das Cyber Risk Rating Portal stellt am Ende des Bewertungsprozesses für jeden Lieferanten mehrere Dokumente aus. Dazu gehören unter anderem das Cyber Risk Rating-Zertifikat, das die Gesamtbewertungspunkte für den Lieferanten sowie den WebRisk-Score enthält, und der Cyber Risk Rating-Report, der die Antworten des Lieferanten zusammen mit den Validierungsergebnissen auflistet.

Um die Integrität der Dokumente zu gewährleisten und potenzielle Kompromisse durch Dritte während des Downloadvorgangs zu verhindern, wird für jedes Dokument eine Signatur hinzugefügt, die den signierten Digest pro Dokument enthält. Durch die Signatur des Digests wird die Integrität des Dokuments garantiert, da eine Änderung des Dokumenteninhalts zwangsläufig einen anderen Digest erzeugen würde, der nicht mit der bereitgestellten Signatur übereinstimmt. Darüber hinaus kann die Signatur nicht verändert werden, da sie mit unserem eigenen geheimen RSA Private Key signiert wurde. Die für den Prozess verwendeten Algorithmen sind SHA256 zur Erstellung des Digests des Dokuments und RSA PKCS#1 v1.5 für die Signatur.

Integrität über die Befehlszeile verifizieren

Es wird empfohlen, die Integrität jedes Dokuments nach dem Herunterladen als ZIP-Archiv zu überprüfen. Für jedes Dokument repräsentiert die entsprechende Signaturdatei `.sig` den signierten Digest in Byte-Form. Darüber hinaus wird der Public Key benötigt, der auf unserer Seite verwendet wurde. Er kann hier heruntergeladen werden: Cyber Risk Rating Signature Public Key

Die Überprüfung kann mit OpenSSL Version `v1.1.1f` oder höher durchgeführt werden.

```
$ openssl dgst -sha256 -verify crr-signature-key.pub -signature Cyber-Risk-Rating-Report-Valid.pdf.sha256.sig
Cyber-Risk-Rating-Report-Valid.pdf
Verified OK
```

Wenn die Dokumente kompromittiert sind, schlägt die Überprüfung fehl. In diesem Fall kontaktieren Sie sofort support@nimbusec.com für weitere Unterstützung.

```
$ openssl dgst -sha256 -verify crr-signature-key.pub -signature Cyber-Risk-Rating-Report-Valid.pdf.sha256.sig
Cyber-Risk-Rating-Report-Compromised.pdf
Verification Failure
```

CyberRisk Rating Signature Public Key

Sie können den Signaturschlüssel als Datei hier herunterladen: Cyber Risk Rating Signature Public Key

Oder Sie verwenden die untenstehende Klartextversion:

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAwGd+TC2FkOrz/CqU9lUk
xNi8uhQ73D9YVlQ93Jkl4plVRYcquGOK0hLqWSTDkHAfd9fKCqgmJWF1X6eF/fz7
B6a7HeCHAPlut3aclEneJef03JWsLZWoMD724v7vDXHolUcDNHuICWQpWMpZ/xaM
E1FzNlzqSH41tF3YPOaxGiQA39+POxaWItYk7hBKBWhU6F4PBzZfM2gE/3AOqcRi
4DRFYPh3ZwIVTGqDtfiYMWUYLDI5u0KzdFne6qvBHflBwB1Nd9l3ckEFiv91s2Sg
3AaiXEqgSvLIL02tbmVnbfImVXksE9VeNWpr0LKWnTApheX++DQ0itB7zbg9JIfv
rEG9JNuP/dXlFjYRsBlsaz950vulzwwWjeHs6LikqHUz+4xy8+GU6vs0QFbvkHlD
DRcJGeCWsCiijh9dtM+yDcZfr8WjEr9AQfskMSfoWuVqAMBqJ05C51fDnZdbNLGy
0ubtIoI4cSIf7Rrow1iq8l4WsPoIZDRq2S0jJc3gLnAS6erlQoox/9A2ZWeCQPw9
iHixIVpQR/h6TKT6M4VQn+Ilw+Nj5o6yTzYEhq5nY64yH9zn0brhycANLhO/PnA1
rYaCorVRMFbr9UeysulqKBEk4TkEAWdUXdqSzM/Wdm2P0pQM7Y0vhMbqMSeYoGkX
o2lNrkxDioheGnwTsaFejtMCAwEAAQ==
-----END PUBLIC KEY-----
```

> **English version:**

Table of contents

The Cyber Risk Rating Portal issues several documents for each supplier at the end of the evaluation process. These include the Cyber Risk Rating Certificate, which contains the overall rating points for the supplier as well as the WebRisk score, and the Cyber Risk Rating Report, which lists the supplier's responses along with the validation results.

To ensure the integrity of the documents and prevent potential compromises by third parties during the download process, a signature containing the signed digest for each document is added. By signing the digest, the integrity of the document is guaranteed, as any alteration of the document's content would inevitably generate a different digest that would not match the provided signature. Furthermore, the signature cannot be altered because it is signed with our own secret RSA private key. The algorithms used for this process are SHA256 for creating the document digest and RSA PKCS#1 v1.5 for the signature.

Integrity check via command line

It is recommended to verify the integrity of each document after downloading as a ZIP archive. For each document, the corresponding signature file `.sig` represents the signed digest in byte form. Additionally, the public key used on our side is required. It can be downloaded here: Cyber Risk Rating Signature Public Key

The verification can be performed using OpenSSL version `v1.1.1f` or higher.

```
$ openssl dgst -sha256 -verify crr-signature-key.pub -signature Cyber-Risk-Rating-Report-Valid.pdf.sha256.sig
Cyber-Risk-Rating-Report-Valid.pdf
Verified OK
```

If the documents are compromised, the verification will fail. In this case, please contact support@nimbusec.com immediately for further assistance.

```
$ openssl dgst -sha256 -verify crr-signature-key.pub -signature Cyber-Risk-Rating-Report-Valid.pdf.sha256.sig
Cyber-Risk-Rating-Report-Compromised.pdf
Verification Failure
```

CyberRisk Rating Signature Public Key

You can download the signature key file here: Cyber Risk Rating Signature Public Key

Or, you can use the plaintext version provided below:

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAwGd+TC2FkOrz/CqU9lUk
xNi8uhQ73D9YVlQ93Jkl4plVRYcquGOK0hLqWSTDkHAfd9fKCqgmJWF1X6eF/fz7
B6a7HeCHAPlut3aclEneJef03JWsLZWoMD724v7vDXHolUcDNHuICWQpWMpZ/xaM
E1FzNlzqSH41tF3YPOaxGiQA39+POxaWItYk7hBKBWhU6F4PBzZfM2gE/3AOqcRi
4DRFYPh3ZwIVTGqDtfiYMWUYLDI5u0KzdFne6qvBHflBwB1Nd9l3ckEFiv91s2Sg
3AaiXEqgSvLIL02tbmVnbfImVXksE9VeNWpr0LKWnTApheX++DQ0itB7zbg9JIfv
rEG9JNuP/dXlFjYRsBlsaz950vulzwwWjeHs6LikqHUz+4xy8+GU6vs0QFbvkHlD
DRcJGeCWsCiijh9dtM+yDcZfr8WjEr9AQfskMSfoWuVqAMBqJ05C51fDnZdbNLGy
0ubtIoI4cSIf7Rrow1iq8l4WsPoIZDRq2S0jJc3gLnAS6erlQoox/9A2ZWeCQPw9
iHixIVpQR/h6TKT6M4VQn+Ilw+Nj5o6yTzYEhq5nY64yH9zn0brhycANLhO/PnA1
rYaCorVRMFbr9UeysulqKBEk4TkEAWdUXdqSzM/Wdm2P0pQM7Y0vhMbqMSeYoGkX
o2lNrkxDioheGnwTsaFejtMCAwEAAQ==
-----END PUBLIC KEY-----
```

Revision #19
Created 2 May 2024 12:24:12 by Edis Hadzic
Updated 24 May 2024 06:58:30 by Edis Hadzic