Verifying PDF Integrity

The Cyber Risk Rating Portal issues multiple documents at the end of the rating process for every supplier. The documents are among others the Cyber Risk Rating Certificate which contains the overall rating scores for the supplier along with the WebRisk score and the Cyber Risk Rating Assessment Report that lists the answers of the supplier along with the validation results.

To ensure the integrity of the documents and prevent potential compromises by others during the download process, a signature file for each document is added that contains the signed digest per document. By signing the digest, the document integrity is guaranteed as changing the document's content would consequently create a different digest, failing to match the provided signature. Additionally, the signature cannot be altered given that it was signed using our own secret RSA private key. The algorithms used for the process are *SHA256* to create digest of the document and *RSA PKCS#1 v1.5* for the signing.

Verifying the integrity on the command line

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

The verification can be done using OpenSSL `v1.1.1f` or above.

```
$ 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, contact `support@nimbusec.com` immediately for further help.

```
$ 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 as file here: Cyber Risk Rating Signature Public Key,

or use the plain text version printed 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 #2
Created 2 August 2021 08:07:49 by Patrick Wall
Updated 2 August 2021 08:13:51 by Patrick Wall