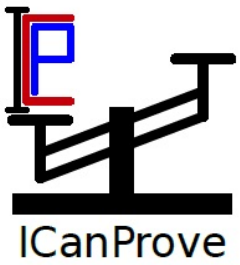
Proof of Website Status
by www.icanprove.de



Date:
Wed Nov 1 14:27:34 UTC 2023 (Wed Nov 1 14:27:34 UTC 2023)

Site visited:

`https://tryhackme-certificates.s3-eu-west-1.amazonaws.com/THM-7LWZYMSLZK.png`

Comments:

Screenshots:

Screenshot #1:

Userlog:

```
Logfile Timezone set to UTC
Browser Timezone set to UTC
Browser Language (locale) set to en_US
Session started at 2023-11-01 14:26:00 (UTC=UTC+0000)  512107  for IP:2a0b:f4c2:1::1

2023-11-01 14:26:09 (UTC=UTC+0000)  714780 : User created Screenshot #1
2023-11-01 14:27:31 (UTC=UTC+0000)  919313 : Session shutdown started.
```

Accesslog (reqxxx and repxxx refer to the logfiles):

```
2023-11-01 14:26:00 (UTC=UTC+0000) 608425 repJbFSCB reqTcXR3B CONNECT tryhackme-certificates.s3-eu-west-1.
    amazonaws.com:443 HTTP/1.1
2023-11-01 14:26:13 (UTC=UTC+0000) 158398 rephsPvMj req7Dn5vb CONNECT firefox.settings.services.mozilla.com:443
     HTTP/1.1
2023-11-01 14:26:13 (UTC=UTC+0000) 371018 rep8kDf9q reqBzG0yF CONNECT content-signature-2.cdn.mozilla.net:443
    HTTP/1.1
2023-11-01 14:26:14 (UTC=UTC+0000) 973383 repqSuQG2 reqFs9qDr CONNECT firefox.settings.services.mozilla.com:443
     HTTP/1.1
2023-11-01 14:26:14 (UTC=UTC+0000) 977060 repqJNfoG req7XYQEf CONNECT firefox.settings.services.mozilla.com:443
     HTTP/1.1
2023-11-01 14:26:14 (UTC=UTC+0000) 979553 repgyT75F reqgqS4DS CONNECT firefox.settings.services.mozilla.com:443
     HTTP/1.1
2023-11-01 14:26:14 (UTC=UTC+0000) 982106 repLZmVPH req8PENfs CONNECT firefox.settings.services.mozilla.com:443
     HTTP/1.1
2023-11-01 14:26:14 (UTC=UTC+0000) 984629 repCBimlg reqfVlHfO CONNECT firefox.settings.services.mozilla.com:443
     HTTP/1.1
2023-11-01 14:26:15 (UTC=UTC+0000) 244250 repXbps6U reqwilZLB CONNECT firefox-settings-attachments.cdn.mozilla.
    net:443 HTTP/1.1
2023-11-01 14:26:15 (UTC=UTC+0000) 247060 repb3o3Es reqSv006y CONNECT firefox-settings-attachments.cdn.mozilla.
    net:443 HTTP/1.1
2023-11-01 14:26:15 (UTC=UTC+0000) 249660 repuNKixa reqE9yQWt CONNECT firefox-settings-attachments.cdn.mozilla.
    net:443 HTTP/1.1
2023-11-01 14:26:15 (UTC=UTC+0000) 252159 repvtDCjK reqsxwWXG CONNECT firefox-settings-attachments.cdn.mozilla.
    net:443 HTTP/1.1
2023-11-01 14:26:15 (UTC=UTC+0000) 254636 repIBFNVg reqK492uw CONNECT firefox-settings-attachments.cdn.mozilla.
    net:443 HTTP/1.1
2023-11-01 14:26:15 (UTC=UTC+0000) 257098 repeFNHie reqRvdrTx CONNECT firefox-settings-attachments.cdn.mozilla.
    net:443 HTTP/1.1
2023-11-01 14:26:43 (UTC=UTC+0000) 998797 repRbaodj reqV0rR4c CONNECT contile.services.mozilla.com:443 HTTP/1.1
2023-11-01 14:26:44 (UTC=UTC+0000) 016469 rep44I2h6 reqDiSckQ CONNECT spocs.getpocket.com:443 HTTP/1.1
2023-11-01 14:26:59 (UTC=UTC+0000) 416169 repBgbdLk reqGX6PcG CONNECT push.services.mozilla.com:443 HTTP/1.1
```

HASHes of zipped Logfiles,Downloads and unmodified Screenshots (stored separately):

MD5(Logfiles.zip)= d3a18fef8f15f57ee9a355b3b61495d3

SHA2-512(Logfiles.zip)= bd3834e6a634910a7137a79ec185084e7bba1e3228c3d30d01799a1f9813c06c56bdebe19b71456685d74d839eddd6e07989dec7483bb2d845f5912ceaeff239

MD5(Downloads.zip)= af37b96a5e17bab05cefcda488a3ef61

SHA2-512(Downloads.zip)= d0ba090f5e6f9e9af6b9301e3987dade2f8acd9561de7b374bfed9fa5661d9d6b8c89f81bb50dbb6d53839c03babfa919e050f1114ac7b81e78416b9ade69040

MD5(OrigShots.zip)= 91fe26042b6435b5459d6187f0d09617

SHA2-512(OrigShots.zip)= 2ee4b1dac2e8b3c2d96e3100c94cbd99a437dddd74326012ff6765adcab98a9d634dcc5ad495d3205effe37a04ccaf83a2ae8303f1445851cba05fce9f6e7263

Why should I believe that these screenshots are authentic?

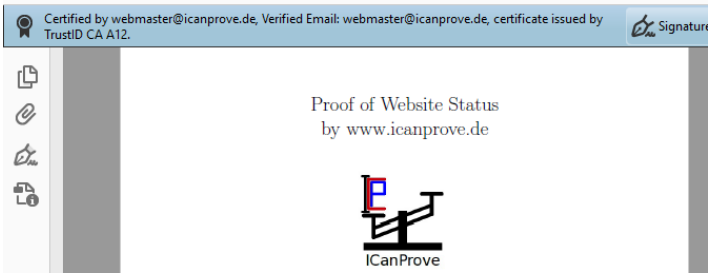
These screenshots have been created by a remote controlled browser that immediately digitally signed this document. After signing the document became immutable so the party that sent you this document had no opportunity to modify them. To verify this you must check, that the embedded signature is valid and belongs to webmaster@icanprove.de. The following sections will guide you through this process.

What is a digitally signed Document?

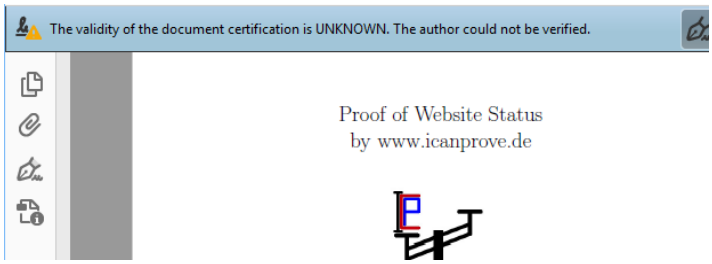
A digitally signed document contains an additional information: A digital signature. This is a mathematical construct so tightly interwoven with the document that it is destroyed if the document is modified. The digital signature is a sequence of numbers that including the name of the signer and a so called hash-value constitutes a solution to a complicated mathematical equation. The hash-value is the result of a mathematical function using all parts of the document as its input. This function has been designed to map small changes of the document to very different values. So modifying any part of the document will change this hash-value invalidating the aforementioned equation. To make this valid again the name of the signer and/or the signature have to be adapted. The equation is so complicated that finding a new adapted signature is so difficult that one needs some secret information (the private key held by the signer) to do so. The certification authorities choose the equations (parametrized the equations) in a way that solving them is virtually impossible without a "secret private key" only held by the authrorized signers. For checking the validity the parameters defining the equation can either be obtained from the signer's website or are included and signed by another party, and so on constituting the so called "chain of trust" that usually ist anchored with an equation built into your operating system, your browser or has been obtained manually.

How do I recognize digitally signed documents ?

Many PDF viewers e.g. AdobeReader® verify and display digital signatures. A PDF-file signed by ICanProve.de looks like the picture to the right:
More Information can be obtained by clicking on the ICanProve logo or choosing the "signatures" tab. You should check that the document is marked as "unchanged" and "LTV enabled". If in doubt have this information checked by an expert for digital signatures and public key infrastructures (PKI).



AdobeReader® reports a digital signature but flags it UNKNOWN.



AdobeReader® can use certificates for digital signatures from different sources. The certificate used by IcanProve.de has not been commissioned by Adobe® but by a different company that cooperates with many operating system vendors. Therefore certificates stored by the operating system have to be applied for verification. To enable these (using Microsoft Windows®) choose Edit - Preferences - Signatures - Verification - More - Windows-Integration and check the two boxes.