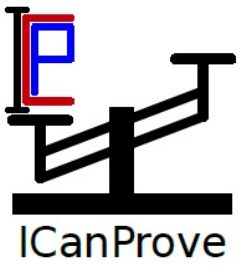
system test - do not use for production
by test.icanprove.de



Date: Thu Aug 26 23:29:58 CEST 2021

Site visited:

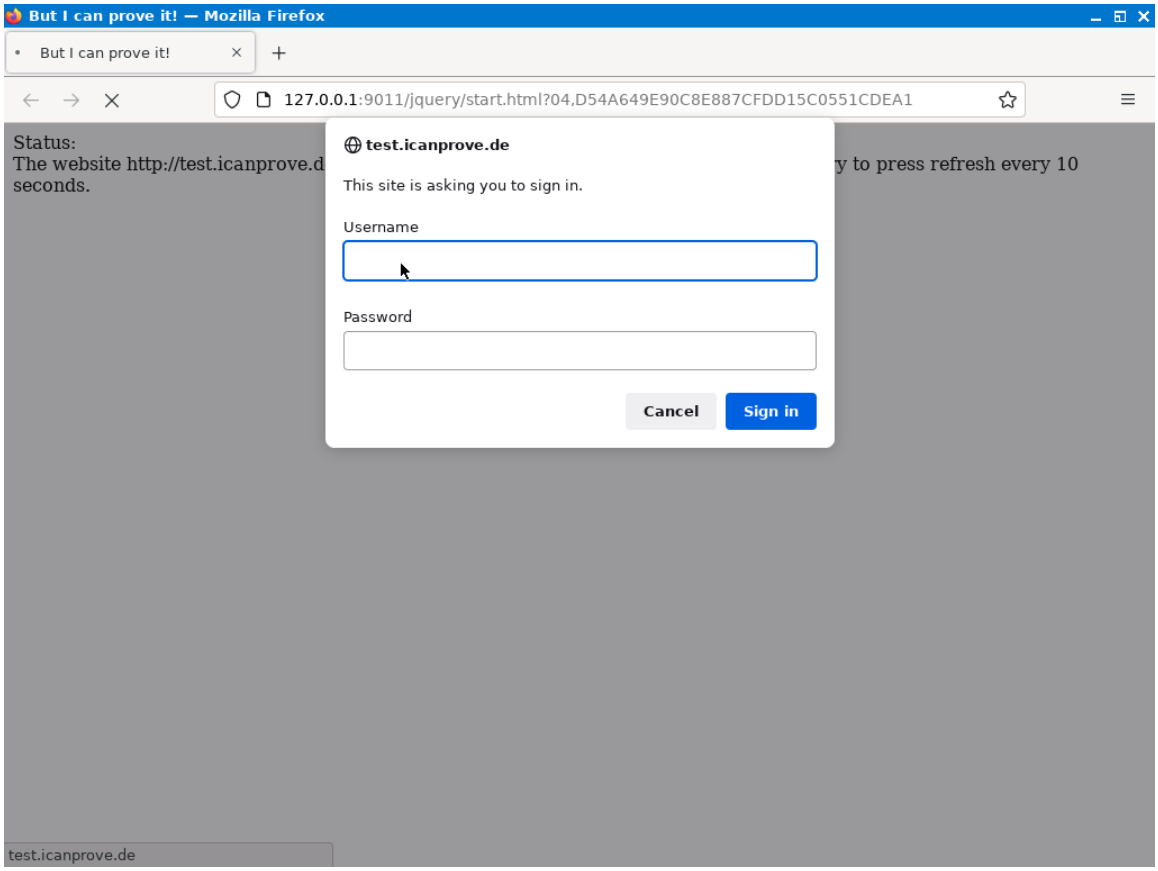
`http://test.icanprove.de/MyProofDemo.pdf`

Comments:

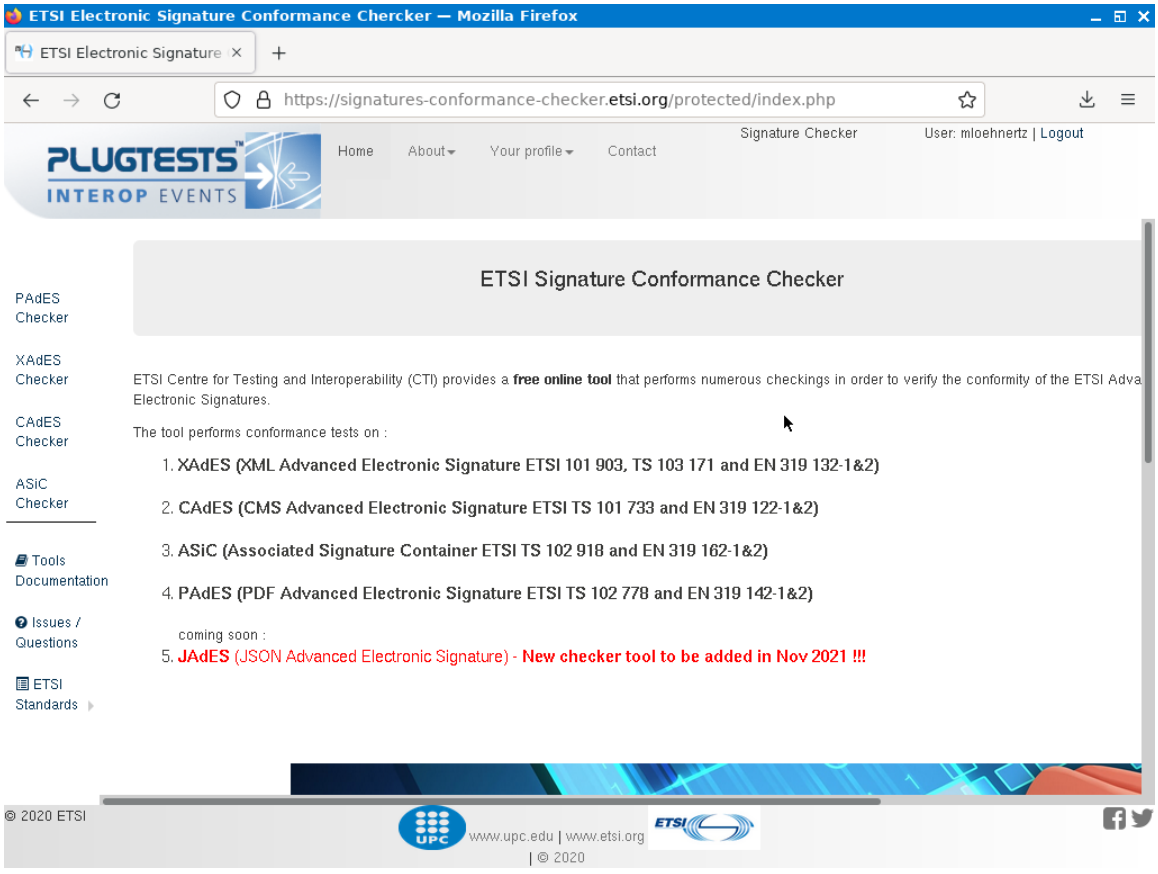
`ETSI`

Screenshots:

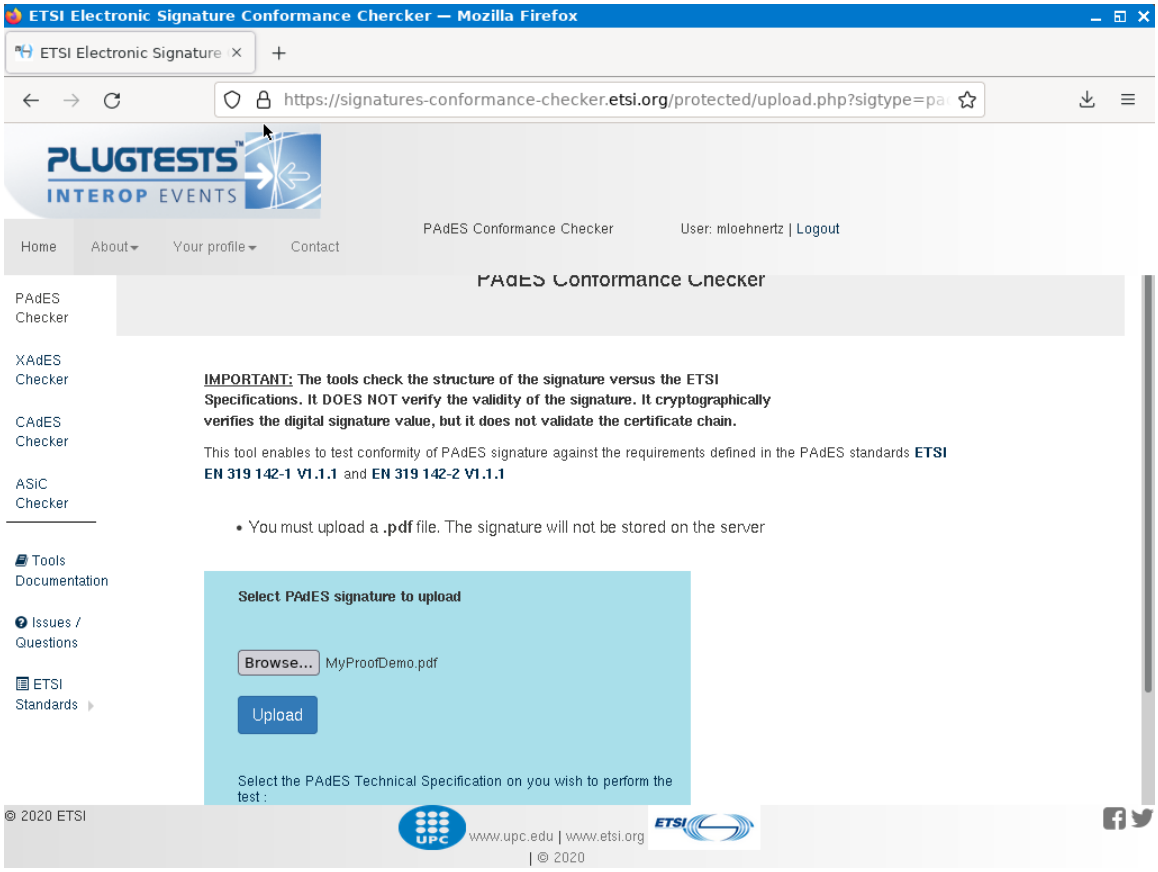
Screenshot #1:



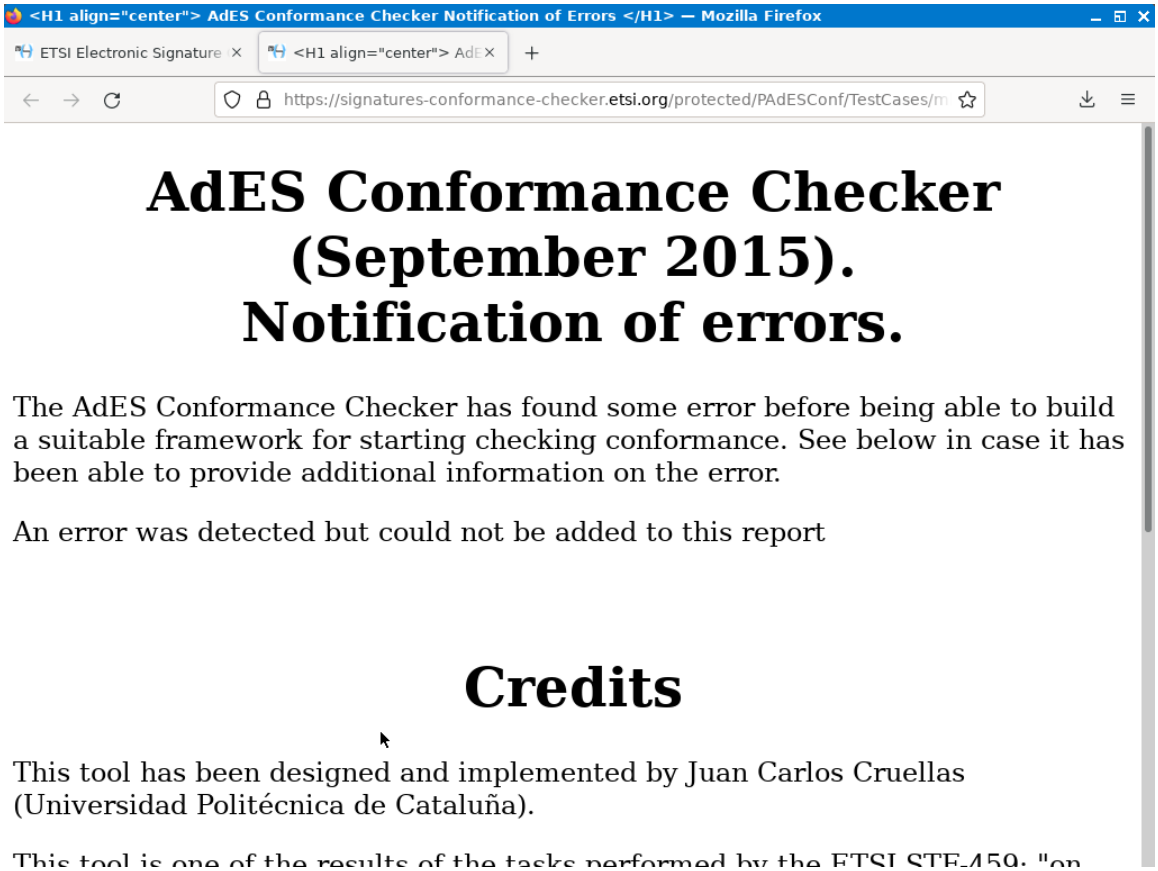
Screenshot #2:



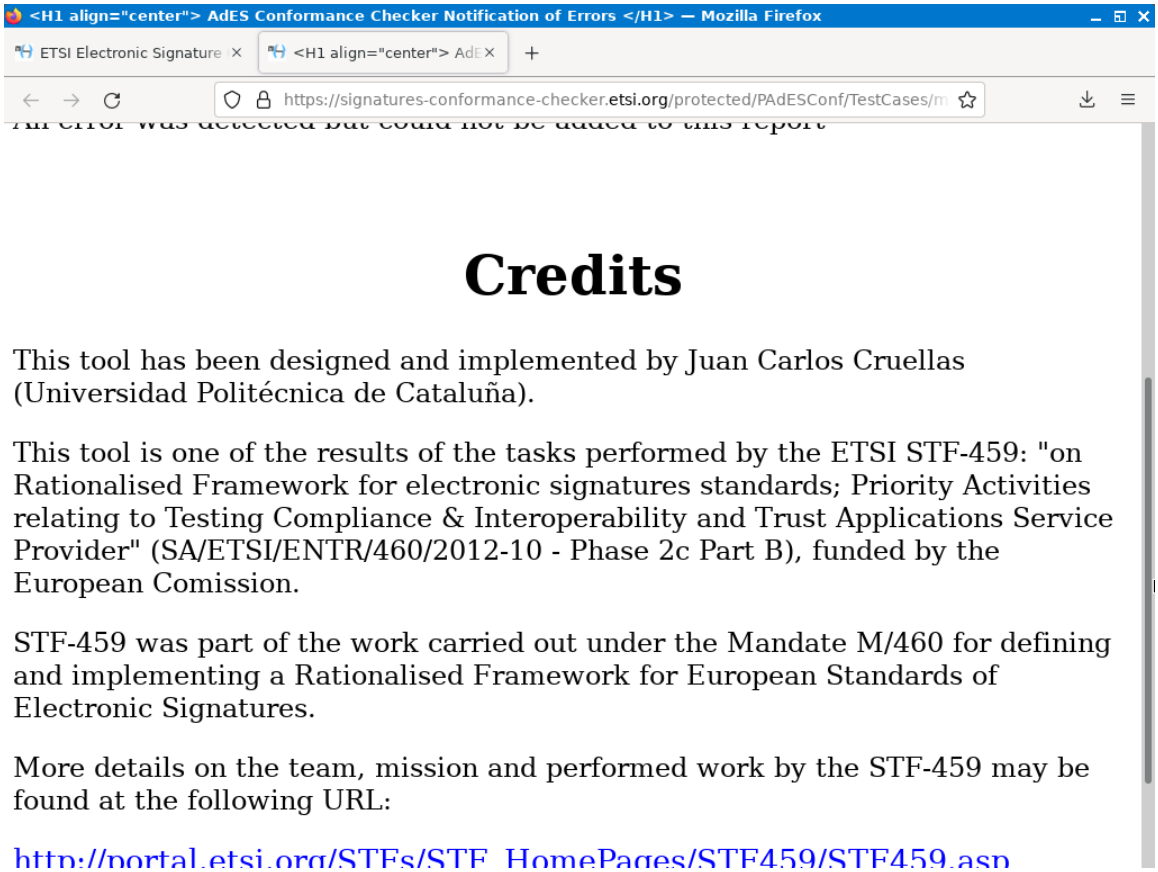
Screenshot #3:



Screenshot #4:



Screenshot #5:



Userlog:

```
Client Timezone set to Europe/Berlin
Session started at 2021-08-26 23:27:27 (CEST=UTC+0200)  579375  for IP:5.100.129.69 to url:http://test.
    icanprove.de/MyProofDemo.pdf

2021-08-26 23:27:32 (CEST=UTC+0200)  652030 : User created Screenshot #1
2021-08-26 23:27:32 (CEST=UTC+0200)  653035 : Mousedown at (353,231)
2021-08-26 23:27:32 (CEST=UTC+0200)  775852 : Mouseup at (353,231)
2021-08-26 23:27:33 (CEST=UTC+0200)  472452 : User typed t
2021-08-26 23:27:33 (CEST=UTC+0200)  705064 : User typed e
2021-08-26 23:27:33 (CEST=UTC+0200)  913913 : User typed s
2021-08-26 23:27:34 (CEST=UTC+0200)  253254 : User typed t
2021-08-26 23:27:37 (CEST=UTC+0200)  778387 : User deactivated key logging.
2021-08-26 23:27:39 (CEST=UTC+0200)  159311 : Mousedown at (386,314)
2021-08-26 23:27:39 (CEST=UTC+0200)  333159 : Mouseup at (386,314)
2021-08-26 23:27:42 (CEST=UTC+0200)  867313 : Mousedown at (689,371)
2021-08-26 23:27:43 (CEST=UTC+0200)  019199 : Mouseup at (689,371)
2021-08-26 23:27:47 (CEST=UTC+0200)  187114 : Mousedown at (952,128)
2021-08-26 23:27:47 (CEST=UTC+0200)  387240 : Mouseup at (952,128)
2021-08-26 23:27:49 (CEST=UTC+0200)  632971 : Mousedown at (682,528)
2021-08-26 23:27:49 (CEST=UTC+0200)  820965 : Mouseup at (682,528)
2021-08-26 23:27:52 (CEST=UTC+0200)  607374 : Mousedown at (531,97)
2021-08-26 23:27:53 (CEST=UTC+0200)  548860 : Mouseup at (252,94)
2021-08-26 23:27:58 (CEST=UTC+0200)  571488 : User activated key logging.
2021-08-26 23:28:11 (CEST=UTC+0200)  951366 : User typed unknown:86
2021-08-26 23:28:11 (CEST=UTC+0200)  978434 : User typed unknown:17
2021-08-26 23:28:14 (CEST=UTC+0200)  219965 : Mousedown at (424,95)
2021-08-26 23:28:14 (CEST=UTC+0200)  220524 : User typed h
2021-08-26 23:28:14 (CEST=UTC+0200)  235567 : User typed t
2021-08-26 23:28:14 (CEST=UTC+0200)  248529 : User typed t
2021-08-26 23:28:14 (CEST=UTC+0200)  261465 : User typed p
2021-08-26 23:28:14 (CEST=UTC+0200)  276301 : User typed s
2021-08-26 23:28:14 (CEST=UTC+0200)  288917 : User typed colon
2021-08-26 23:28:14 (CEST=UTC+0200)  306163 : User typed slash
2021-08-26 23:28:14 (CEST=UTC+0200)  318834 : User typed slash
2021-08-26 23:28:14 (CEST=UTC+0200)  331536 : User typed s
2021-08-26 23:28:14 (CEST=UTC+0200)  345030 : User typed i
2021-08-26 23:28:14 (CEST=UTC+0200)  359530 : User typed g
2021-08-26 23:28:14 (CEST=UTC+0200)  372130 : User typed n
2021-08-26 23:28:14 (CEST=UTC+0200)  384728 : Mouseup at (424,95)
2021-08-26 23:28:14 (CEST=UTC+0200)  387478 : User typed a
2021-08-26 23:28:14 (CEST=UTC+0200)  400466 : User typed t
2021-08-26 23:28:14 (CEST=UTC+0200)  413176 : User typed u
2021-08-26 23:28:14 (CEST=UTC+0200)  426451 : User typed r
2021-08-26 23:28:14 (CEST=UTC+0200)  443619 : User typed e
2021-08-26 23:28:14 (CEST=UTC+0200)  457647 : User typed s
2021-08-26 23:28:14 (CEST=UTC+0200)  470377 : User typed minus
2021-08-26 23:28:14 (CEST=UTC+0200)  483297 : User typed c
2021-08-26 23:28:14 (CEST=UTC+0200)  495840 : User typed o
2021-08-26 23:28:14 (CEST=UTC+0200)  509959 : User typed n
2021-08-26 23:28:14 (CEST=UTC+0200)  524064 : User typed f
2021-08-26 23:28:14 (CEST=UTC+0200)  536860 : User typed o
2021-08-26 23:28:14 (CEST=UTC+0200)  549485 : User typed r
2021-08-26 23:28:14 (CEST=UTC+0200)  562319 : User typed m
2021-08-26 23:28:14 (CEST=UTC+0200)  574855 : User typed a
2021-08-26 23:28:14 (CEST=UTC+0200)  587422 : User typed n
2021-08-26 23:28:14 (CEST=UTC+0200)  600253 : User typed c
2021-08-26 23:28:14 (CEST=UTC+0200)  622290 : User typed e
2021-08-26 23:28:14 (CEST=UTC+0200)  634900 : User typed minus
2021-08-26 23:28:14 (CEST=UTC+0200)  648565 : User typed c
2021-08-26 23:28:14 (CEST=UTC+0200)  661137 : User typed h
2021-08-26 23:28:14 (CEST=UTC+0200)  673792 : User typed e
2021-08-26 23:28:14 (CEST=UTC+0200)  686338 : User typed c
2021-08-26 23:28:14 (CEST=UTC+0200)  698869 : User typed k
2021-08-26 23:28:14 (CEST=UTC+0200)  711720 : User typed e
2021-08-26 23:28:14 (CEST=UTC+0200)  726396 : User typed r
2021-08-26 23:28:14 (CEST=UTC+0200)  741313 : User typed period
2021-08-26 23:28:14 (CEST=UTC+0200)  753846 : User typed e
2021-08-26 23:28:14 (CEST=UTC+0200)  766425 : User typed t
2021-08-26 23:28:14 (CEST=UTC+0200)  783466 : User typed s
2021-08-26 23:28:14 (CEST=UTC+0200)  797152 : User typed i
2021-08-26 23:28:14 (CEST=UTC+0200)  809698 : User typed period
2021-08-26 23:28:14 (CEST=UTC+0200)  822259 : User typed o
2021-08-26 23:28:14 (CEST=UTC+0200)  837607 : User typed r
2021-08-26 23:28:14 (CEST=UTC+0200)  851182 : User typed g
2021-08-26 23:28:18 (CEST=UTC+0200)  496464 : User typed Return
2021-08-26 23:28:24 (CEST=UTC+0200)  124905 : Mousedown at (557,291)
2021-08-26 23:28:24 (CEST=UTC+0200)  296872 : Mouseup at (557,291)
2021-08-26 23:28:28 (CEST=UTC+0200)  311989 : User deactivated key logging.
2021-08-26 23:28:29 (CEST=UTC+0200)  742317 : Mousedown at (387,240)
2021-08-26 23:28:29 (CEST=UTC+0200)  869011 : Mouseup at (387,240)
2021-08-26 23:28:48 (CEST=UTC+0200)  910170 : Mousedown at (376,314)
2021-08-26 23:28:49 (CEST=UTC+0200)  060057 : Mouseup at (376,314)
2021-08-26 23:28:55 (CEST=UTC+0200)  523328 : Mousedown at (403,319)
2021-08-26 23:28:55 (CEST=UTC+0200)  631734 : Mouseup at (403,319)
2021-08-26 23:28:57 (CEST=UTC+0200)  122848 : Mousedown at (694,366)
2021-08-26 23:28:57 (CEST=UTC+0200)  300328 : Mouseup at (694,366)
2021-08-26 23:29:01 (CEST=UTC+0200)  905993 : User created Screenshot #2
2021-08-26 23:29:03 (CEST=UTC+0200)  929709 : Mousedown at (51,268)
2021-08-26 23:29:04 (CEST=UTC+0200)  049961 : Mouseup at (51,268)
2021-08-26 23:29:06 (CEST=UTC+0200)  398589 : Mousedown at (259,636)
2021-08-26 23:29:06 (CEST=UTC+0200)  535647 : Mouseup at (259,636)
2021-08-26 23:29:10 (CEST=UTC+0200)  864042 : Mousedown at (238,590)
2021-08-26 23:29:10 (CEST=UTC+0200)  973090 : Mouseup at (238,590)
2021-08-26 23:29:13 (CEST=UTC+0200)  906071 : Mousedown at (238,50)
2021-08-26 23:29:13 (CEST=UTC+0200)  984724 : Mouseup at (239,50)
2021-08-26 23:29:15 (CEST=UTC+0200)  506691 : Mousedown at (232,130)
2021-08-26 23:29:15 (CEST=UTC+0200)  652363 : Mouseup at (232,130)
2021-08-26 23:29:15 (CEST=UTC+0200)  724962 : Mousedown at (232,130)
2021-08-26 23:29:15 (CEST=UTC+0200)  848594 : Mouseup at (232,130)
2021-08-26 23:29:17 (CEST=UTC+0200)  398191 : Mousedown at (231,107)
2021-08-26 23:29:17 (CEST=UTC+0200)  490063 : Mouseup at (231,107)
2021-08-26 23:29:17 (CEST=UTC+0200)  592295 : Mousedown at (231,107)
2021-08-26 23:29:17 (CEST=UTC+0200)  694203 : Mouseup at (231,107)
2021-08-26 23:29:20 (CEST=UTC+0200)  738587 : User created Screenshot #3
2021-08-26 23:29:22 (CEST=UTC+0200)  628621 : Mousedown at (268,638)
2021-08-26 23:29:22 (CEST=UTC+0200)  777925 : Mouseup at (268,638)
2021-08-26 23:29:25 (CEST=UTC+0200)  432034 : MouseScrollDown at (427,642)
2021-08-26 23:29:25 (CEST=UTC+0200)  832232 : MouseScrollDown at (427,675)
2021-08-26 23:29:25 (CEST=UTC+0200)  868074 : MouseScrollDown at (427,675)
2021-08-26 23:29:29 (CEST=UTC+0200)  884111 : Mousedown at (390,668)
2021-08-26 23:29:30 (CEST=UTC+0200)  007719 : Mouseup at (390,668)
2021-08-26 23:29:33 (CEST=UTC+0200)  194637 : MouseScrollUp at (681,627)
2021-08-26 23:29:35 (CEST=UTC+0200)  739757 : Mousedown at (1030,676)
2021-08-26 23:29:35 (CEST=UTC+0200)  840167 : Mouseup at (1030,676)
2021-08-26 23:29:37 (CEST=UTC+0200)  720247 : Mousedown at (335,648)
2021-08-26 23:29:37 (CEST=UTC+0200)  860545 : Mouseup at (335,648)
2021-08-26 23:29:41 (CEST=UTC+0200)  423530 : User created Screenshot #4
2021-08-26 23:29:47 (CEST=UTC+0200)  413228 : Mousedown at (1026,512)
```

```
2021-08-26 23:29:47 (CEST=UTC+0200)  546852 : Mouseup at (1026,512)
2021-08-26 23:29:52 (CEST=UTC+0200)  043096 : User created Screenshot #5
2021-08-26 23:29:55 (CEST=UTC+0200)  555505 : Session shutdown started.
```

Accesslog (reqxxx and repxxx refer to the logfiles):

```
2021-08-26 23:27:28 (CEST=UTC+0200) 437058 repEXES5H reqtQAmoJ GET http://test.icanprove.de/MyProofDemo.pdf
    HTTP/1.1
2021-08-26 23:27:43 (CEST=UTC+0200) 100008 repdSYdvl reqYFRiCX GET http://test.icanprove.de/MyProofDemo.pdf
    HTTP/1.1
2021-08-26 23:27:43 (CEST=UTC+0200) 538071 reptoLDPA req0dT22d GET http://test.icanprove.de/favicon.ico HTTP
    /1.1
2021-08-26 23:28:18 (CEST=UTC+0200) 597464 repnuXCfh reqjcq9tk CONNECT signatures-conformance-checker.etsi.org
    :443 HTTP/1.1
2021-08-26 23:28:19 (CEST=UTC+0200) 769467 repTnYAEq reqGozXZC CONNECT maxcdn.bootstrapcdn.com:443 HTTP/1.1
2021-08-26 23:28:19 (CEST=UTC+0200) 770746 repGRJgPw reqTDjZaJ CONNECT signatures-conformance-checker.etsi.org
    :443 HTTP/1.1
2021-08-26 23:28:19 (CEST=UTC+0200) 876360 repdafiC8 req162nml CONNECT signatures-conformance-checker.etsi.org
    :443 HTTP/1.1
2021-08-26 23:28:19 (CEST=UTC+0200) 877599 repP6aof2 reqD4OdZe CONNECT signatures-conformance-checker.etsi.org
    :443 HTTP/1.1
2021-08-26 23:28:19 (CEST=UTC+0200) 879064 repTCjCJr reqVbG16x CONNECT signatures-conformance-checker.etsi.org
    :443 HTTP/1.1
2021-08-26 23:28:19 (CEST=UTC+0200) 880657 repFqJIwP reqTESASV CONNECT signatures-conformance-checker.etsi.org
    :443 HTTP/1.1
2021-08-26 23:28:19 (CEST=UTC+0200) 900145 repOZI2BE reqymYb7K CONNECT ajax.googleapis.com:443 HTTP/1.1
2021-08-26 23:28:20 (CEST=UTC+0200) 361998 repSzo7LS reqMlqer0 CONNECT maxcdn.bootstrapcdn.com:443 HTTP/1.1
2021-08-26 23:28:57 (CEST=UTC+0200) 337922 rephx6NVC reqHQ0yqf CONNECT signatures-conformance-checker.etsi.org
    :443 HTTP/1.1
2021-08-26 23:29:04 (CEST=UTC+0200) 084411 repTj24Q8 reqJczWh2 CONNECT signatures-conformance-checker.etsi.org
    :443 HTTP/1.1
2021-08-26 23:29:22 (CEST=UTC+0200) 877376 repwNIISG reqPGXxul CONNECT signatures-conformance-checker.etsi.org
    :443 HTTP/1.1
2021-08-26 23:29:37 (CEST=UTC+0200) 944054 repVxFBVB reqnR1QmS CONNECT signatures-conformance-checker.etsi.org
    :443 HTTP/1.1
```

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

MD5(Logfiles.zip)= 898dbf5f5ce7c41ce1b0fdddbb85aa5e

SHA512(Logfiles.zip)= 619f65ca2da4e1fe6bc20b84749107549275d84739cc6e6ebb15b18cf86ba95d07fb1996ef6370f9959f05c41488b9a54af813f252ea8da6f881989e28222d54

MD5(Downloads.zip)= 1da6caef862615f5a6e2e8ead52cca5f

SHA512(Downloads.zip)= 19bf6185abe99e936775c04f0d95aad096dc5310b1af48c87e71952444199bf7987f6e3db5f90c7592844a891e8751a974a9c3f8cd80a85a879390b05bd45add

MD5(OrigShots.zip)= fd65cdc4cce3d31be2ac56b97cdc7d7b

SHA512(OrigShots.zip)= 56f9ac14b6aad9fb704b080682519bb7ed5710cbf5d89d2b6a2a2e9ff21acde70cbdf6182018a807c06ace095d36d2a16e2a83abbe6f0b1d734804a5d5b31ceb

Why should I believe that these screenshots are authentic?

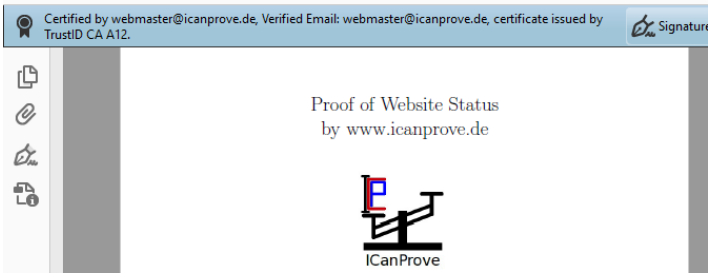
These screenshots have been created by a remote controlled browser that immediately digitally signed this document. After signing the document became immutable so the party that sent you this document had no opportunity to modify them. To verify this you must check, that the embedded signature is valid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

What is a digitally signed Document?

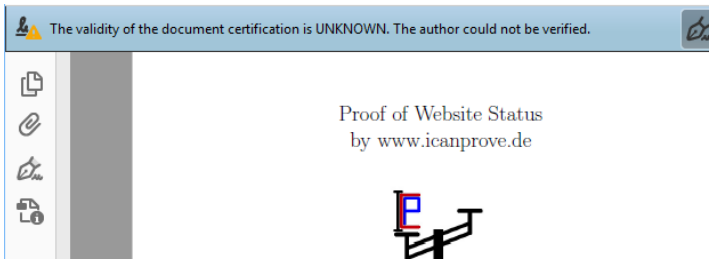
A digitally signed document contains an additional information: A digital signature. This is a mathematical construct so tightly interwoven with the document that it is destroyed if the document is modified. The digital signature is a sequence of numbers that including the name of the signer and a so 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 informaton (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 validiy the parameters defining the equation can either be optained 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 optained 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 ICanProveLogo 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 oparating system vendors. Therefore certificates stored by the operating system have to be applied for verification. To enable these (using Windows) choose Edit - Preferences - Signatures - Verification - More - Windows-Integration and check the two boxes.