

Nikhef

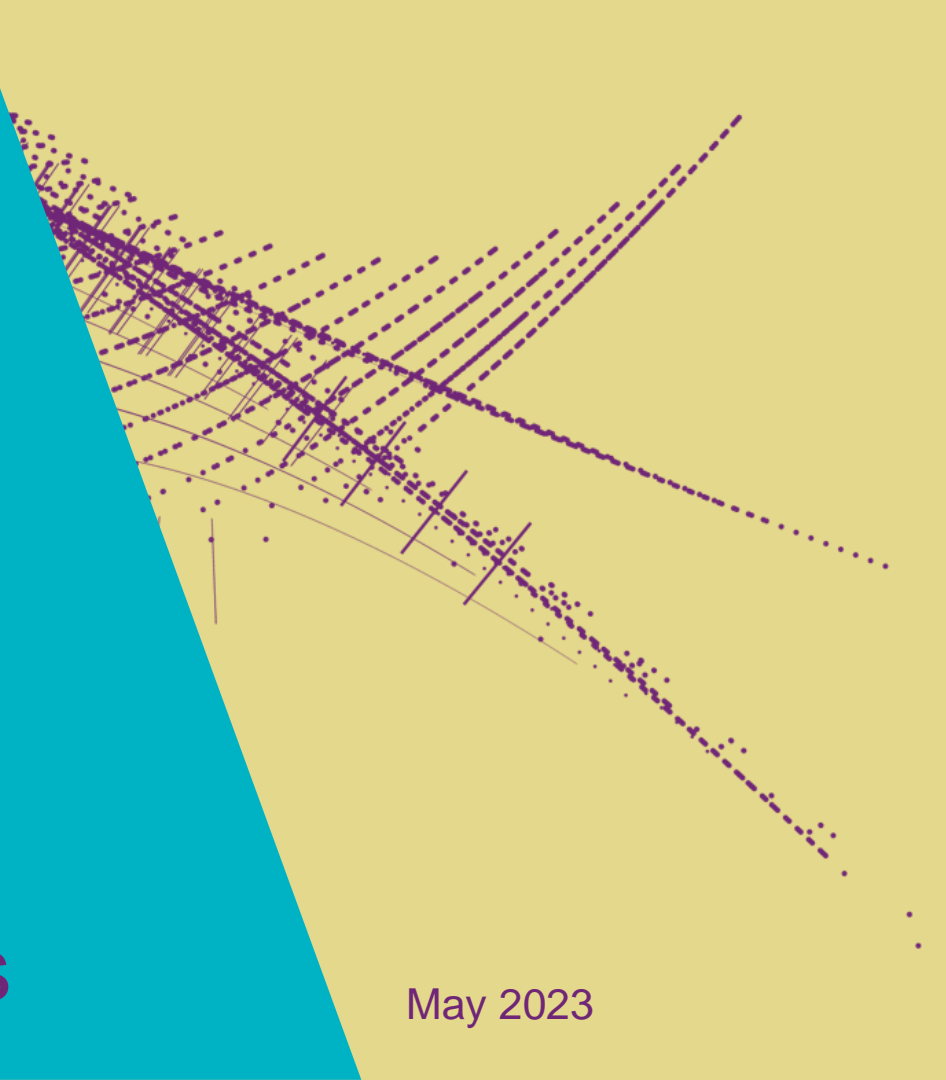


Maastricht University

David Groep

# RedHat 9+ & FF103: the issue of sha-1 roots

May 2023



# What happened in FF103?

▼ edu

SRCE CA

Software Security Device

ra.srce.hr has a security policy called HTTP Strict Transport Security (HSTS), which means that Firefox can only connect to it securely. You can't add an exception to visit this site.

The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.

[Learn more...](#)

Go Back

Advanced...

Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for ra.srce.hr.

Error code: `SSL_ERROR_BAD_CERT_DOMAIN`

[View Certificate](#)

Go Back

## Although it conceptually makes no sense ...

- SHA-1 is no longer secure (and all EECs and ICAs moved away)
- Now, some projects and distros are uselessly deprecating SHA-1 *also for self-signed (root) certificates*
- This affects at least
  - FF103+
  - RHEL9+ (and rebuilds)
- yet ... in the cases we could find *only* for CA certs that are not in the WebPKI (and distro) public trust list

This impacts both joint-trust and igtf-only trust when installed in a non-system location. But thy system locations are different is not obvious from the doc ...



# Firefox 103+

On 2022-08-03 16:12, Emir Imamagic wrote:

*seems that Firefox removed support for SHA-1 signatures in version 103.0: <https://www.mozilla.org/en-US/firefox/103.0/releasenotes/>*

*DavidG and me did some tests and seems that you can still import SHA-1 based CA certificates (there are still 26 of those in the bundle).*

*However, it will not trust sites protected by host certificates issued by SHA-1 based CA certificate.*

This at least holds for imported CAs (but there are still SHA-1 CAs as a built-in object that do work correctly).

For me at least, the error message FF103 produced was very unexpected:

"SSL\_ERROR\_BAD\_CERT\_DOMAIN"

even through the `_domain_` was perfectly fine, but the self-signed root was SHA-1, and the EEC for the server (I tried with <https://ra.srce.hr/>) was (correctly!) SHA\_256. In FF99, this still worked as expected.

And if you have HTST enabled on a site, then an override also does not work ...



# Rocky9+, AlmaLinux9+, RHEL9+ and

With RHEL9 also deprecating SHA-1, but *at the same time* still having self-signed SHA-1 based root certs in the ca-certificates package,

unknown why that distribution treats SHA-1 certs in the X509\_CERT\_DIR differently

At least there is a policy override for now  
(`update-crypto-policies --set DEFAULT:SHA1`),  
even if that is a rather course-grained and blunt tool

# The ca-certificates package in RH9

Interestingly, EL9 *does* ship with a lot of SHA-1 root CAs in `ca-certificates-2022.2.54-90.2.el9.noarch.rpm` and the `p11-kit` sources thereof (and thus e.g. `/etc/pki/tls/certs/ca-bundle.crt`) contain SHA-1 self-signed roots that do work on EL9.

So `p11-kit` and the directories are somehow whitelisted in the crypto policies

- but I have not found where that is yet.
- If you do find out why system roots with SHA-1 are fine with the default policy, but for the same self-signed trust anchors in another place the LEGACY policy has to be set? please share!

Maybe, if you have the ability to file tickets with RedHat, their answer may give us some insight. (Un)fortunately, not many have a RH support contract to notify them ...

# Mitigations?

Meanwhile,

- if you still have a SHA-1 root
  - and you are able to re-issue with the same key (and new serial)
  - and your EECs *do not* have dirname+serial in their AKI
- your CAs should probably re-issuing its root because that is easier.

But for the large ones, esp. the DigiCert Assured ID Root from 2006 for instance, that will be hard.

And migrating to another (SHA-2 rooted) signing hierarchy will take at least 395 days ... and a lot of engineering on the RP and CA side

The root cause is with RH not understanding what a self-signed trust anchor is, but that will not help us in the short term.

# Reissuance of roots?

ASGCCA-2007

BYGCA

CNIC

DZeScience

DigiCertGridRootCA-Root

KEK

MARGI

RDIG

SRCE

TRGrid

ArmeSFo

CESNET-CA-Root

DFN-GridGermany-Root

**DigiCertAssuredIDRootCA-Root**

IHEP-2013

LIPCA

**QuoVadis-Root-CA2**

RomanianGRID

SiGNET-CA

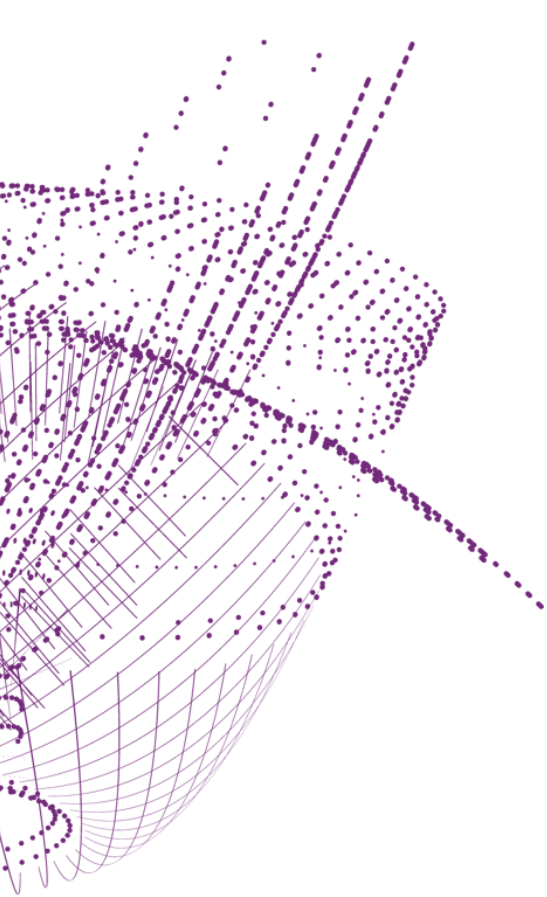
seegrid-ca-2013

**Fixed by now:** GridCanada, CILogon basic/silver/OpenID, UKeScienceRoot-2007

**Removed:** DigiCertGridCA-1-Classic, DigiCertGridTrustCA-Classic

**Will be discontinued soon:** GermanGrid (GridKA)





*Discussion*

# Time lines?



Maastricht University

Nikhef

David Groep

davidg@nikhef.nl

<https://www.nikhef.nl/~davidg/presentations/>

 <https://orcid.org/0000-0003-1026-6606>

