

TLS/PKI

- 1) Open different https websites from at least 3 different browsers and take a close look at the certificates:

- ParameterCertificate
- Chain
- Expiry date
- Root CA
- other fields

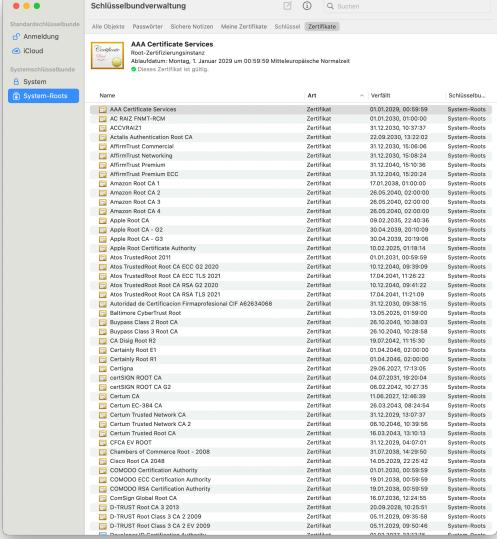
Chrome:

Safari:

Firefox:

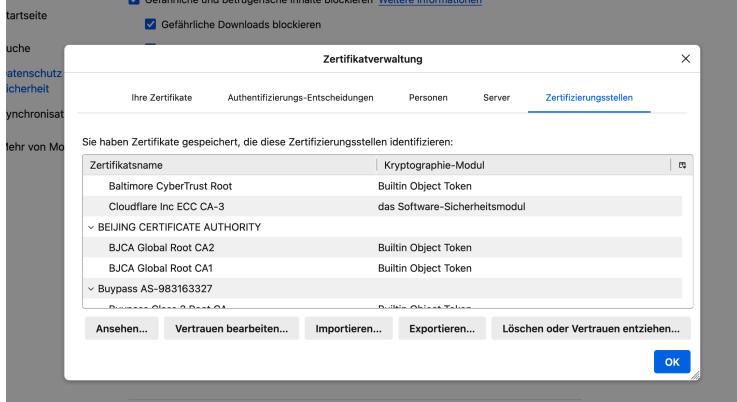
2) Open and see at least 3 different browsers on a total of at least 2 different operating systems, look at the installed root CAs, and compare the list.

Chrome is leading to the macOS keychain in my case:



The screenshot shows the 'Schlüsselbundverwaltung' (Keychain Management) window in macOS. The 'Zertifikate' tab is selected. A search bar at the top right contains the query 'Root-Zertifizierungsinstanz'. Below it, a table lists various certificates, including:

Name	Art	Verd.	Schließen...
AAA Certificate Services	Zertifikat	01.01.2018, 08:58:59	System-Roots
AAA Root - Zertifizierungsinstanz	Zertifikat	01.01.2018, 00:00:00	System-Roots
ACCVRA1	Zertifikat	31.12.2030, 10:37:37	System-Roots
Actalis Authentication Root CA	Zertifikat	22.09.2010, 10:22:02	System-Roots
Amazon Root CA	Zertifikat	31.12.2030, 10:37:37	System-Roots
AffirmTrust Networking	Zertifikat	31.12.2030, 10:08:24	System-Roots
AffirmTrust Premium	Zertifikat	09.01.2013, 22:40:36	System-Roots
Alcatel-Lucent ECC	Zertifikat	30.06.2013, 10:00:00	System-Roots
Amazon Root CA 1	Zertifikat	17.01.2018, 01:00:00	System-Roots
Amazon Root CA 2	Zertifikat	26.05.2010, 02:00:00	System-Roots
Amazon Root CA 3	Zertifikat	26.05.2010, 02:00:00	System-Roots
Amazon Root CA 4	Zertifikat	26.05.2010, 02:00:00	System-Roots
Apple Root CA	Zertifikat	09.01.2013, 22:40:36	System-Roots
Apple Root CA 02	Zertifikat	31.12.2030, 10:37:37	System-Roots
Apple Root CA_03	Zertifikat	30.04.2019, 21:09:08	System-Roots
Apple Root Certificate Authority	Zertifikat	10.12.2018, 01:18:14	System-Roots
Alos TrustRoot Root CA ECC 02 2020	Zertifikat	10.12.2018, 09:59:09	System-Roots
Alos TrustRoot Root CA ECC 10 2021	Zertifikat	17.04.2018, 11:26:22	System-Roots
Alos TrustRoot Root CA RSA 10 2030	Zertifikat	10.12.2018, 09:59:09	System-Roots
Alos TrustRoot Root CA RSA 11 2021	Zertifikat	17.04.2018, 11:21:09	System-Roots
Autorized de Certification Firmaprofessional CIF Af263406B	Zertifikat	31.12.2030, 10:37:37	System-Roots
Baltimore CyberTrust Root	Zertifikat	12.02.2018, 01:00:00	System-Roots
Buypass Class 2 Root CA	Zertifikat	26.01.2004, 02:38:03	System-Roots
Buypass Class 3 Root CA	Zertifikat	26.01.2004, 02:38:03	System-Roots
CACI Root CA	Zertifikat	16.03.2013, 10:30:13	System-Roots
Chambers of Commerce Root - 2008	Zertifikat	17.01.2018, 14:29:00	System-Roots
Cisco Root CA 2048	Zertifikat	14.02.2018, 22:23:42	System-Roots
Comodo CA Root	Zertifikat	01.01.2018, 00:00:00	System-Roots
comodooo ROOT CA	Zertifikat	04.01.2018, 19:23:04	System-Roots
overstock ROOT CA G2	Zertifikat	06.01.2018, 10:27:35	System-Roots
Overstock Root CA G2	Zertifikat	11.01.2018, 10:27:35	System-Roots
Centum EC -984 CA	Zertifikat	26.03.2018, 09:24:54	System-Roots
Centum Trusted Network CA	Zertifikat	31.12.2030, 10:37:37	System-Roots
Centum Trusted Network CA 2	Zertifikat	06.01.2018, 10:27:35	System-Roots
Centum Trusted Root CA	Zertifikat	16.03.2013, 10:30:13	System-Roots
CGI Root CA	Zertifikat	31.12.2030, 10:37:37	System-Roots
Chambers of Commerce Root - 2008	Zertifikat	17.01.2018, 14:29:00	System-Roots
DigiCert Root R1	Zertifikat	01.01.2018, 00:00:00	System-Roots
DigiCert Root R2	Zertifikat	26.01.2018, 00:00:00	System-Roots
digiCert ROOT CA	Zertifikat	04.01.2018, 19:23:04	System-Roots
overstock ROOT CA G2	Zertifikat	06.01.2018, 10:27:35	System-Roots
Overstock Root CA G2	Zertifikat	11.01.2018, 10:27:35	System-Roots
Centum EC -984 CA	Zertifikat	26.03.2018, 09:24:54	System-Roots
Centum Trusted Network CA	Zertifikat	31.12.2030, 10:37:37	System-Roots
Centum Trusted Network CA 2	Zertifikat	06.01.2018, 10:27:35	System-Roots
Centum Trusted Root CA	Zertifikat	16.03.2013, 10:30:13	System-Roots
CGI Root CA	Zertifikat	31.12.2030, 10:37:37	System-Roots
Chambers of Commerce Root - 2008	Zertifikat	17.01.2018, 14:29:00	System-Roots
Cisco Root CA 2048	Zertifikat	14.02.2018, 22:23:42	System-Roots
Comodo CA Root	Zertifikat	01.01.2018, 00:00:00	System-Roots
comodooo ECC Certification Authority	Zertifikat	19.01.2018, 00:59:09	System-Roots
comodooo RSA Certification Authority	Zertifikat	19.01.2018, 00:59:09	System-Roots
comodooo SHA256 Certification Authority	Zertifikat	19.01.2018, 00:59:09	System-Roots
D-TRUST Root CA 2 2013	Zertifikat	20.01.2028, 10:23:01	System-Roots
D-TRUST Root Class 3 CA 2 2009	Zertifikat	05.11.2028, 09:56:58	System-Roots
D-TRUST Root Class 3 CA 2 EV 2009	Zertifikat	05.11.2028, 09:56:48	System-Roots
DigiCert IS-Certificate Authority	Zertifikat	01.03.2018, 10:00:00	System-Roots

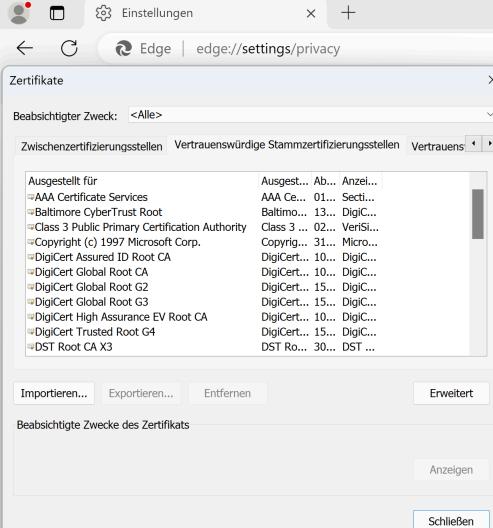


The screenshot shows the 'Zertifikatverwaltung' (Certificate Management) dialog box in Windows. The 'Zertifizierungsstellen' (Issuing Authorities) tab is selected. It lists several certificates, including:

- Baltimore CyberTrust Root (Kryptographie-Modul: Built-in Object Token)
- Cloudflare Inc ECC CA-3 (Kryptographie-Modul: das Software-Sicherheitsmodul)
- BEIJING CERTIFICATE AUTHORITY
 - BJCA Global Root CA2 (Built-in Object Token)
 - BJCA Global Root CA1 (Built-in Object Token)
 - Bypass AS-983163327

Buttons at the bottom include 'Ansehen...', 'Vertrauen bearbeiten...', 'Importieren...', 'Exportieren...', 'Löschen oder Vertrauen entziehen...', and 'OK'.

Windows:

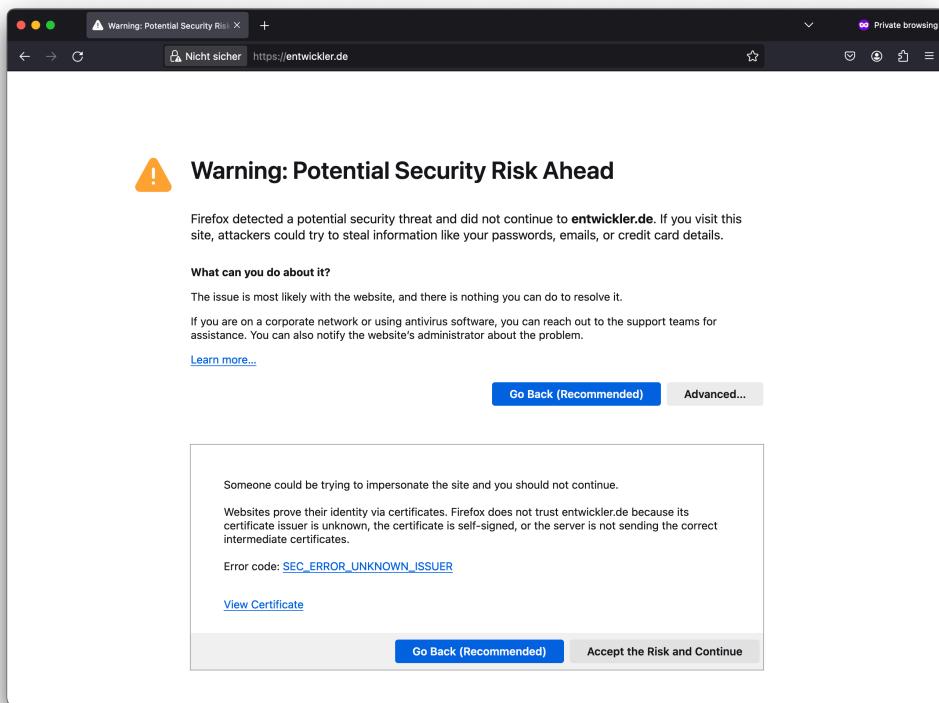
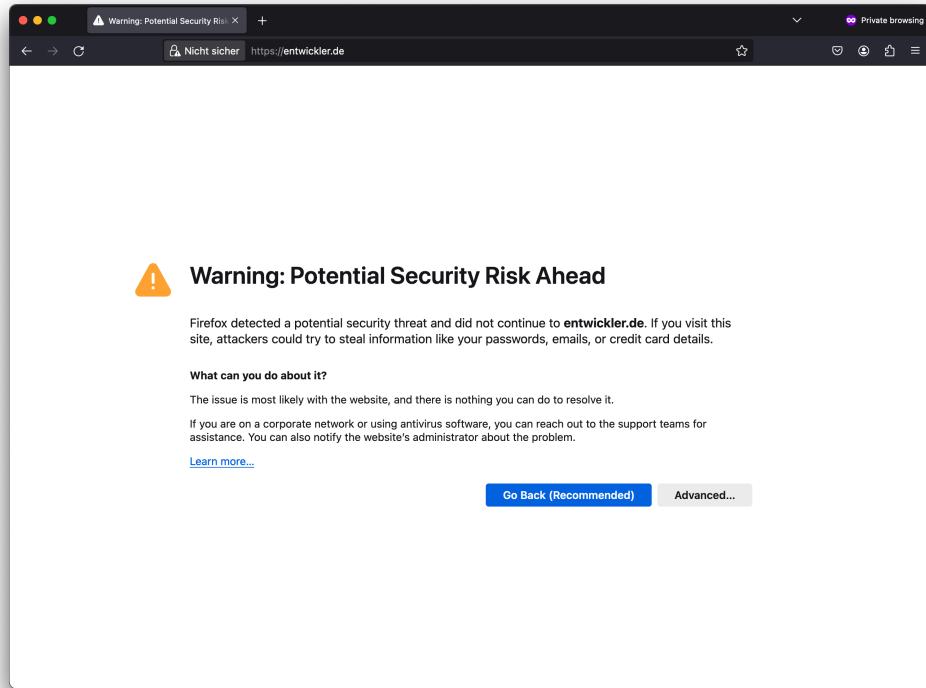


The screenshot shows the 'Einstellungen' (Settings) window in Microsoft Edge. The 'Zertifikate' (Certificates) section is open. It displays a list of certificates under 'Ausgestellt für' (Issued for) and 'Ausgest... Ab... Anzei...' (Issued... by... display...). Both lists show many of the same certificates as the macOS keychain, such as Baltimore CyberTrust Root, Cloudflare Inc ECC CA-3, and various DigiCert and Comodo roots. Buttons at the bottom include 'Importieren...', 'Exportieren...', 'Entfernen', 'Erweitert', 'Anzeigen', and 'Schließen'.

The root certificate authority lists from macOS and Windows, accessed via Chrome, Firefox or Edge, are not identical but have several CAs in common, such as Baltimore CyberTrust Root, Buypass, Amazon Root CAs, and DigiCert. This overlap ensures cross-platform security and trust, while the differences reflect each platform's unique trust ecosystem.

3) Install the Firefox browser, visit any https website, and look at the root CA of that website. Then withdraw trust in Firefox from this root CA and visit the website again. What error message do you get?

I received the error „SEC_ERROR_UNKNOWN_ISSUER.“ It has to be noted that I had to open an incognito tab to provoke the error after trust withdrawal.



Diffie-Hellman Key Exchange

1)

```

    > class DiffieHellman {
    >
    >     public static void main(String[] args) {
    >         BigInteger prime = new BigInteger(val: "17");
    >         BigInteger base = new BigInteger(val: "12");
    >         BigInteger secretA = new BigInteger(val: "88");
    >         BigInteger secretB = new BigInteger(val: "104");
    >
    >         BigInteger publicA = base.modPow(secretA, prime);
    >         BigInteger publicB = base.modPow(secretB, prime);
    >
    >         BigInteger sharedSecretA = publicB.modPow(secretA, prime);
    >         BigInteger sharedSecretB = publicA.modPow(secretB, prime);
    >
    >         System.out.println("Public Key A: " + publicA);
    >         System.out.println("Public Key B: " + publicB);
    >         System.out.println("Shared Secret: " + sharedSecretA);
    >         System.out.println("Shared Secret the same? " + sharedSecretB.equals(sharedSecretA));
    >     }
    > }

```

ug DiffieHellman x

Threads & Variables Console

/Users/tim.herbst/Library/Java/JavaVirtualMachines/temurin-21.0.2/Contents/Home/bin/java -agentlib:jdwp=transport=socket,address=127.0.0.1:52036,server=y,com

Connected to the target VM, address: '127.0.0.1:52036', transport: 'socket'

Public Key A: 16

Public Key B: 16

Shared Secret: 1

Shared Secret the same? true

Disconnected from the target VM, address: '127.0.0.1:52036', transport: 'socket'

2)

```

    > class DiffieHellman {
    >
    >     public static void main(String[] args) {
    >         BigInteger prime = new BigInteger(val: "21");
    >         BigInteger base = new BigInteger(val: "16");
    >         BigInteger secretA = new BigInteger(val: "145");
    >         BigInteger secretB = new BigInteger(val: "389");
    >
    >         BigInteger publicA = base.modPow(secretA, prime);
    >         BigInteger publicB = base.modPow(secretB, prime);
    >
    >         BigInteger sharedSecretA = publicB.modPow(secretA, prime);
    >         BigInteger sharedSecretB = publicA.modPow(secretB, prime);
    >
    >         System.out.println("Public Key A: " + publicA);
    >         System.out.println("Public Key B: " + publicB);
    >         System.out.println("Shared Secret: " + sharedSecretA);
    >         System.out.println("Shared Secret the same? " + sharedSecretB.equals(sharedSecretA));
    >     }
    > }

```

ug DiffieHellman x

Threads & Variables Console

/Users/tim.herbst/Library/Java/JavaVirtualMachines/temurin-21.0.2/Contents/Home/bin/java -agentlib:jdwp=transport=socket,address=127.0.0.1:52128,server=y,com

Connected to the target VM, address: '127.0.0.1:52128', transport: 'socket'

Public Key A: 16

Public Key B: 4

Shared Secret: 4

Shared Secret the same? true