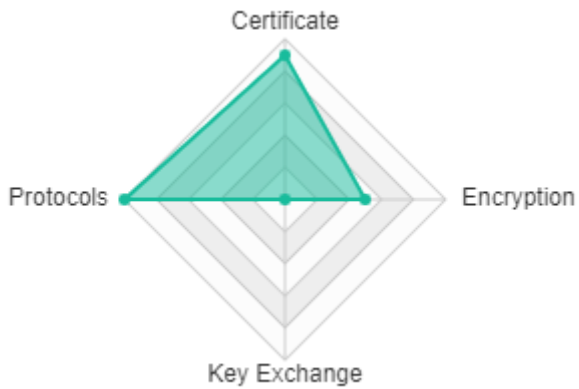
try another

RESULTS

SUMMARY

SSL Report: dbissql.informatik.uni-freiburg.de

C



CERTIFICATE

Subject	dbissql.informatik.uni-freiburg.de
alternate Names	dbissql.informatik.uni-freiburg.de
Serial	100482715934945974134867695 62
Valid From	2019-02-04 13:31:38
Valid Until	2021-05-08 13:31:38
Key algorithm	RSA
Key Size	2048
Exponent	65537
Signature Algorithm	sha256
SHA1 fingerprint	0f35e7169837a4078de811a3e462431b94fb798e
Issuer	DFN-Verein Global Issuing CA
OSCP	null
CRL	ok
CRL URL	http://cdp1.pca.dfn.de/dfn-ca-global-g2/pub/crl/cacrl.crl http://cdp2.pca.dfn.de/dfn-ca-global-g2/pub/crl/cacrl.crl

ADDITIONAL CERTIFICATES

certificates provided	3
contains Anchor	No
Certificate #0	
common Name	Uni-FR CA - G02
Valid Until	2019-07-09 23:59:00

Issuer	DFN-Verein PCA Global - G01
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	sha256
SHA1 fingerprint	6b0ae2a2aceff1bedc851cccd5783a35deb9ed33

Certificate #1	
common Name	DFN-Verein PCA Global - G01
Valid Until	2019-07-09 23:59:00
Issuer	Deutsche Telekom Root CA 2
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	sha256
SHA1 fingerprint	f4c538c3bb994f13f8fdc240b679a64b1934a1b5

Certificate #2	
common Name	Deutsche Telekom Root CA 2
Valid Until	2019-07-09 23:59:00
Issuer	Deutsche Telekom Root CA 2
Key Algorithm	RSA
Key Size	2048
Signature Algorithm	sha1
SHA1 fingerprint	85a408c09c193e5d51587dcdd61330fd8cde37bf

CERTIFICATE CHAIN

- **DBISSQL.INFORMATIK.UNI-FREIBURG.DE**
  SHA1: 0f35e7169837a4078de811a3e462431b94fb798e
- **UNI-FR CA - G02**

SHA1: 6b0ae2a2aceff1bedc851cccd5783a35deb9ed33

DFN-VEREIN PCA GLOBAL - G01

SHA1: f4c538c3bb994f13f8fdc240b679a64b1934a1b5

DEUTSCHE TELEKOM ROOT CA 2

SHA1: 85a408c09c193e5d51587dcdd61330fd8cde37bf

PROTOCOLS

SSLv2	No
SSLv3	No
TLSv1.0	No
TLSv1.1	No
TLSv1.2	Yes
TLSv1.3	No

CIPHER SUITES

TLSv1.2	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384:DH256bits	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384:DH256bits	256
TLS_RSA_WITH_AES_256_CBC_SHA256	256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	256

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	256
TLS_RSA_WITH_AES_256_GCM_SHA384	256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	256
RSA_WITH_AES_256_CCM	256
RSA_WITH_AES_256_CCM_8	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256:DH256bits	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256:DH256bits	128
TLS_RSA_WITH_AES_128_CBC_SHA256	128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	128
RSA_WITH_AES_128_CCM_8	128
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	128
RSA_WITH_AES_128_CCM	128
TLS_RSA_WITH_AES_128_GCM_SHA256	128

ADDITIONAL DETAILS

AEAD-Ciphers	offered
(Perfect) Forward Secrecy	offered ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-CHACHA20-POLY1305 ECDHE-RSA-CAMELLIA256-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-CAMELLIA128-SHA256
HSTS-Header	offered
ServerBanner	Apache/2.4.29 (Ubuntu)
Redirection	incorrectly configured (200 OK ('/'))
Cipher Order	server sets order
TLS_FALLBACK_SCSV	offered

EXPLOITS

Freak	not Vulnerable
Secure Client Renegotiation	not Vulnerable
CCS-Injection	not Vulnerable
RC4 Ciphers	not Vulnerable
ROBOT	not Vulnerable
secure_renego	not Vulnerable
Drown	not Vulnerable
Ticketbleed	not Vulnerable
Lucky13	Vulnerable
logjam	not Vulnerable
CRIME	not Vulnerable
Heartbleed	not Vulnerable
Sweet32	not Vulnerable
Poodle	not Vulnerable
BEAST	not Vulnerable

BROWSER COMPATIBILITY

android_237	No connection
android_411	No connection
android_43	No connection
android_442	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
android_500	TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256
android_60	TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256
android_70	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
chrome_51_win7	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
chrome_57_win7	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
firefox_49_win7	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384

firefox_53_win7	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
ie_6_xp	No connection
ie_7_vista	No connection
ie_8_xp	No connection
ie_8_win7	No connection
ie_11_win7	TLSv1.2 ECDHE-RSA-AES256-SHA384
ie_11_win81	TLSv1.2 ECDHE-RSA-AES256-SHA384
ie_11_winphone81update	TLSv1.2 ECDHE-RSA-AES256-SHA384
ie_11_win10	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
edge_13_win10	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
edge_13_winphone10	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
opera_17_win7	TLSv1.2 ECDHE-RSA-AES128-SHA256
safari_519_osx1068	No connection
safari_7_ios71	TLSv1.2 ECDHE-RSA-AES256-SHA384
safari_9_osx1011	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
safari_10_osx1012	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
apple_ats_9_ios9	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
tor_1709_win7	No connection
java_6u45	No connection
java_7u25	No connection
java_8u31	TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256
openssl_101l	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384
openssl_102e	TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384

Back to Top

LOCATION

Herman-Herder-Strasse
Freiburg, 79100

(https://www.rz.uni-freiburg.de/frits)

ABOUT

This Website is provided by the data centre (https://www.rz.uni-freiburg.de) .