

Print Date & Time: 24/03/2025-17:56:38

New, TLSv1.3, Cipher is TLS AES 256 GCM SHA384

Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)

[SENDER SECTION] www.db.com:443

CONNECTED(00000003)

Certificate chain

0 s:jurisdictionC = DE, jurisdictionST = Hessen, jurisdictionL = Frankfurt am Main,
businessCategory = Private Organization, serialNumber = HRB 30000, C = DE, L = Frankfurt am Main,
postalCode = 60325, street = Taunusanlage 12, O = DEUTSCHE BANK AG, CN = www.db.com
i:C = US, O = DigiCert Inc, CN = DigiCert EV RSA CA G2
a:PKKEY: id-ecPublicKey, 256 (bit); sigalg: RSA-SHA256
v:NotBefore: Nov 8 00:00:00 2024 GMT; NotAfter: Nov 7 23:59:59 2025 GMT
1 s:C = US, O = DigiCert Inc, CN = DigiCert EV RSA CA G2
i:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root G2
a:PKKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
v:NotBefore: Jul 2 12:42:50 2020 GMT; NotAfter: Jul 2 12:42:50 2030 GMT

Server certificate

-----BEGIN CERTIFICATE-----

MIIGaTCCBVGgAwIBAgIQB0eFD0P50uC9+Aw3LKVuyjANBgkqhkiG9w0BAQsFADBE
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNLcnQgSW5jMR4wHAYDVQQDEwVE
awdpQ2VydCBFViBSU0EgQ0EgRzIwHhcnMjQxMTA4MDAwMDAwWhcnMjUxMTA3MjM1
OTU5WjCCAQgxExARBgSrBgEEAYI3PAIBAxMCREUxXfzAVBgSrBgEEAYI3PAIBAhMG
SGVzc2VuMSIwIAYLKwYBBAGCNzWCAQETEUZyYW5rZnVydCBhbSBNYWluMR0wGwYD
VQOPDBRQcm12YXRlIE9yZ2FuaXphdGlvbjESMBAGA1UEBRMJJSFJCIDMwMDAwMQsw
CQYDVQQGEwJERTFAeBgGA1UEBxMRRnJhbmtdmdXJ0IGFtIE1haW4xZDjAMBgNVBBET
BTYwMzI1MRgwFgYDVQQJEUwUYXVudXNhbmhZ2UgMTIxGTAXBgNVBAoTEERFVVRT
Q0hFIEJBTksGQUcxExARBgNVBAMTCnd3dy5kYi5jb20wWTATBgqcqhkjOPQIBBggq
hkjOPQMBBwNCAAAQf8tR0xKkK4zUfCs4rtfsDYXRUo0ChL3FEq2vB8Lng0sV7BFj3
6z0UcAVEjQyH0feamHtmHluczM1tAuD/O2do4IDWjCCAIYwHwYDVR0jBBGwFoAU
ak5Qv5honVt7IHxUWQF5SGaSMgYwHQYDVR00BBYEFDV6sOPSwpCqG1GSwd/Xi0lf
jVmZMB0GA1UdEQQWMBSCCnd3dy5kYi5jb22CBmRiLmNvbTBKbG9NVHSAEQzBBMA5G
CWCGSAGG/WwCAtAYBgVngQwBATApMCCGCCsGAQUFBwIBFhtodHRw0i8vd3d3LmRp
Z2ljZXJ0LmNvbS9DUFMwDgYDVROPAQH/BAQDAg0IMB0GA1UdJjQWMB0GCCsGAQUF
BwMBBggrBgEFB0cDAjB1BgNVHR8EbjBsMDSGMAwhi5odHRw0i8vY3J3sMy5kaWdp
Y2VydC5jb20vRGlnaUNLcnRFVLJTTQUNBRzIuY3J3sMDSGMAwhi5odHRw0i8vY3J3s
M5kaWdpY2VydC5jb20vRGlnaUNLcnRFVLJTTQUNBRzIuY3J3sMHMGCCsGAQUFBwEB
BGcwZTAKBggrBgEFB0cwAYYYaHR0cDovL29jc3AuZGlnaWNlcnQuY29tMD0GCCsG
AQUFBzAChjFodHRw0i8vY2FjZXJ0cy5kaWdpY2VydC5jb20vRGlnaUNLcnRFVLJTT
QUNBRzIuY3J0MAwGA1UdEwEB/wQCMAAwgGF+BgorBgEEAdZ5AgQCBIIIBbgSCAWoB
aAB3ABLxTjS9U3JMHAYZw48/ehP457Vih4icbTAFh0vLhiY6AAABkwvX0ycAAAQD
AegwRgIhAMdgtA2qIC9ESET26+N41PFdyPoQDra0QWkxxXGENRTAiEA14N6twTd
JGUSNnzcPcrsC19oBC2DlFVP5wJPqghVRo+0AdQB9WR4S4XgqexxhZ3xe/fjQh1wU
oE6VnrkDL9k0jC55uAAAAZML1zthAAAEawBGMEQCIE/nK0vxH/5bLT57bN8UxaZ7
yelsyt7G6BHVH9QDLJkA1B3U+HIziJXpV9Qvwz8Nj0Vkv2aIcXStXnrhHPRRokq
6wB2A0bSMWNAd4zBEEEG13G5zsHSQPaWhIb7uocyHf0eN45QAAABkwvX03kAAAQD
AEcwRQIhAICCB12BVkXuW2d0Hswgc5E8Q2y7EFmoDpFmXc7BIbSmAiB0iCBRMjU+
Y+vgZtwWPHNk9x/YCUml//gTGov/9RLS9DANBgkqhkiG9w0BAQsFAAOCAQEAT+bj
2nwn3QlI4R2700UoYJ3Su+FgM8dIYjNNfakZSmBcHTnmI7XjYSDAzCr4KvGJ3BpoE
gVpNIffjYgnraZeTsIjZHNXS0X1WLv9+KAuBo6bes4hy4tLEWmNPVt09KbRTJiHq
uCzQ0pxwi81j5Vaf18D0AC2Tsr+PC3NCWTTti4/7w0FYMLE/slySPxaoN0zNSEeQ
2aMjTiP6tR3mCKTtc+PckIWGDd4801hSBq0KMsrzS8yBZ5537r8JkeMygN9scpdK
Cg2Btwfovvd06b6zxrmSCb8cTJ6piRXf8K0nLBANKtL+orPms+LgJzEiscZVz4jy
Xrj6UWoHrdjogBqePw==

-----END CERTIFICATE-----

subject=jurisdictionC = DE, jurisdictionST = Hessen, jurisdictionL = Frankfurt am Main,
businessCategory = Private Organization, serialNumber = HRB 30000, C = DE, L = Frankfurt am Main,
postalCode = 60325, street = Taunusanlage 12, O = DEUTSCHE BANK AG, CN = www.db.com
issuer=C = US, O = DigiCert Inc, CN = DigiCert EV RSA CA G2

No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits

SSL handshake has read 3378 bytes and written 392 bytes
Verification: OK

New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
