Assignment 2

CS21B050

Certificate Details

Google:

Version	V3
Serial Number	5a42ed068fcc038709fa132a7f24e66b
Signature Algorithm	sha256RSA
Signature Hash Algorithm	sha256
Issuer	WR2, Google Trust Services, US
Valid From	05 August 2024 12:49:58
Valid To	28 October 2024 12:49:57
Subject	www.google.com
Subject Public Key Algorithm	Elliptic Curve Public Key
Subject's Public Key Algorithm	00 04 DD 6C A0 E9 A4 8F CE 99 0D D0 52 36 73 B7 44 02 BB 07 A3 8F 0C 24 6B 58 27 8B 64 7C A0 E0 D8 C1 49 86 E6 6A B6 6E 5B 61 70 8B 22 FF 0C 31 DD BE 60 B8 CE 06 69 29 05 B6 EF 64 B6 2C DD 57 8C A1
Public Key Parameters	ECDSA_P256
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)
Subject Key Identifier	998a049bd4887aeeefc9c7f23ff28a9921323f83
Authority Key Identifier	KeyID=de1b1eed7915d43e3724c321bbec34396d42b230
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://o.pki.goog/wr2 [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://i.pki.goog/wr2.crt
Subject Alternative Name	DNS Name=www.google.com
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.23.140.1.2.1
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://c.pki.goog/wr2/9UVbN0w5E6Y.crl
Signed Certificate Timestamp List	04 81 F1 00 EF 00 76 00 76 FF 88 3F 0A B6 FB 95 51 C2 61 CC F5 87 BA 34 B4 A4 CD BB 29 DC 68 42 0A 9F E6 67 4C 5A 3A 74 00 00 01 91 21 9F B2 1C 00 00 04 03 00 47 30 45 02 21 00 E4 48 C7 9D 04 5A 79 0D BB 59 F6 44 5E 86 0E 10 EA 9E 87 E1 26 F4 BF 02 57 3C 92 1B 8A 80 86

	65 02 20 29 EA 82 09 CC D2 70 51 55 93 4F DB B8 9D 49 5C 4B 63 D6 6C 51 BA EB 34 67 32 44 0C 24 B4 A8 4B 00 75 00 3F 17 4B 4F D7 22 47 58 94 1D 65 1C 84 BE 0D 12 ED 90 37 7F 1F 85 6A EB C1 BF 28 85 EC F8 64 6E 00 00 01 91 21 9F B2 00 00 00 04 03 00 46 30 44 02 20 39 0D AE 95 6B 8A E9 3B BF 47 B0 43 B6 99 F9 13 AD 56 E7 65 1C E2 8F 4E AA 6F A7 9D 1D 0A E2 1C 02 20 11 23 E6 34 6C 00 EA 39 A4 57 15 4D 73 FE 68 79 FF 3F BD 01 F7 7F 20 06 BC 3A B1 31 12 40 D1 71
Key usage	Digital Signature (80)
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Thumbprint	e5f57667a7f7fe5fbf24ede29a3c07640e7074aa

LinkedIn:

Version	V3
Serial Number	05:C4:5C:6F:DD:E1:08:9D:4C:DB:62:6E:F7:0D:EE:E1
Certificate Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Issuer	CN = DigiCert SHA2 Secure Server CA O = DigiCert Inc C = US
Valid From	8/27/24, 5:30:00 AM GMT+5:30
Valid To	2/28/25, 5:29:59 AM GMT+5:30
Subject	CN = www.linkedin.com O = LinkedIn Corporation L = Sunnyvale ST = California C = US
Subject Public Key Algorithm	PKCS #1 RSA Encryption
Subject's Public Key	Modulus (2048 bits): C0 AF 8D 9D 4B E4 C2 10 96 CA D3 A4 5E F9 41 00 61 E9 80 E2 4A A1 8A E9 47 77 3D 9C B0 FC 03 CC C4 A5 0F 0D 1F 26 63 53 C3 65 D0 14 FB 6C CB 86 72 7E 9D 67 B5 11 5E B5 BF 67 FD D8 02 52 19 43 82 58 10 D3 48 F6 3D 35 2B 9E C8 0A A8 11 0D C4 2F 0D AB 89 DB FF B4 E5 C3 9A B8 CE BF AD 1D E4 52 D2 94 95 A6 CE CC DE 0D FA CC 02 9B CF E2 03 B2 C1 30 98 20 09 D0 65 B5 8E F9 44 AF BA 08 26 07 D8 08 5F C4 E2 AF 1C 9C 16 7E D7 DA A2 B9 FE 1C 82 42 00 B6 52 31 A7 86 7B 2D 45 F6 C3 F5 06 92 28 3E A3 D1 24 F6 1D 47 54 B0 DB 8B 5B BE 06 95 97 20 44 15 28 B7 74 A9 4C 0C 8B E9 6B AE C9 F4 C2 F1 92 95 F8 C6 83 D9 64 9C D5 74 E7 2E C1 03 B5 4C 98 7D 41 0D A6 A8 CB 92 F1 EE 0E 2F 97 5B DD FD 44 FD 7B DD 36 E1 68 B7 62 FD 58 FF 55 17 DB 5C 89 6F 60 84 D3 B1 9E DE 17 43 F9 1B 71 Public Exponent (17 bits): 01 00 01
Certification Authority Key Id	Key ID: 0F 80 61 1C 82 31 61 D5 2F 28 E7 8D 46 38 B4 2C E1 C6 D9 E2
Certificate Subject Key Id	Key ID: 30 F2 B1 C8 27 1A 9D 1F 31 9D AE 5B CC 3F FA B6 28 6E DC 5E
Certificate Subject Alternative Name	DNS Name=www.linkedin.com DNS Name=linkedin.com

	DNS Name=rum5.perf.linkedin.com DNS Name=exp4.www.linkedin.com DNS Name=exp3.www.linkedin.com DNS Name=exp2.www.linkedin.com DNS Name=exp1.www.linkedin.com DNS Name=rum2.perf.linkedin.com DNS Name=rum4.perf.linkedin.com DNS Name=rum6.perf.linkedin.com DNS Name=rum17.perf.linkedin.com DNS Name=rum8.perf.linkedin.com DNS Name=rum9.perf.linkedin.com DNS Name=afd.perf.linkedin.com DNS Name=rum14.perf.linkedin.com DNS Name=rum18.perf.linkedin.com DNS Name=rum19.perf.linkedin.com DNS Name=exp5.www.linkedin.com DNS Name=realtime.www.linkedin.com DNS Name=px.ads.linkedin.com DNS Name=px4.ads.linkedin.com DNS Name=dc.ads.linkedin.com DNS Name=lnkd.in DNS Name=px.jobs.linkedin.com DNS Name=mid4.linkedin.com DNS Name=lan.sdk.linkedin.com DNS Name=www.linkedin-measure.com DNS Name=status.linkedin.com DNS Name=payment.www.linkedin.com DNS Name=afd-wcs.www.linkedin.com
Certificate Policies	OID.2.23.140.1.2.2: Certification Practice Statement Pointer: http://www.digicert.com/CPS
Certificate Key Usage	Signing Key Encipherment
Extended Key Usage	TLS WWW Server Authentication (OID.1.3.6.1.5.5.7.3.1) TLS WWW Client Authentication (OID.1.3.6.1.5.5.7.3.2)
CRL Distribution Points	URI: http://crl3.digicert.com/DigicertSHA2SecureServerCA-1.crl URI: http://crl4.digicert.com/DigicertSHA2SecureServerCA-1.crl
Authority Information Access	OCSP Responder: URI: http://ocsp.digicert.com CA Issuers: URI: http://cacerts.digicert.com/DigiCertSHA2SecureServerCA-2.crt
Basic Constraints	Is not a Certification Authority
Signed Certificate Timestamp List	04 82 01 69 01 67 00 75 00 4E 75 A3 27 5C 9A 10 C3 38 5B 6C D4 DF 3F 52 EB 1D F0 E0 8E 1B 8D 69 C0 B1 FA 64 B1 62 9A 39 DF 00 00 01 91 94 A5 E6 B7 00 00 04 03 00 46 30 44 02 20 2E 89 6E A1 D7 36 56 B7 5E 76 6D 23 6D 23 C7 92 26 C5 F1 88 DB 98 53 48 5C F4 0E A5 E8 5C E2 4E 02 20 50 E3 7A 77 A4 DB ED 25 4A DD 91 B0 16 9C 59 82 32 61 FF B0 34 2E FC 1D 7A 51 77 81 2F 3E 62 C7 00 75 00 E6 D2 31 63 40 77 8C C1 10 41 06 D7 71 B9 CE C1 D2 40 F6 96 84 86 FB BA 87 32 1D FD 1E 37 8E 50 00 00 01 91 94 A5 E6 77 00 00 04 03 00 46 30 44 02 20 55 0D 03 E8 73 54 14 43 1A 79 17 8B 9B 67 28 8F 9D C7 3C A6 84 5F 6E 8E 38 7D 1E 6C 25 DC CA 68 02 20 68 F5 9A 69 00 16 CB 87 D2 85 E9 DC 94 9B 16 39 F8 63 3B 0D 60 B0 A2 3D E0 EE C3 48 3D 32 E0 10 00 77 00 CC FB 0F 6A 85 71 09 65 FE 95 9B 53 CE E9 B2 7C 22 E9 85 5C 0D 97 8D B6 A9 7E 54

	C0 FE 4C 0D B0 00 00 01 91 94 A5 E6 86 00 00 04 03 00 48 30 46 02 21 00 D8 BC 7A B3 48 EC 74 90 EE 2C 4E A1 CD 04 F4 5B 5A 91 70 D4 BE 23 BA 07 58 CE 10 89 CA FB D0 26 02 21 00 D3 95 AB 59 58 2F 5B 43 AA F5 2F 51 57 DA 20 3A 8A 1D 09 0A 73 11 5C 95 E5 8C CC 99 31 8D 68 82
Certificate Signature Algorithm	PKCS #1 SHA-256 With RSA Encryption
Certificate Signature Value	0F 76 15 47 86 5D D6 6A FD 35 1A FD 21 80 90 4B 1A 70 1B 62 F9 75 87 73 4E C8 5E 09 05 AE 0C A1 00 8C A5 58 5F E1 31 52 A8 B0 7F 1F 3E 2C 1B 19 D3 67 4E 2B 57 C4 95 BB 10 35 BD B9 66 6F 51 CD B8 42 88 7B 5E D1 49 8D 66 9D C5 66 34 22 DB 54 4E C0 90 60 1A 96 48 1D 85 FE FD A9 88 71 A9 CB CD E5 D8 6A A5 1D 14 E0 8F AC C2 AE F7 8E 31 B7 4F 76 E9 D4 C1 1A 32 09 8E 3F BB F5 7A DF 06 0B E4 99 7E 63 2A DF 56 B7 5C A3 B1 7F 7A EA 17 77 D5 9A 05 ED 2D 87 45 0B 4B 1F 95 10 C3 A6 FC 1F C1 BB 44 98 E4 28 E5 D5 6B 36 1D 48 DF A3 3F C0 EC 4A 08 B3 6A 07 E4 24 B4 47 07 AB 92 E1 40 89 0C 0A C9 B0 62 A6 EF D3 1D EF 35 85 C1 B0 30 C4 2C 39 F7 38 87 41 C3 96 0F 9B A6 72 9F 8D 55 DD 9F 16 8A D4 2C AB 29 B0 82 D7 BA ED 3F 46 B6 EA 96 08 D1 67 42 F7 DA 80 01 38 CE BD FD 9F FF 52
SHA256 fingerprint: Certificate	3c908b466a14ae2c125d86598a6c52f6b8bb702522187765e89f3ec331fc5a44
SHA256 fingerprint: Public Key	224ee6d54c9fff29c16f8013595f59ec3e27fd277d0678486af8ae69e6f9a596

GitHub:

Version	V3
Serial Number	4E:28:F7:86:B6:6C:1A:3B:94:2C:D2:C4:0E:B7:42:A5
Certificate Signature Algorithm	X9.62 ECDSA Signature with SHA-256
Issuer	CN = Sectigo ECC Domain Validation Secure Server CA O = Sectigo Limited L = Salford ST = Greater Manchester C = GB
Valid From	3/7/24, 5:30:00 AM GMT+5:30
Valid To	3/8/25, 5:29:59 AM GMT+5:30
Subject	CN = github.com
Subject Public Key Algorithm	Elliptic Curve Public Key
Subject's Public Key	00 04 04 4E FC 7A 3D 5D D9 18 D6 A8 7D 98 08 23 39 49 16 99 74 DB D3 98 E0 46 E9 4A 72 23 15 06 E2 81 DD 91 DE C6 F0 9D CA 88 82 44 71 0C 05 F1 57 A1 98 56 91 05 4C A2 03 4B A3 F9 56 DB 5E 57 DE 91
Certification Authority Key Id	Key ID: F6 85 0A 3B 11 86 E1 04 7D 0E AA 0B 2C D2 EE CC 64 7B 7B AE
Certificate Subject Key Id	Key ID: 3B 68 3F 34 3A F5 47 34 CA EF A6 4E 3D 9A BD 5E 6E 7A CC 9F

Certificate Subject Alternative Name	DNS Name: github.com DNS Name: www.github.com
Certificate Policies	OID.1.3.6.1.4.1.6449.1.2.2.7: Certification Practice Statement Pointer: https://sectigo.com/CPS OID.2.23.140.1.2.1
Certificate Key Usage	Signing
Extended Key Usage	TLS WWW Server Authentication (OID.1.3.6.1.5.5.7.3.1) TLS WWW Client Authentication (OID.1.3.6.1.5.5.7.3.2)
Authority Information Access	CA Issuers: URI: http://crt.sectigo.com/SectigoECCDomainValidationSecureServerCA.crt OCSP Responder: URI: http://ocsp.sectigo.com
Basic Constraints	Is not a Certification Authority
Signed Certificate Timestamp List	04 82 01 6C 01 6A 00 77 00 CF 11 56 EE D5 2E 7C AF F3 87 5B D9 69 2E 9B E9 1A 71 67 4A B0 17 EC AC 01 D2 5B 77 CE CC 3B 08 00 00 01 8E 16 3A F0 19 00 00 04 03 00 48 30 46 02 21 00 FB A0 DC FF DA 83 BC 54 66 96 5A BA AB B0 14 01 CD 01 F4 85 18 4C 2E 6D 75 A1 E3 29 83 57 CD 6B 02 21 00 A5 9C D2 AE D9 FA 6C 43 55 85 7F EA 8B FB 7F F8 B4 1F F6 80 70 74 82 22 2F D0 25 C1 02 AD A3 A9 00 76 00 A2 E3 0A E4 45 EF BD AD 9B 7E 38 ED 47 67 77 53 D7 82 5B 84 94 D7 2B 5E 1B 2C C4 B9 50 A4 47 E7 00 00 01 8E 16 3A EF F8 00 00 04 03 00 47 30 45 02 21 00 CA EA 44 21 50 0C 93 47 3C 05 55 69 17 44 1B 8A C7 E8 13 0C B9 C4 94 0A 40 E7 BC 12 F3 14 E1 6F 02 20 60 08 22 EC E3 C4 11 65 1E 99 2A 72 C6 BB 51 9C B6 E3 2F C1 EB 16 67 92 D5 30 FC D7 B9 AB 98 42 00 77 00 4E 75 A3 27 5C 9A 10 C3 38 5B 6C D4 DF 3F 52 EB 1D F0 E0 8E 1B 8D 69 C0 B1 FA 64 B1 62 9A 39 DF 00 00 01 8E 16 3A EF F7 00 00 04 03 00 48 30 46 02 21 00 FB C3 AF 43 3A 60 45 FD F5 B8 B0 6C 08 4F 24 B4 25 1F BE C8 91 4F BC D6 4A A7 97 96 20 34 F5 35 02 21 00 DC 07 B5 E7 F7 B6 84 0C C0 4A 5C 86 DD 9B 92 99 F4 68 EF 47 2A 05 F6 C9 03 E7 FE 06 9D EA 0C 5B
Certificate Signature Algorithm	X9.62 ECDSA Signature with SHA-256
Certificate Signature Value	30 45 02 21 00 AE ED 8C 70 FA F4 78 DC 1C 58 DB 83 11 8D 1A FE B1 B3 5D 17 D1 AE 6F BA 5D F6 5E 4B 38 58 65 EC 02 20 1A B8 4D 41 01 0A 06 A9 BF BC 6F 02 D4 4A 75 57 62 FD BE 26 DF A5 32 7A 3D 60 83 22 6C 89 EB 00
SHA256 fingerprint: Certificate	fd6e9b0ef398bcd904c3b2ec167a7b0fda7201c903c53a6a6ae5d0414363ef65
SHA256 fingerprint: Public Key	1acf9d4fd9140b5ee70d86571f9da62b31a795453f439992d14aee4d05b71f45

Certificate Details Explained

Certificates contain various pieces of information, some of which are listed below:

1. **Version:** The version of the X.509 standard that the certificate adheres to. Most certificates are version 3.
2. **Serial Number:** A unique identifier assigned by the certificate authority (CA) that issued the certificate.
3. **Signature Algorithm:** The algorithm used to sign the certificate, such as sha256RSA.
4. **Issuer:** The entity (Certificate Authority) that issued the certificate. This includes information like the organization's name and location.
5. **Validity Period:**
    - **Not Before:** The start date when the certificate is valid.
    - **Not After:** The expiration date when the certificate is no longer valid.
6. **Subject:** The entity to whom the certificate was issued. This usually includes the common name (CN), which is the domain name of the website, and other organizational details.
7. **Subject Public Key Information:**
    - **Public Key Algorithm:** The algorithm used for the public key (e.g., RSA).
    - **Public-Key:** The actual public key.
8. **Extensions:**
    - **Key Usage:** Specifies the purpose of the public key (e.g., digital signature, key encipherment).
    - **Subject Alternative Name (SAN):** Lists alternative domain names for which the certificate is also valid.
    - **Extended Key Usage:** Specifies further purposes (e.g., server authentication, client authentication).
    - **Basic Constraints:** Indicates whether the certificate is a CA certificate or an end- entity certificate.
    - **CRL Distribution Points:** URLs where the certificate revocation list (CRL) can be checked.
9. **Signature:** The digital signature of the certificate, used to verify its authenticity.