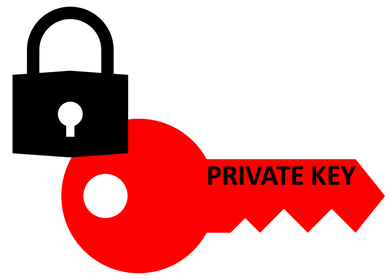
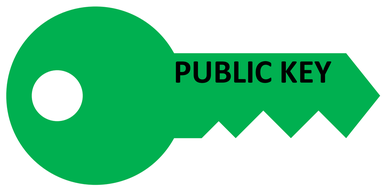
Decryption Using Private Key == Verification

Encrypt Using Private Key == Signature





The client performs a chain of trust verification by checking each certificate in the chain, starting from the server's certificate and moving up to the root certificate. It ensures that each certificate is valid and has not expired. Because the Intermediate was signed with the Root CA and we have the Root preinstalled in our trusted certificates we will trust anything the intermediate CA signs

INTERMEDIATE
PUBLIC KEY EXPONENT
SHA-256 HASH of Certificate Info
MODULUS #

The recipient of the Certificate will use the public key of the sender to decrypt the HASH.

The recipient will HASH the certificates data and compare the HASH to the decrypted HASH to verify the authenticity of the certificate.

The Info for the Child Certificate will include information of the parent

INTERMEDIATE
PUBLIC KEY EXPONENT
SHA-256 HASH of Certificate Info
MODULUS #

The recipient of the Certificate will use the public key of the sender to decrypt the HASH aka Verify the HASH.

The recipient will HASH the certificates data and compare the HASH to the decrypted HASH to verify the authenticity of the certificate.

The Info for the Child Certificate will include information of the parent

ROOT PUBLIC
KEY EXPONENT
SHA-256 HASH of Certificate Info
MODULUS #

Client

DIGITAL CERTIFICATE

Subject Name
Common Name: *.google.com

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS CA 1c3

FINGERPRINT
SHA-256: EB:D4:10:40:E4:BB:3E:C7:42:C9:E3:81:D3:1E:F2:A4:1A:48:B6:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:99
SHA-1: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:0E:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:68:EA:48:1F:F1:2A:B0:4B:D0:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:2D:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:D5:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:88:6C:89:CC:98:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96:

SERVER

DIGITAL CERTIFICATE

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS CA 1c3

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:0E:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:68:EA:48:1F:F1:2A:B0:4B:D0:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:2D:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:D5:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:88:6C:89:CC:98:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96

Encrypted HASH signature Using Private key
EB:D4:10:40:E4:BB:3E:C7:42:C9:E3:81:D3:1E:F2:A4:1A:48:B6:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:9
DA:0E:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:68:EA:48:1F:F1:2A:B0:4B:D0:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:2D:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:D4:8C:50:15:1C:EF:50:EE:C4:2E:F7

The Certificate Data will get HASHED using any one of the hashing algorithms. That HASH is then encrypted with the private key of the certificates owner.

SERVER
PRIVATE KEY EXPONENT
SHA-256 HASH of Certificate Info
MODULUS #

DIGITAL CERTIFICATE

Subject Name
Common Name: *.google.com

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS CA 1c3

FINGERPRINT
SHA-256: EB:D4:10:40:E4:BB:3E:C7:42:C9:E3:81:D3:1E:F2:A4:1A:48:B6:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:99
SHA-1: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:0E:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:68:EA:48:1F:F1:2A:B0:4B:D0:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:2D:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:D5:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:88:6C:89:CC:98:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96:

Intermediate Certificate Authority

DIGITAL CERTIFICATE

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS CA 1c3

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:0E:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:68:EA:48:1F:F1:2A:B0:4B:D0:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:2D:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:D5:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:88:6C:89:CC:98:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96:

Encrypted HASH signature Using Private key
EB:D4:10:40:E4:BB:3E:C7:42:C9:E3:81:D3:1E:F2:A4:1A:48:B6:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:9
DA:0E:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:68:EA:48:1F:F1:2A:B0:4B:D0:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:2D:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:D4:8C:50:15:1C:EF:50:EE:C4:2E:F7

The Certificate Data will get HASHED using any one of the hashing algorithms. That HASH is then encrypted with the private key of the certificates owner.

INTERMEDIATE
PRIVATE KEY EXPONENT
SHA-256 HASH of Certificate Info
MODULUS #

DIGITAL CERTIFICATE

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS Root R1

FINGERPRINT
SHA-256: EB:D4:10:40:E4:BB:3E:C7:42:C9:E3:81:D3:1E:F2:A4:1A:48:B6:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:99
SHA-1: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:0E:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:68:EA:48:1F:F1:2A:B0:4B:D0:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:2D:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:D5:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:88:6C:89:CC:98:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96:

ROOT Certificate Authority

DIGITAL CERTIFICATE

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS CA 1c3

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:0E:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:68:EA:48:1F:F1:2A:B0:4B:D0:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:2D:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:D5:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:88:6C:89:CC:98:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96:

Encrypted HASH signature Using Private key
EB:D4:10:40:E4:BB:3E:C7:42:C9:E3:81:D3:1E:F2:A4:1A:48:B6:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:9
DA:0E:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:68:EA:48:1F:F1:2A:B0:4B:D0:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:2D:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:D4:8C:50:15:1C:EF:50:EE:C4:2E:F7

The Certificate Data will get HASHED using any one of the hashing algorithms. That HASH is then encrypted with the private key of the certificates owner.

ROOT PRIVATE KEY
EXPONENT
SHA-256 HASH of Certificate Info
MODULUS #

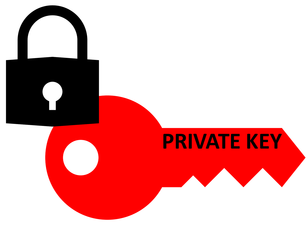
DIGITAL CERTIFICATE

ISSUER NAME
Country: BE
Organization: GlobalSign nv-sa
Organizational Unit Root: CA
Common Name: GlobalSign Root CA

FINGERPRINT
SHA-256: EB:D4:10:40:E4:BB:3E:C7:42:C9:E3:81:D3:1E:F2:A4:1A:48:B6:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:99
SHA-1: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:0E:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:68:EA:48:1F:F1:2A:B0:4B:D0:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:2D:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:D5:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:88:6C:89:CC:98:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96:

Encrypt Using Private Key == Signature



Client

DIGITAL CERTIFICATE

Subject Name
Common Name: *.google.com

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS CA 1c3

FINGERPRINT
SHA-256: E8:04:10:40:E4:88:3E:C7:42:C9:E3:81:03:1E:F2:A4:1A:48:86:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:99
SHA-1: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:DE:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:B0:4D:F0:63:D1:E2:67:66:CF:1C:DD:C
F:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:20:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:
D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:05:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:
3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:B8:6C:89:CC:9B:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96

Encrypted HASH signature Using Private key
EB:04:10:40:E4:88:3E:C7:42:C9:E3:81:03:1E:F2:A4:1A:48:86:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:9
DA:DE:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:B04:8D:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:20:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:04:8C:50:15:1C:EF:50:EE:C4:2E:F7

SERVER

DIGITAL CERTIFICATE

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS CA 1c3

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:DE:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:B04:8D:F0:63:D1:E2:67:66:CF:1C:DD:C
F:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:20:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:
D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:05:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:
3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:B8:6C:89:CC:9B:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96

Encrypted HASH signature Using Private key
EB:04:10:40:E4:88:3E:C7:42:C9:E3:81:03:1E:F2:A4:1A:48:86:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:9
DA:DE:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:B04:8D:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:20:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:04:8C:50:15:1C:EF:50:EE:C4:2E:F7

The Certificate Data will get HASHED using any one of the hashing algorithms. That HASH is then encrypted with the private key of the certificates owner.

DIGITAL CERTIFICATE

Subject Name
Common Name: *.google.com

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS CA 1c3

FINGERPRINT
SHA-256: E8:04:10:40:E4:88:3E:C7:42:C9:E3:81:03:1E:F2:A4:1A:48:86:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:99
SHA-1: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:DE:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:B04:8D:F0:63:D1:E2:67:66:CF:1C:DD:C
F:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:20:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:
D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:05:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:
3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:B8:6C:89:CC:9B:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96

SERVER PRIVATE KEY EXPONENT
SHA-256 HASH of Certificate Info
MODULUS #

Intermediate Certificate Authority

The Certificate Data will get HASHED using any one of the hashing algorithms. That HASH is then encrypted with the private key of the certificates owner.

DIGITAL CERTIFICATE

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS CA 1c3

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:DE:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:B04:8D:F0:63:D1:E2:67:66:CF:1C:DD:C
F:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:20:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:
D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:05:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:
3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:B8:6C:89:CC:9B:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96

Encrypted HASH signature Using Private key
EB:04:10:40:E4:88:3E:C7:42:C9:E3:81:03:1E:F2:A4:1A:48:86:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:9
DA:DE:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:B04:8D:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:20:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:04:8C:50:15:1C:EF:50:EE:C4:2E:F7

DIGITAL CERTIFICATE

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS Root R1

FINGERPRINT
SHA-256: E8:04:10:40:E4:88:3E:C7:42:C9:E3:81:03:1E:F2:A4:1A:48:86:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:99
SHA-1: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:DE:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:B04:8D:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:20:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:04:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:05:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:B8:6C:89:CC:9B:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96

INTERMEDIATE PRIVATE KEY EXPONENT
SHA-256 HASH of Certificate Info
MODULUS #

ROOT Certificate Authority

The Certificate Data will get HASHED using any one of the hashing algorithms. That HASH is then encrypted with the private key of the certificates owner.

DIGITAL CERTIFICATE

ISSUER NAME
Country: US
Organization: Google Trust Services LLC
Common Name: GTS CA 1c3

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:DE:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:B04:8D:F0:63:D1:E2:67:66:CF:1C:DD:C
F:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:20:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:
D4:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:05:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:
3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:B8:6C:89:CC:9B:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96

Encrypted HASH signature Using Private key
EB:04:10:40:E4:88:3E:C7:42:C9:E3:81:03:1E:F2:A4:1A:48:86:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:9
DA:DE:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:B04:8D:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:20:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:04:8C:50:15:1C:EF:50:EE:C4:2E:F7

DIGITAL CERTIFICATE

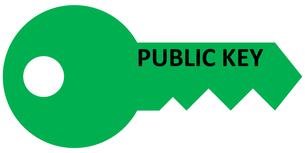
ISSUER NAME
Country: BE
Organization: GlobalSign nv-sa
Organizational Unit Root: CA
Common Name: GlobalSign Root CA

FINGERPRINT
SHA-256: EB:04:10:40:E4:88:3E:C7:42:C9:E3:81:03:1E:F2:A4:1A:48:86:68:5C:96:E7:CE:F3:C1:DF:6C:D4:33:1C:99
SHA-1: B1:BC:96:8B:D4:F4:9D:62:2A:A8:9A:81:F2:15:01:52:A4:1D:82:9C

PUBLIC KEY INFO
Algorithm: RSA
Key Size: 2048
Exponent: 65537
Modulus:
DA:DE:E6:99:8D:CE:A3:E3:4F:8A:7E:FB:F1:8B:83:25:6B:EA:48:1F:F1:2A:B04:8D:F0:63:D1:E2:67:66:CF:1C:DD:CF:1B:48:2B:EE:8D:89:8E:9A:AF:29:80:65:AB:E9:C7:20:12:CB:AB:1C:4C:70:07:A1:3D:0A:30:CD:15:8D:4F:F8:DD:04:8C:50:15:1C:EF:50:EE:C4:2E:F7:FC:E9:52:F2:91:7D:E0:6D:05:35:30:8E:5E:43:73:F2:41:E9:D5:6A:E3:82:89:3A:56:39:38:6F:06:3C:88:69:5B:2A:4D:C5:A7:54:B8:6C:89:CC:9B:F9:3C:CA:E5:FD:89:F5:12:3C:92:78:96

ROOT PRIVATE KEY EXPONENT
SHA-256 HASH of Certificate Info
MODULUS #

Decryption Using Private Key == Verification



The client performs a chain of trust verification by checking each certificate in the chain, starting from the server's certificate and moving up to the root certificate. It ensures that each certificate is valid and has not expired. Because the Intermediate was signed with the Root CA and we have the Root preinstalled in our trusted certificates we will trust anything the intermediate CA signs

INTERMEDIATE PUBLIC KEY EXPONENT
SHA-256 HASH of Certificate Info

MODULUS #

The recipient of the Certificate will use the public key of the sender to decrypt the HASH.

The recipient will HASH the certificates data and compare the HASH to the decrypted HASH to verify the authenticity of the certificate.

The Info for the Child Certificate will include information of the parent

INTERMEDIATE PUBLIC KEY EXPONENT
SHA-256 HASH of Certificate Info

MODULUS #

The recipient of the Certificate will use the public key of the sender to decrypt the HASH.

The recipient will HASH the certificates data and compare the HASH to the decrypted HASH to verify the authenticity of the certificate.

The Info for the Child Certificate will include information of the parent

ROOT PUBLIC KEY EXPONENT
SHA-256 HASH of Certificate Info

MODULUS #

Client

SERVER

Intermediate Certificate Authority

ROOT Certificate Authority