Secure Communication

USABILITY AND NECESSITY OF SSL / TLS

We're going to talk about:

1. **Why** is this important?
2. **What** is SSL?
3. **Where** is SSL being used?
4. **Features**: What to look for in an SSL library?

Why is This Important?

- Number of connected devices is ever increasing

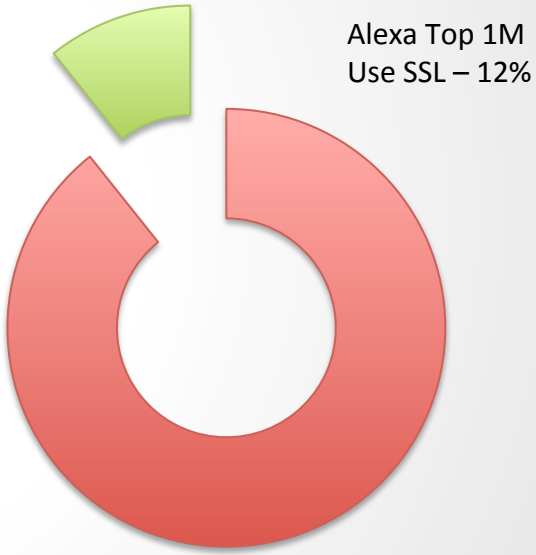
- Frequent Road-blocks:
  - Lack of understanding
  - Insufficient funding
  - Tight deadlines

Why is This Important?

Ivan Ristic: Internet SSL Survey 2010
http://www.ssllabs.com

- Alexa Top 1M Sites

  120,000 Use SSL (12%)



What is SSL?

X509, Encryption, handshakes, and more.

yaSSL

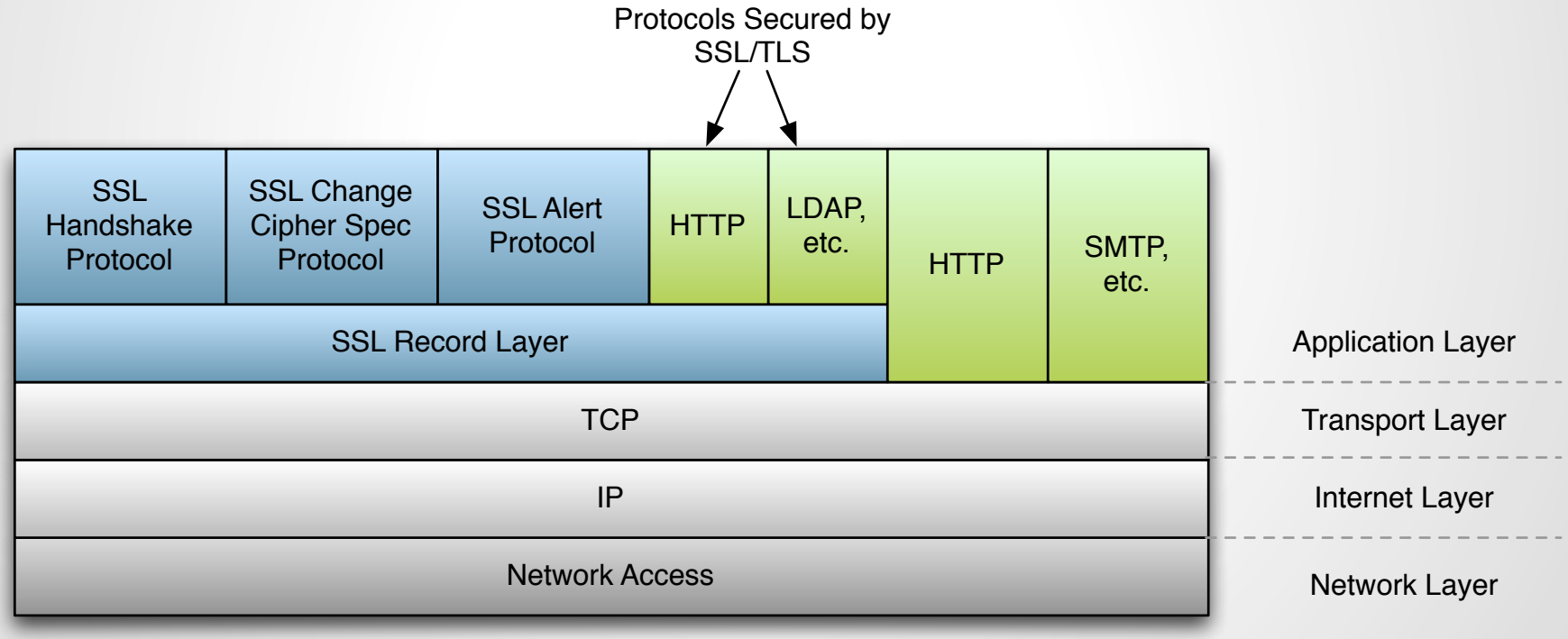
What is SSL?

- Enables secure client / server communication, providing:

Privacy	+ Prevent eavesdropping
Authentication	+ Prevent impersonation
Integrity	+ Prevent modification

Where does SSL fit?

- Layered between **Transport** and **Application** layers



SSL: Authentication

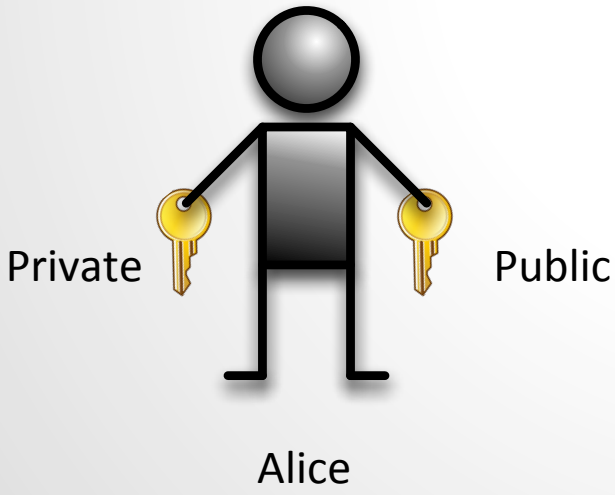
- Do you really know who you're communicating with?

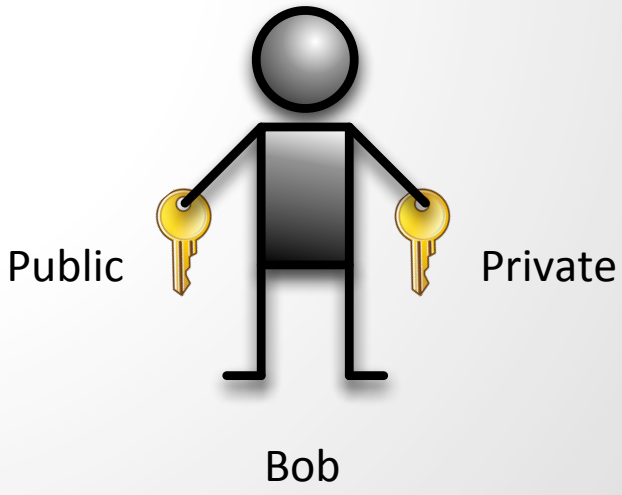
Alice

Bob

SSL: Authentication

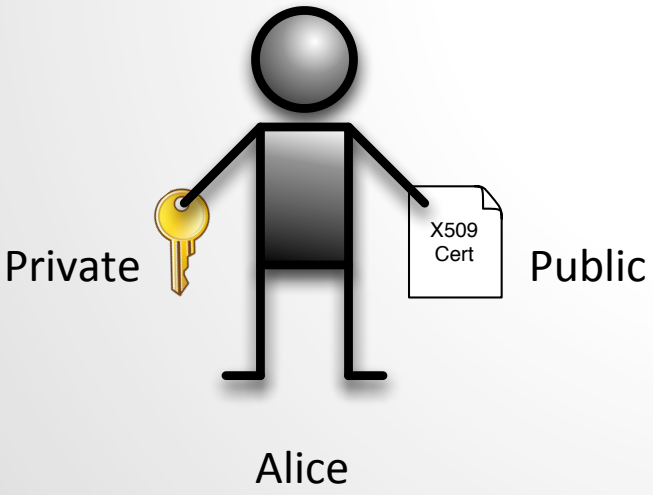
- Generate a key pair (private and public key)

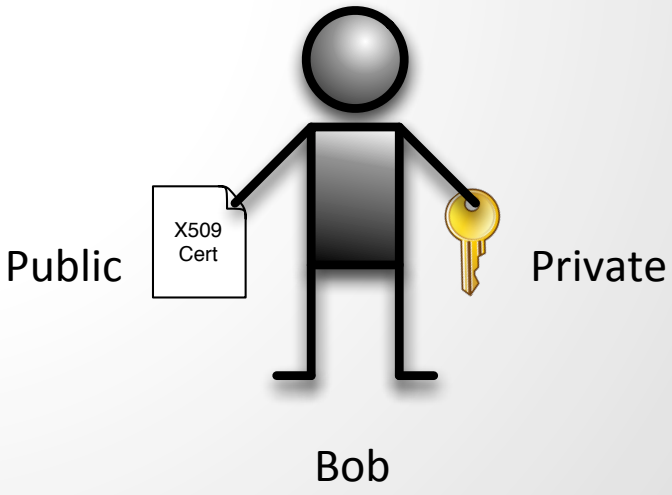




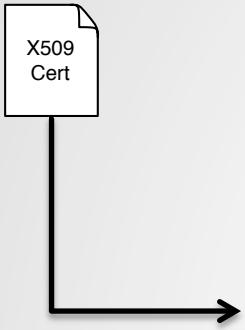
SSL: Authentication

- X.509 Certificate == Wrapper around public key





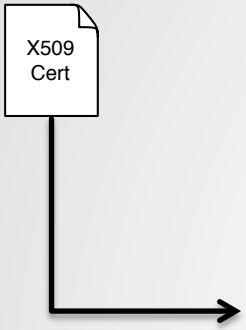
SSL: X.509 Certificates




```
-----BEGIN CERTIFICATE-----
MIIEmDCCA4CgAwIBAgIJAIdKdb6RZtg9MA0GCSqGSIb3DQEBBQUAMIGOMQswCQYD
VQQGEwJVUzEPMA0GA1UECBMGT3JlZ29uMREwDwYDVQQHEwhQb3J0bGFuZDEOMAwG
A1UEChMFeWFTU0wxFDASBgNVBAsTC1Byb2dyYW1taW5nMRYwFAYDVQQDEw13d3cu
eWFzc2wuY29tMR0wGwYJKoZIhvcNAQkBFg5pbmZvQHlhc3NsLmNvbTAeFw0xMTEw
MjQxODIxNTVaFw0xNDA3MjAxODIxNTVaMIGOMQswCQYDVQQGEwJVUzEPMA0GA1UE
CBMGT3JlZ29uMREwDwYDVQQHEwhQb3J0bGFuZDEOMAwGA1UEChMFeWFTU0wxFDAS
BgNVBAsTC1Byb2dyYW1taW5nMRYwFAYDVQQDEw13d3cueWFzc2wuY29tMR0wGwYJ
KoZIhvcNAQkBFg5pbmZvQHlhc3NsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAMMD0Sv+OaQyRTtTyIQrKnx0mr2qKlIHR9amNrIHMo7Quml7xsNE
ntSBSP0taKKLZ7uhdcg2LErSG/eLus8N+e/s8YEee5sDR5q/Zcx/ZSRppugUiVvk
NPfFsBST9Wd7Onp44QFWVpGmE0KN0jxAnEzv0YbfN1EbDKE79fGjSjXk4c6W3xt+
v06X0BDoqAgwga8gC0MUxXRntDKCb42GwohAmTaDuh5AciIX11JlJHOwzu8Zza7/
eGx7wBID1E5yDVBtO6M7o5lencjZDIWz2YrZVCbbbfqsu/8lTMTRefRx04ZAGBOw
Y7VyTjDEl4SGLVYv1xX3f8Cu9fxb5fuhutMCAwEAAaOB9jCB8zAdBgNVHQ4EFgQU
M9hFZtdohxh+VA1wJ5HHJteFZcAwgcMGA1UdIwSBuzCBuIAUM9hFZtdohxh+VA1w
J5HHJteFZcChgZSkgZEwgY4xCzAJBgNVBAYTAlVTMQ8wDQYDVQQIEwZPcmVnb24x
ETAPBgNVBAcTCFBvcnRsYW5kMQ4wDAYDVQQKEwV5YVNTTDEUMBIGA1UECxMLUHJv
Z3JhbW1pbmcxFjAUBgNVBAMTDXd3dy55YXNzbC5jb20xHTAbBgkqhkiG9w0BCQEW
DmluZm9AeWFzc2wuY29tggkAh0p1vpFm2D0wDAYDVR0TBAUwAwEB/zANBgkqhkiG
9w0BAQUFAAOCAQEAHHxCgSmeIc/Q2MFUb8yuFAk4/2iYmpVTdhh75jB27CgNdafe
4M2O1VUjakcrTo38fQaj2A+tXtYEyQAz+3cn07UDs3shdDELSq8tGrOTjszzXz2Q
P8zjVRmRe3gkLkoJuxhOYS2cxgqgNJGIcGs7SEe8eZSioE0yR1TCo9wu0lFMKTkR
/+IVXliXNvbpBgaGDo2dlQNysosZfOkUbqGIc2hYbXFewtXTE9Jf3uoDvuIAQOXO
/eaSMVfD67tmrMsvGvrgYqJH9JNDKktsXgov+efmSmOGsKwqoeu0W2fNMuS2EUua
cmYNokp2j/4ivIP927fVqe4FybFxfhsr4eOvwA==
-----END CERTIFICATE-----
```


yaSSL

SSL: X.509 Certificates



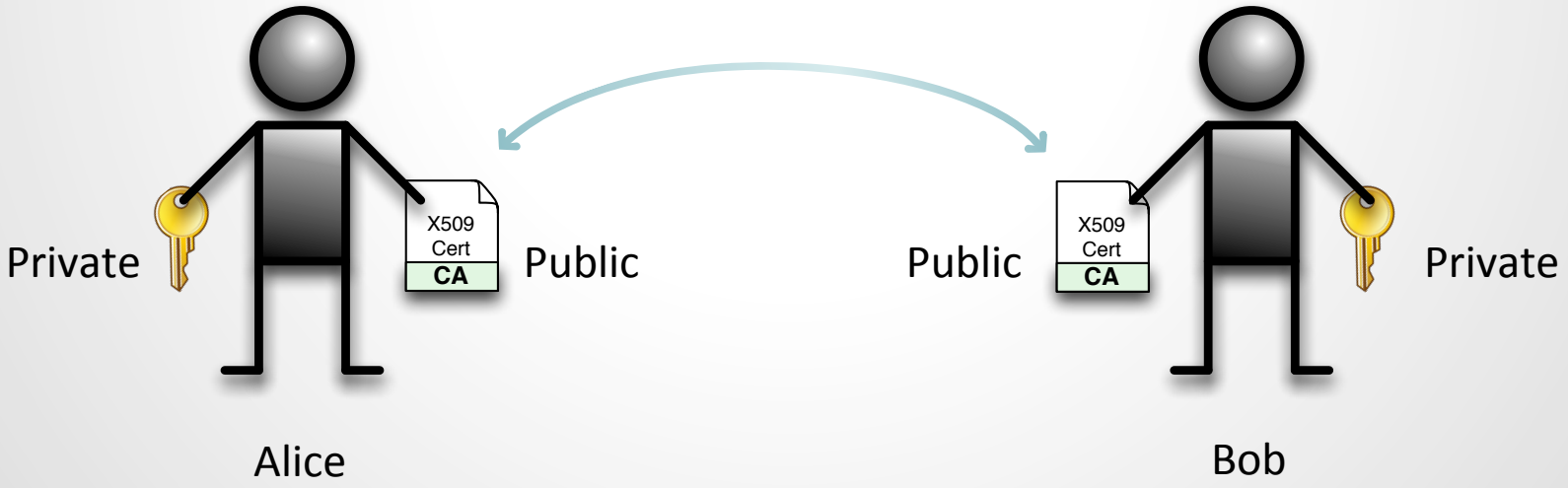

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            87:4a:75:be:91:66:d8:3d
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=Oregon, L=Portland, O=yaSSL, OU=Programming, CN=www.yassl.com/
emailAddress=info@yassl.com
        Validity
            Not Before: Oct 24 18:21:55 2011 GMT
            Not After : Jul 20 18:21:55 2014 GMT
        Subject: C=US, ST=Oregon, L=Portland, O=yaSSL, OU=Programming, CN=www.yassl.com/
emailAddress=info@yassl.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus: 00:c3:03:d1:2b:fe:39:a4 …
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                33:D8:45:66:D7:68:87:18:7E:54:0D:70:27:91:C7:26:D7:85:65:C0
            X509v3 Authority Key Identifier:
                keyid:33:D8:45:66:D7:68:87:18:7E:54:0D:70:27:91:C7:26:D7:85:65:C0
                DirName:/C=US/ST=Oregon/L=Portland/O=yaSSL/OU=Programming/CN=www.yassl.com/
emailAddress=info@yassl.com
                serial:87:4A:75:BE:91:66:D8:3D

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        … 1c:7c:42:81:29:9e:21:cf:d0:d8
```


yaSSL

SSL: Authentication

- Alice and Bob exchange **CA-signed** public keys



SSL: Authentication

- How do you get a CA-signed cert?

Buy

VeriSign, DigiCert, Comodo, etc.

- *Costs $$$*
- *Trusted*

Create

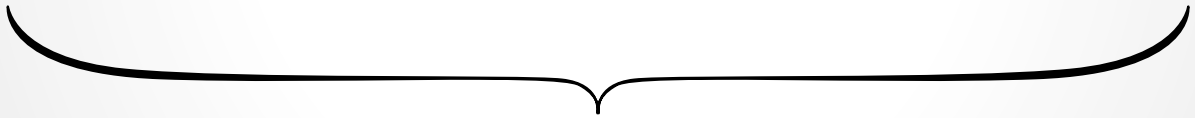
Created yourself (self-sign)

- *Free!*
- *Trusted (if you control both sides)*

SSL: Encryption

- Uses a variety of encryption algorithms to secure data

Hashing Functions	*MD4, MD5, SHA …*
Block and Stream Ciphers	*DES, 3DES, AES, ARC4 …*
Public Key Options	*RSA, DSS …*



CIPHER SUITE

yaSSL

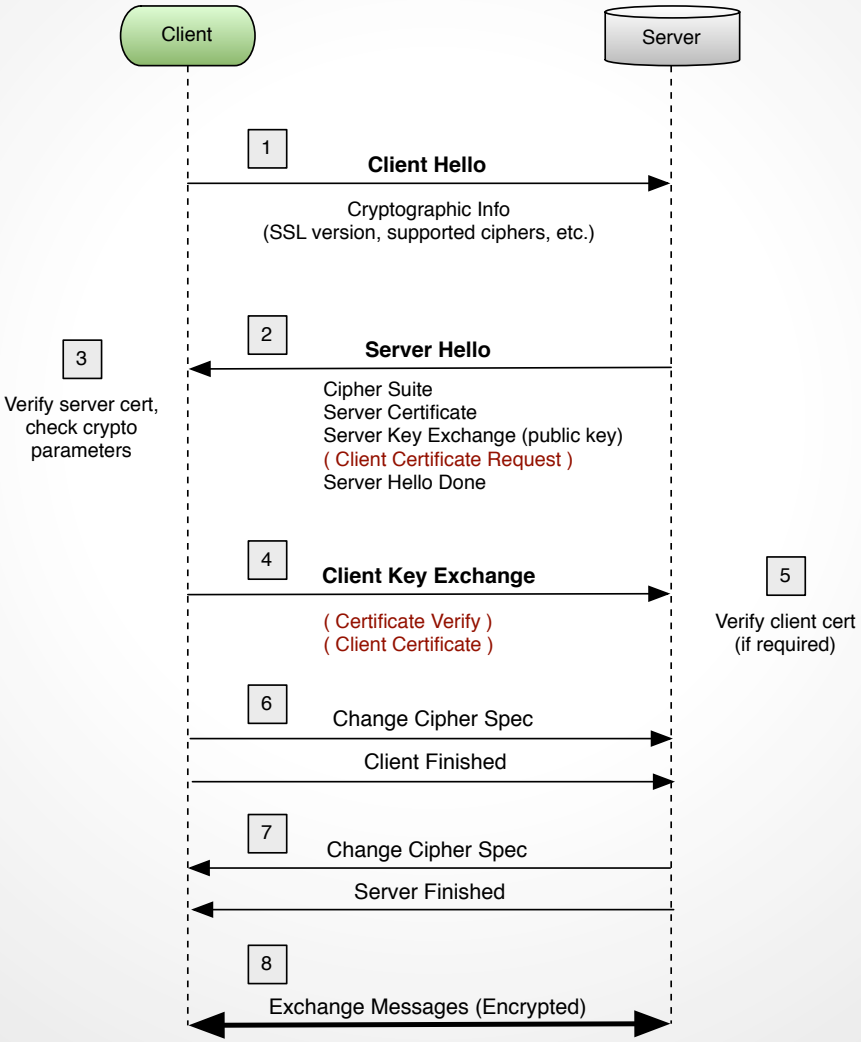
SSL: Encryption

- A common **CIPHER SUITE** is negotiated

Protocol_keyexchange_WITH_bulkencryption_mode_messageauth

SSL_RSA_WITH_DES_CBC_SHA
SSL_DHE_RSA_WITH_DES_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA

SSL: Handshake



Where is SSL used?

Everywhere!

SSL: Where is it used?

- Energy Monitoring
- Gaming
- Databases
- Sensors
- VoIP
- M2M communication
- And much more...

yaSSL

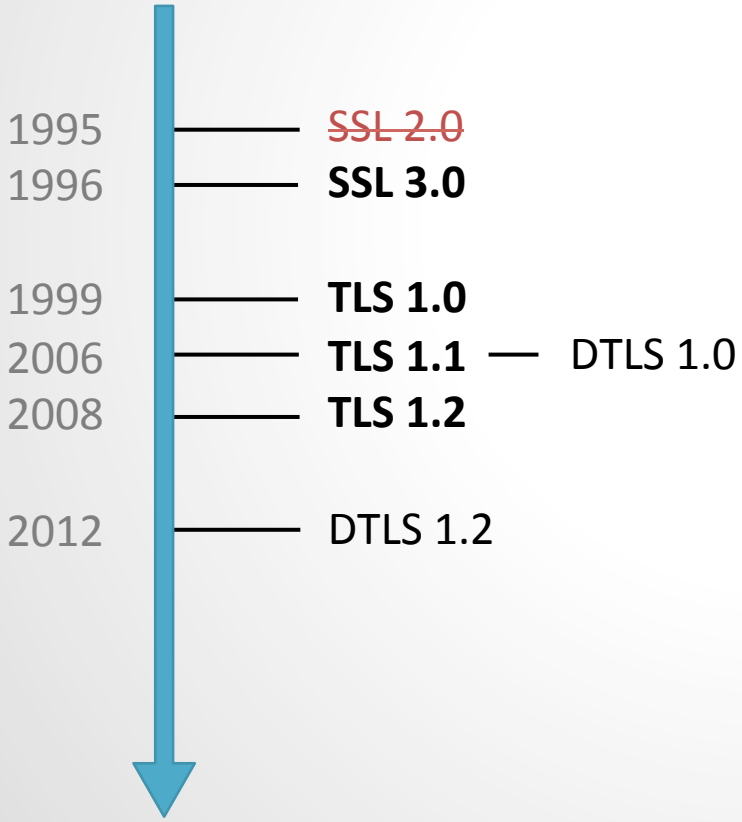
What to look for?

When shopping for an SSL stack.

yaSSL

1: Protocols

- Support for current protocols?



Notes:

- SSL 2.0 is insecure
- SSL = “Secure Sockets Layer”
- TLS = “Transport Layer Security”
- DTLS = “Datagram TLS”

2: Ciphers

- Support for needed cipher suites?

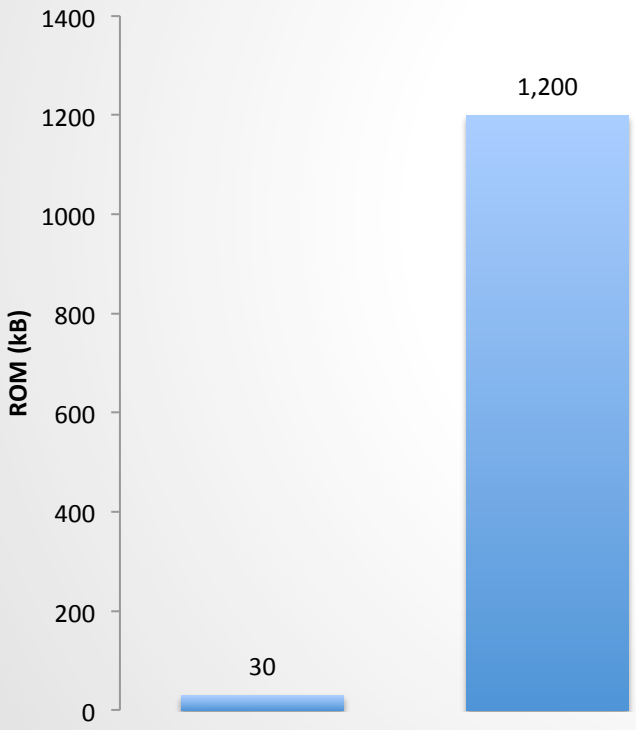
Public Key	Block / Stream	Hash
RSA, DSS, DH, NTRU …	DES, 3DES, AES, ARC4, RABBIT, HC-128 …	MD2, MD4, MD5, SHA-128, SHA-256, RIPEMD …

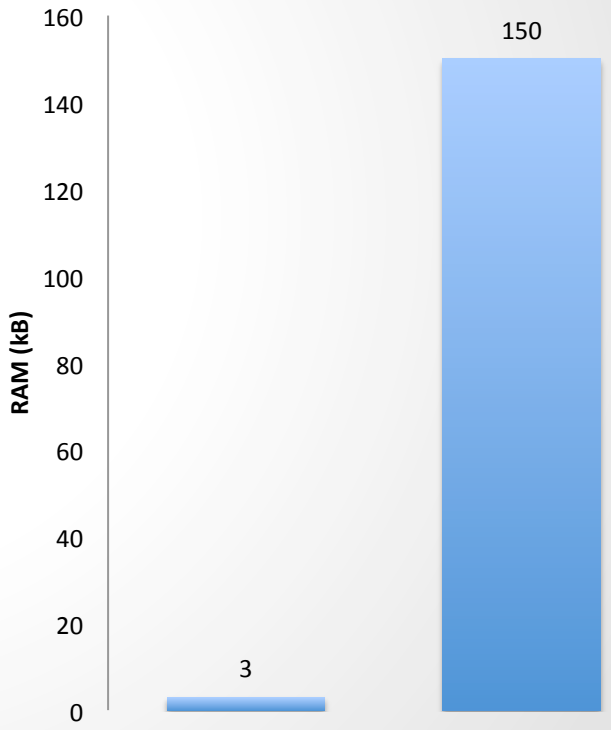
Ex: *TLS_RSA_WITH_AES_128_CBC_SHA*

yaSSL

3: Memory Usage

- ROM / RAM usage





4: Simple to Use

- Learning curve?
- Myth: Encryption is too hard to use.

5: Portability

- OS support out-of-the-box?
- Customizable?

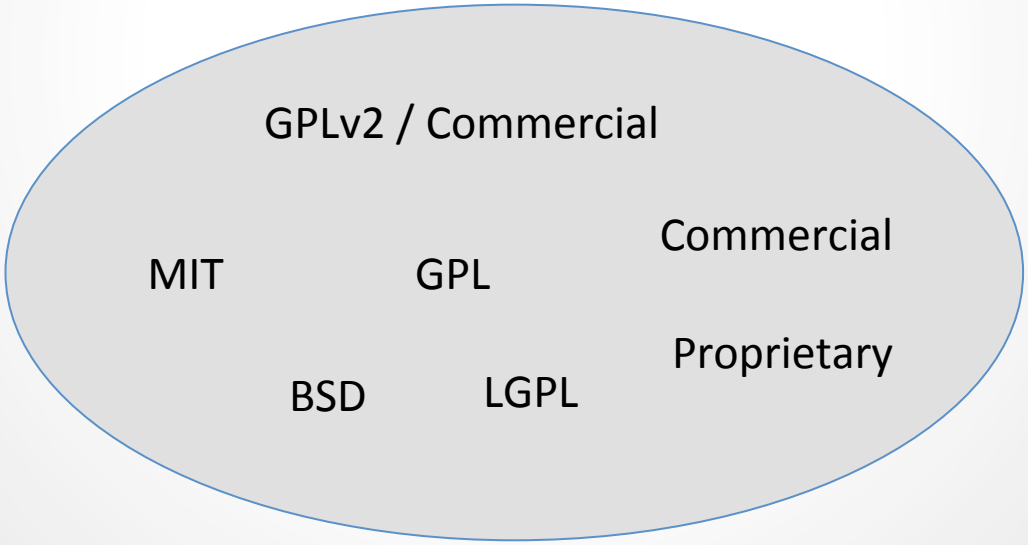
yaSSL

6: Hardware Acceleration

- Support for hardware acceleration?
- Assembly code optimizations

7: License

- Flexible license model?
- Does it meet your license needs?



8: Maturity

- Track record?
- Code origin?
- Actively developed?

9: Compatibility

- Is interoperability testing being conducted?
- What browsers is the library actively tested against?

10: Crypto Access

- Direct access to crypto?

Many reasons:

- Direct encryption
- Code Signing
- Verifying hashes, etc.

11: Support

- What happens if:
  - Something goes wrong
  - You can't get it to work on your system
  - New vulnerability comes out
  - You need a new cipher/feature
- Is there support available to help you out?

SSL: Shopping List

1. Protocols
2. Ciphers
3. Memory Usage
4. Simple to Use
5. Portability
6. Hardware Acceleration
7. License
8. Maturity
9. Compatibility
10. Crypto Access
11. Support

Thanks!

www.yassl.com

chris@yassl.com

info@yassl.com