

E-Business Security Introduction

– Statistics - UK

- 88% of businesses use e-mail every day.
- 66% have marketing websites.
- 57% conduct online ordering with customers or suppliers.
- 34% receive or make payments online - ahead of Germany and the US

Source : UK Online website : <http://www.ukonline.gov.uk>

– The advantage of e-Business

- Conduct business :
 - Anytime
 - Anyplace
 - Anywhere
 - Anyone
- Buyers leverage competition to get best deal
- Vendors can get greater coverage and increase market share

– The security issues

- Need to authenticate people
 - Cannot do business with anonymous people
 - Need to manage risk
- How do we authenticate someone who :
 - Never seen before
 - May never seen again
- Authentication must :
 - Require no previous agreements between vendor a purchaser
 - Must be relatively easy and cost-effective

– The security issues

- Need to prove a transaction as valid
 - Need to prove beyond doubt a message came from alleged originator
 - Non-repudiation
- Solution must be highly scaleable

– What is e-commerce security ?

- Most people's e-commerce experience is purchasing something from a web site using a credit card
 - Same protection as purchasing in a store
 - Not good enough for large business transactions
- Essential component of applications
 - Analysts reports that third party access to systems will drive increase in external security breaches
- Anything the vendor tries to sell you !

— What is e-commerce security ?

- Why not use userid and password :
 - Requires some prior agreement
 - Centralised solution for each system
 - Site specific - many sites use this
 - How many userids/passwords do you have ?
 - We discuss Microsoft Passport later
- E-commerce law does not cover userid/password specifically
 - Law focuses certificates and signatures

— What is e-commerce security ?

- Is this a new and unique challenge ?
 - No !
 - There are established parallels
- Person shopping with a credit card can shop :
 - Anytime
 - Anyplace
 - Anywhere
 - Vendor does not trust buyer
 - Buyer does not trust vendor

– What is e-commerce security ?

- Why does the credit card model work so well ?
 - Both Vendor and Buyer have a common trust
 - The banking system

– The technology solution

- Public Key Cryptography
 - Two types of encryption - Symmetric and Asymmetric
 - Symmetric
 - Uses the same key to encrypt and decrypt
 - Fast - can be used to encrypt large volumes
 - Difficult to deploy
 - Examples : DES, Triple DES, Blowfish, Rijndael (AES)
 - Asymmetric
 - Uses different keys to encrypt and decrypt
 - Slow - not practical for large volumes
 - Easy to deploy
 - Examples : RSA, Diffie-Hellman

- The technology solution

- A user is identified by a Certificate
 - Signed by a commonly trusted third party - a certificate authority (CA)
 - Contains (amongst others) :

Certificate serial number
Signature algorithm (RSA with MD5)
Issuer Name (X.500)
Subject Name (X.500) CN=Mike McNamee, OU=Home, O=MyDotCom, C=UK
Validity Period
Subject Public Key
Key Usage
CA Signature

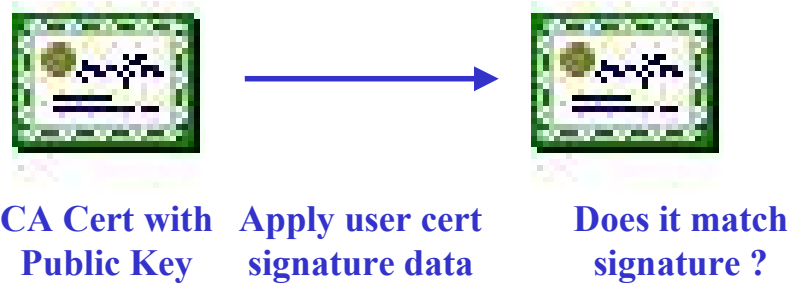
- The technology solution

- A CA is identified by a Certificate
 - Self Signed
 - Provides Public Key for CA
 - Allows all Certificates for this CA to be verified

Certificate serial number
Signature algorithm (RSA with MD5)
Issuer Name (X.500)
Subject Name (X.500) CN=Mike McNamee, OU=Home, O=MyDotCom, C=UK
Validity Period
Subject Public Key
Key Usage
CA Signature

- The technology solution

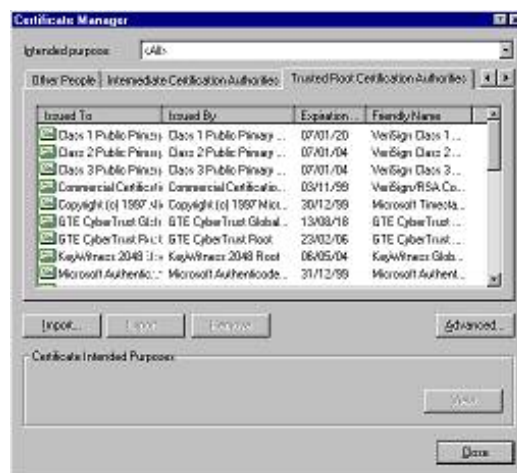
- How do I validate a user certificate ?



My certificate is signed by the CA private key - we get the public Key from the CAs certificate (which is self signed) and use this to check the CAs signature on my certificate

- The technology solution

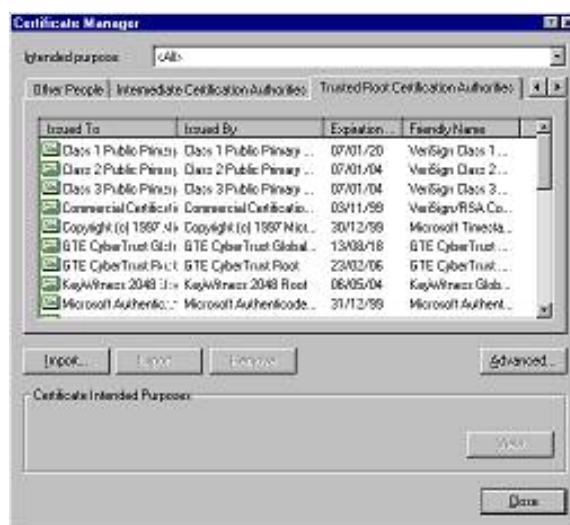
- How do I validate a CA certificate ?



The CA certificate is self signed - we have the CA certificates we trust shipped in our browsers or software

- The technology solution

- Possession and Access to the private Key controls who can use an identity
- Commercial Software has Root CA Certificates supplied to enable most certificates to be validated



- The technology solution

- **Sample Certificate (formatted) :**

Certificate:
Data:
Version: 1 (0x0)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=UK, ST=Glos, O=e3sciences, OU=Dev, CN=Test CA /Email=testca@home.com
Validity
Not Before: May 1 17:09:35 2001 GMT
Not After : May 1 17:09:35 2002 GMT
Subject: C=UK, ST=Glos, O=e3Sciences, OU=Dev, CN=Mike McNamee/Email=mikem@e3sciences.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
 00:9b:8c:a9:db:1f:12:15:1f:4c:5b:8e:e1:53:b1:
 cd:3c:f6:c4:60:f4:5e:d2:96:46:4c:3f:f0:ea:91:
 e9:08:04:b3:3b:98:a1:7c:ee:4e:fb:d0:39:cc:f0:
 bd:15:6f:0c:5f:2b:2b:ba:ad:1d:b8:6e:b6:4b:4b:
 77:45:d0:06:6b:e2:46:f8:f6:d8:fa:9c:69:f3:d4:
 02:f5:cb:77:bb:ba:44:13:5e:4e:83:b1:c4:fb:15:
 2a:da:87:e9:5b:72:29:55:f8:4a:76:ef:a9:28:74:
 38:a4:d5:8b:cc:91:94:09:ca:13:c8:85:cd:25:16:
 20:e6:b1:bc:ca:fd:8c:4f:23
Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
 39:39:6c:ff:0a:7b:fe:76:37:47:28:a0:17:2a:65:fb:b3:b4:

- The technology solution

- What does a certificate buy me ?
 - Ability to sign emails = Digital Signature
 - Data can be verified that user signed data
 - Data can be protected from modification
 - Ability to encrypt data in transport = Secure Socket Layer
 - Secure method of exchanging data across networks
 - Client optionally requires Certificate, Server mandatory
 - A URL with https://... uses SSL
 - When you have a Padlock on the browser:

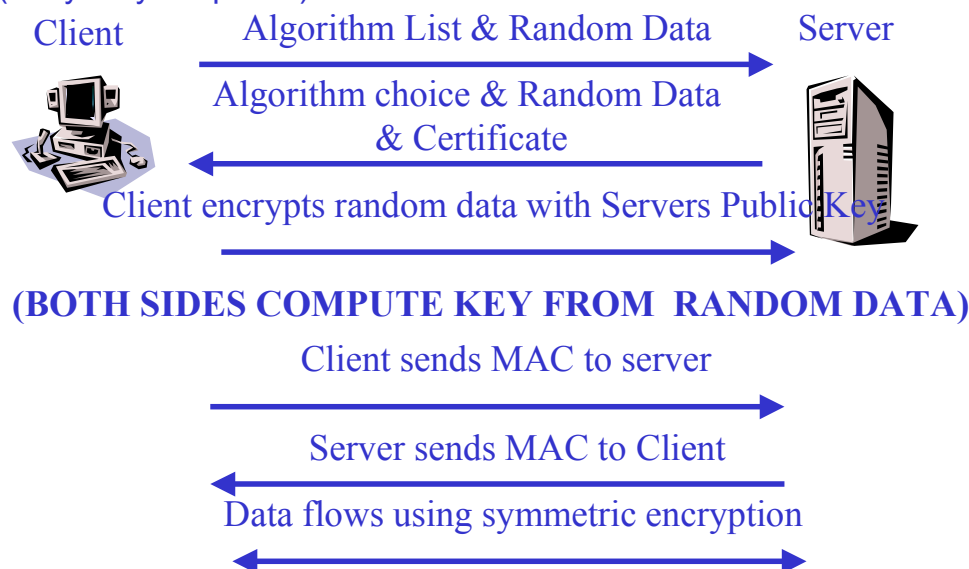


- NB : Does not protect data after receipt

- The technology solution

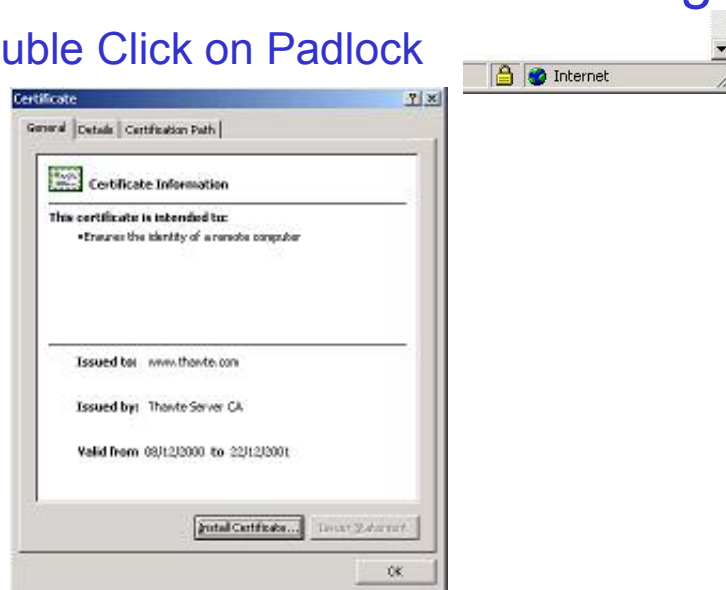
- How does Secure Socket Layer work ?

(very very simplified)



– The technology solution

- How do I know who I am talking to ?
 - Double Click on Padlock



– The technology solution

- What happens if my Private Key is lost or compromised ?
 - A Certificate Revocation List (CRL) keeps track of the certificates that are no longer valid
Authentication Server

– The technology solution

- Sample CRL

Certificate Revocation List (CRL):

Version 1 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: /C=UK/ST=Glos/O=e3Sciences/OU=Dev/CN=Test CA /Email=testca@home.co

m

Last Update: May 8 19:13:05 2001 GMT

Next Update: Jun 7 19:13:05 2001 GMT

Revoked Certificates:

Serial Number: 01

Revocation Date: May 8 19:04:36 2001 GMT

Signature Algorithm: md5WithRSAEncryption

54:9e:87:ed:04:70:37:1f:5e:df:e5:b0:91:d7:32:a5:27:11:

a2:5a:2f:57:02:cb:af:b3:29:33:e8:aa:90:2b:11:fb:c9:01:

51:25:05:56:e3:23:e7:18:d6:e3:8b:0d:ec:9f:37:73:80:8c:

b5:25:cb:9e:b9:30:96:90:50:19:80:b6:3c:28:46:75:c0:9e:

53:20:63:e2:df:70:e9:21:44:2f:48:0b:28:c9:63:40:2a:d9:

5c:15:2a:77:74:90:62:2d:84:47:bb:d4:48:0f:fl:d8:3a:e1:

2f:cf:1d:88:45:b4:ef:ce:3e:3e:9b:00:33:cc:0d:d1:0b:5d:

a7:c6

– The technology solution

- Where does LDAP fit in all this ?

- Storage medium for certificates and CRLs
- Authentication Server for solutions such as WebSphere
 - Certificate
 - Userid/Password

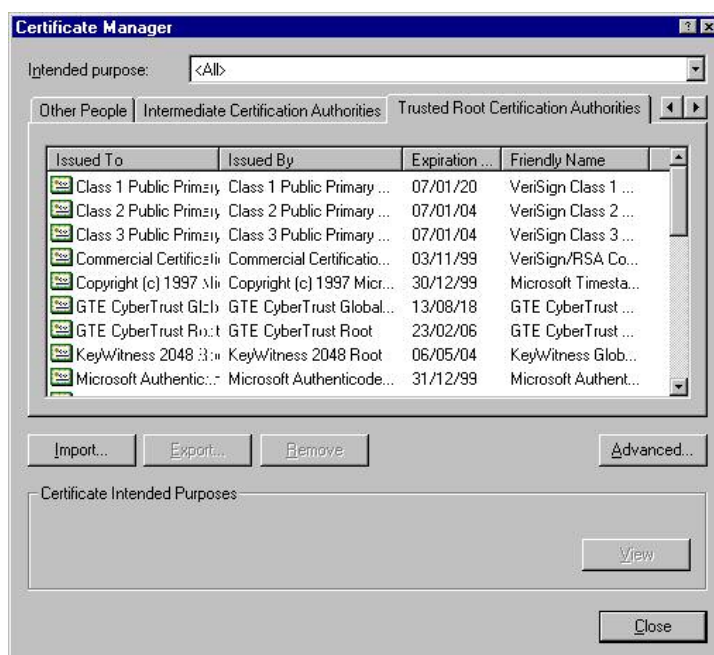
– The catch

- This sounds great - where's the catch :

CA commercial liability
unclear for business
transactions

CA not part of established
commercial infrastructure

Do you trust these ?



This document is the property of e3 Sciences Ltd. It may not be copied or distributed without permission.

25

– The catch

- This sounds great - where's the catch :
 - Legal foundation is not global
 - Varies between country and region
 - No centralised authentication
 - Invalid or stolen certificates not immediately detected
 - Depends on implementation of Certificate Revocation List (CRL)



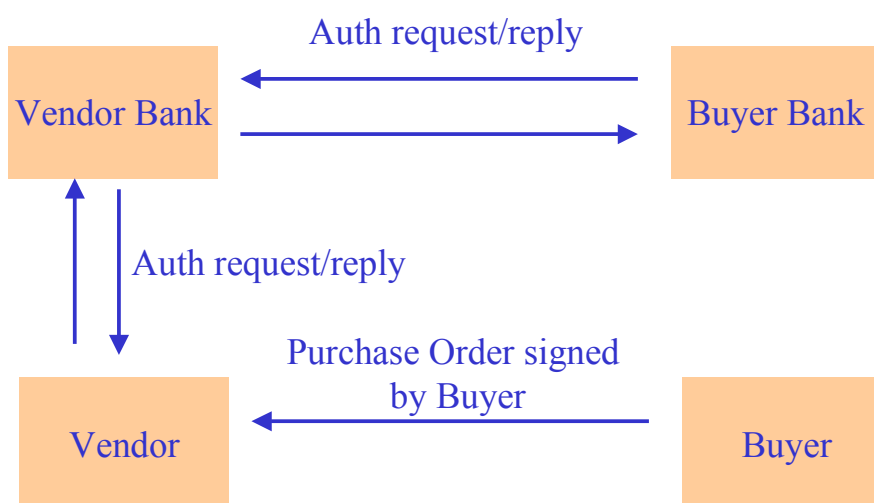
This document is the property of e3 Sciences Ltd. It may not be copied or distributed without permission.

26

– The business solution

- Identrus is a consortium of Financial and Technology companies
 - Provide framework to deliver technology solutions with backing of Financial institutions you know and love
 - Provide Guarantees against loss
 - Highly Trusted
 - Provides a 4 point structure to give assurance of trust
 - Coming to a bank near you relatively soon

– Sample Identrus based transaction



– How do I use all this on zSeries ?

- OS/390 V2R4 X.509 certificate support
 - RACF
 - HTTP Server and WebSphere
- OS/390 V2R6
 - Communications Server
 - SSL based TN3270 sessions
- OS/390 V2R7
 - Communication server
 - SSL based TN3270 client authentication
 - System SSL
 - Develop your own applications

– How do I use all this on zSeries ?

- OS/390 V2R8 X.509 certificate support
 - RACF provides certificate management
 - Key storage in RACF Key rings
 - Generate certificates
 - Be a Certificate Authority
 - Replace System SSL key database
- OS/390 V2R10 PKIServ sample
 - RACF provides improved Web based PKI
- z/OS V1R3 provides full function PKI

– Getting started with RACF

- Create a Self signed Certificate
 - RACDCERT ID(mike)
GENCERT
SUBJECTSDN(CN('Mike McNamee')
OU('DEV')
O('e3 Sciences')
SP('GL')
L('Stonehouse')
C('UK')) xx = 2 byte country name
WITHLABEL('Mikes test cert')
SIGNWITH(CERTAUTH 'Mikes CA Cert')

– Getting started with RACF

- Add a certificate authority
 - RACDCERT CERTAUTH
ADD(my.certca.dsn)
WITH(LABEL('CertAuth')) HIGHTRUST
- Request a certificate for a server
 - RACDCERT ID(WEBSRV)
GENREQ(LABEL('Production Webserver'))
DSN(my.cert.req.dsn)

You send this to your CA to get a server cert

– Getting started with RACF

- Add your certificate to RACF
**RACDCERT ADD('MIKE.CERT.ARM') TRUST
ID(MIKE)**

RACF will associate user MIKE with this certificate
and provide an ACEE

– Getting started with RACF

- Create your own Certificate Authority Certificate
**RACDCERT GENCERT CERTAUTH
SUBJECTSDN(CN('My CA')
OU('DEV')
O('e3 Sciences')
SP('GL')
L('Stonehouse')
C('UK')) xx = 2 byte country name
WITHLABEL('Mikes CA cert')**

– Getting started without RACF

- Open Source software available
 - **OPENSSL** provides an crypto toolkit that is free <http://www.openssl.org>
- **Commercial Software**
 - Windows 2000 Server provides certificate management and web server
- **Obtain a free certificate for email and signature**
 - <http://www.thawte.com>

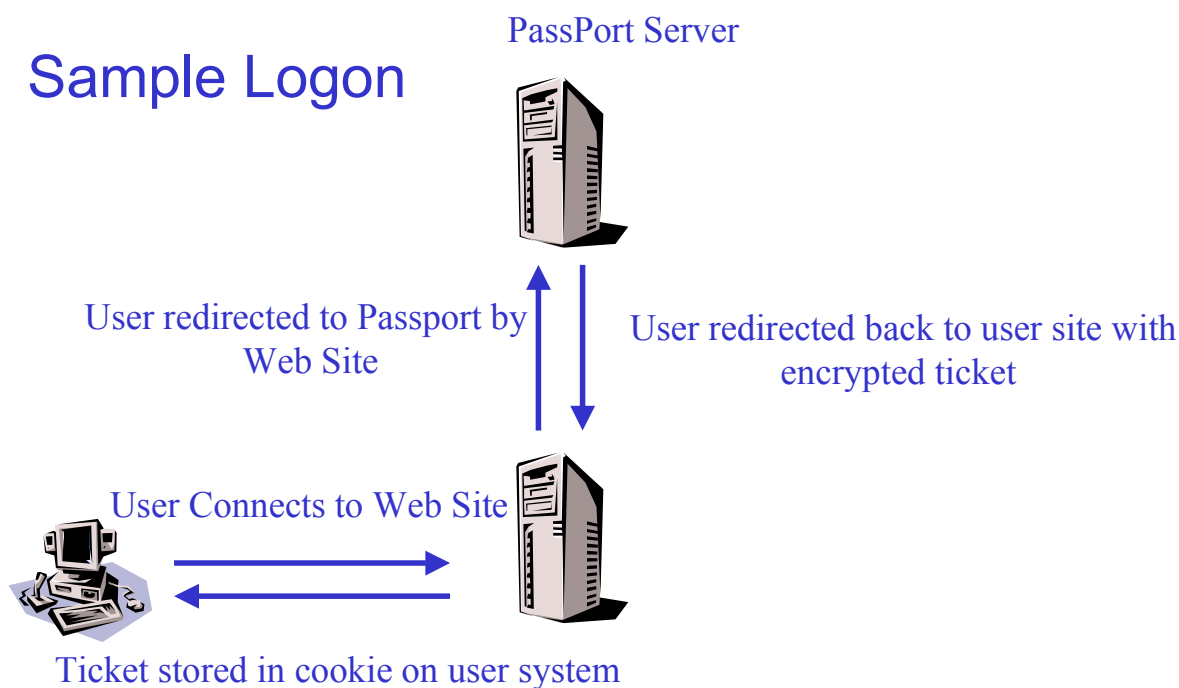
– Alternatives

- Microsoft have an alternative for e-commerce : **Passport**
 - Single point of logon for Web sites
 - User can sign on once and roam across many sites
 - Provides Express Purchasing facility - single click purchase - caches credit card number

NB : WebSphere HTTP SSO is similar in some respects - more secure though !

– Microsoft Passport

- Sample Logon



– Microsoft Passport

- Always read the T & Cs (offending sections removed 4/2001 after protest - could be added back)

LICENSE TO MICROSOFT

By posting messages, uploading files, inputting data, submitting any feedback or suggestions, or engaging in any other form of communication with or through the Passport Web Site, you warrant and represent that you own or otherwise control the rights necessary to do so and you are granting Microsoft and its affiliated companies permission to:

Use, modify, copy, distribute, transmit, publicly display, publicly perform, reproduce, publish, sublicense, create derivative works from, transfer, or sell any such communication.

Sublicense to third parties the unrestricted right to exercise any of the foregoing rights granted with respect to the communication.

Publish your name in connection with any such communication.

The foregoing grants shall include the right to exploit any proprietary rights in such communication, including but not limited to rights under copyright, trademark, service mark or patent laws under any relevant jurisdiction. No compensation will be paid with respect to Microsoft's use of the materials contained within such communication. Microsoft is under no obligation to post or use any materials you may provide and may remove such materials at any time in Microsoft's sole discretion.

– Microsoft Passport

- Watch the press for vulnerabilities :

ZD Net November 2, 2001 5:57 PM PT

Software flaws in the security of Microsoft's Passport authentication system left consumers' financial data wide open, causing the software giant to remove a key service from the Internet to protect people from having their data stolen, a company representative acknowledged Friday.

– Useful Info

- Baker & McKenzie e-commerce site
 - Doing E-Commerce in Europe (Free Book) - documents law in various regions
<http://www.bmck.com/ecommerce/Doing%20E-Commerce%20in%20Europe/Doing%20E-Commerce%20in%20Europe>
- RACF Web site
 - PKIServ <http://www-1.ibm.com/servers/eserver/zseries/zos/racf/webca.html>
 - Presentations <http://www-1.ibm.com/servers/eserver/zseries/zos/racf/presentations.html>

– Useful Info

- IBM Redbooks (www.redbooks.ibm.com)
 - Deploying a Public Key Infrastructure SG24-5512
 - Websphere Advanced edition : Security SG24-6520
 - OS/390 Security Server 1999 updates SG24-5627
- IBM Developerworks
 - Learn more about WebSphere security http://www-4.ibm.com/software/webervers/appserv/security_v35.pdf
 - IBM Framework for e-business - security <http://www-106.ibm.com/developerworks/library/security/index.html>

– Useful Info

- Secrets and Lies - Bruce Schneier ISBN 0-471-25311-1
 - Discussion of Security in networked world
- SSL and TLS - Eric Rescorla 0-201-61598-3
 - Detailed SSL discussion
 - Tutorials for OpenSSL