Secure Sockets Layer (SSL)

Juan David González Cobas

Mayo de 2005

Secure Sockets Layer

Secure Sockets Layer y *Transport Layer Security* (SSL/TLS) es una familia de protocolos que proporciona servicios de seguridad a una conexión TCP.

SSL está contruida sobre TCP, lo que tiene dos consecuencias

- funciona como un proceso de usuario, i.e., no requiere alteraciones del sistema operativo
- funciona encima de TCP, de forma que se basa en una conexión (*stream* de datos) fiable y no tiene que ocuparse de secuencias de paquetes ni de retransmisión o timeouts.

Historia de SSL/TLS

1. La primera versión de SSL (SSLv2) fue introducida por Netscape en su navegador con la intención (fallida) de crear un monopolio de certificación.
2. Microsoft, de acuerdo con su práctica habitual, introdujo algunas “mejoras” y creó un producto paralelo e incompatible conocido por PCT (Private Communications Technology).
3. Netscape creó en consecuencia una vasta mejora del protocolo, bajo el nombre de SSLv3.
4. La IETF, en vista del daño que para la industria representaría la existencia de tres estándares similares pero incompatibles, introdujo un cuarto protocolo similar pero incompatible denominado TLS (*Transport Layer Security*) [3].
5. La versión del protocolo más ampliamente desarrollada y extendida es SSL versión 3.

Protocolo SSL/TLS básico

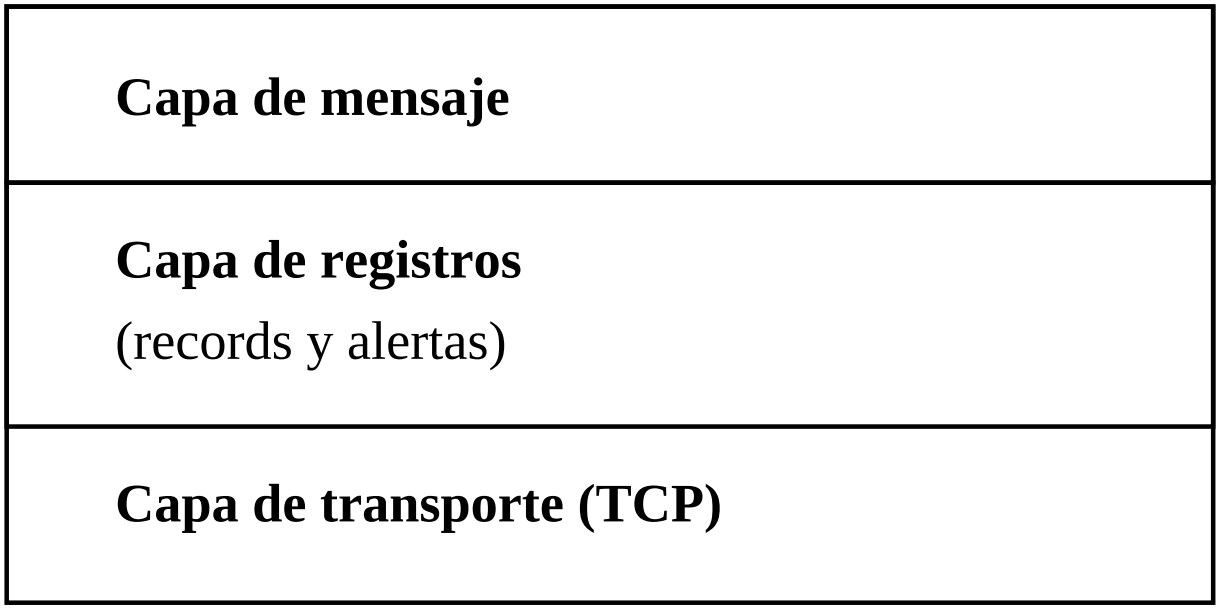
El objetivo de SSL consiste en construir, sobre el servicio de *stream* fiable de TCP, un *stream* fiable

- cifrado
- con protección de integridad y
- con autenticación (posiblemente mutua) entre cliente y servidor.

Para esto, el *stream* se divide en *registros* (*records*) dotados de cabecera y protección criptográfica.

En el protocolo básico, Alicia (el cliente) inicia contacto con Bernardo (el servidor). Éste le envía su certificado. Alicia lo verifica y extrae de él la clave pública de Bernardo. Alicia genera un número aleatorio secreto S y se lo envía a Bernardo cifrado con su clave pública, $E_B(S)$. A partir de aquí se generan *seis* claves de sesión que permiten que el resto de la comunicación sea cifrada y protegida en su integridad.

Capas del protocolo SSL/TLS



Etapas del *handshake* SSL

Mensaje 1 Alicia comunica a Bernardo su intención de hablar, la lista de algoritmos de cifrado que soporta, y un número aleatorio R_A.

Mensaje 2 Bernardo envía a Alicia su certificado C_B, un número aleatorio R_B y responde con uno de los cifrados soportados por Alicia que él también esté capacitado para utilizar.

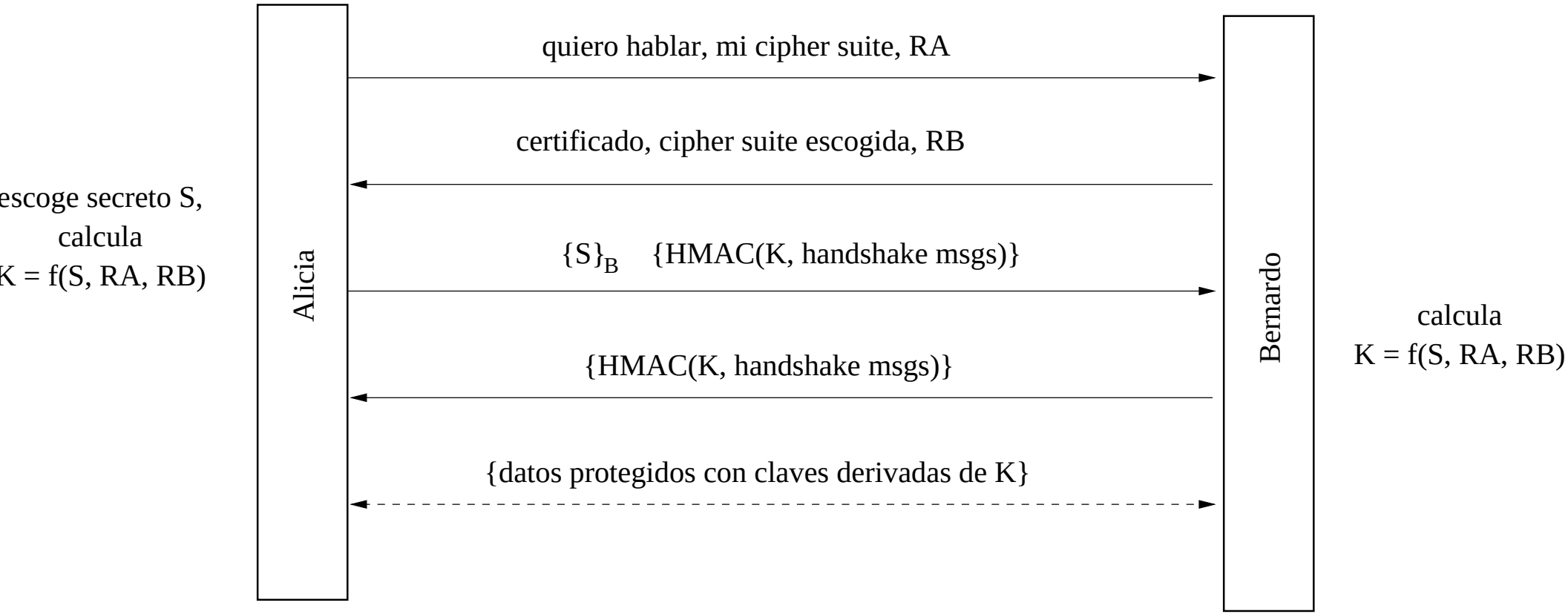
En este momento, Alicia puede verificar la identidad de su interlocutor validando su certificado.

Alicia genera un número aleatorio S (el secreto pre-master*) del que deriva el secreto* master, $K = f(S, R_A, R_B)$, *que será el padre de todos los secretos.*

Mensaje 3 Alicia envía S cifrado para Bernardo, $E_B(S)$, junto con un hash con clave del secreto *master* K y los mensajes de handshake hasta el momento, $HMAC(K, \textit{handshake})$.

Bernardo puede calcular el pre-master S *y derivar el master* $K = f(S, R_A, R_B)$. *De él, tanto Alicia como Bernardo podrán derivar las seis claves de sesión que SSL establece.*

Mensaje 4 Bernardo prueba su conocimiento de las claves de sesión y la integridad del handshake enviando un hash con clave del handshake completo, $HMAC(K, \textit{handshake})$.


escoge secreto S,
calcula
K = f(S, RA, RB)
Alicia
quiero hablar, mi cipher suite, RA
certificado, cipher suite escogida, RB
{S}B {HMAC(K, handshake msgs)}
{HMAC(K, handshake msgs)}
{datos protegidos con claves derivadas de K}
Bernardo
calcula
K = f(S, RA, RB)

¿Qué proporciona el *handshake* SSL?

Cuando termina el *handshake*, tenemos

- Una conexión cuyo flujo de datos es cifrado mediante un algoritmo simétrico, proporcionando *confidencialidad*.
- La conexión está formada por *registros* cifrados y con un MAC para verificar su integridad, dependiente de un *número de secuencia*, lo que proporciona *integridad* y protección contra interceptación o reproducción de la conexión
- Autenticación del servidor por medio de certificado
- Potencialmente, autenticación del cliente por el mismo mecanismo (opcional)

Claves de sesión

En el *handshake* SSL intervienen diversos materiales simétricos.

pre-master S Es un secreto compartido a partir del cual se elaborará el master K. Lo genera el cliente (Alicia) como un valor aleatorio de 48 bytes de longitud

master K Es un valor derivado del pre-master $K = f(S, R_A, R_B)$, y del que deriva todo el material de clave simétrica de la sesión (que puede reutilizarse en varias conexiones)

claves de cifrado Se emplean para encriptar los datos.

claves de integridad Se usan como claves en los MACs.

IVs son los vectores iniciales requeridos en la inicialización de algunas series de cifrado.

Las claves simétricas de cifrado, integridad e IV van a pares, llamadas *de lectura y escritura*. Las primeras son para recepción y las segundas para envío.

Las claves de escritura del servidor son las de lectura del cliente. ¿Está claro?

Los seis elementos derivan del *master* y los números aleatorios R_A, R_B intercambiados en el inicio de la conexión

$$\begin{aligned} K_{\text{cifrado}} &= g_1(K, R_A, R_B) \\ K_{\text{integridad}} &= g_2(K, R_A, R_B) \\ IV &= g_3(K, R_A, R_B) \end{aligned}$$

e igual para las claves de escritura

Negociación de *cipher suites*

Las dos partes deben comunicarse qué algoritmos de cifrado entienden y acordar cuál utilizar. Esto comprende, posiblemente

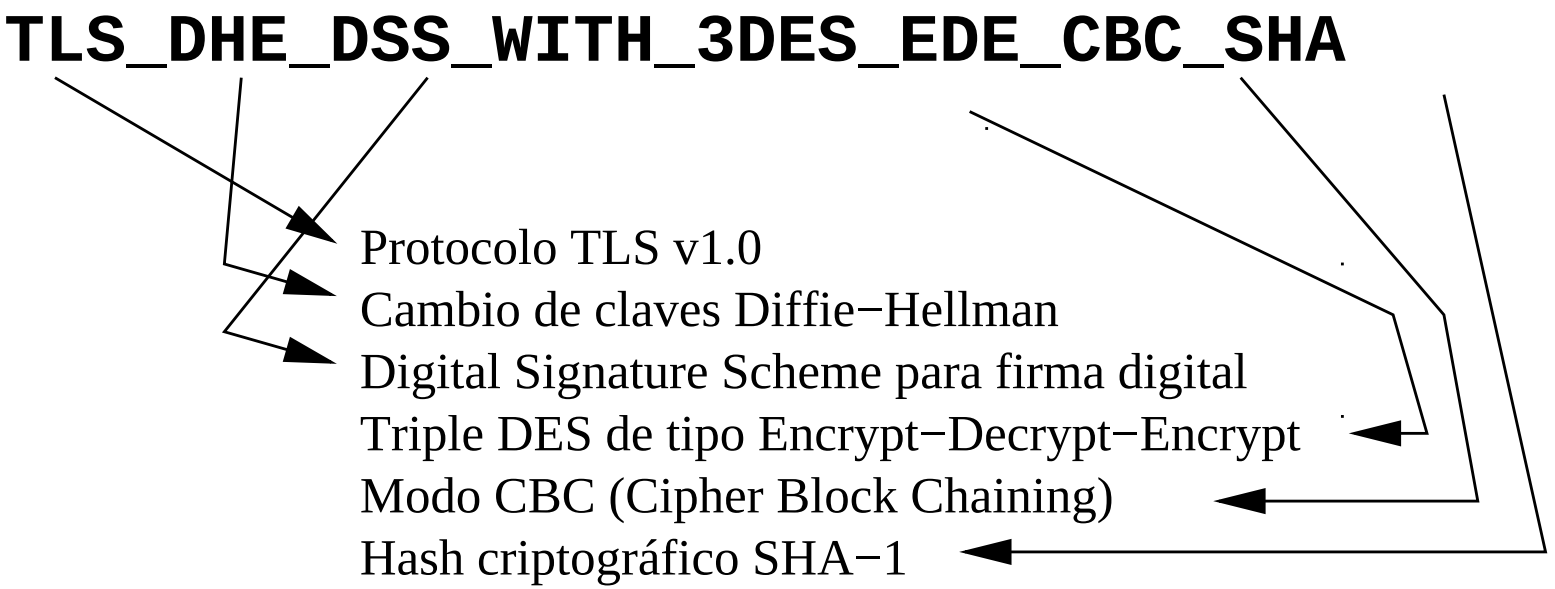
- un algoritmo de clave pública
- un algoritmo de clave simétrica
- un modo de operación de éste
- longitudes de clave
- un hash criptográfico

Existe un completo catálogo de suites a los que el estándar se refiere por identificadores con el aspecto siguiente:

`TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA`

En SSLv2, Alicia manda su conjunto de suites soportadas, Bernardo indica cuáles de ellas soporta y Alicia decide la elegida. En SSLv3, Alicia ofrece y Bernardo escoge directamente.

Desglose de una *suite*



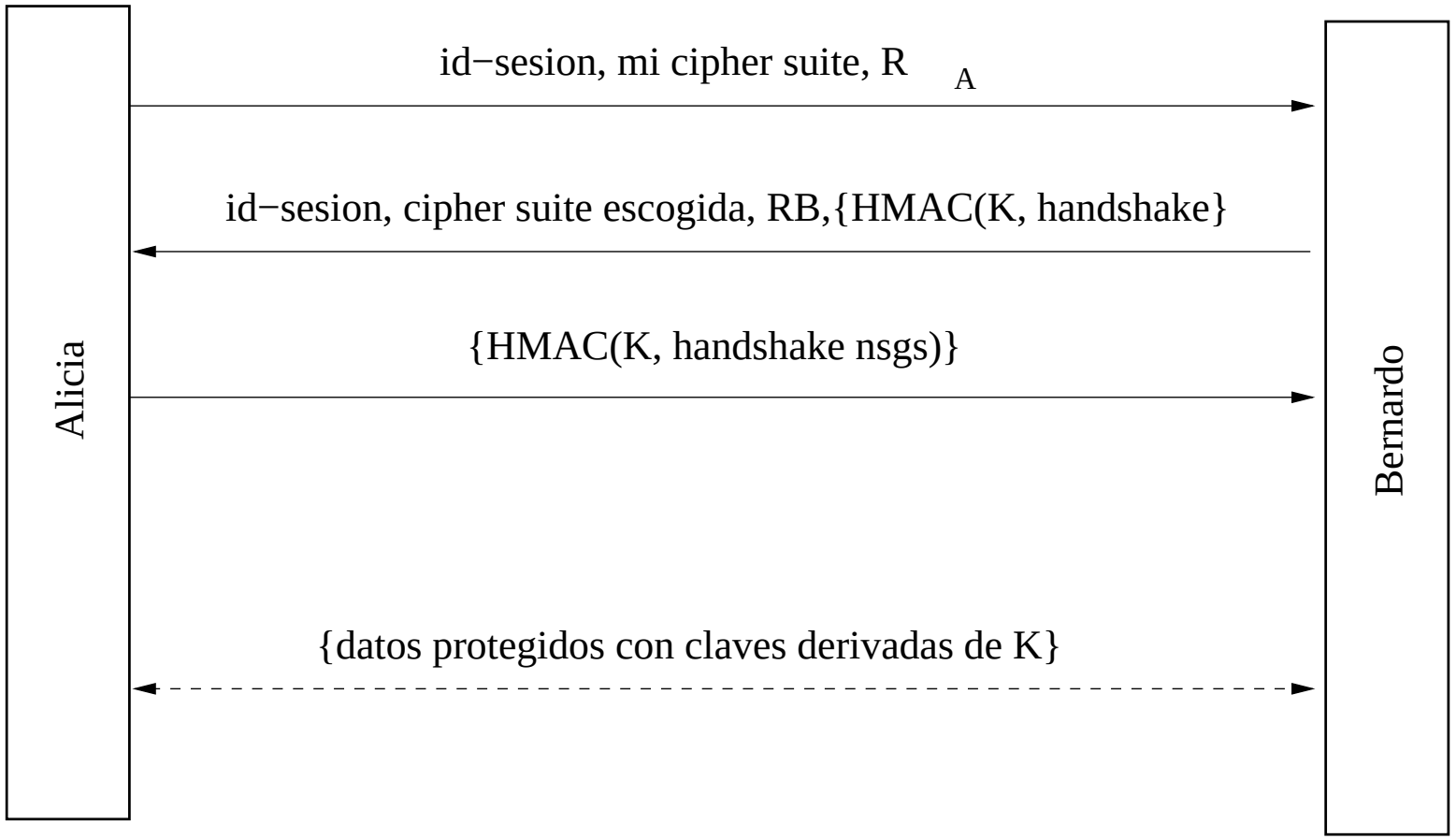
Reconexión SSL

La fase de *handshake* involucra un protocolo costoso con cómputos criptográficos de clave pública.

SSL prevé la posibilidad de *reinicio de sesión* sin repetición de un handshake. Así, una *sesión* puede dar lugar a múltiples *conexiones*.

En el establecimiento de una sesión, el servidor suministra (en el mensaje 2) un *identificador de sesión*, que será compartido por todas las conexiones.

Si se pretende reiniciar una sesión, el protocolo de conexión se esquematiza en el siguiente diagrama


Alicia
Bernardo
id−sesion, mi cipher suite, R A
id−sesion, cipher suite escogida, RB,{HMAC(K, handshake}
{HMAC(K, handshake nsgs)}
{datos protegidos con claves derivadas de K}

Autenticación

SSL proporciona autenticación del servidor por medio de un certificado emitido por una autoridad certificadora reconocida en el software del cliente.

En teoría, SSL prevé una autenticación similar del cliente por medio de certificado similar a la del servidor. Esta fase es *opcional*. Además, es asimétrica: el servidor *especifica* las CAs en las que confía.

En la práctica, se emplea rara vez: el cliente se autentica por contraseña una vez dispone de una sesión SSL protegida criptográficamente.

Certificados

Los certificados de uso en SSL siguen el formato estándar X.509, que se basa en los nombres X.500.

Por tanto, los certificados no registran nombres de dominio, sino monstruosidades como

```
C=ES, O=Universidad de Oviedo, OU=Informatica,
        CN=Juan David Gonzalez Cobas
```

que han de ser violentados a las formas más corrientes.

E.g.: en SSL se asigna el nombre DNS al campo CN (*Common Name*).

SSL en la práctica

El uso inicial (y más extendido) de SSL es la securización de las transacciones electrónicas realizadas a través de la WWW.

SSL garantiza teóricamente

- La confidencialidad de los datos transmitidos durante la sesión.
- La identidad del servidor con el que nos comunicamos

Los dos factores se postulan como el fundamento de la seguridad en el Comercio Electrónico actual.

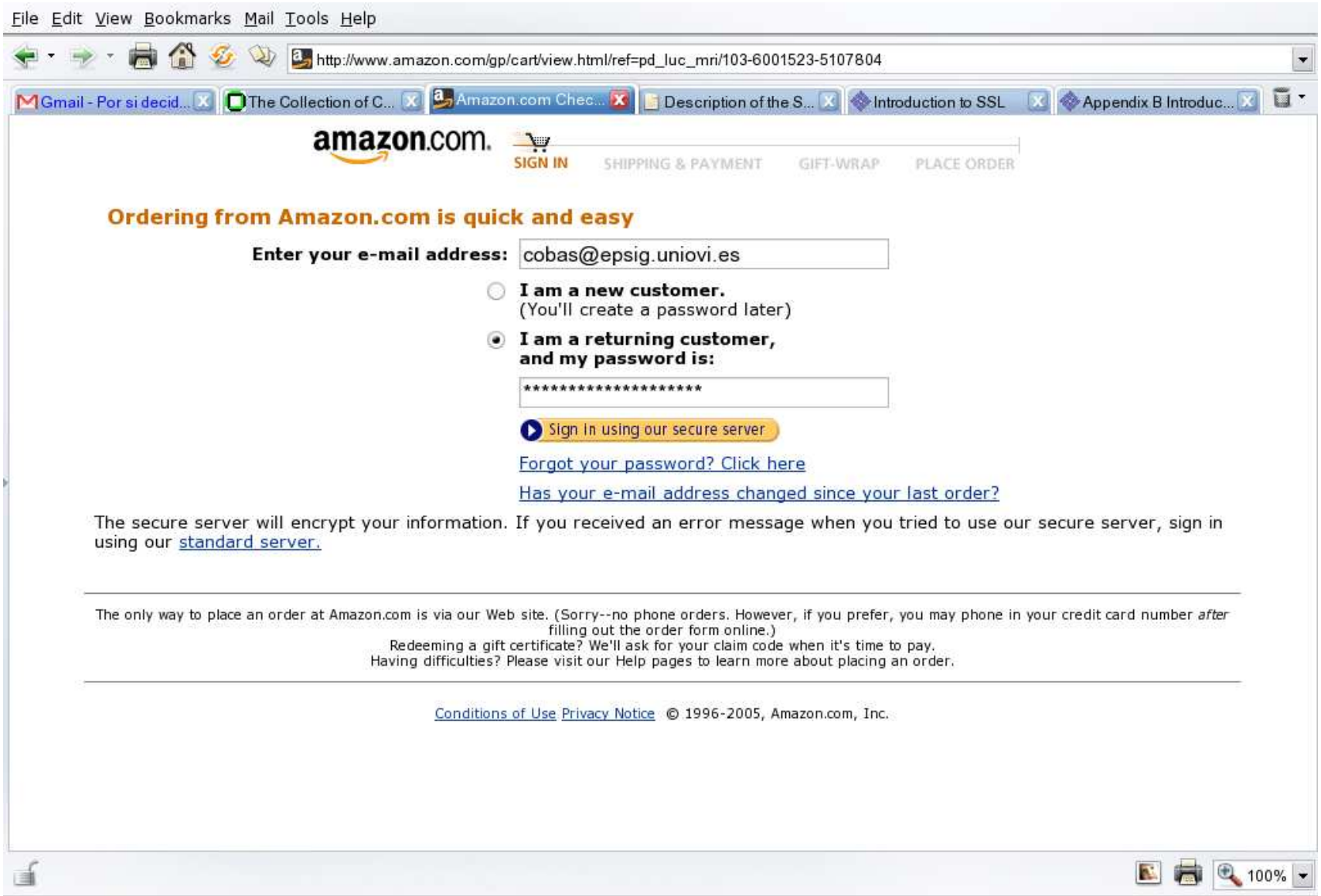
Pero, ¿es cierto?

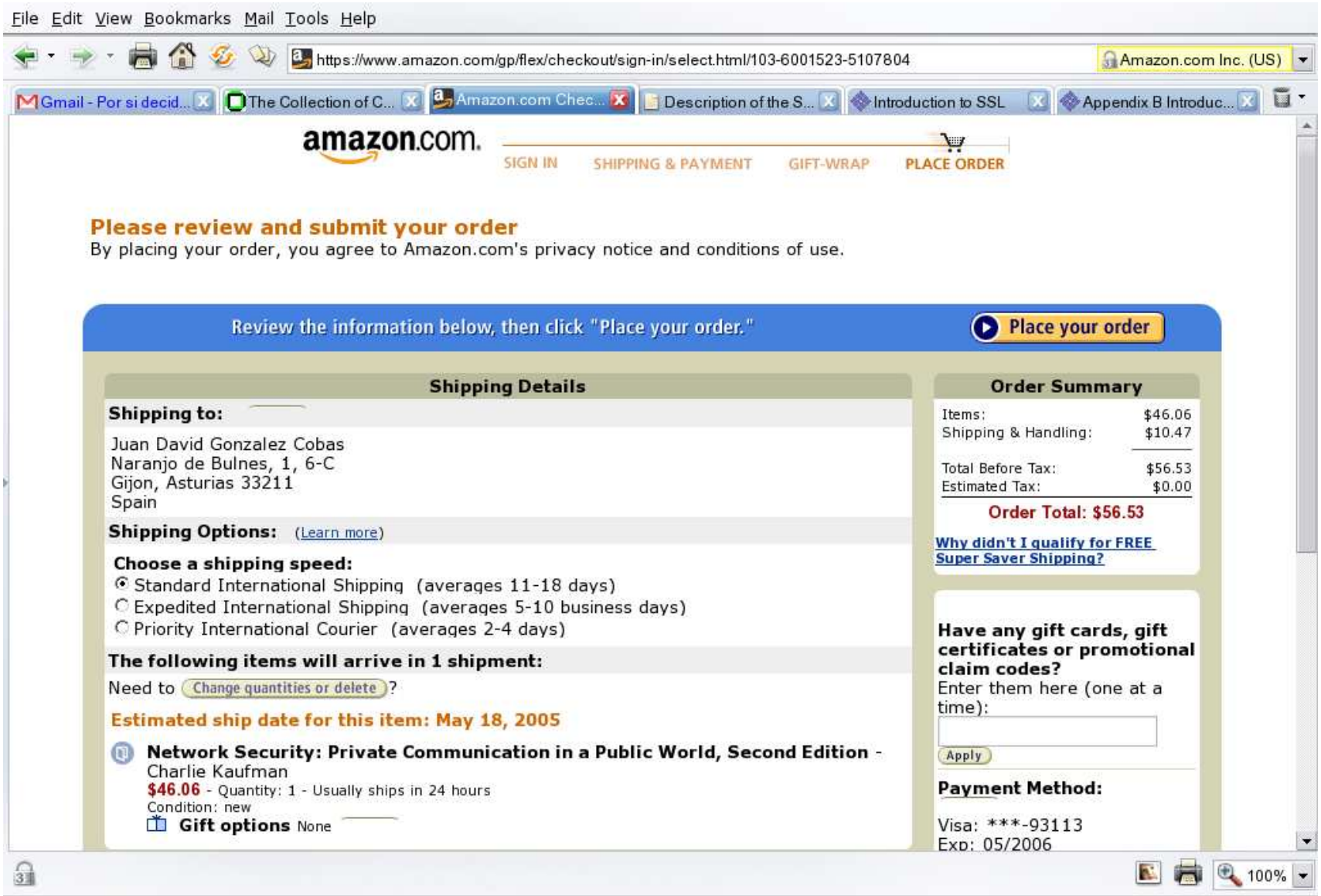
Una compra por Internet

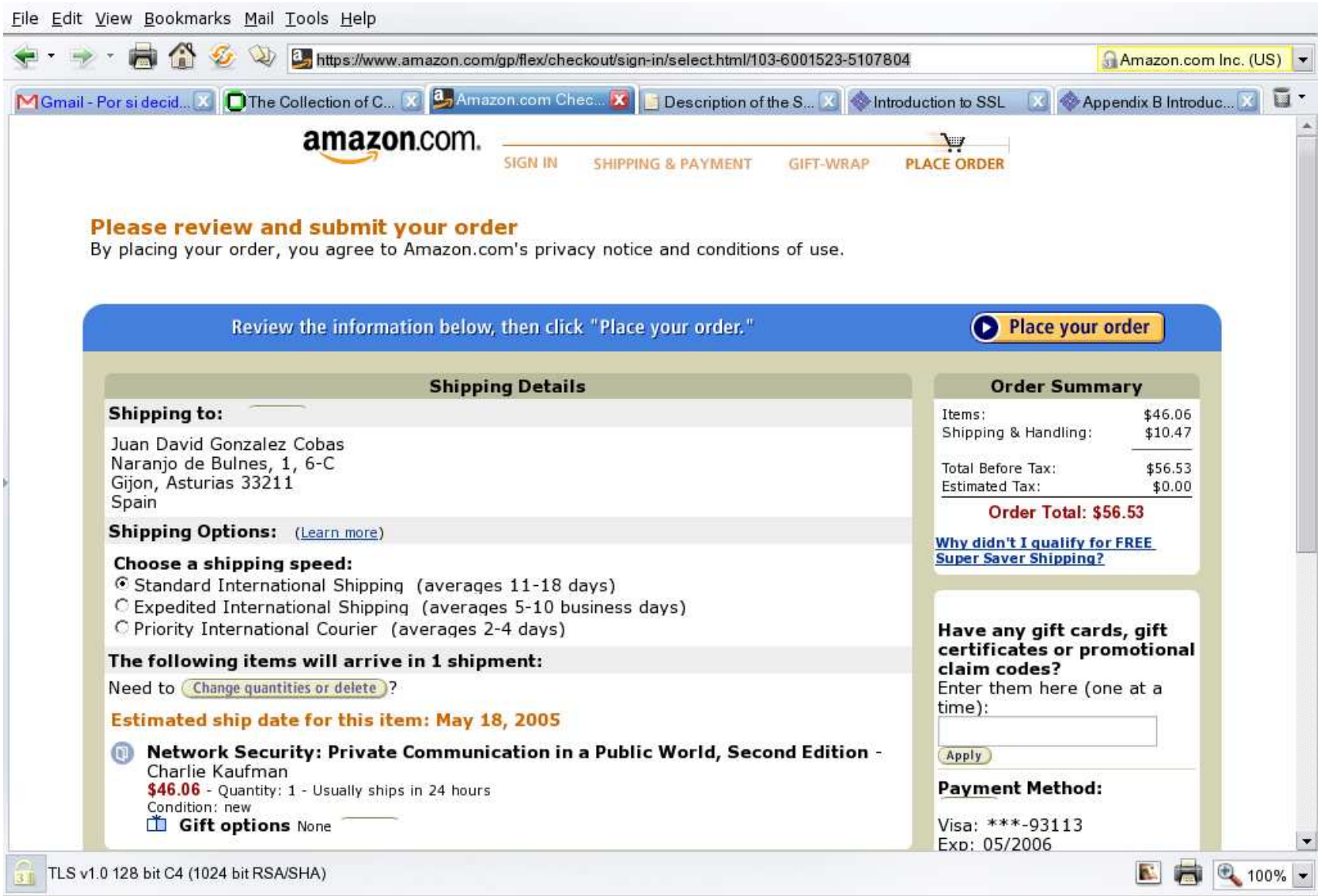

File Edit View Bookmarks Mail Tools Help
http://www.amazon.com/exec/obidos/search-handle-form/103-6001523-5107804
Gmail - Por si decid...
The Collection of C...
Amazon.com: All P...
Description of the S...
Introduction to SSL
Appendix B Introduc...
Shop in Sports & Outdoors (Beta-What is this?)
amazon.com.
VIEW CART | WISH LIST | YOUR ACCOUNT | HELP
Most Wished For Items
WELCOME | YOUR STORE | BOOKS | APPAREL & ACCESSORIES | ELECTRONICS | TOYS & GAMES | KITCHEN & HOUSEWARES | BABY | SEE MORE STORES
INTERNATIONAL | NEW RELEASES | TOP SELLERS | TODAY'S DEALS | SELL YOUR STUFF
Hello. Sign in to get personalized recommendations. New customer? Start here.
All results for: perlman kaufman speciner
Search: Amazon.com for perlman kaufman speciner GO!
Refine your search:
Find perlman kaufman speciner in these categories:
Books (2)
So You'd Like to...
Offer your advice
be a computer security expert.: by unicityd, Programmer/C...
Page You Made
LOOK INSIDE
Network Security: Private Communication in a Public World, Second Edition by Charlie Kaufman, et al (Hardcover)
Books: See all 2 items (Rate this item)
Buy new: $46.06 Used & new from $31.00 Usually ships in 24 hours
100%


File Edit View Bookmarks Mail Tools Help
http://www.amazon.com/exec/obidos/tg/detail/-/0130460192/qid=1116360738/sr=8-1/ref=sr_8_xs_ap_i1_xgl14/103-60(
Images: 43/50
Gmail - Por si decid...
The Collection of C...
Amazon.com: Book...
Description of the S...
Introduction to SSL
Appendix B Introduc...
Shop in Sports & Outdoors (Beta-What is this?)
amazon.com.
VIEW CART | WISH LIST | YOUR ACCOUNT | HELP
Most Wished For Items
WELCOME | YOUR STORE | BOOKS | APPAREL & ACCESSORIES | ELECTRONICS | TOYS & GAMES | MUSIC | CELL PHONES & SERVICE | SEE MORE STORES
SEARCH | BROWSE SUBJECTS | BESTSELLERS | THE NEW YORK TIMES® BEST SELLERS | MAGAZINES | CORPORATE ACCOUNTS | E-BOOKS & DOCS | BARGAIN BOOKS | USED BOOKS
EXTREME DEALS! 30%-60% Savings on gear from Altrec at amazon.com. SHOP
Search: Books GO! Web Search: GO!
Join Amazon Prime and ship Two-Day for free and Overnight for $3.99. Already a member? Sign in .
BOOK INFORMATION
Explore this item
buying info
customer reviews
editorial reviews
look inside
Share your thoughts
write a review
write a So You'd Like to... guide
e-mail a friend about this item
rate this item
RECENTLY VIEWED
Java Cryptography (Java Series (O'Reilly & Associates).) by
Network Security: Private Communication in a Public World, Second Edition
by Charlie Kaufman, Radia Perlman, Mike Speciner
LOOK INSIDE!
Look inside this book
Share your own customer images
List Price: $59.99
Price: $46.06 & This item ships for FREE with Super Saver Shipping. See details
You Save: $13.93 (23%)
Availability: Usually ships within 24 hours from Amazon.com. Sold by Amazon.com.
Want it delivered Wednesday, May 18? Choose One-Day Shipping at checkout. See details
30 used & new from $31.00
Edition: Hardcover
Other Editions: | List Price: | Our Price: | Other Offers:
Textbook Binding (1st) | $86.65 | | 29 used & new from $5.79
READY TO BUY?
Add to Shopping Cart
or
Sign in to turn on 1-Click ordering.
MORE BUYING CHOICES
30 used & new from $31.00
Have one to sell? Sell yours here
Add to Wish List
Add to Wedding Registry
Don't have one? We'll set one up for you.
100%


File Edit View Bookmarks Mail Tools Help
http://www.amazon.com/exec/obidos/tg/stores/static/-/generic/shopping-cart-gp-add/ref=dp_start-buy-box-form_1/103-6001523-5107804?%
Gmail - Por si decid...
The Collection of C...
Amazon.com Shop...
Description of the S...
Introduction to SSL
Appendix B Introduc...
Search: BOOKS
GO!
Browse: Choose a subject.
GO!
Your order qualifies for free shipping! (Some restrictions apply)
Make sure to select FREE Super Saver Shipping as your shipping speed at checkout.
You could save $30 today with the Amazon Visa® Card:
Your current subtotal: $46.06
Amazon Visa discount: - $30.00
Your new subtotal: $16.06
Find out how
Save $30 off your first purchase, earn 3% rewards, get a 0% APR*, and pay no annual fee.
Customers who bought Network Security also bought:
Authentication
by Richard E. Smith
Price: $34.12
Used & new from $15.00
Add to cart
Security in Computing, Third Edition
by Charles P. Pfleeger, Shari Lawrence Pfleeger
Price: $79.00
Used & new from $29.99
Add to cart
Applied Cryptography
by Bruce Schneier
Price: $78.21
Used & new from $50.00
Add to cart
Explore similar items
Customers who shopped for Network Security also shopped for:
YOUR SHOPPING CART
Proceed to Checkout
Show gift options during checkout
Added to your Shopping Cart:
Network Security: Private Communication in a Public World, Second Edition- Charlie Kaufman Hardcover
$46.06
- Quantity: 1
Subtotal: $46.06
Edit shopping cart
Proceed to Checkout
Sign in to turn on 1-Click ordering.
Items in your Shopping Cart always reflect the most recent price displayed on their product pages.
100%

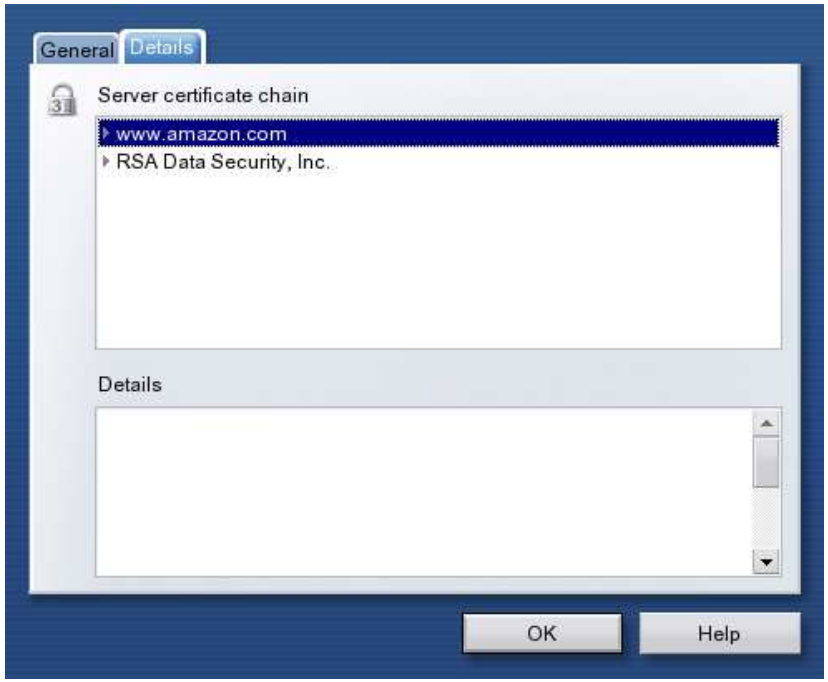

File Edit View Bookmarks Mail Tools Help
http://www.amazon.com/gp/cart/view.html/ref=pd_luc_mri/103-6001523-5107804
Gmail - Por si decid...
The Collection of C...
Amazon.com Chec...
Description of the S...
Introduction to SSL
Appendix B Introduc...
amazon.com.
SIGN IN
SHIPPING & PAYMENT
GIFT-WRAP
PLACE ORDER
Ordering from Amazon.com is quick and easy
Enter your e-mail address:
cobas@epsig.uniovi.es
I am a new customer.
(You'll create a password later)
I am a returning customer,
and my password is:
Sign In using our secure server
Forgot your password? Click here
Has your e-mail address changed since your last order?
The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server.
The only way to place an order at Amazon.com is via our Web site. (Sorry--no phone orders. However, if you prefer, you may phone in your credit card number after filling out the order form online.)
Redeeming a gift certificate? We'll ask for your claim code when it's time to pay.
Having difficulties? Please visit our Help pages to learn more about placing an order.
Conditions of Use Privacy Notice © 1996-2005, Amazon.com, Inc.
100%

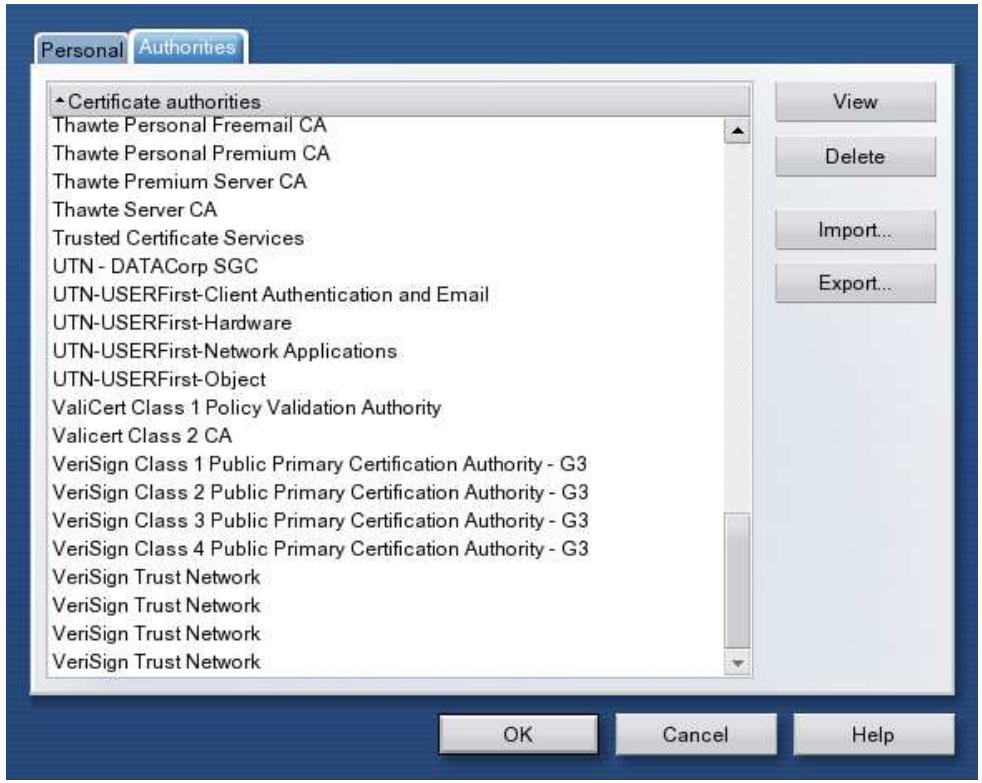

File Edit View Bookmarks Mail Tools Help
https://www.amazon.com/gp/flex/checkout/sign-in/select.html/103-6001523-5107804
Amazon.com Inc. (US)
Gmail - Por si decid...
The Collection of C...
Amazon.com Chec...
Description of the S...
Introduction to SSL
Appendix B Introduc...
amazon.com.
SIGN IN
SHIPPING & PAYMENT
GIFT-WRAP
PLACE ORDER
Please review and submit your order
By placing your order, you agree to Amazon.com's privacy notice and conditions of use.
Review the information below, then click "Place your order."
Place your order
Shipping Details
Shipping to:
Juan David Gonzalez Cobas
Naranjo de Bulnes, 1, 6-C
Gijon, Asturias 33211
Spain
Shipping Options: (Learn more)
Choose a shipping speed:
Standard International Shipping (averages 11-18 days)
Expedited International Shipping (averages 5-10 business days)
Priority International Courier (averages 2-4 days)
The following items will arrive in 1 shipment:
Need to Change quantities or delete ?
Estimated ship date for this item: May 18, 2005
Network Security: Private Communication in a Public World, Second Edition - Charlie Kaufman
$46.06 - Quantity: 1 - Usually ships in 24 hours
Condition: new
Gift options None
Order Summary
Items: $46.06
Shipping & Handling: $10.47
Total Before Tax: $56.53
Estimated Tax: $0.00
Order Total: $56.53
Why didn't I qualify for FREE Super Saver Shipping?
Have any gift cards, gift certificates or promotional claim codes?
Enter them here (one at a time):
Apply
Payment Method:
Visa: ***-93113
Exp: 05/2006
100%

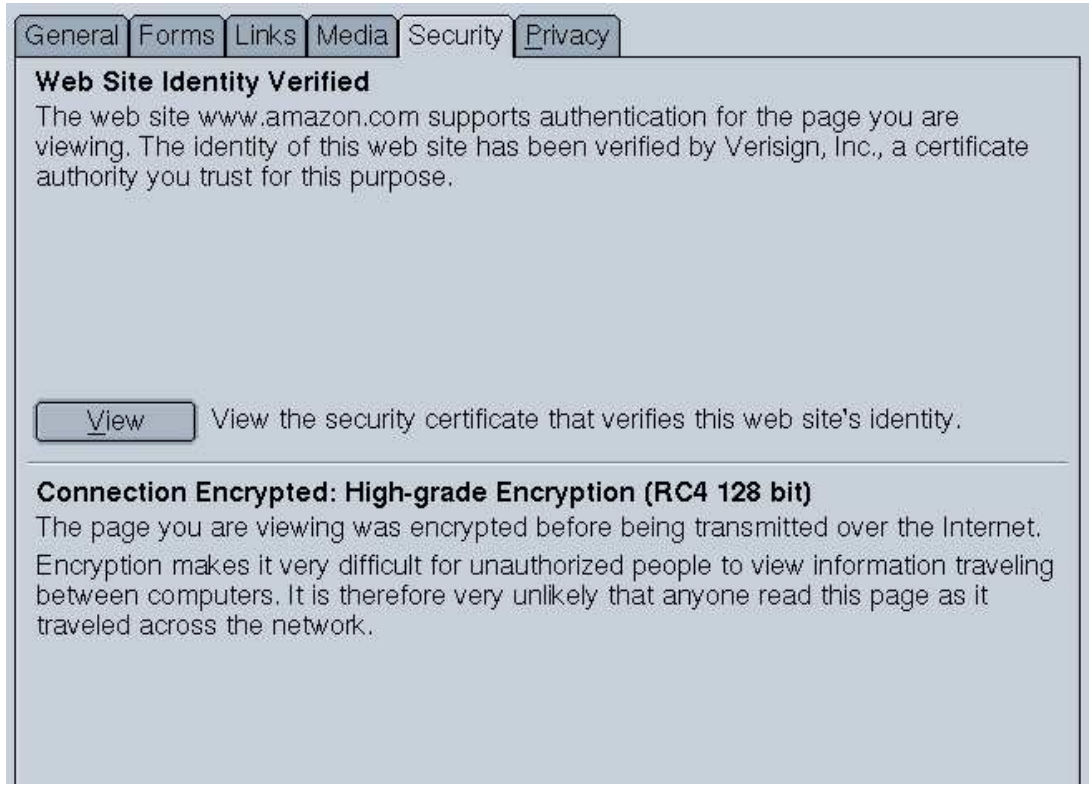

File Edit View Bookmarks Mail Tools Help
https://www.amazon.com/gp/flex/checkout/sign-in/select.html/103-6001523-5107804
Amazon.com Inc. (US)
Gmail - Por si decid...
The Collection of C...
Amazon.com Chec...
Description of the S...
Introduction to SSL
Appendix B Introduc...
amazon.com.
SIGN IN
SHIPPING & PAYMENT
GIFT-WRAP
PLACE ORDER
Please review and submit your order
By placing your order, you agree to Amazon.com's privacy notice and conditions of use.
Review the information below, then click "Place your order."
Place your order
Shipping Details
Shipping to:
Juan David Gonzalez Cobas
Naranjo de Bulnes, 1, 6-C
Gijon, Asturias 33211
Spain
Shipping Options: (Learn more)
Choose a shipping speed:
Standard International Shipping (averages 11-18 days)
Expedited International Shipping (averages 5-10 business days)
Priority International Courier (averages 2-4 days)
The following items will arrive in 1 shipment:
Need to Change quantities or delete ?
Estimated ship date for this item: May 18, 2005
Network Security: Private Communication in a Public World, Second Edition - Charlie Kaufman
$46.06 - Quantity: 1 - Usually ships in 24 hours
Condition: new
Gift options None
Order Summary
Items: $46.06
Shipping & Handling: $10.47
Total Before Tax: $56.53
Estimated Tax: $0.00
Order Total: $56.53
Why didn't I qualify for FREE Super Saver Shipping?
Have any gift cards, gift certificates or promotional claim codes?
Enter them here (one at a time):
Apply
Payment Method:
Visa: ***-93113
Exp: 05/2006
TLS v1.0 128 bit C4 (1024 bit RSA/SHA)
100%

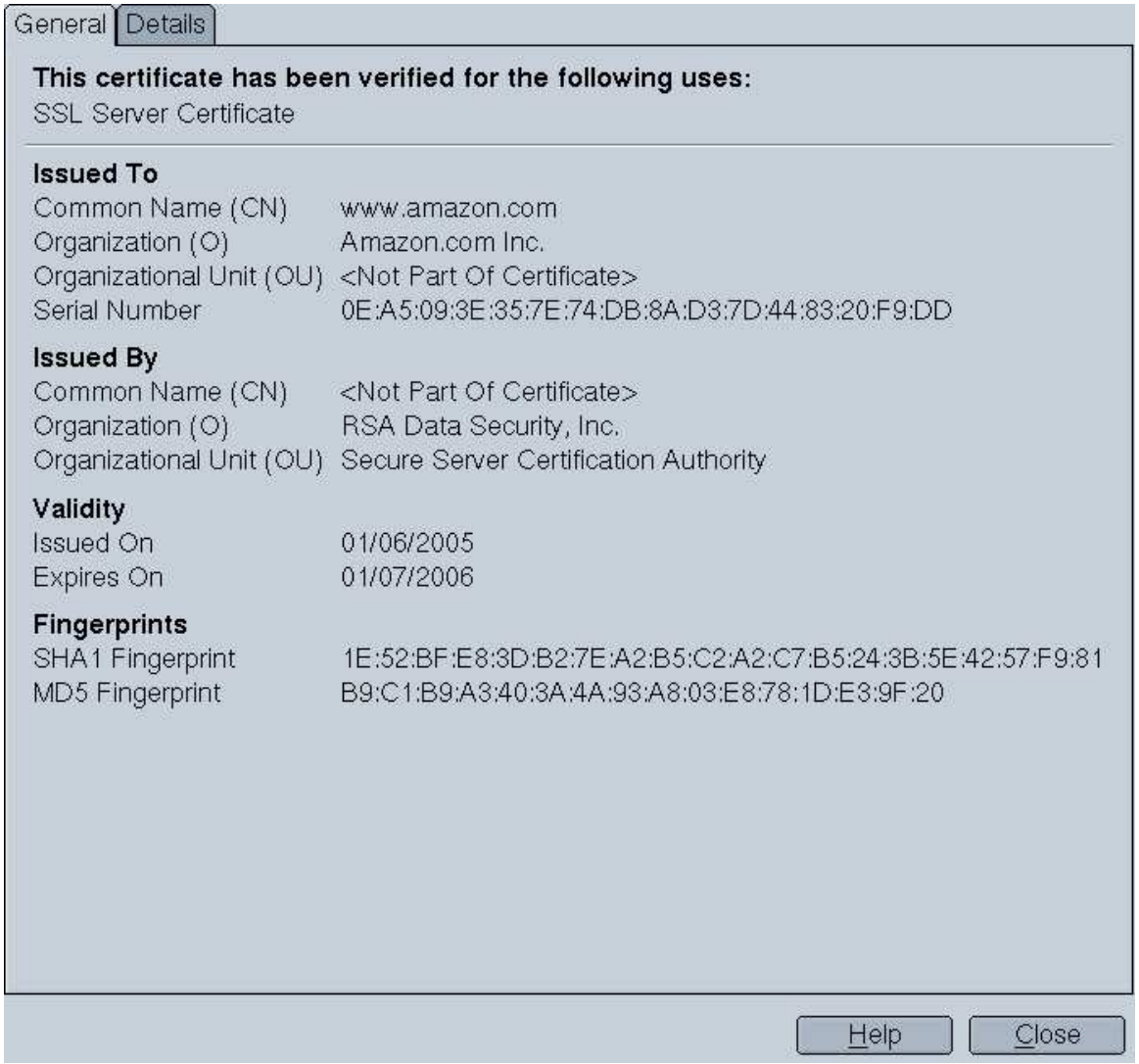

The following items will arrive in
Need to Change quantities or delete ?
Estimated ship date for this item
Network Security: Private Co
Charlie Kaufman
$46.06 - Quantity: 1 - Usually ships in
Condition: new
Gift options None
TLS v1.0 128 bit C4 (1024 bit RSA/SHA)


General
Details
Your communication with the server www.amazon.com is encrypted.
Opera has classified the encryption as strong (3).
the server www.amazon.com has identified itself with an electronic certificate. The certificate is signed and verified by an issuer that is on this browser's list of trusted authorities.
Certificate holder:
Certificate issuer:
www.amazon.com
Amazon.com Inc.
RSA Data Security, Inc.
Secure Server Certification Authority
Seattle
Washington, US
US
Not valid before:
Jan 6 2005
Expires:
Jan 6 2006
Encryption protocol:
TLS v1.0 128 bit C4 (1024 bit RSA/SHA)
OK
Help


General
Details
Server certificate chain
www.amazon.com
RSA Data Security, Inc.
Details
OK
Help

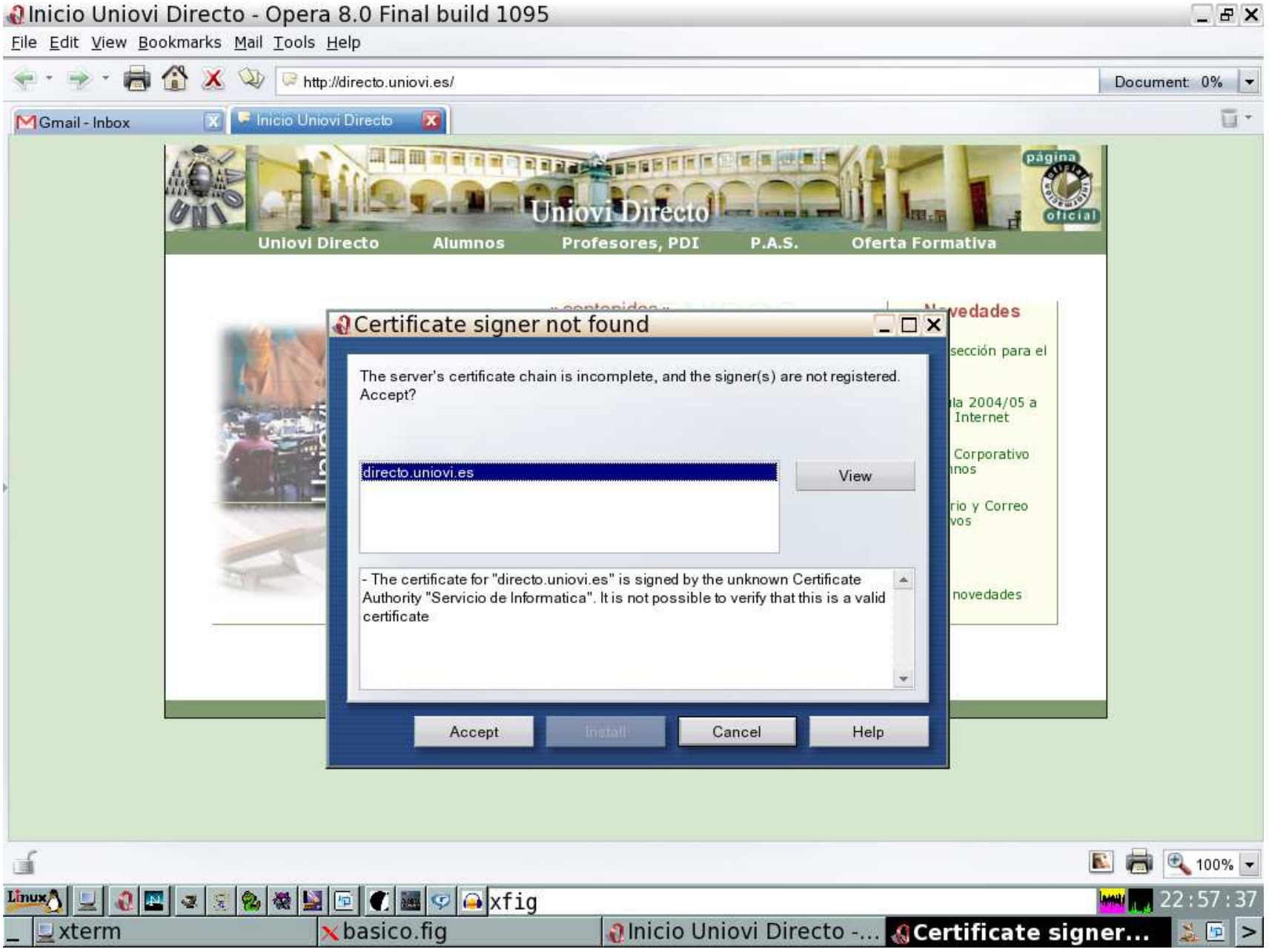

Personal
Authorities
Certificate authorities
Thawte Personal Freemail CA
Thawte Personal Premium CA
Thawte Premium Server CA
Thawte Server CA
Trusted Certificate Services
UTN - DATACorp SGC
UTN-USERFirst-Client Authentication and Email
UTN-USERFirst-Hardware
UTN-USERFirst-Network Applications
UTN-USERFirst-Object
ValiCert Class 1 Policy Validation Authority
Valicert Class 2 CA
VeriSign Class 1 Public Primary Certification Authority - G3
VeriSign Class 2 Public Primary Certification Authority - G3
VeriSign Class 3 Public Primary Certification Authority - G3
VeriSign Class 4 Public Primary Certification Authority - G3
VeriSign Trust Network
VeriSign Trust Network
VeriSign Trust Network
VeriSign Trust Network
View
Delete
Import...
Export...
OK
Cancel
Help


General
Forms
Links
Media
Security
Privacy
Web Site Identity Verified
The web site www.amazon.com supports authentication for the page you are viewing. The identity of this web site has been verified by Verisign, Inc., a certificate authority you trust for this purpose.
View
View the security certificate that verifies this web site's identity.
Connection Encrypted: High-grade Encryption (RC4 128 bit)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.


General
Details
This certificate has been verified for the following uses:
SSL Server Certificate
Issued To
Common Name (CN) www.amazon.com
Organization (O) Amazon.com Inc.
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 0E:A5:09:3E:35:7E:74:DB:8A:D3:7D:44:83:20:F9:DD
Issued By
Common Name (CN) <Not Part Of Certificate>
Organization (O) RSA Data Security, Inc.
Organizational Unit (OU) Secure Server Certification Authority
Validity
Issued On 01/06/2005
Expires On 01/07/2006
Fingerprints
SHA1 Fingerprint 1E:52:BF:E8:3D:B2:7E:A2:B5:C2:A2:C7:B5:24:3B:5E:42:57:F9:81
MD5 Fingerprint B9:C1:B9:A3:40:3A:4A:93:A8:03:E8:78:1D:E3:9F:20
Help
Close

¿Qué garantiza la autenticación SSL?

- Específicamente, *lo único que garantiza es que el servidor posee un certificado extendido por una CA que nuestro navegador incluye*.
- Los usuarios rara vez comprueban la validez de los certificados, ni poseen la pericia que ello requiere
- Un certificado no válido (autofirmado, CA no reconocida, etc.) desencadena una advertencia que *el usuario suele ignorar sistemáticamente*
- Caso PayPai: `www.paypal.com = www.paypai.com`


Inicio Uniovi Directo - Opera 8.0 Final build 1095
File Edit View Bookmarks Mail Tools Help
http://directo.uniovi.es/
Document: 0%
Gmail - Inbox
Inicio Uniovi Directo
Uniovi Directo
Uniovi Directo
Alumnos
Profesores, PDI
P.A.S.
Oferta Formativa
Certificate signer not found
The server's certificate chain is incomplete, and the signer(s) are not registered. Accept?
directo.uniovi.es
View
- The certificate for "directo.uniovi.es" is signed by the unknown Certificate Authority "Servicio de Informatica". It is not possible to verify that this is a valid certificate
Accept
Install
Cancel
Help
Novedades
100%
xfig
22:57:37
xterm
basico.fig
Inicio Uniovi Directo -...
Certificate signer...

Otros problemas de seguridad

SSL proporciona una protección razonable contra escuchas y secuestro de sesiones, y asegura la integridad de las mismas. Pero ese es un aspecto *minúsculo* de la seguridad WWW.

NO tiene nada que ver con la seguridad del servidor WWW. Puede ser tan vulnerable como se quiera.

El software cliente también almacena información sensible que puede ser utilizada por virus.

Es muy vulnerable a los ataques contra el DNS (caso PAYPAI).

Aporta una seguridad cuestionable respecto a la autenticidad del servidor. El usuario es responsable de su comprobación.

Servidores WWW “seguros”

Se da este (equívoco) nombre a los servidores WWW capaces de hablar HTTP sobre SSL, i.e., HTTPS.

El software servidor HTTP (habitualmente Apache) posee una extensión o módulo que lo capacita para hablar SSL (Apache-SSL).

El protocolo HTTPS se vincula habitualmente al puerto 443.

Además de un servidor Web capacitado para SSL, el servidor debe poseer un *certificado* de su *clave pública*, extendido por una *autoridad de certificación*.

Existen varias implementaciones de SSL: SSLeay (Eric A. Young), OpenSSL, etc.

OpenSSL (`http://www.openssl.org`)

Se trata de una implementación *open source* de SSL que proporciona una librería con las funciones necesarias para la programación del protocolo, y un conjunto de programas que permiten realizar las tareas básicas de mantenimiento (generación de claves, certificados, firmas, hashes, cifrados, etc).

La sintaxis del comando `openssl` es infernal y la documentación es muy espartana.

¿Cómo se configura un “servidor seguro”?

1. Se instala un servidor Web capacitado para SSL (e.g. Apache-SSL).
2. Se crea una clave pública con una implementación de SSL. E.g., con OpenSSL:

   ```
   openssl genrsa -des3 -out privkey.pem 2048
   ```

3. Se genera una *solicitud de firma de certificado* con otro conjuro similar:

   ```
   openssl req -new -key privkey.pem -out cert.csr
   ```

4. Se remite la solicitud a una CA, que nos devolverá un certificado (un fichero en formato PEM).
5. Se instala el certificado donde el servidor Web está configurado para encontrarlo.
6. Podemos prescindir de una CA si nos basta un certificado

autofirmado:

```
openssl req -new -x509 -key privkey.pem  \
        -out cacert.pem -days 1095
```

SSL y otros servicios

Además de su objetivo original (HTTP), SSL puede emplearse para proteger otros protocolos orientados a conexión: SMTP, POP, IMAP, TELNET e incluso FTP.

Los requisitos son como en el caso de HTTP:

- Un servidor capacitado para hablar SSL.
- Idem para el cliente.
- Un certificado para la autenticación del servidor.
- Opcionalmente, idem para el cliente

Así, existen versiones *SSL-parlantes* de servidores y clientes de correo electrónico SMTP, POP/IMAP, Telnet, y, por supuesto, HTTP.

SSL y tunelización

Existe otra forma más flexible de recubrir con SSL un servicio TCP para aportar a éste las ventajas de integridad, confidencialidad y autenticación que el protocolo soporta: envolver la conexión en un *túnel*

Conceptualmente, el túnel añade una capa más a la torre de protocolos (o un nivel más de encapsulación) que soporta la comunicación, añadiendo un servicio que la conexión TCP desnuda no tiene.

La ventaja del uso de un túnel frente al uso de servidores y clientes *SSL-aware* es doble:

- no requiere alteraciones en el software (parches, recompilaciones ni módulos adicionales). Se pueden usar los servidores “normales”. Sólo hay que especificar configuración, no código.
- SSL puede blindar parte de la ruta de datos, sin afectar necesariamente a toda ella, protegiendo los enlaces potencialmente más peligrosos (e.g., enlaces inalámbricos).

Túneles SSL: `sslwrap` y `stunnel`

Son los dos programas de encapsulado SSL más populares. `sslwrap`es el más sencillo de manejar y configurar.

`sslwrap` es invocado desde `inetd` (el super-server de Internet) para que realice el *handshake* SSL con el cliente que pretende emplear un servicio.

Una vez completado y establecido un canal cifrado SSL, `sslwrap` reenvía el *stream* TCP en claro al verdadero servidor, normalmente al servidor que escucha una dirección exclusivamente local.

Esto garantiza, al menos, que las contraseñas en tránsito no sean visibles, y puede proporcionar una forma parcial de autenticación.

Nota: con FTP no se puede (no es tan fácil).

Puertos asignados

Servicio	Puerto TCP	Puerto SSL	Nombre SSL	Tipo de Servicio
POP3	110	995	POP3S	fetch mail
IMAP	143	993	IMAPS	fetch/manage mail
SMTP	25	465	SMTPS	deliver mail
telnet	23	992	telnets	terminal
http	80	443	HTTPS	WWW
ftp	21	990	FTPS	transf. de ficheros (control)
ftp/data	20	989	FTPS-data	transf. de ficheros (datos)

```
# sslwrap
one of -port or -exec must be supplied
usage: sslwrap [args ...]

 -addr arg     - address to connect to (default is 127.0.0.1)
 -port arg     - port to connect to
 -accept arg   - port to accept on (default is stdin for inetd)
 -verify arg   - turn on peer certificate verification
 -Verify arg   - turn on peer certificate verification, must have a cert.
 -cert arg     - certificate file to use, PEM format assumed
                 (default is server.pem)
 -key arg      - RSA file to use, PEM format assumed, in cert file if
                 not specified (default is server.pem)
 -nbio         - Run with non-blocking IO
 -nbio_test    - test with the non-blocking test bio
 -debug        - Print more output
 -state        - Print the SSL states
 -nocert       - Don't use any certificates (Anon-DH)
 -cipher arg   - play with 'ssleay ciphers' to see what goes here
 -quiet        - No server output
 -no_tmp_rsa   - Do not generate a tmp RSA key
 -ssl2         - Just talk SSLv2
```

```
-ssl3          - Just talk SSLv3
-bugs          - Turn on SSL bug compatability
```

Algunos ejemplos

```
/usr/sbin/sslwrap -cert /etc/sslwrap/server.pem -port 80 \
          -accept 443 &
       /usr/sbin/sslwrap -cert /etc/sslwrap/server.pem -port 143 \
          -accept 993 &
       /usr/sbin/sslwrap -cert /etc/sslwrap/server.pem -port 23 \
          -accept 992 &
       /usr/sbin/sslwrap -cert /etc/sslwrap/server.pem -port 110 \
          -accept 995 &
```

Bibliografía

Esta descripción de SSL/TLS está desvergonzadamente extraída de los textos [3] y [2]

Referencias

[1] Network working group T. dierks request for comments: 2246 certicom category: Standards track C. allen certicom january 1999 the TLS protocol, Mar. 27 2002.

[2] S. Garfinkel and G. Spafford. *Web Security, Privacy & Commerce*. O'Reilly & Associates, Inc., 103a Morris Street, Sebastopol, CA 95472, USA, Tel: +1 707 829 0515, and 90 Sherman Street, Cambridge, MA 02140, USA, Tel: +1 617 354 5800, second edition, 2002.

[3] C. Kaufman, R. Perlman, and M. Speciner. *Network Security: Private Communication in a Public World*. Prentice Hall PTR, 2nd edition edition, 2002.