SECURITY IN ELECTRONIC COMMERCE - SOLUTION

Final exam OpenCourseWare

Name:

MULTIPLE-CHOICE QUESTIONS

Each question has only one correct answer, which ought to be clearly pointed out with an 'X'. Each question incorrectly answered will be evaluated as minus one third of the mark obtained had it been correctly answered.

1.- Time stamping authorities:

- □ Need to know the contents of the message to issue its time stamp.
- □ May issue the time stamp by concatenating the message with the date and time.
- □ **Take the date and time data from a trusted source.**

2.- The set of specifications developed by the IETF PKIX group:

- □ They are the same that the ones developed by ISO/IEC under the X.509 identifier.
- □ **One of them follows partially the ISO/IEC X.509 Recommendation.**
- □ None of them is based on the ISO/IEC X.509 Recommendation.

3. - The purpose of the specification ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES) is:

- □ To define a set of XML formats for the signatures used in the SET protocol
- □ **To define a set of XML formats for signatures that remain valid over long periods**
- □ To define a set of XML formats for signatures that must be used to create electronic invoices

4.- SSL:

- □ Does not allow data compression.
- □ **Supports RSA and DH as public key algorithms.**
- □ SSL acceleration is usually performed at client's side to make up for its usually less computing power.

5.- SET:

- □ It is relatively simple and has a low consumption of computer resources.
- □ **Demands all the participants to have an X.509 public-key certificate.**
- □ Simplifies the process of authenticating the client by using a password instead of public key certificates.

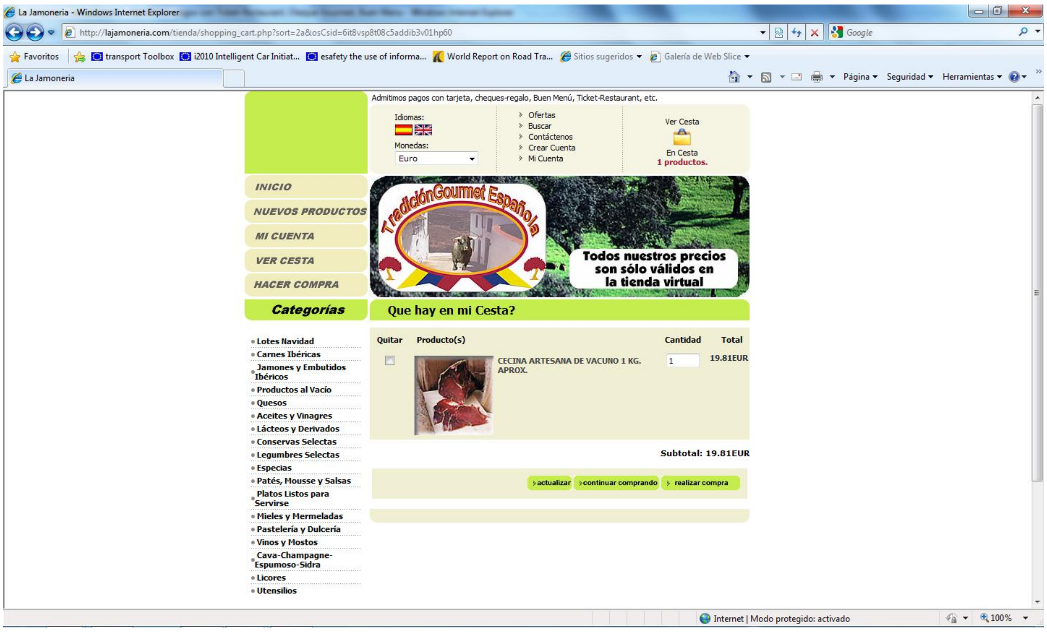
6.- 3D-Secure:

- □ Uses the mechanism known as dual signature to provide non-repudiation.
- □ Requires the merchant and the buyer to install specific software.
- □ **Helps issuer to verify that the person making an e-commerce purchase is an authorized cardholder.**

Authors: Arturo Ribagorda Garnacho, Ana Isabel González-Tablas Ferreres, José María de Fuentes García Romero de Tejada
Security in Electronic Commerce Open Course Ware. Computer Science Department. Universidad Carlos III de Madrid.

Question 1 . Next figures show the different steps of the purchase process followed in certain virtual shop. Answer the following questions:

a. **Mention existing security elements and assess the global security level that a typical user may sense.**
b. **List security services (not protocols) that have not been considered in this process (a maximum of three). Explain why they are important.**
c. **Do you miss the mandatory mention of some law?**
d. **Enumerate a maximum of five issues not specifically related to security that have an influence on the sensed security/insecurity. Do you miss some external endorsement that may help to increase the potential buyer's trust?**



http://lajamoneria.com/tienda/shopping_cart.php?sort=2a&osCsid=6it8vsp8t08c5addib3v01hp60

Admitimos pagos con tarjeta, cheques-regalo, Buen Menú, Ticket-Restaurant, etc.

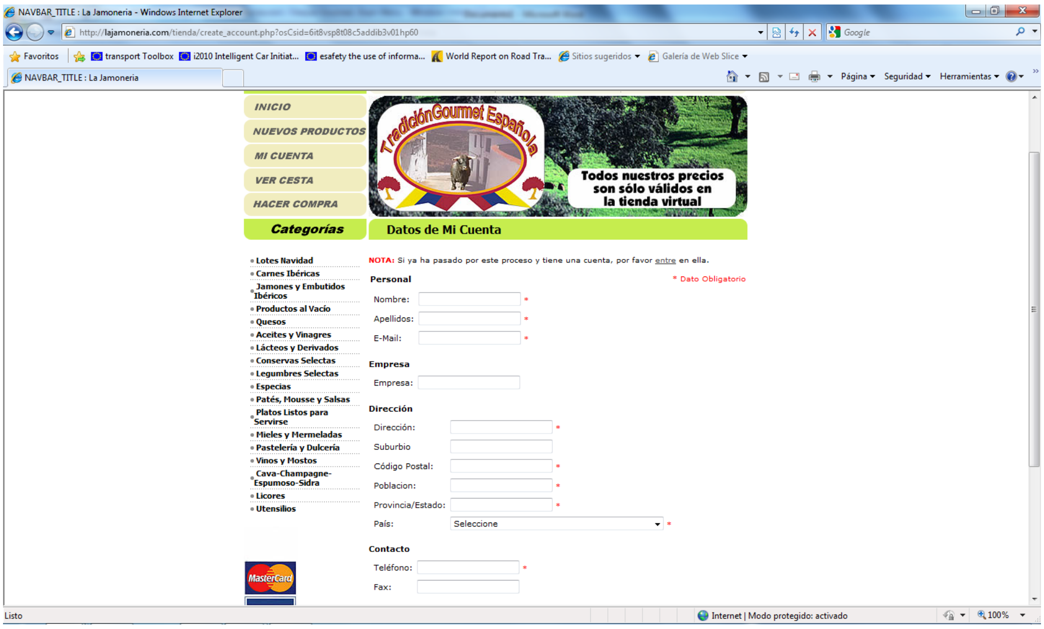
Todos nuestros precios son sólo válidos en la tienda virtual

Que hay en mi Cesta?

Quitar	Producto(s)	Cantidad	Total
□	CECINA ARTESANA DE VACUNO 1 KG. APROX.	1	19.81EUR

Subtotal: 19.81EUR

Figure 1. Product information


NAVBAR_TITLE : La Jamoneria - Windows Internet Explorer
http://lajamoneria.com/tienda/create_account.php?osCsid=6it8vsp8t08c5addib3v01hp60
Favoritos
transport Toolbox
i2010 Intelligent Car Initiat...
esafety the use of informa...
World Report on Road Tra...
Sitios sugeridos
Galería de Web Slice
NAVBAR_TITLE : La Jamoneria
Página
Seguridad
Herramientas
INICIO
NUEVOS PRODUCTOS
MI CUENTA
VER CESTA
HACER COMPRA
TradiciónGourmet Española
Todos nuestros precios son sólo válidos en la tienda virtual
Categorías
Lotes Navidad
Carnes Ibéricas
Jamones y Embutidos Ibéricos
Productos al Vacío
Quesos
Aceites y Vinagres
Lácteos y Derivados
Conservas Selectas
Legumbres Selectas
Especias
Patés, Mousse y Salsas
Platos Listos para Servirse
Mieles y Mermeladas
Pastelería y Dulcería
Vinos y Mostos
Cava-Champagne-Espumoso-Sidra
Licores
Utensilios
MasterCard
Listo
Internet | Modo protegido: activado
100%

Datos de Mi Cuenta

NOTA: Si ya ha pasado por este proceso y tiene una cuenta, por favor entre en ella.

Personal * Dato Obligatorio

Nombre: *

Apellidos: *

E-Mail: *

Empresa

Empresa:

Dirección

Dirección: *

Suburbio

Código Postal: *

Poblacion: *

Provincia/Estado: *

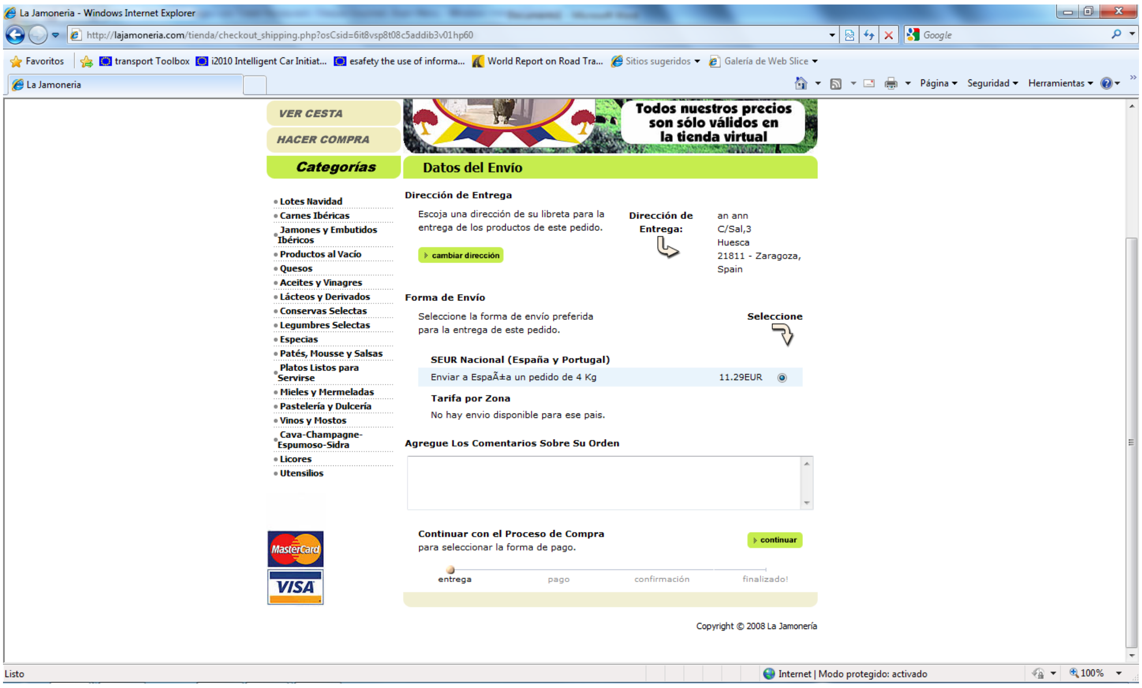
País: Seleccione *

Contacto

Teléfono: *

Fax:

Figure 2. Purchase process, step 1. Creation of an account.



Datos del Envío

Dirección de Entrega

Escoja una dirección de su libreta para la entrega de los productos de este pedido.

Dirección de Entrega:

an ann
C/Sal,3
Huesca
21811 - Zaragoza,
Spain

Forma de Envío

Seleccione la forma de envío preferida para la entrega de este pedido. Seleccione

SEUR Nacional (España y Portugal)

Enviar a EspaÃ±a un pedido de 4 Kg 11.29EUR ●

Tarifa por Zona

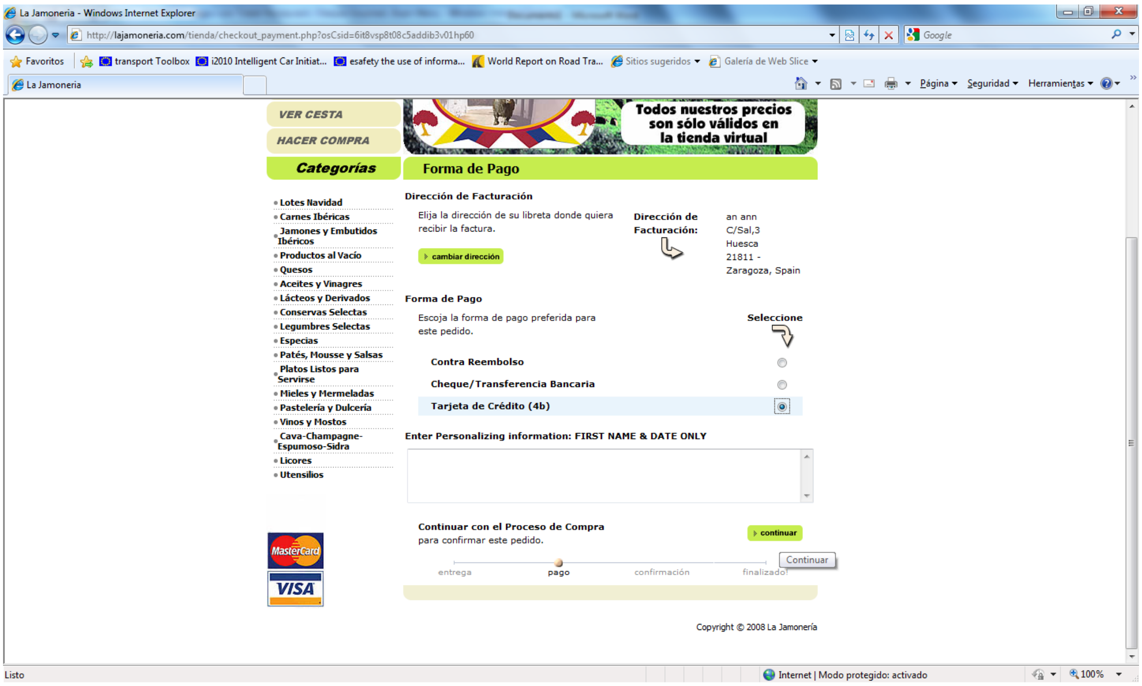
No hay envio disponible para ese pais.

Agregue Los Comentarios Sobre Su Orden

Continuar con el Proceso de Compra para seleccionar la forma de pago.

Copyright © 2008 La Jamonería

Figure 3. Purchase process, step 2. Confirmation of delivery information


La Jamoneria - Windows Internet Explorer
http://lajamoneria.com/tienda/checkout_payment.php?osCsid=6it8vsp8t08c5addib3v01hp60
Google
Favoritos
transport Toolbox
i2010 Intelligent Car Initiat...
esafety the use of informa...
World Report on Road Tra...
Sitios sugeridos
Galería de Web Slice
La Jamoneria
Página
Seguridad
Herramientas
VER CESTA
HACER COMPRA
Categorías
Todos nuestros precios son sólo válidos en la tienda virtual
cambiar dirección
continuar
Continuar
MasterCard
VISA
Listo
Internet | Modo protegido: activado
100%

Forma de Pago

- Lotes Navidad
- Carnes Ibéricas
- Jamones y Embutidos Ibéricos
- Productos al Vacío
- Quesos
- Aceites y Vinagres
- Lácteos y Derivados
- Conservas Selectas
- Legumbres Selectas
- Especias
- Patés, Mousse y Salsas
- Platos Listos para Servirse
- Mieles y Mermeladas
- Pastelería y Dulcería
- Vinos y Mostos
- Cava-Champagne-Espumoso-Sidra
- Licores
- Utensilios

Dirección de Facturación

Elija la dirección de su libreta donde quiera recibir la factura.

Dirección de Facturación:

an ann
C/Sal,3
Huesca
21811 -
Zaragoza, Spain

Forma de Pago

Escoja la forma de pago preferida para este pedido.

Seleccione

Contra Reembolso ○
Cheque/Transferencia Bancaria ○
Tarjeta de Crédito (4b) ●

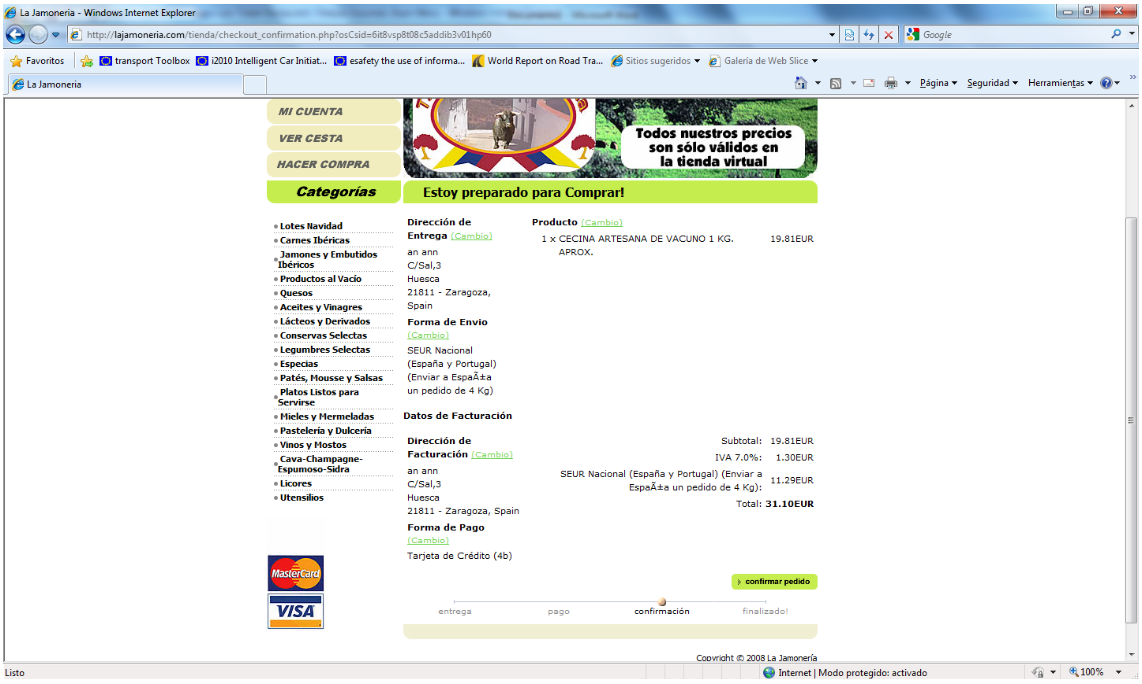
Enter Personalizing information: FIRST NAME & DATE ONLY

Continuar con el Proceso de Compra
para confirmar este pedido.

entrega — pago — confirmación — finalizado!

Copyright © 2008 La Jamonería

Figure 4. Purchase process, step 3. Selection of payment method


La Jamoneria - Windows Internet Explorer
http://lajamoneria.com/tienda/checkout_confirmation.php?osCsid=6it8vsp8t08c5addib3v01hp60
Google
Favoritos
transport Toolbox
i2010 Intelligent Car Initiat...
esafety the use of informa...
World Report on Road Tra...
Sitios sugeridos
Galería de Web Slice
La Jamoneria
Página
Seguridad
Herramientas
MI CUENTA
VER CESTA
HACER COMPRA
Categorías
Todos nuestros precios son sólo válidos en la tienda virtual
confirmar pedido
MasterCard
VISA
Listo
Internet | Modo protegido: activado
100%

Estoy preparado para Comprar!

- Lotes Navidad
- Carnes Ibéricas
- Jamones y Embutidos Ibéricos
- Productos al Vacío
- Quesos
- Aceites y Vinagres
- Lácteos y Derivados
- Conservas Selectas
- Legumbres Selectas
- Especias
- Patés, Mousse y Salsas
- Platos Listos para Servirse
- Mieles y Mermeladas
- Pastelería y Dulcería
- Vinos y Mostos
- Cava-Champagne-Espumoso-Sidra
- Licores
- Utensilios

Dirección de Entrega (Cambio)
an ann
C/Sal,3
Huesca
21811 - Zaragoza,
Spain

Forma de Envio (Cambio)
SEUR Nacional (España y Portugal) (Enviar a EspaÃ±a un pedido de 4 Kg)

Producto (Cambio)

1 x CECINA ARTESANA DE VACUNO 1 KG. APROX.	19.81EUR

Datos de Facturación

Dirección de Facturación (Cambio)
an ann
C/Sal,3
Huesca
21811 - Zaragoza, Spain

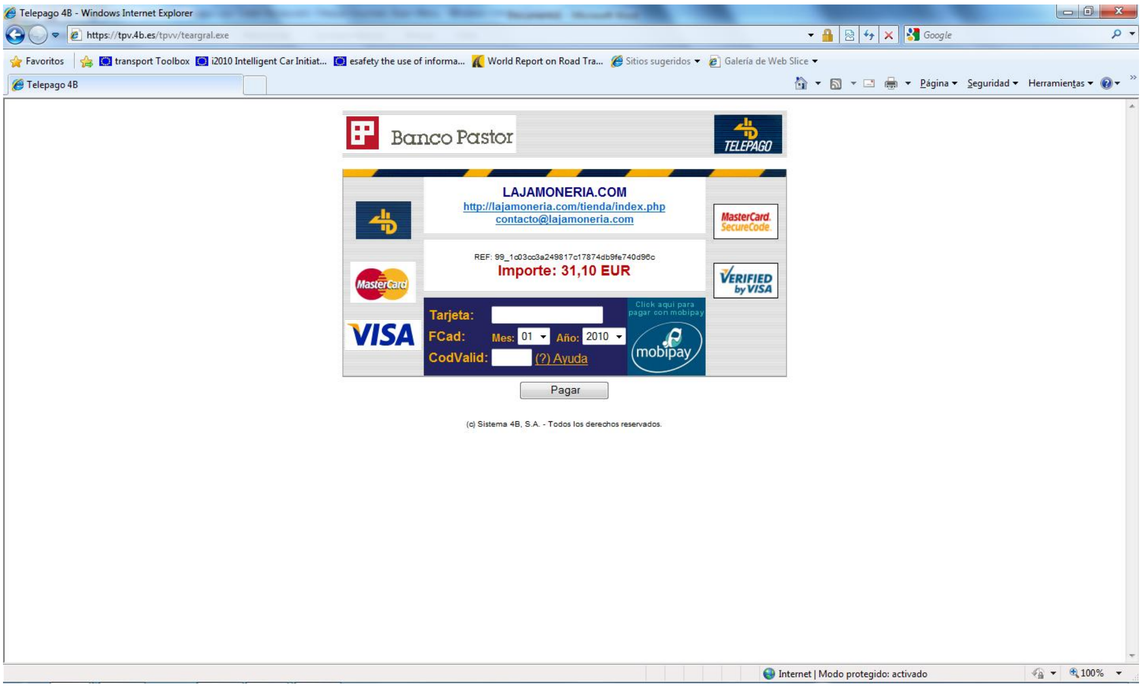
Forma de Pago (Cambio)
Tarjeta de Crédito (4b)

Subtotal:	19.81EUR
IVA 7.0%:	1.30EUR
SEUR Nacional (España y Portugal) (Enviar a EspaÃ±a un pedido de 4 Kg):	11.29EUR
Total:	**31.10EUR**

entrega — pago — confirmación — finalizado!

Copyright © 2008 La Jamonería

Figure 5. Purchase process, step 4. Purchase request confirmation


Telepago 4B - Windows Internet Explorer
https://tpv.4b.es/tpvv/teargral.exe
Google
Favoritos
transport Toolbox
i2010 Intelligent Car Initiat...
esafety the use of informa...
World Report on Road Tra...
Sitios sugeridos
Galería de Web Slice
Telepago 4B
Página
Seguridad
Herramientas
Banco Pastor
TELEPAGO
MasterCard SecureCode
MasterCard
VISA
VERIFIED by VISA
Click aqui para pagar con mobipay
mobipay
Pagar
Internet | Modo protegido: activado
100%

LAJAMONERIA.COM
http://lajamoneria.com/tienda/index.php
contacto@lajamoneria.com

REF: 99_1c03cc3a249817c17874db9fe740d96c
Importe: 31,10 EUR

Tarjeta:
FCad: Mes: 01 Año: 2010
CodValid: (?) Ayuda

(c) Sistema 4B, S.A. - Todos los derechos reservados.

Figure 6. Payment details using 4B payment system.

SOLUTION:

a) **The SSL socket is only established in the payment process. However, personal data is sent during the process. This fact, along with the comments that will be shown in the following parts of this exercise, leads to a low confidence level.**

b)

- **Data encryption, to avoid unauthorized access by third parties.**
- **Data integrity, to avoid message alteration during its transmission**
- **Server authentication, to be sure that the server is who it claims to be.**

c) **At least, the European Directive on Personal Data Protection (or, equivalently, the Spanish Data Protection Law) should be mentioned. Moreover, there are other legal references that could be introduced as well – the Spanish Information Society and E-Commerce Services Law).**

d) **There are several issues to be commented:**

- **The total amount is not correct – VAT is not included in it.**
- **There are several uncommon words (like "Suburbio").**

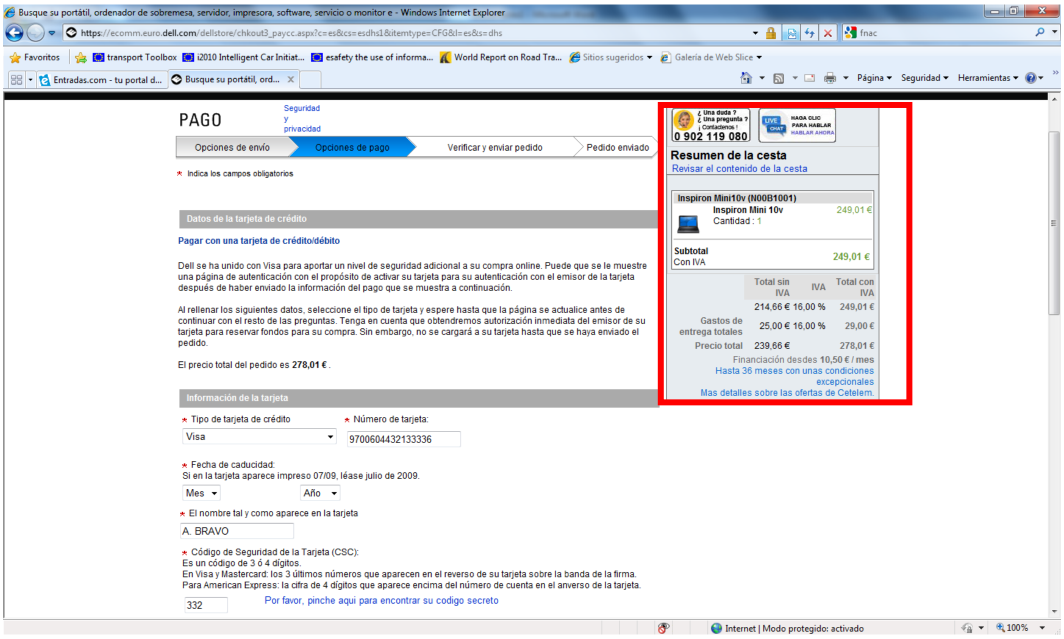
SECURITY IN ELECTRONIC COMMERCE - SOLUTION

Final exam OpenCourseWare
Name:

- ○ **There are several spelling mistakes**
- ○ **The purchase reference is not user friendly**
- ○ **There are some fields that could lead to misunderstandings – i.e. FCad.**
- ○ **There are English sentences inserted in the Spanish text.**
- ○ **The date does not appear in any screen**

Some good practice examples could be the following ones:

- **Price calculation clearly stated**


Busque su portátil, ordenador de sobremesa, servidor, impresora, software, servicio o monitor e - Windows Internet Explorer
https://ecomm.euro.dell.com/dellstore/chkout3_paycc.aspx?c=es&cs=esdhs1&itemtype=CFG&l=es&s=dhs
fnac
Favoritos
transport Toolbox
i2010 Intelligent Car Initiat...
esafety the use of informa...
World Report on Road Tra...
Sitios sugeridos
Galería de Web Slice
Entradas.com - tu portal d...
Busque su portátil, ord...
Página
Seguridad
Herramientas
Internet | Modo protegido: activado
100%

PAGO

Seguridad y privacidad

Opciones de envío | Opciones de pago | Verificar y enviar pedido | Pedido enviado

* Indica los campos obligatorios

Datos de la tarjeta de crédito

Pagar con una tarjeta de crédito/débito

Dell se ha unido con Visa para aportar un nivel de seguridad adicional a su compra online. Puede que se le muestre una página de autenticación con el propósito de activar su tarjeta para su autenticación con el emisor de la tarjeta después de haber enviado la información del pago que se muestra a continuación.

Al rellenar los siguientes datos, seleccione el tipo de tarjeta y espere hasta que la página se actualice antes de continuar con el resto de las preguntas. Tenga en cuenta que obtendremos autorización inmediata del emisor de su tarjeta para reservar fondos para su compra. Sin embargo, no se cargará a su tarjeta hasta que se haya enviado el pedido.

El precio total del pedido es **278,01 €** .

Información de la tarjeta

* Tipo de tarjeta de crédito: Visa
* Número de tarjeta: 9700604432133336

* Fecha de caducidad:
Si en la tarjeta aparece impreso 07/09, léase julio de 2009.
Mes Año

* El nombre tal y como aparece en la tarjeta
A. BRAVO

* Código de Seguridad de la Tarjeta (CSC):
Es un código de 3 ó 4 dígitos.
En Visa y Mastercard: los 3 últimos números que aparecen en el reverso de su tarjeta sobre la banda de la firma.
Para American Express: la cifra de 4 dígitos que aparece encima del número de cuenta en el anverso de la tarjeta.
332 Por favor, pinche aqui para encontrar su codigo secreto

¿ Una duda ? ¿ Una pregunta ? ¡ Contactenos !
0 902 119 080

LIVE CHAT HAGA CLIC PARA HABLAR HABLAR AHORA

Resumen de la cesta

Revisar el contenido de la cesta

Inspiron Mini10v (N00B1001)

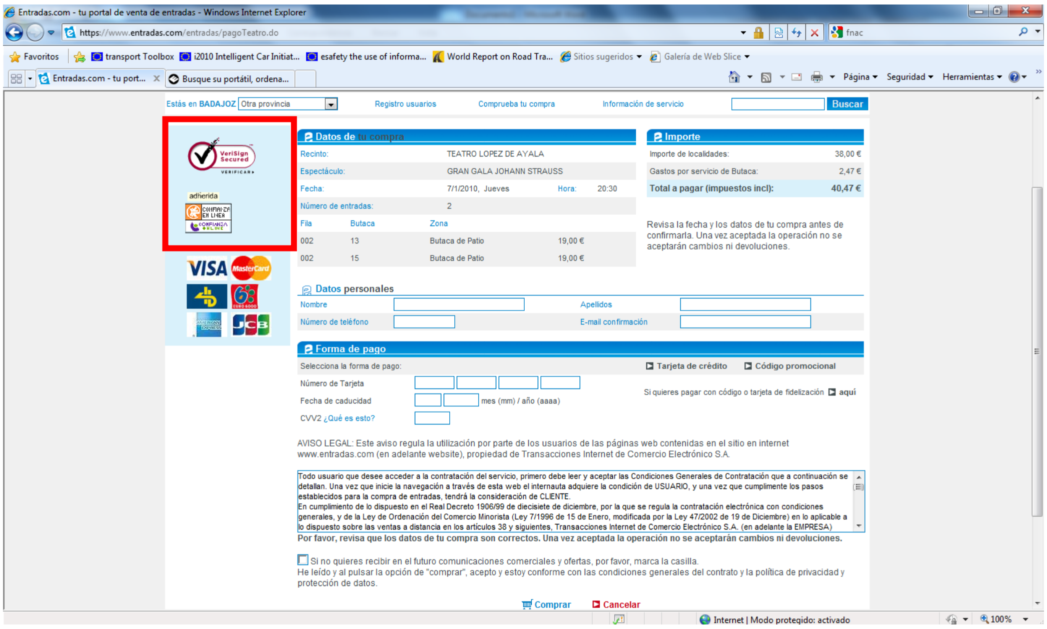
Inspiron Mini 10v 249,01 €
Cantidad : 1

Subtotal Con IVA 249,01 €

	Total sin IVA	IVA	Total con IVA
	214,66 €	16,00 %	249,01 €
Gastos de entrega totales	25,00 €	16,00 %	29,00 €
Precio total	239,66 €		278,01 €

Financiación desdes **10,50 € / mes**
Hasta 36 meses con unas condiciones excepcionales
Mas detalles sobre las ofertas de Cetelem.

- **Using external confidence seals (like Confianza online, Verisign seal, etc.)**


Entradas.com - tu portal de venta de entradas - Windows Internet Explorer
https://www.entradas.com/entradas/pagoTeatro.do
fnac
Favoritos
transport Toolbox
i2010 Intelligent Car Initiat...
esafety the use of informa...
World Report on Road Tra...
Sitios sugeridos
Galería de Web Slice
Entradas.com - tu port...
Busque su portátil, ordena...
Página
Seguridad
Herramientas
Estás en BADAJOZ
Otra provincia
Registro usuarios
Comprueba tu compra
Información de servicio
Buscar
VeriSign Secured
VERIFICAR
adherida
CONFIANZA EN LINEA
CONFIANZA ONLINE
VISA
MasterCard
AMERICAN EXPRESS
JCB
Internet | Modo protegido: activado
100%

Datos de tu compra

Recinto:	TEATRO LOPEZ DE AYALA		
Espectáculo:	GRAN GALA JOHANN STRAUSS		
Fecha:	7/1/2010, Jueves	Hora:	20:30
Número de entradas:	2		

Fila	Butaca	Zona	
002	13	Butaca de Patio	19,00 €
002	15	Butaca de Patio	19,00 €

Importe

Importe de localidades:	38,00 €
Gastos por servicio de Butaca:	2,47 €
Total a pagar (impuestos incl):	**40,47 €**

Revisa la fecha y los datos de tu compra antes de confirmarla. Una vez aceptada la operación no se aceptarán cambios ni devoluciones.

Datos personales

Nombre Apellidos

Número de teléfono E-mail confirmación

Forma de pago

Selecciona la forma de pago: **Tarjeta de crédito** **Código promocional**

Número de Tarjeta

Fecha de caducidad mes (mm) / año (aaaa)

CVV2 ¿Qué es esto?

Si quieres pagar con código o tarjeta de fidelización **aquí**

AVISO LEGAL: Este aviso regula la utilización por parte de los usuarios de las páginas web contenidas en el sitio en internet www.entradas.com (en adelante website), propiedad de Transacciones Internet de Comercio Electrónico S.A.

Todo usuario que desee acceder a la contratación del servicio, primero debe leer y aceptar las Condiciones Generales de Contratación que a continuación se detallan. Una vez que inicie la navegación a través de esta web el internauta adquiere la condición de USUARIO, y una vez que cumplimente los pasos establecidos para la compra de entradas, tendrá la consideración de CLIENTE.

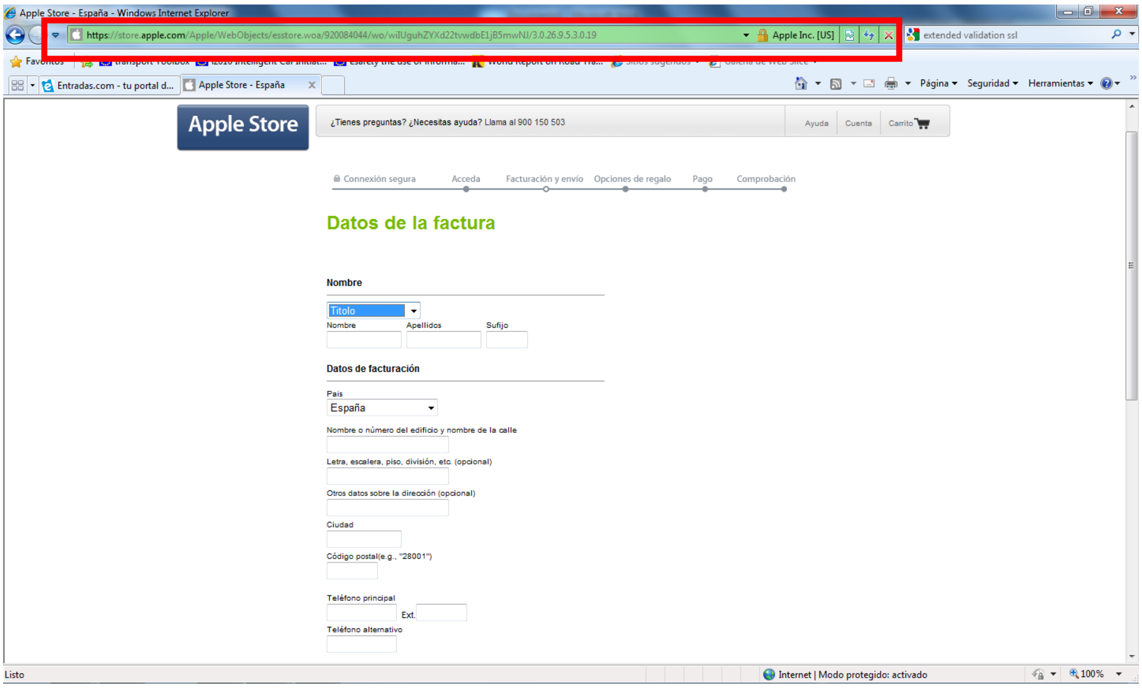
En cumplimiento de lo dispuesto en el Real Decreto 1906/99 de diecisiete de diciembre, por la que se regula la contratación electrónica con condiciones generales, y de la Ley de Ordenación del Comercio Minorista (Ley 7/1996 de 15 de Enero, modificada por la Ley 47/2002 de 19 de Diciembre) en lo aplicable a lo dispuesto sobre las ventas a distancia en los artículos 38 y siguientes, Transacciones Internet de Comercio Electrónico S.A. (en adelante la EMPRESA)

Por favor, revisa que los datos de tu compra son correctos. Una vez aceptada la operación no se aceptarán cambios ni devoluciones.

☐ Si no quieres recibir en el futuro comunicaciones comerciales y ofertas, por favor, marca la casilla.
He leído y al pulsar la opción de "comprar", acepto y estoy conforme con las condiciones generales del contrato y la política de privacidad y protección de datos.

Comprar Cancelar

- **Use of EV-SSL**


Apple Store - España - Windows Internet Explorer
https://store.apple.com/Apple/WebObjects/esstore.woa/920084044/wo/wiIUguhZYXd22tvwdbE1jB5mwNJ/3.0.26.9.5.3.0.19
Apple Inc. [US]
extended validation ssl
Favoritos
Entradas.com - tu portal d...
Apple Store - España
Página
Seguridad
Herramientas
Apple Store
Ayuda
Cuenta
Carrito
Listo
Internet | Modo protegido: activado
100%

¿Tienes preguntas? ¿Necesitas ayuda? Llama al 900 150 503

Connexión segura Acceda Facturación y envío Opciones de regalo Pago Comprobación

Datos de la factura

Nombre

Titolo

Nombre Apellidos Sufijo

Datos de facturación

Pais
España

Nombre o número del edificio y nombre de la calle

Letra, escalera, piso, división, etc. (opcional)

Otros datos sobre la dirección (opcional)

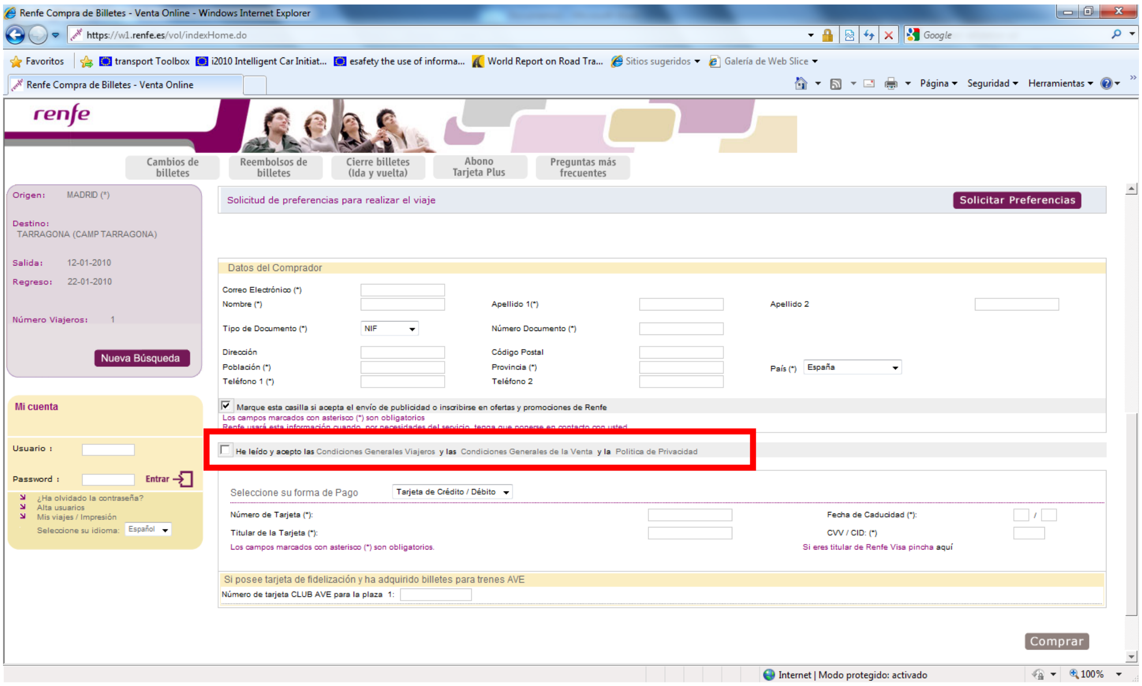
Ciudad

Código postal(e.g., "28001")

Teléfono principal Ext.

Teléfono alternativo

- **Reference to the Agreement conditions, the Terms of use and the privacy policy**


Renfe Compra de Billetes - Venta Online - Windows Internet Explorer
https://w1.renfe.es/vol/indexHome.do
Google
Favoritos
transport Toolbox
i2010 Intelligent Car Initiat...
esafety the use of informa...
World Report on Road Tra...
Sitios sugeridos
Galería de Web Slice
Renfe Compra de Billetes - Venta Online
Página
Seguridad
Herramientas
renfe
Cambios de billetes
Reembolsos de billetes
Cierre billetes (Ida y vuelta)
Abono Tarjeta Plus
Preguntas más frecuentes
Solicitar Preferencias
Nueva Búsqueda
Entrar
Comprar
Internet | Modo protegido: activado
100%

Origen: MADRID (*)

Destino: TARRAGONA (CAMP TARRAGONA)

Salida: 12-01-2010

Regreso: 22-01-2010

Número Viajeros: 1

Mi cuenta

Usuario :

Password :

¿Ha olvidado la contraseña?
Alta usuarios
Mis viajes / Impresión
Seleccione su idioma: Español

Solicitud de preferencias para realizar el viaje

Datos del Comprador

Correo Electrónico (*)					
Nombre (*)		Apellido 1(*)		Apellido 2	
Tipo de Documento (*)	NIF	Número Documento (*)			
Dirección		Código Postal			
Población (*)		Provincia (*)		País (*)	España
Teléfono 1 (*)		Teléfono 2			

☑ Marque esta casilla si acepta el envío de publicidad o inscribirse en ofertas y promociones de Renfe

Los campos marcados con asterisco (*) son obligatorios

Renfe usará esta información cuando, por necesidades del servicio, tenga que ponerse en contacto con usted

□ He leído y acepto las Condiciones Generales Viajeros y las Condiciones Generales de la Venta y la Política de Privacidad

Seleccione su forma de Pago: Tarjeta de Crédito / Débito

Número de Tarjeta (*):		Fecha de Caducidad (*):	/
Titular de la Tarjeta (*):		CVV / CID: (*)	

Los campos marcados con asterisco (*) son obligatorios.

Si eres titular de Renfe Visa pincha aquí

Si posee tarjeta de fidelización y ha adquirido billetes para trenes AVE

Número de tarjeta CLUB AVE para la plaza 1:

Question 2 - Describe in detail the process that has to be followed to validate an X.509 public key certificate.

Check the following issues:

- **Cryptographically valid signature of the certificate using issuer's public key**
- **Correct validity period**
- **Compliance with critical extensions**
- **Appropriate intended purpose**
- **Adequacy of other policy constraints**
- **It has not been revoked or suspended**
- **Validate issuer's public key certificate and all the public key certificates of the certification path (check the same previous issues for each certificate).**
- **Check that the names in the certificates must be consistent with a valid certification path, that is, the subject of every certificate (except the last) is the issuer of the next certificate.**
- **Check appropriate trust of root certificate (last certificate in the certification path).**

Question 3 – During the process of retrieving a web page from a web server using an SSL connection during Christmas Eve of 2009, you receive the certificate shown below. Mention several reasons to not trust this certificate. Mention also if some of the used algorithms is considered insecure nowadays.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 65 (0x41)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1
        Validity
            Not Before: Jul 31 00:00:00 2004 GMT
            Not After : Sep  2 00:00:00 2004 GMT
        Subject: CN=MD5 Collisions Inc. (http://www.phreedom.org/md5)
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ba:a6:59:c9:2c:28:d6:2a:b0:f8:ed:9f:46:a4:
                    a4:37:ee:0e:19:68:59:d1:b3:03:99:51:d6:16:9a:
                    5e:37:6b:15:e0:0e:4b:f5:84:64:f8:a3:db:41:6f:
                    35:d5:9b:15:1f:db:c4:38:52:70:81:97:5e:8f:a0:
                    b5:f7:7e:39:f0:32:ac:1e:ad:44:d2:b3:fa:48:c3:
                    ce:91:9b:ec:f4:9c:7c:e1:5a:f5:c8:37:6b:9a:83:
                    de:e7:ca:20:97:31:42:73:15:91:68:f4:88:af:f9:
                    28:28:c5:e9:0f:73:b0:17:4b:13:4c:99:75:d0:44:
                    e6:7e:08:6c:1a:f2:4f:1b:41
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage:
                CRL Sign
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                A7:04:60:1F:AB:72:43:08:C5:7F:08:90:55:56:1C:D6:CE:E6:38:EB
            X509v3 Authority Key Identifier:
                keyid:BE:A8:A0:74:72:50:6B:44:B7:C9:23:D8:FB:A8:FF:B3:57:6B:68:6C

            Netscape Comment:
                3
    Signature Algorithm: md5WithRSAEncryption
        a7:21:02:8d:d1:0e:a2:80:77:25:fd:43:60:15:8f:ec:ef:90:
        47:d4:84:42:15:26:11:1c:cd:c2:3c:10:29:a9:b6:df:ab:57:
        75:91:da:e5:2b:b3:90:45:1c:30:63:56:3f:8a:d9:50:fa:ed:
        58:6c:c0:65:ac:66:57:de:1c:c6:76:3b:f5:00:0e:8e:45:ce:
        7f:4c:90:ec:2b:c6:cd:b3:b4:8f:62:d0:fe:b7:c5:26:72:44:
        ed:f6:98:5b:ae:cb:d1:95:f5:da:08:be:68:46:b1:75:c8:ec:
        1d:8f:1e:7a:94:f1:aa:53:78:a2:45:ae:54:ea:d1:9e:74:c8:
        76:67
```

```
SOLUTION:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 65 (0x41)
        Signature Algorithm: md5WithRSAEncryption

        Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1

        Validity
            Not Before: Jul 31 00:00:00 2004 GMT
            Not After : Sep  2 00:00:00 2004 GMT

        Subject: CN=MD5 Collisions Inc. (http://www.phreedom.org/md5)

        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ba:a6:59:c9:2c:28:d6:2a:b0:f8:ed:9f:46:a4:
                    a4:37:ee:0e:19:68:59:d1:b3:03:99:51:d6:16:9a:
                    5e:37:6b:15:e0:0e:4b:f5:84:64:f8:a3:db:41:6f:
                    35:d5:9b:15:1f:db:c4:38:52:70:81:97:5e:8f:a0:
                    b5:f7:7e:39:f0:32:ac:1e:ad:44:d2:b3:fa:48:c3:
                    ce:91:9b:ec:f4:9c:7c:e1:5a:f5:c8:37:6b:9a:83:
                    de:e7:ca:20:97:31:42:73:15:91:68:f4:88:af:f9:
                    28:28:c5:e9:0f:73:b0:17:4b:13:4c:99:75:d0:44:
                    e6:7e:08:6c:1a:f2:4f:1b:41
                Exponent: 65537 (0x10001)

        X509v3 extensions:

            X509v3 Key Usage:
                CRL Sign

         X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                A7:04:60:1F:AB:72:43:08:C5:7F:08:90:55:56:1C:D6:CE:E6:38:EB
            X509v3 Authority Key Identifier:
                keyid:BE:A8:A0:74:72:50:6B:44:B7:C9:23:D8:FB:A8:FF:B3:57:6B:68:6C
            Netscape Comment:
                3
    Signature Algorithm: md5WithRSAEncryption
        a7:21:02:8d:d1:0e:a2:80:77:25:fd:43:60:15:8f:ec:ef:90:
        47:d4:84:42:15:26:11:1c:cd:c2:3c:10:29:a9:b6:df:ab:57:
        75:91:da:e5:2b:b3:90:45:1c:30:63:56:3f:8a:d9:50:fa:ed:
        58:6c:c0:65:ac:66:57:de:1c:c6:76:3b:f5:00:0e:8e:45:ce:
        7f:4c:90:ec:2b:c6:cd:b3:b4:8f:62:d0:fe:b7:c5:26:72:44:
```

```
ed:f6:98:5b:ae:cb:d1:95:f5:da:08:be:68:46:b1:75:c8:ec:
1d:8f:1e:7a:94:f1:aa:53:78:a2:45:ae:54:ea:d1:9e:74:c8:
76:67
```

Question 4 - Explain the circumstances that lead to a successful Lebanese Loop attack at an ATM. What countermeasures can be applied?

It is critical for a Lebanese Loop attack to success that victim trusts attacker and gives him/her the PIN of the victim's credit card.

The most important countermeasures are to make users aware of the threats and educate them to safeguard their personal information while transacting at the ATM or on the Internet and prevent them from the possible frauds and attacks that are being committed

Problem 1 The protocol 3-D Secure by VISA™ allows the payment within e-commerce transactions. The entity known as Access Control Server (ACS) in this protocol has as main goal to authenticate the buyer in the transaction. As a result of the authentication process, the ACS sends a signed message (M1) to the merchant who verifies it. After interbank communications finish, the merchant sends the buyer an encrypted message (M2) showing the result of the purchase. As part of VISA's auditing process, we require you to check the following issues:

1. Message M1 comprises the following data items:

    a. Date: 20012010

    b. PAN: 1701001012211001

The signature algorithm is RSA.

The public key of the ACS is: K_p(ACS) = (e= 13 , n= 91)

The hash algorithm applied on the numeric data items of M1 works as follows: First, each data item is divided in groups of two digits. Then, it is calculated the sum of the set of two digits numbers identified in the previous step (for example: if data item is '4432', the resulting sum will be '76'). The hash of the complete message M1 is calculated by summing up the hashes of each data item and applying modulo operation with modulus 91.

Check if 32 is the correct signature over message M1.

2. Message M2 comprises the following data items:

    a. Date: 17

b. Price: 18

Encrypt message M2. Take into account the following information regarding the keys:

K_p(merchant's public key) = (e= 32 , n= 64); K_v(buyer's prívate key) = (d= 37 , n= 143)

3. Forget the results obtained in the previous question of the problem. Suppose that message M2 only comprises a data item indicating the hour. Let 92 be the resulting ciphertext after encrypting message M2 using the keys previously specified in question 2. **Decrypt the ciphertext and explain briefly whether you consider reasonable or not the result of the decryption process.**

RSA operations reminder:

Sign / Decrypt: Result = M^d mod n

Verify / Encrypt: Result = M^e mod n

SOLUTION

1. **Hash(M1)= 17+1+0+10+12+21+10+1+20+1+20+10 mod 91 = 123 mod 91 = 32**

We have to check that:

32 = 32^e mod n = 32^{13} mod 91 = 32. The signature is correct, as the following expression holds:

32 = 32 mod 91

2.

K_p(Client) = (e= 13 , n= 143)

M2_1 = 17^{13} mod 143 = 95

M2_2 = 18^{13} mod 143 = 57

Encryption(M2) = M2_1 || M2_2 = 95 || 57

(The message must be divided because it cannot be sent at once. The modulo, 143, makes it impossible).

3.

Decryption of 92:

Decrypted = 92^{37} mod 143 = 27.

27 is not a valid hour, as the day has 24 hours. This error could be due to:

- **An incorrect sender configuration**
- **A malicious message alteration. Integrity cannot be assumed in this scenario – it is not explicitly stated in the problem description.**
- **A malicious third party, that has injected the message in the channel.**