Aufgabenblatt der Lernkontrolle: InfSi1_V09

Name der Lernkontrolle:	InfSi1_V09
Beschreibung:	
Startzeitpunkt:	01. May 2016 09:59:00
Endzeitpunkt:	08. May 2016 09:59:00
Maximale Punktezahl:	61
Anzahl Fragen:	19
Anzahl eigene Teilnahmen:	1
Teilnehmer:	Rico Akermann (rakerman@hsr.ch)
Startzeitpunkt Teilnahme:	30. July 2016 10:03:44
Endzeitpunkt Teilnahme:	30. July 2016 10:25:09
Benötigte Zeit:	00:21:25
Punkte:	26/61 (43%)

Frage 1: Welche beiden Firmen beherrschen 2016 den weltweiten Zertifikate Markt (für Web Server Zertifikate)?

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	Symantec
✓	✓	Comodo
✗	✗	Go Daddy Group
✗	✗	GlobalSign
✗	✗	DigiCert

Frage 2: Welche Signatur ist der handschriftlichen Signatur rechtlich gleichgestellt (im Rahmen des Schweizer Signaturgesetztes)?

Richtige Antwort	Deine Antwort	Fragetext
O	O	digitale Signatur
O	◉	elektronische Signatur
O	O	fortgeschrittene elektronische Signatur
◉	O	qualifizierte elektronische Signatur

Frage 3: Die Certificate Revocation Liste wird ...

Richtige Antwort	Deine Antwort	Fragetext
✗	✗	☐ bei jedem https-Aufruf abgefragt.
✓	✓	☐ vom der Zertifizierungsstelle unterhalten.
✓	✗	☐ beim Google Chrome Browser immer konsultiert, wenn ein Extended Evaluation Certificate vorlieft.
✗	✓	☐ im Browser lokal abgespeichert.
✗	✗	… wird immer am 1. des Monats aktualisiert.

Frage 4: Welche Organisation wurde in der Schweiz dafür akkreditiert, Zertifikate-Diensteanbieter anzuerkennen?

Richtige Antwort	Deine Antwort	Fragetext
O	O	Verisign
◉	O	KPMG

O	◉	SwissSign
O	O	Swisscom

Frage 5: Was versteht man unter Schlüsselbeglaubigung mittels "Web of Trust"?

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	Die Beglaubigung der Zertifikate erfolgt nicht durch eine CA, sondern durch Person.
✗	✗	Die Beglaubigung der Zertifikate erfolgt durch eine CA namens "Web of Trust".
✗	✗	Die Beglaubigung der Zertifikate erfolgt ausschliesslich durch enge Freunde.
✓	✓	Ein Beglaubigungsverfahren, welches unter anderem auch bei PGP verwendet wurde.

Frage 6: Welche "Certificate Validation" Art ist bei Webserver Zertifikaten am weitesten verbreitet?

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	Domain Validation
O	O	Organisation Validation
O	O	Extended Validation

Frage 7: Falls man ein Zertifikat für einen Webserver beschaffen will, welches von einer CA herausgegeben ist, die in den meisten Browsern bekannt ist, ?

Richtige Antwort	Deine Antwort	Fragetext
✗	✗	so muss man mit Kosten von mehreren 100 Fr. pro Jahr rechnen.
✗	✗	so muss man dazu zu einem Notar gehen.
✓	✓	so kann man dies in wenigen Minuten bewerkstelligen, wenn man die Rechte für die Domain oder Webserverad
✓	✓	so kann man dies tun, ohne die Antwortzeiten bei der Anzeige der Webseiten wesentlich zu erhöhen.

Frage 8: Für "Code Signing" benötigt der Ersteller des Codes von öffentlichen Anwendungen ...

Richtige Antwort	Deine Antwort	Fragetext
O	O	unterschiedliche Zertifikate für Java Applets und AktiveX Komponenten.
◉	◉	bei jeder Signierung des Codes ein gültiges, von einer offiziellen Zertificate Authority aufgestelltes Zertifikat.
O	O	bei jeder neuen Version seines Codes ein neues Zertifikat.
O	O	eine private Certificate Authority, welche Self Signed Zertifikate ausgeben kann.

Frage 9: Was ist ein Fingerprint?

Richtige Antwort	Deine Antwort	Fragetext
✓	-	Ein Message Digest
✗	-	Der Hash über den Public Exponenten des RSA Algorithmus
✓	-	Ein Hashwert, welcher von Browsern für Server Zertifikate berechnet wurde.
✗	✓	Ein kryptologisch geschützter Hashwert.

Frage 10: Welche Aussagen treffen auf einen "Extended Validation Zertifikate" zu?

Richtige Antwort	Deine Antwort	Fragetext
✓	✗	werden vor allem von Finanzinstituten verwendet
✗	✗	liefern höhere Sicherheit bei der Verschlüsselung
✓	✓	werden in den meisten Browsern speziell angezeigt
✗	✗	können nur von Comodo bezogen werden

Frage 11: Welche Aussagen treffen auf "Root Zertifikate" zu?

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	sind self-signed
✓	✓	haben in der Regel eine längere Gültigkeitsdauer
✗	✗	werden vor allem bei bekannten Webservern eingesetzt
✗	✗	enthalten immer RSA-Schlüssel

Frage 12: Der zum Zertifikat im Browser angezeigte Fingerprint ist immer derjenige Hash, welcher signiert wird.

Richtige Antwort	Deine Antwort	Fragetext
O	◉	Richtig
◉	O	Falsch

Frage 13: Die EU-Richtlinien bzw. das Schweizer Signaturgesetz bezeichnen die Informationen, welche unten an die Email-Zeilen angefügt werden als ?

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	elektronische Signatur
O	O	fortgeschrittene elektronische Signatur
O	O	qualifizierte elektronische Signatur

Frage 14: Welche Aussagen treffen für einen PKCS#12 "Transport Container" zu?

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	Kann alle Zertifikate der Certificate Chain enthalten.
✗	✓	Kann keinen Private Key enthalten.
✗	✗	Besteht aus druckbaren ASCII-Characters.
✓	✓	Kann mehrere Zertifikate enthalten.

Frage 15: Mit welchem Zertifikatetyp kann man Domainnamen aus unterschiedlichen Domains abdecken?

Richtige Antwort	Deine Antwort	Fragetext
O	O	Wild Card Certificate
O	O	Extended Validation Certificate
◉	O	Unified Communication Certificate
O	◉	Domain Validated Certificate

Frage 16: Was sind bekannte CA's?

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	Comodo
✓	✓	Symantec
✓	✓	GoDaddyGroup
✗	✓	Seagate
✓	✓	GlobalSign

Frage 17: Im Browser wird der Anfang des öffentlichen Schlüssels so angegeben: "30 48 02 41 00 fe 1b 84 35?.". Im Cryptool jedoch fängt der öffentliche Schlüssel so an: "fe 1b 84 35?.". Was ist der Grund für diesen Unterschied?

Richtige Antwort	Deine Antwort	Fragetext
O	O	Das Cryptool zeigt das Zertifikat im .crt Format an, der Browser im .pem Format.
◉	◉	Das Cryptool zeigt nicht die Rohdaten des DER-codierten Zertifikats an, der Browser schon.

O	O	Das sind zwei unterschiedliche öffentliche Schlüssel.
O	O	Das Cryptool verwendet einen anderes Padding.

Frage 18: Was sind Hauptaufgaben einer Certificate Authority?

Richtige Antwort	Deine Antwort	Fragetext
✓	✓	Überprüfung der Echtheit des Besitzers eines Public Keys
✓	✓	Signierung und Aushändigung des Zertifikats
✗	✓	Registrierung der Herausgeber von Zertifikaten
✗	✓	Akkreditierung von Zertifikate-Herausgebern

Frage 19: Welche Aussagen treffen auf "Certificat Classes" zu?

Richtige Antwort	Deine Antwort	Fragetext
◉	◉	Sie liefern eine Aussage über die Güte der Überprüfung der Inhaber von Zertifikaten.
O	O	Sie liefern eine Aussage über die Güte der Überprüfung der Herausgeber von Zertifikaten.
O	O	Sie sind Standardisiert und haben bei allen Zertifikatsanbietern die genau gleiche Bedeutung.
O	O	Sie werden von den Browsern sehr genau beachtet.