The European Journal for the Informatics Professional
http://www.upgrade-cepis.org
Edizione italiana a cura di ALSI e Tecnoteca
http://upgrade.tecnoteca.it

Una Guida Pratica al Commercio Elettronico Sicuro

di
Sokratis K. Katzikas e Stefanos A. Gritzalis
(Traduzione italiana, a cura di Luigi Caso (ALSI), dell'articolo "A Best Practice Guide for Secure Electronic Commerce", pubblicato sul Vol. III, No. 6, Dicembre 2002, della rivista online UPGrade, a cura del CEPIS)

Parole chiave: e-Commerce, Public Key Infrastructure (PKI), Sicurezza.

1 Introduzione

Internet sta cambiando ogni aspetto della nostra vita, ma nessuna area sta subendo dei cambiamenti così rapidi e significativi come il modo di fare "business". Oggi le aziende, piccole, medie e grandi, stanno usando Internet per comunicare con i propri clienti, fornitori e partner, per agevolare la comunicazione tra i propri dipendenti e tra le varie sedi, per connettersi con i propri sistemi di back-end per la gestione dati e per effettuare transazioni commerciali, cioè fanno "e-business". In questa situazione, in cui quasi tutte le organizzazioni fanno sempre più affidamento sulle informazioni e su strutture informatiche, l'e-Commerce sta portando con sè nuove dipendenze e nuovi rischi.

Un'indagine tra le industrie ha scoperto che "organizzazioni impegnate in Web commerce, electronic supply chain ed Enterprise Resource Planning (ERP) subiscono un numero di incidenti di perdita di informazioni e di furto di segreti commerciali tre volte superiore rispetto a tutte le altre" [1].

L'Information Security Breaches Survey of the British Department of Trade and Industry [2] mostra che il 60% delle organizzazioni interpellate (su un totale di 1′000) ha subito una violazione della sicurezza negli ultimi 2 anni.

Le implicazioni finanziarie di un tale tipo di incidenti sono tutt'altro che trascurabili. Nel 1999 sono stati persi 7′600 milioni di dollari a causa del worm Melissa e di altri virus. Una banca internazionale perde 12 milioni di dollari in trasferimenti elettronici di fondi, non autorizzati, per l'insufficienza della sicurezza nell'EFT (Electronic Funds Transfer). Sei milioni di consumatori online sono stati vittime di frodi legate alle carte di credito o al loro uso non autorizzato sul Web [3]. Cittadini e aziende della Comunità Europea hanno perso tra i 6′000 e i 60′000 milioni di Euro su Internet, la maggior parte dei quali, apparentemente, per frode [4] [5]. Visa International sostiene che la metà di tutte le vertenze legate alle carte di credito riguardano transazioni via Internet: questo a dispetto del fatto che le transazioni online assommano soltanto al 2% del giro d'affari totale di Visa [6].

È evidente che fare e-Commerce non è sufficiente: quello che le aziende dovrebbero realmente analizzare bene è come dedicarsi ad un e-Commerce *sicuro*. In questo articolo vengono indirizzati alcuni aspetti dell'e-Commerce sicuro, in particolare quelli relativi alle Public Key Infrastructure. Nel paragrafo 2 viene fornito un modello per le transazioni e-Commerce e vengono tracciati i requisiti di sicurezza per l'e-Commerce basato su tale modello. Nel paragrafo 3 viene dimostrato come si possono soddisfare questi requisiti, usando una Public Key Infrastructure, PKI, e anche perchè rendere sicuro l'e-Commerce non è semplicemente implementare dei meccanismi tecnologici di sicurezza. Infine, il paragrafo 4 contiene alcune osservazioni conclusive.

2 Un Modello per l'e-Commerce

Le applicazioni di e-Commerce possono sembrare piuttosto diverse tra loro, a prima vista. Tuttavia, un esame più accurato rivela che esistono delle fasi distinte in ciascuna di esse, fatto questo che consente di costruire un modello generico che può definirle tutte. Un modello del genere è stato proposto in [7] per le "business transaction" ed è stato dimostrato [8] essere adatto anche a descrivere transazioni commerciali. Il modello è costruito sull'osservazione del fatto che il più elementare "building block" del commercio è l'*accordo di scambio* (*exchange transaction*). In una transazione di questo tipo, due parti, A e B, si accordano su delle condizioni di reciproca soddisfazione e le rispettano. La prima, A, è di solito chiamata *cliente* o *compratore*; la seconda, B, è solitamente chiamata *esecutore* o *venditore*. B accetta la richiesta di A di fornirgli qualcosa, in cambio della quale A garantirà un pagamento a B. La transazione può essere visualizzata come un ciclo di quattro fasi:

1. *Richiesta*. A fa richiesta a B di fornirgli un servizio (spesso questo porta alla trattativa sull'offerta fornita da B).
2. *Negoziazione*. A e B giungono ad un accordo su cosa sarà fornito esattamente (condizione di soddisfazione di A) e quale pagamento sarà effettuato (condizione di soddisfazione di B).
3. *Prestazione*. B compie le azioni necessarie ad adempiere la sua parte del contratto e notifica ad A quando ha terminato.
4. *Liquidazione*. A accetta il lavoro di B, dichiarandolo soddisfacente, e paga.

Le ultime due fasi possono essere – e di solito lo sono – combinate in una fase composta, chiamata fase di *Esecuzione*. Il modello è adatto per qualsiasi tipo di transazione, non solo per quelle elettroniche. Perchè una transazione si possa qualificare come elettronica, almeno una delle fasi viste sopra deve essere supportata dalle tecnologie dell'informazione e della comunicazione.

L'e-Commerce ha certamente molto da dare alle aziende. I suoi vantaggi sono generalmente riconosciuti e storie di successi riguardanti aziende che fanno "e-business" si possono trovare quasi ogni giorno sui giornali. Tuttavia, le società più grandi sono state piuttosto lente nel dedicarsi a questo tipo di transazioni, facendolo con cautela. Esse sostengono che la ragione più rilevante di questo comportamento è la preoccupazione riguardo la sicurezza delle transazioni elettroniche [9]. È un timore giustificato? Ebbene, diamo una sguardo più da vicino ai requisiti di sicurezza dell'e-Commerce nei termini del modello generico di transazione descritto sopra.

Durante la fase di Richiesta, le due parti della transazione hanno dei requisiti di sicurezza differenti. Da una parte, il compratore ha bisogno di essere certo che un'offerta che sta prendendo in considerazione sia valida, cioè deve essere sicuro che l'integrità delle informazioni che gli vengono presentate non sia stata compromessa. Dalla parte opposta, il venditore deve essere sicuro che l'offerta che sta facendo sia accessibile dal compratore. Se la transazione non è di quelle al dettaglio, il venditore può esigere che la sua offerta rimanga riservata tra sè e il compratore, per timore che un qualsiasi concorrente interferisca con la transazione. Il bisogno di confidenzialità è evidente anche, per entrambe le parti, nella fase di Negoziazione, in particolare quando questa riguarda negoziazioni di contratti. È anche importante, in questa fase, rendere impossibile il fatto che l'una o l'altra parte possano ripudiare la propria offerta, ma il principio di "non-repudiation" è ancora più importante nell'ultima fase, quella di Esecuzione. In questa fase deve anche essere garantita una forma di pagamento sicuro, così come la consegna assicurata dei beni. C'è anche da notare che alcuni beni sono di natura immateriale, per cui possono essere consegnati al compratore elettronicamente (ad es. azioni, rappresentate in modo digitale): questo, naturalmente, presenta alcuni requisiti di sicurezza abbastanza interessanti. Infine, altra cosa da osservare è che ciò che fondamentalmente differenzia l'e-Commerce dal commercio tradizionale è l'assenza di una comunicazione faccia a faccia. Le macchine non hanno alcun modo di sapere chi c'è realmente all'altra estremità della linea, una volta ricevute le informazioni concordate che le convincono delle identità dei soggetti coinvolti.

Per riassumere questa discussione, si può concisamente affermare che i requisiti di sicurezza dell'e-Commerce sono imperniati sulla necessità di salvaguardare la *confidenzialità*, l'*integrità* e la *disponibilità* di informazioni e sistemi, l'*autenticità* delle parti in comunicazione ed il principio di *non-repudiation* delle transazioni.

3 Indirizzare i Requisiti per l'e-Commerce Sicuro

Basandosi sulle conclusioni tracciate nel paragrafo precedente, è possibile affermare che la crittografia può indirizzare la maggior parte dei requisiti di sicurezza delle applicazioni di e-Commerce. Tuttavia, la crittografia simmetrica non è una soluzione praticabile per l'e-Commerce: le entità coinvolte nelle transazioni elettroniche possono essere completamente sconosciute l'una all'altra prima che abbia luogo la transazione, per cui condividere una chiave segreta (come richiesto dalla crittografia simmetrica), prima di effettuare una transazione, potrebbe essere utopistico per tali entità.

A livello di crittografia, quella asimmetrica, insieme ai certificati digitali, costituisce il meccanismo essenziale da usare nell'e-Commerce per garantire i servizi di sicurezza descritti nel precedente paragrafo. Ciononostante, resta comunque il problema della gestione della chiave e del certificato per il gran numero di utenti che fanno uso di strumenti inter-organizzativi di livello non elevato, anche se completamente automatizzati. In questi casi, viene richiesto un approccio più consolidato e più automatizzato, basato su una Public Key Infrastructure (PKI).

3.1 Public Key Infrastructure

Una PKI consiste di cinque diversi componenti [10]:

1. Certification Authorities, CA, che generano e revocano i certificati;
2. Organizational Registration Authorities, ORA, che fanno da garanti riguardo al legame tra le chiavi pubbliche e le identità (ed altri attributi) dei possessori dei certificati;
3. I possessori dei certificati, per i quali questi sono stati emessi e che possono firmare documenti digitali e criptarli;
4. I clienti, che convalidano le firme digitali ed il loro percorso di certificazione, a partire da una chiave pubblica nota di una CA affidabile;
5. I Repository, che conservano e rendono disponibili i certificati e le Certificate Revocation List, CRL.

Inoltre, una Time Stamping Authority, TSA, può essere considerata come parte della PKI. Le entità che operano collettivamente come CA, ORA, Repository e TSA sono state comunemente individuate come Trusted Third Parties, TTP, o, più di recente, come Certification Service Providers, CSP.

La maggior parte dei tentativi di definire un insieme di servizi che una PKI dovrebbe offrire non sono stati orientati alle necessità degli utenti [11]. I requisiti degli utenti da parte di una PKI sono stati riportati in diversi riferimenti [12]-[20]. Ciascuno di questi lavori ha indicato i requisiti utente per il proprio dominio applicativo. Tuttavia, un terreno comune può essere, ed è, stato trovato [21] [22]. Questo "insieme minimale" di requisiti include autenticazione degli utenti, integrità, privacy e riservatezza dei messaggi, non-repudiation da parte dell'origine e della destinazione del messaggio, disponibilità dei servizi, facilità d'uso. In aggiunta a questo insieme minimale, questioni come l'anonimità dei partecipanti, il time stamping, l'univocità dei documenti, l'interoperabilità tra elementi diversi, la protezione dall'inganno da parte di un partecipante verso l'altro e i problemi legali sono stati identificati come importanti.

Qui di seguito viene data una lista completa di servizi di una PKI che soddisfano i requisiti sopra esposti [23] [24]; questa lista include tutti i servizi specificati in [10]. Le funzioni richieste per rendere operativo ciascuno di questi servizi possono essere definite successivamente.

I servizi specifici di una PKI sono:

1. *Registrazione*. Affinchè un utente possa partecipare ad un ambiente PKI, si deve registrare presso un'ORA facente parte della PKI. Lo scopo principale di questo servizio è quello di stabilire un affidabile ed univoco legame tra un utente e la sua chiave pubblica.
2. *Firme Digitali*. Perchè siano soddisfatti i requisiti di autenticazione ed integrità dei messaggi e la non-repudiation della loro origine, la PKI dovrebbe offrire dei servizi di firma digitale.
3. *Cifratura*. La cifratura è un servizio di base che fornisce le funzioni di crittografia per la protezione della riservatezza dei messaggi in una rete di computer.

4. *Time Stamping*. Il servizio di time stamping è descritto come il processo di attribuzione di data e ora ad un documento, in modo da provarne l'esistenza in una particolare collocazione temporale.
5. *Non-repudiation*. La non-repudiation comporta la generazione, la conservazione, il recupero e l'interpretazione della prova che una particolare entità ha processato un determinato item di dati. Tale prova deve essere in grado di convincere una terza entità, indipendente, potenzialmente in tempi successivi, riguardo la legittimità di una richiesta.
6. *Gestione delle Chiavi*. La gestione della chiave è un servizio fondamentale all'interno di una architettura PKI. Questo servizio ha a che fare principalmente con la gestione delle chiavi di crittografia in modo appropriato, efficiente, scalabile e sicuro. Esso include la generazione di numeri casuali, la generazione della chiavi, la loro personalizzazione, la loro memorizzazione, il loro ritrovamento, il loro ripristino, il loro aggiornamento, la distribuzione delle chiavi, le funzioni relative alla compromissione della chiave, i servizi di backup e restore, le funzioni per la validazione di richieste di accesso alle chiavi e la determinazione dei diritti di accesso del personale alle funzioni di gestione delle chiavi.
7. *Gestione dei Certificati*. Un certificato digitale è un contrassegno elettronico che assicura il legame tra una certa entità e la sua chiave pubblica.
8. *Repository delle Informazioni*. Questo servizio tiene in efficienza l'insieme dei dati critici per l'operatività del sistema PKI. Esso specifica le regole generali per la memorizzazione, l'archiviazione e la manutenzione di diversi tipi di dati, dai requisiti legali dell'organizzazione alle necessità di system recovery.
9. *Directory Service*. Per poter interagire, un membro di una PKI deve avere accesso alle informazioni riguardanti gli altri membri. Questo obiettivo viene ottenuto attraverso l'utilizzo di Directory Service, dove le informazioni relative ai certificati di membri della PKI possono essere memorizzate dai CSP e recuperate da altri.
10. *Comunicazioni Mimetizzate*. Le comunicazioni mimetizzate non forniscono soltanto la riservatezza dei dati, ma nascondono anche l'effettiva comunicazione. Questo viene ottenuto aggiungendo dei finti messaggi al flusso di dati, consentendo ai CSP ed agli utenti di nascondere i trasferimenti effettivi di dati, sia in termini del loro effettivo verificarsi che della loro frequenza.
11. *Autorizzazione*. La PKI dovrebbe permettere, alle entità che lo richiedono, di delegare i diritti di accesso ad altre entità della PKI. Questo significa che un utente della PKI che è proprietario di una risorsa può concedere il diritto di accedervi ad un altro utente della PKI. I CSP dovrebbero assicurare la concessione dei diritti, inclusa la capacità di accedere a specifiche risorse o informazioni.
12. *Audit*. Per poter assicurare che certi requisiti operativi, procedurali, legali, qualitativi e di altro tipo siano soddisfatti, così che si accresca la fiducia, è richiesto un servizio di auditing.
13. *Assicurazione della Qualità e Servizi per l'Accrescimento della Fiducia*. Ci si attende che gli utenti potenziali di servizi PKI richiedano che vengano forniti servizi e prodotti di una certa qualità, o che siano disponibili entro un certo tempo, e che siano valutati in modo tale da avere il miglior prezzo possibile. Per raggiungere questi livelli, i servizi di PKI devono avere l'assicurazione della qualità.
14. *Servizi Orientati al Cliente*. Questo gruppo di servizi PKI include quelli che coinvolgono direttamente gli utenti o che richiedono dei contatti, o un certo tipo di relazione o contrattazione con l'utente finale. Esempi di questo tipo di servizi sono gli aspetti legali e le negoziazioni di pagamento tra un utente ed un CSP.
15. *Interoperabilità tra CSP*. È difficile che in un sistema PKI di grandi dimensioni tutti gli utenti siano collegati ad un unico CSP. I servizi di interoperabilità trattano le problematiche legate alla costituzione di una rete di CSP, magari operanti in aziende diverse, con politiche diverse e diversi domini di specializzazione.

3.2 Attività a Supporto della PKI

Sia i governi che il mondo dell'industria hanno compreso l'importanza della PKI per lo sviluppo dell'e-Commerce. Questo è il motivo per cui, negli ultimi anni, sono comparse delle leggi, nazionali e internazionali, che trattano questa materia. L'Unione Europea ha emesso una direttiva [25] che riguarda il problema legale delle firme digitali. Diversi Stati membri dell'Unione hanno già provveduto ad adottare misure legislative sulla stessa questione. Nel campo delle standardizzazioni, l'IETF (Internet Engineering Task Force) ha realizzato un importante lavoro sulla PKI [10], mentre l'Europa ha istituito la European Electronic Signature Standardization Initiative [26] come lavoro congiunto dell'European Telecommunications Standards Institute, ETSI, e l'European Standardization

Commitee, CEN. Queste attività mirano a rendere possibile la fornitura del servizio numero 15 descritto in precedenza, ossia ad assicurare interoperabilità tra diversi CSP.

Posto che diverse aziende si sono ormai convinte che la PKI è la soluzione ai problemi di sicurezza legati all'e-Commerce, come andrebbe affrontata la sua realizzazione? In base a [27], cinque sono le domande importanti da prendere in considerazione nella realizzazione di una PKI:

- *Qual è la strategia riguardo la PKI all'interno dell'organizzazione?* Tale strategia si concentra tipicamente o su una singola applicazione oppure sul consolidamento delle funzioni PKI per operazioni diverse.
- *Come viene ottenuta l'interoperabilità?* Ci sono due approcci di base a questo problema: puntare su prodotti di un particolare fornitore o puntare sugli standard.
- *Le applicazioni sono pronte per la PKI?* In molti casi, le aziende hanno due opzioni: spingere i fornitori di software a rendere le loro applicazioni adatte alla PKI oppure utilizzare propri sviluppatori di software, o programmatori a contratto, per fare questo lavoro.
- *Quanti clienti saranno coinvolti nella realizzazione iniziale?* I fornitori potrebbero suggerire che il coinvolgimento di migliaia di clienti sia un primo passo ragionevole. In realtà, molte aziende partono con progetti pilota con non più di poche centinaia – e spesso con meno di un centinaio – di clienti.
- *Quali sono i requisiti dello staff tecnico per la pianificazione e la realizzazione?* Meno della metà del costo di realizzazione di una PKI è imputabile all'acquisto ed all'installazione dell'hardware e del software. I rimanenti costi sono per la maggior parte associati all'assicurarsi il personale tecnico qualificato per pianificare e realizzare la PKI. Poichè questo è un lavoro che si esegue una volta sola, è preferibile darlo in outsourcing a consulenti di esperienza piuttosto che assumere e poi licenziare personale altamente "skillato", che è anche difficile a trovarsi.

3.3 Rendere Sicuro l'e-Commerce

Sembra, quindi, che la PKI sia *la* soluzione al problema del rendere sicuro l'e-Commerce. Con l'eccezione di quello della disponibilità (che, per inciso, può essere indirettamente indirizzato dalle accresciute capacità di autenticazione offerte da una PKI), tutti gli altri requisiti sono stati soddisfatti in pieno. Se così fosse davvero, allora gli incidenti riguardanti la sicurezza che il mondo reale dell'e-Commerce subisce ogni giorno non sarebbero dovuti succedere. Qual è, allora, il problema?

Il problema più frequente è che, mentre tutti riconoscono la necessità di rendere sicuro l'e-Commerce, ciò che non si sa è che la sicurezza è più che erigere barriere fisiche ed elettroniche. La cifratura più complessa ed il più robusto dei firewall sono praticamente inutili senza una politica della sicurezza che definisca chiaramente come questi strumenti debbano essere usati. Una politica del genere comporta dei rischi; essa è di alto livello e neutrale dal punto di vista tecnologico. Il suo obiettivo è quello di fissare direttive e procedure, e di definire contromisure e sanzioni in caso di non conformità ad esse [9]. È grave vedere che solo una organizzazione britannica, su sette, ha messo in piedi una politica formale di sicurezza della gestione delle informazioni [2].

4 Conclusione

La grande maggioranza delle aziende sono oggi in competizione l'una con l'altra nel campo dell'e-Commerce. Gli incentivi più comunemente usati per attrarre i clienti includono il fatto che il cliente tratta direttamente con il fornitore del servizio o del prodotto, prezzi ridotti (derivanti principalmente dall'assenza di intermediari) e la facilità di trovare un servizio o un prodotto.

Quello che il mondo degli affari sembra stia tralasciando è l'uso di un modello per le transazioni di e-Commerce, un modello che renderebbe chiari i requisiti funzionali che devono essere soddisfatti per poter saltare sul treno dell'e-Commerce. In questo articolo è stato fornito un modello del genere: la conclusione, basata su tale modello, è che il miglior incentivo verso l'e-Commerce per un cliente sono probabilmente i servizi integrati di sicurezza. Questo può indurre un cliente a fidarsi dell'e-Commerce ed a partecipare a transazioni elettroniche.

È stato mostrato quali servizi di una PKI le aziende necessitano di utilizzare per poter fare e-Commerce. Le tecnologie per la sicurezza delle informazioni ci sono; tutto ciò che si deve fare è usarle nella maniera opportuna. Quello che è necessario è un attento esame dei rischi implicati dal processo, un piano adeguato per gestirli e l'accettazione o l'attenuazione degli altri.

La sicurezza delle informazioni – se usata nel modo giusto – si dimostra ancora una volta essere un fattore di crescita, piuttosto che di impedimento, per il mondo del business.

Riferimenti

[1]
G. Dalton, "Acceptable Risks", Information Week, August 31, 1998.
[2]
DTI, Information Security Breaches Survey 2000, <http://www.dti.gov.uk/cii/dtiblue/dti_site/new_pages/>
[4]
A. Ghosh, e-Commerce Security, John Wiley & Sons, 1998.
[3]
Information Security Magazine, July 1999.
[5]
Edupage Editors, "EC Study Cites Fraud on the Internet", RISKS Digest, 18:35, August 19, 1996.
[6]
BBC Money Programme on Internet fraud, BBC 2, 21 November 1999 GMT 20:30.
[7]
T. Winograd and F. Flores, Understanding Computers and Cognition, Addison-Wesley, 1997.
[8]
P. J. Denning, "Electronic Commerce", in D. E. Denning & P. J. Denning (Eds), Internet Besieged, Addison-Wesley & ACM Press, 1998.
[9]
Andersen Consulting & CERIAS-Purdue University, Policy Framework for Interpreting Risk in eCommerce Security, 1999.
[10]
A. Arsenault and S. Turner, IETF PKIX WG, Internet draft, Internet X.509 Public Key Infrastructure PKIX Roadmap, March 10, 2000.
[11]
A. van Rensburg and S. von Solms, "A reference framework for Certi.cation Authorities / Trusted Third Parties", in L. Yngstrom and J. Carlsen (Eds.), Proceedings, IFIP 13th International Information Security Conference, Chapman & Hall, 1996.
[12]
Trusted Health Information Systems (THIS) project, Final report: Requirements on electronic signature services and TTP services, Swedish Institute for Health Services Development, 1995.
[13]
TrustHealth-ETS project, Functional speci.cation of TTP services, Swedish Institute for Health Services Development, 1995.
[14]
TTP & Electronic Signature Trial for Inter-Modal Transport (TESTFIT) project, Final report, CEC/DGXIII/B6, 1995
[15]
BOLERO project, Final Report, CEC/DGXIII/B6, 1995.
[16]
Ebridge project, Final Report, CEC/DGXIII/B6, 1995.
[17]

EAGLE project, Software description and functional specification of the TTP demonstrator, Deliverable 3, CEC/DGXIII/B6, 1997.
[18]
S2101 Project, User requirements for TTP services, CEC/DGXIII/B6, 1993.
[19]
EUROMED-ETS project, Final Report, CEC/DGXIII/B6, 1998.
[20]
A. Nilson, European Trusted Services (ETS) – Results of 1995 TTPs Projects. Final Report, Marinade Ltd., 1997
[21]
KEYSTONE project, KEYSTONE deliverable 1.1: User Requirements Statement, 1998.
[22]
KEYSTONE project, KEYSTONE deliverable 9.1: Final project report, 1998.
[23]
S. Gritzalis, S. K. Katsikas, D. Lekkas, K. Moulinos and E. Polydorou, "Securing the electronic market: The KEYSTONE Public Key Infrastructure Architecture", submitted for publication.
[24]
D. Lekkas, S.K. Katsikas, D.D. Spinellis, P. Gladychev and A. Patel, "User Requirements of Trusted Third Parties in Europe", in Proceedings, User identification and Privacy Protection Joint IFIP WG 8.5 and WG 9.6 Working Conference, Stockholm University, 1999.
[25]
European Union, Directive 1999/93/EC on a Community framework for electronic signatures, Official Journal of the European Communities, L13/12, 19 January 2000.
[26]
<http://www.ict.etsi.org/eessi/eessi-homepage.htm>
[27]
RSA Security Inc., Understanding PKI Infrastructure, 2000.

Note biografiche sugli autori

Sokratis K. Katzikas è nato ad Atene, Grecia, nel 1960. Ha ottenuto un Diploma di Laurea in Electrical Engineering all'Università di Patrasso, Grecia, nel 1982, un M.S. in Electrical and Computer Engineering dall'Università del Massachussets, ad Amherst, USA, nel 1984, ed un Ph. D. in Computer Engineering dall'Università di Patrasso, nel 1987. Ha avuto incarichi di docenza e di ricerca all'Università del Massachussets, all'Università di Patrasso, all'Istituto di Computer Technology a Patrasso, all'Università del LaVerne Athens Campus, all'Ufficio di Ricerca Navale della Marina Ellenica, al Technological Education Institute di Atene e all'Università di Economics & Business ad Atene. Attualmente è professore presso il Dipartimento di Information and Communication Systems Engineering ed è Vice-Rettore, riguardo a Finances and Development, dell'Università dell'Egeo. Ha preso parte a molti progetti R&D della Comunità Europea in ambiti di sicurezza, robotica e intelligenza artificiale. E' autore, o co-autore, di più di 100 tra articoli tecnici e presentazioni riguardanti le sue aree di interesse per la ricerca, che includono la sicurezza nei sistemi ICT, la teoria del calcolo approssimativo, l'adaptive control e l'intelligenza artificiale. Ha fatto parte di comitati di direzione, programmazione e organizzazione di conferenze internazionali sull'Informatica ed è recensore per diversi giornali scientifici. E' membro di numerose associazioni e società di computer ed è il delegato per la Grecia all'Assemblea Generale dell'IFIP. <ska@aegean.gr>

Stefanos A. Gritzalis è nato in Grecia nel 1961. Ha ottenuto un BSc in Fisica, un MSc in Automazione Elettronica ed un PhD in Informatica, tutti all'Università di Atene, Grecia. Attualmente è Assistente al Dipartimento di Information and Communication Systems Engineering, Università dell'Egeo, Grecia. Le sue esperienze professionali includono incarichi come senior consultant e ricercatore presso varie istituzioni, pubbliche e private. Ha partecipato a diversi progetti R&D, nazionali e della Comunità Europea, in aree legate all'Information and Communication Systems. Le sue pubblicazioni scientifiche includono tre libri (in greco) su argomenti relativi all'ICT e più di quaranta articoli per giornali e conferenze, nazionali e internazionali. Argomento principale di tali pubblicazioni è la sicurezza nei sistemi ICT. Ha fatto parte di comitati di programmazione e organizzazione di conferenze nazionali ed internazionali sull'Informatica ed è recensore per svariati giornali scientifici. E' stato Membro del Consiglio (Segretario Generale, Tesoriere) della Greek Computer Society. E' membro dell'ACM e dell'IEEE. E' inserito nelle liste di "Who's Who in the World" e di "International Who's Who of Information Technology". <sgritz@aegean.gr>

Luigi Caso, Laurea nel 1989 all'Università di Salerno in Scienze dell'Informazione. Attualmente lavora presso la Delos S.p.A., società del gruppo Getronics, come SW Engineer. Ha ottenuto Certificazioni Microsoft (MCP e MCSD), e partecipa, come Team Leader, alle fasi di analisi, progettazione ed implementazione di progetti SW in diversi ambiti (Gestione Documentale, Banking, Help Desk/CRM) (luigi.caso@getronics.com).

