

La sicurezza sulla *mobile-Internet*

di Nico Bondi

gennaio 2001



Da qualche tempo echeggia tra i ben informati un teorema non dimostrato: "il futuro di Internet è nel *mobile*". Se ciò corrisponda a verità avremo modo di scoprirlo a breve, visti i ritmi frenetici cui la Net Economy ci ha ormai abituati. Di certo c'è che molti a questo teorema sono, a torto o a ragione, ben disposti a credere. E a dimostrare questa convinzione stanno le esorbitanti cifre sborsate dai grandi operatori di telecomunicazioni per aggiudicarsi le aste indette in tutto il mondo per la concessione delle licenze UMTS.

Se il 'teorema' in questione ha un fondamento, è allora il caso di sviluppare qualche ragionamento ulteriore.

Internet nell'ultimo biennio ha progressivamente spostato il proprio asse dal cosiddetto *infotainment* verso una natura più orientata al business. Tale spostamento ha implicato necessariamente un aumento dell'attenzione rispetto ai problemi della sicurezza in rete, portando agli onori della cronaca temi sino ad oggi trascurati quali, per esempio, l'uso dei certificati digitali nella securizzazione delle transazioni elettroniche.

Ragionevolmente, se la tendenza generale di Internet è di enfatizzare la propria natura commerciale, anche la *mobile Internet* si dovrebbe delineare sempre di più come un veicolo per la gestione di servizi bancari, finanziari e business. Come molti sostengono, anzi, l'Internet mobile, condizionata quale è in termini di potenzialità multimediali dei supporti *wireless* (smart phones, PDA, etc.), avrà una intrinseca vocazione per tutti quei servizi che privilegiano il trattamento di dati sintetici in tempo reale come, appunto, il *mobile-banking* o il *mobile-trading*.

Ad ogni modo una *mobile Internet* rivolta alle utenze business o, comunque, a servizi economico-finanziari, non può fare a meno di confrontarsi col problema sicurezza. Non a caso nella seconda metà del 2000, tutti i principali providers di certificazione elettronica e di firma digitale hanno annunciato di avere raggiunto un avanzato stato di implementazione dei certificati digitali per il mondo mobile. VeriSign™, Entrust™, Baltimore™, GlobalSign™ e altre *certification authorities* hanno approntato certificati elettronici per architetture client/server WAP, in grado di consentire la comunicazione sicura tra un supporto wireless ed un WAP server, analogamente a quanto avviene nell'Internet 'fissa' con le connessioni supportate da SSL (il più diffuso sistema per rendere sicure le transazioni on-line). I certificati digitali mobili devono fare i conti con l'attuale scarsa capacità in termini di *storage* e di capacità di calcolo dei supporti wireless (telefonini WAP, palmari, etc.). Per questo motivo tutti le principali CA (certification authorities), in sinergia coi grandi produttori di hardware (Ericsson, Nokia e Motorola) hanno sviluppato un sistema basato su WTLS, ovvero il livello sicurezza del protocollo WAP. I certificati digitali WTLS sono una versione 'ridotta' rispetto allo standard X.509v3, usato comunemente sull'Internet fissa, e consentono l'elaborazione crittografica anche su device di scarsa potenza, utilizzando le funzioni crittografiche

incluse nel linguaggio WML.

La chiave di volta per la concretizzazione e la diffusione di sistemi di questo tipo sta in larga misura nella realizzazione di supporti wireless predisposti per queste tecnologie (con l'introduzione dei chip WIM) e nella rapida introduzione delle nuove tecnologie di trasmissione (GPRS e a seguire, UMTS). Solo una volta superato questo nodo strutturale si potrà iniziare a parlare in termini concreti della nuova frontiera del commercio elettronico, il cosiddetto M-commerce, e si inizieranno ad intravedere le reali potenzialità di tale mondo.

Corollario finale: "il futuro di Internet è nel *mobile* sicuro".

Nico Bondi

bondi@omegacube.it

Related links

<http://www.wapforum.org/>

http://www.globalsign.net/digital_certificate/wireless_security/index.cfm

<http://www.entrust.com/products/wireless/index.htm>

<http://www.verisign.com/wireless/index.html>

<http://www.baltimore.com/telepathy/index.html>

Nico Bondi, 25 anni, lavora attualmente come responsabile marketing e comunicazione presso OmegaCube, una società bolognese che si occupa di e-security. Laureato in Scienze della Comunicazione all'Università di Bologna si occupa di ICT dal 1995. Dal 1998 al 2000 ha lavorato come consulente per Iperbole, Rete Civica del Comune di Bologna, seguendo anche diversi progetti europei rivolti alla IT. Ha partecipato in qualità di relatore a diversi seminari e conferenze riguardo il community networking e la sicurezza informatica.



Le professioni di Internet

www.internos.it

Tutto il materiale contenuto in questo file è protetto dalle leggi del diritto d'autore. È proibita la riproduzione di tutto o in parte del contenuto senza l'autorizzazione scritta dell'Editore.