WebBook

SICUREZZA DELLA CERTIFICAZIONE DIGITALE

La certificazione digitale come sistema primario per la sicurezza del web

Massimo Penco
Vice presidente Gruppo Comodo,
Presidente Associazione Cittadini di Internet

Sicurezza della certificazione digitale

La certificazione digitale come sistema primario per la sicurezza del web

Massimo Penco
Vice presidente Gruppo Comodo, Presidente Associazione Cittadini di Internet

Ritengo che per usare gli strumenti che garantiscono la sicurezza, non solo nella propria organizzazione ma, soprattutto, per i propri clienti ed i probabili futuri clienti, bisogna conoscerne in modo approfondito le funzioni e l'uso, altrimenti si finisce per utilizzare tali sistemi in modo improprio e a discapito della sicurezza stessa.
Si parla spesso di certificati digitali, attribuendo a queste due parole un significato impreciso. Il certificato digitale altro non è che la parte finale del complesso sistema per la creazione di una comunicazione sicura tra un'entità ed un'altra. Nel caso del protocollo https, si tratta della creazione di un canale sicuro di comunicazione, attraverso la rete Internet, tra il sito web (che ha la titolarità del certificato digitale) ed un utente che entra in contatto con quello stesso sito web.
Quest'ultimo entra in possesso dei dati personali dell'utente solo quando questi inizia a comunicarli ai server del sito. Ciò accade per qualsiasi operazione legittima in cui si richiedano i dati personali (ad esempio, per effettuare una procedura di login), necessari per l'erogazione di un servizio.
Spetta quindi all'utente la facoltà di rilasciare tutte quelle informazioni ad un sito e tale libertà decisionale è il principio fondamentale sul quale si basa la Rete. Del resto, chi si approccia ad un sito web ha, oggi, tutte le informazioni necessarie per controllare se il sito al quale si sta collegando sia, più o meno, sicuro.
Il protocollo SSL è solo un tassello, ma di fondamentale importanza, per trasmettere e ricevere qualsiasi tipo d'informazione garantita. Tuttavia si tratta di un sistema imperfetto, come tutti quelli realizzati dall'uomo, dal momento che la "sicurezza totale" non è che una semplice utopia. Dopo oltre 15 anni la cer-

tificazione digitale e l'infrastruttura a chiavi pubbliche (PKI) commerciale è, e rimane, l'unica forma di sicurezza nella rete che, ormai, le Istituzioni finanziarie usano in tutto il mondo; si tratta di un periodo molto lungo per un sistema informatico che, in genere, ha un ciclo vitale molto più corto.
In tutti questi anni si sono irrobustite le chiavi, passate da 40 a 256/2048 bit, ma in sostanza nulla è cambiato: l'algoritmo è sempre quello, X509[1], e nulla di nuovo è stato inventato.
È dal 1978 che questo sistema trova la sua applicazione reale. Infatti sono tre i ricercatori del MIT (Ronald Rivest, Adi Shamir e Leonard Adleman) che hanno saputo implementare tale logica, utilizzando particolari proprietà formali dei numeri primi con alcune centinaia di cifre. L'algoritmo concepito da loro,(denominato RSA per via delle iniziali dei loro cognomi), non è sicuro da un punto di vista matematico teorico, poichè esiste la possibilità che, tramite la conoscenza della chiave pubblica, si possa decrittare un messaggio. Tuttavia l'enorme mole di calcoli e la quantità di tempo necessaria per trovare una soluzione, fa di questo algoritmo un sistema di affidabilità pressoché assoluta.
Ronald Rivest, Adi Shamir e Leonard Adleman, nel 1983, hanno brevettato l'algoritmo negli Stati Uniti dal MIT (brevetto 4.405.829, scaduto il 21 settembre 2000 e hanno dato vita alla società RSA Data Security che, successivamente, è divenuta nel 1995 Verisign, ovvero lo spin-off di RSA Security Inc. Ed è proprio da lì che è iniziata la mia avventura nel campo della sicurezza attraverso la certificazione digitale.
Una variante del sistema RSA è utilizzato nel pacchetto di crittografia Pretty Good Privacy (PGP). L'algoritmo RSA costituisce la base dei sistemi crittografici su cui si fondano i sistemi di sicurezza informatici utilizzati sulla rete Internet per autentificare gli utenti. Ultimamente sono state mosse critiche, più o meno eque in materia, nei confronti della Certification Authority ma, in ultima analisi, nulla è cambiato: i certificati digitali SSL restano come sono e assicurano lo scambio d'informazioni sulla totalità dei siti di banche ed assicurazioni in tutto il mondo.
Lo sfruttamento completo delle potenzialità dello strumento è ancora un obi-

---

[1] L'algoritmo X509 la pki

ettivo lontano dall'essere raggiunto e, molto spesso, l'uso dei certificati SSL e dei certificati digitali di firma è svilito, usato non correttamente e, ancor peggio, viene utilizzato in modo tale da non garantire quella sicurezza che lo stesso, invece, può e deve fornire. Inoltre, tali strumenti si acquistano sovente da chi propone il prezzo più basso e vengono impiegati nelle pagine web senza un reale criterio. Si perdono così di vista gli obiettivi primari della certificazione digitale ed è pertanto necessario stilare una sorta di best practise, ovvero un breve elenco di elementi da tener presenti per usare il certificato SSL in modo corretto.

Dare fiducia a chiunque navighi nel propri siti web

L'approccio migliore riservato all'utente quando entra in un sito web è quello di sentirsi a proprio agio. E' più facile per un hacker creare un clone di qualsiasi pagina web mancante di SSL e dirottare poi l'utente dove vuole con link falsi. Pertanto installare il certificato SSL nell'intero sito web, e non solo nelle pagine che si vogliono mettere in sicurezza, significa per l'utente entrare nel sito dalla porta principale: la Home page. Le vecchie considerazioni che imputavano all'installazione del certificato nell'intero sito, il rallentamento dello stesso sono ormai delle convinzioni superate e obsolete, alla luce della potenza di calcolo che tutti hanno a disposizione.

Usare strumenti avanzati di certificazione SSL

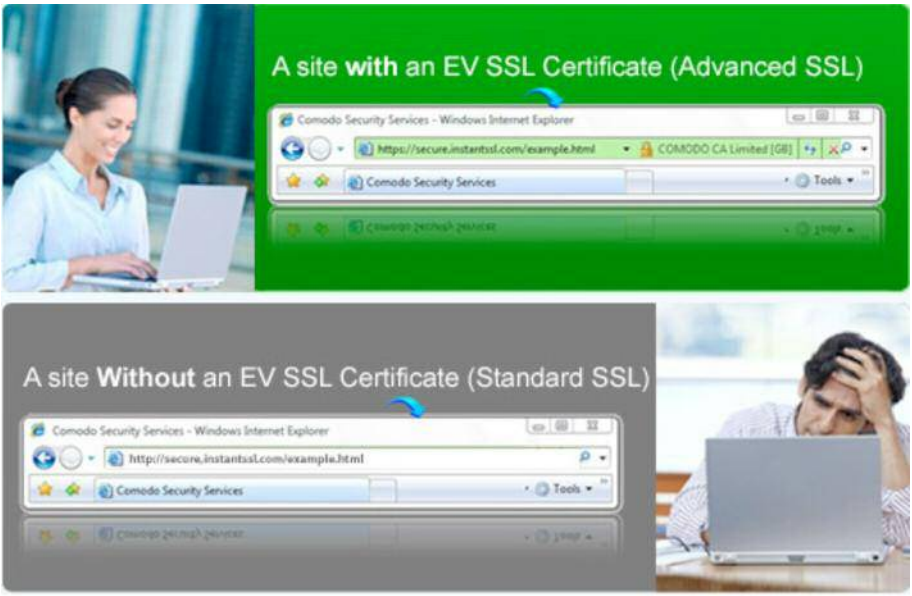
Pochissime banche ed assicurazioni in Italia usano certificati EV[2]. Oltre ad una migliore certificazione del sito web, lo strumento visivo della banda verde mostra subito all'utente che il sito è protetto da certificato SSL di classe EV, come si può vedere dall'immagine qui sotto.

Il canale di comunicazione sicura verso l'utente

Il certificato SSL crea un canale di comunicazione sicura da e per l'utente. Qualora si possa accedere ad una parte del sito con una connessione normale,

---

[2] Definizione del certificato EV



la vulnerabilità è estrema poiché, attraverso differenti tecniche, l'hacker può fare ciò che vuole e, di conseguenza, installare certificati SSL su alcune pagine e non su tutto il sito è come mettere una cassaforte piena di soldi nel deserto. L'uso del pc dell'utente come un vero è proprio Cavallo di Troia all'interno di uno o di più portali web è una prassi collaudata dagli hacker, dove il cliente dell' organizzazione diventa a sua insaputa complice del criminale informatico. Proteggere quindi l'intero sito con un certificato SSL non solo è consigliabile ma necessario e non richiede investimenti maggiori.

La protezione dei contenuti

Una delle funzioni del SSL che pochi conoscono è quella della protezione dei contenuti di un sito web definiti dalla funzione Content Verification Certificate (CVC). Una dimostrazione esplicativa di tale funzione si può trovare consul-

tando questo link[3] dove si mostra agli utenti la funzione che verifica l'autenticità del sito web, il suo contenuto e come agire contro lo spoofing, il phishing e i rischi di clonazione, come mostrato nell'immagine che segue.

Si tratta di un sistema di sicurezza è molto usato per la protezione dei marchi d'impresa e per garantire all'utente la loro originalità.

I form/moduli on-line

È il sistema migliore sfruttato dagli hacker per impossessarsi dei dati di un utente. Troppo spesso, infatti, le pagine che contengono moduli online sono prive del certificato SSL e l'utente che usa il sito web di una banca o di una compagnia di assicurazione parte dal legittimo convincimento che la stessa avrà usato tutti i migliori sistemi per garantire l'integrità dei dati del proprio cliente. Prive del certificato SSL le pagine della modulistica potrebbero essere intercettate nella Rete e i dati del malcapitato potrebbero essere usati da terzi per un'infinità di scopi fraudolenti, fino al vero e proprio furto d'identità.
Molto spesso alcune banche, che forniscono sistemi di pagamento online, tendono ad assicurare questo servizio nei propri server, che sono ovviamente protetti da SSL, ignorando però quel che accade a monte ovvero nel server del commerciante, dove il cliente compilerà con i propri dati l'ordine di beni/servizi, passando poi al server della banca per il pagamento con la carta di credito in zona sicura. Con questa metodologia, se da un lato si evita l'intercettazione dei dati della carta di credito del cliente, dall'altro non lo si protegge dal rischio del furto dei propri dati personali. L'uso di questa pratica, a mio avviso, non è corretto e la banca dovrebbe controllare cosa viene fatto dal *merchant* quando gli si concede un POS on-line di pagamento richiedendo di mettere in sicurezza la parte relativa al modulo d'ordine. Oltre al rischio di essere coinvolti, con una

[3] La funzione CVC

forma di responsabilità indiretta, in caso di danno ne andrebbe del buon nome della società che eroga questo servizio e che spesso concede l'uso del proprio logo in siti di terzi.

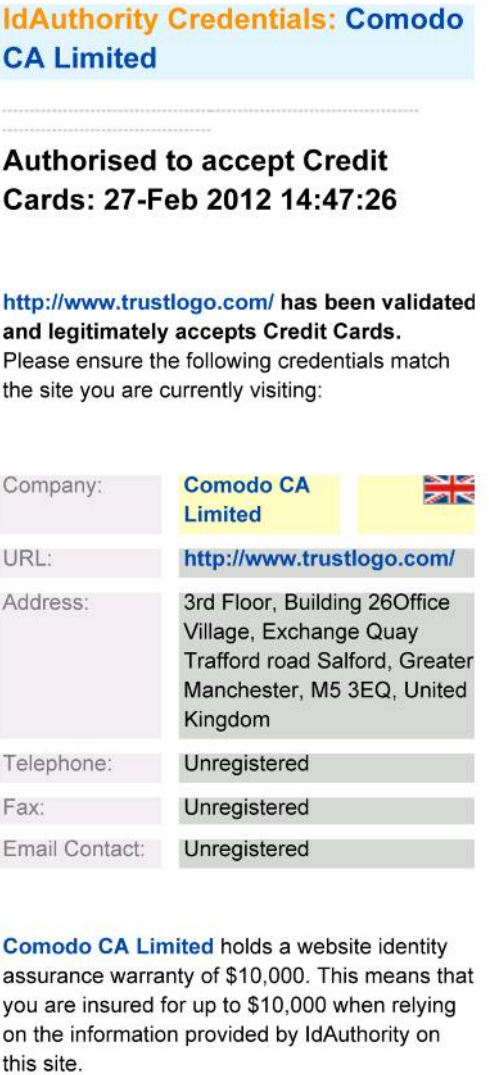
Cessione del proprio logo a terzi (Sistemi di pagamento raccolta dati on-line)

Tutti i siti web che utilizzano pagamenti tramite carte di credito hanno interesse a pubblicare sul proprio sito i loghi delle card, nonché quelli di coloro che erogano il servizio; si tratta di loghi facilmente reperibili su internet che chiunque può inserire nel proprio sito web: chi garantisce, allora, all'utente che il *merchant* sia proprio quello che dice di essere e che la sua transazione andrà a buon fine? Tutti noi abbiamo interesse che l'e-commerce, nelle sue varie forme, fiorisca, e nessuno dei *player* di questo mercato ha interesse che un utente subisca un danno. Tutte le carte di credito si sono, già da alcuni anni, consorziate dando vita al Payment Card Industry (PCI) security standard council[4] che, non solo impone degli standard per la navigazione, ma determina le misure minime di sicurezza che un merchant deve avere. Questo, però, non risolve il problema dei loghi che sono uno strumento efficace di convinzione per coloro che si avvicinano ad un sito web. Ancora una volta il certificato SSL viene in aiuto attraverso un' altra delle sue funzioni che, se fossero adottate su scala mondiale, darebbero ottimi risultati contro le truffe on-line. Si tratta di certificare la genuinità del logo delle carte di credito ma anche la legittimità di chi lo usa e lo espone sul proprio sito: la combinazione di queste due certificazioni riduce le truffe al minimo.

La tecnologia è piuttosto semplice: consiste nell'autenticare e rendere valido il sito web, la sua proprietà e la documentazione relativa alla licenza di *merchant* on-line, concessa dal provider del servizio. Emettere quindi un certificato SSL, verificabile al click del logo che segue

[4] Le guide line del Payment Card Industry (PCI) Data Security Standard Navigazione in PCI DSS

la CA interessata, fornirà le relative credenziali come avviene nell'altra immagine sotto ai loghi delle carte di credito.
Una copertura assicurativa esplicitata dalla CA completa il servizio di questo tipo di certificazione che, a mio avviso, dovrebbe essere estesa al logo del provider del servizio, normalmente usato in una banca.



Funzioni di Autenticazione e validazione di un sito web, i certificati SSL

Molto spesso queste funzioni vengono ignorate da coloro che acquistano certificati SSL, convinti di acquistare quello che viene definito comunemente "*Certificato SSL*". È bene, quindi, specificare la procedura che porta poi all' erogazione finale di un certificato SSL.
Il protocollo con cui viene generato un certificato SSL è in effetti sempre lo stesso da oltre 15 anni. L'evoluzione tecnica si è concentrata esclusivamente sulla robustezza della chiave crittografica. Come già puntualizzato, però, la procedura che

consente di arrivare all'erogazione di un certificato digitale è molto complessa. La parte più complicata e costosa non è più la *royalty* sull'uso del protocollo di proprietà di RSA - ormai di pubblico dominio, dal momento che il brevetto è "scaduto" - bensì le procedure di autenticazione e validità di chi richiede il certificato SSL. **
Il mondo della certificazione digitale, in realtà, si muove su tre pilastri principali:

***ROOT AUTHORITY**:* Detiene la chiave principale ("root") indispensabile per la gestione dell'infrastruttura a chiavi pubbliche (PKI). Essa permette di far funzionare l'intero sistema e consente la generazione delle relative chiavi per il rilascio di tutte le chiavi pubbliche dei richiedenti. Il principale compito della *root authority* è quello di garantire l'integrità della "chiave master", oltre al funzionamento della PKI per l'erogazione dei certificati. La rapidissima diffusione della rete Internet a livello globale ha richiesto una successiva autorità intermedia definita come "*crossing certification authority*": si tratta di una sorta di "prova del nove" della prima chiave o di un certificatore che ri-certifica la *root authority*. Al di fuori del "mondo digitale", questa forma di ri-certificazione viene definita "apostilla" ed è usata per certificare il notaio primario (una specie di secondo notaio che certifica il primo notaio).

** *In Italia la complessità del quadro viene ulteriormente esacerbata "grazie" ad una serie di leggi e regolamenti tecnici che creano una vera e propria "Torre di Babele" normativa. L'Italia è un paese unico per questo genere di cose, con la creazione di quelle che vengono definite Certification Authority accreditate dal CNIPA (oggi DIGITPA) come CA e che, propriamente, non lo sono. Si tratta infatti di "Sub CA" della CA Root, la sola ed unica ad aver la responsabilità dell'intero processo di certificazione e revoca dei certificati. In virtù di queste disposizioni, che hanno avuto un valore autarchico solo Italiano negli anni '90 con l'avvento della legge Bassanini, non pochi istituti bancari ed assicurativi erano assurti come Certification Authority proprio per questa unica normativa. Fortunatamente quasi tutti, dopo un paio di anni, hanno rinunciato. Si arrivava quindi al paradosso che una CA certificava se stessa ed i propri clienti, andando ad intaccare un principio internazionalmente riconosciuto ed intuitivo che la certificazione deve essere eseguita da una terza parte; un po' come se un notaio stipulasse un atto dove partecipi se stesso come contraente.*

***CERTIFICATION AUTHORITY (CA)**:* La "figura" della CA spesso coincide con l'ente denominato *root authority*.
È la stessa ad avere la proprietà della "chiave madre" del complesso sistema di Infrastruttura a chiavi pubbliche che genera le chiavi successive, facendo partire quella che viene definita "catena di certificazione" (vedi schema di un certificato digitale). Detiene e genera con assoluta discrezionalità la revoca dei certificati, pubblicando le relative liste di revoca. Il suo compito è il controllo approfondito dell'esistenza della proprietà del dominio, che il richiedente sia proprietario dello stesso o che comunque sia in possesso dei necessari poteri di rappresentanza, e la verifica incrociata di tutte le informazioni fornite nella fase di richiesta del certificato attraverso l'accesso ai database ufficiali come quelli delle Camere di Commercio ed altre risorse.
Si tratta, come facilmente comprensibile, di una procedura piuttosto complessa che varia da Paese a Paese. A seconda delle varie disposizioni, la documentazione relativa deve essere conservata dalla CA per la stessa durata della chiave radice o "*root key*", talvolta per vent'anni e oltre. Dal momento che la documentazione stessa viene redatta nella lingua originale di ogni singolo Paese, si è resa necessaria la creazione di una "*registration authority*" che, di solito, opera solo a livello locale.

***REGISTRATION AUTHORITY**:* ha la funzione di effettuare l'autenticazione e la validità dei richiedenti il certificato digitale su delega della CA con la quale si rapporta.
Tutte queste entità operano in tutto il mondo in base ad una *best practice* pubblica denominata *Certificate Practice Statement* (CPS) che ormai, dopo oltre 10 anni, è divenuta un documento standard da leggere prima di richiedere un certificato. All'interno di tale documentazione sono raccolte le condizioni di fornitura del certificato digitale, universalmente accettate e confermate da ogni singolo richiedente.
Le denominazioni EV, OV e DV rappresentano i diversi gradi di autenticazione e validità del certificato. Contrariamente a quel che si crede, il certificato digitale nel suo formato tecnico è assolutamente identico. Ne consegue che il valore del certificato stesso, ed il relativo costo, sono strettamente in relazione alle procedure di gestione che, come già detto, sono le più dispendiose. Ogni tipo

di certificato ha il proprio CPS legato, per l'appunto, al tipo di autenticazione e validazione eseguita.

***DV Domain Validation**:* Per questo tipo di certificato viene effettuata la validità solo a livello di intestazione del dominio. Si tratta del certificato più "scadente" sotto il profilo degli accertamenti eseguiti.

***OV Organization Validation**:* Questo tipo di certificato richiede una completa autenticazione e validità del richiedente. Vengono controllati:

- rispondenza tra il registro delle imprese ed il registro dei nomi a dominio. Molto spesso non si tende a considerare il registro dei nomi come dominio ma, in realtà, esso rappresenta una vera e propria "anagrafe dei siti web", una delle fonti d'informazione che qualsiasi utente può usare per controllare la proprietà degli stessi.
- estrazione del certificato di vigenza del registro imprese
- controllo della rispondenza dei dati (persone fisiche) dotati dei necessari poteri
- controllo della rispondenza degli indirizzi con le utenze pubbliche (linee telefoniche, forniture di energia elettrica e così via)
- conferma telefonica con intervista dei dati di cui sopra
- ogni ed altro controllo necessario a stabilire quanto indicato

***EV Extended Validation**:* È una forma di certificazione più approfondita ed avanzata dell'OV. In questo caso, viene richiesto un contatto diretto con il richiedente che firmerà l' apposita documentazione. Il processo da seguire è regolato dal CA/Browser Forum, il consesso internazionale di tutti i produttori di browser web e delle CA che emettono certificati EV. E' proprio il CA/Browser Forum che provvede ad aggiornare periodicamente "le regole del gioco".

Certification Authorities WebTrust Ernst & Young

Nessuno ne parla, infatti, ma per poter esercitare il "mestiere" di CA, a qualsiasi livello, bisogna stipulare un'apposita polizza assicurativa che copre gli eventi relativi alla malagestione.

Molti governi hanno cercato di regolamentare l'attività delle CA che in Europa è regolata dalla direttiva comunitaria 93/99,

normativa per la quale sono state promesse revisioni non ancora attuate. Ad ogni modo, l'attività delle CA è sottoposta ad una verifica e l'autorità preposta, ormai unica al mondo, è WebTrust
Essa provvede a rilasciare apposite certificazioni che vengono pubblicate nei siti web delle CA e revisionate ogni anno e fornisce informazioni sulla certificazione della CA e relativo Audit in tempo reale, cliccando semplicemente sul logo apposto da ogni CA nel proprio sito web.
Tutti i documenti relativi ad ogni certificato emesso sono soggetti ad "audit". L'inserimento in qualsiasi browser web come CA definita "*attendibile*" non viene effettuato se non si è in possesso della relativa certificazione.
Si tratta di procedure non bypassabili che costituiscono il requisito essenziale per il rilascio, da parte di una CA, di qualunque certificato digitale.

La soluzione per la centralizzazione, controllo ed acquisto dei certificati digitali

L'acquisto e la scelta della CA è un complemento della sicurezza in special modo per gruppi importanti. Centralizzare responsabilità ed acquisti è oggi l' esigenza di ogni azienda per realizzare un maggior controllo, accompagnato da notevoli economie di scala, pur lasciando agli uffici periferici e/o alle aziende del gruppo la loro necessaria autonomia. Emissione, revoca, certificati SSL, gestione e controllo da parte di una unità decisionale centrale che, a sua volt,a potrà delegare alcune funzioni a tutte le aziende/filiali del gruppo in base alle esigenze aziendali, con assoluta autonomia di scelta del modello di gestione in base alle proprie esigenze.
Attraverso il controllo centralizzato degli acquisti**,** oltre ad avere una precisa attuazione dei piani ed obbiettivi di budget, si riescono ad avere ottime economie

Central purchasing programs can generate substantial savings for all of a state's public entities by reducing administrative costs and lowering prices.

di scala ed una notevole riduzione dei costi di acquisto, sia di amministrazione che di gestione, pur lasciando piena autonomia alle aziende o alle filiali periferiche sulla parte tecnica. I certificati normalmente hanno scadenza annuale, generare gli stessi *randomicamente* può generare una confusione estrema di scadenze diverse nel corso dell'anno e ciò può provocare una mancanza di copertura delle pagine web e di interi siti, qualora ci si dimentichi di rinnovare un solo certificato, esponendo, così, a gravi rischi l'azienda ed i propri clienti. L'acquisto può oggi essere fatto per più di un anno. In tal modo, oltre ad avere notevoli risparmi, si evitano problematiche come quelle appena descritte. Le moderne CA danno la possibilità, non solo di riposizionare i certificati in server diversi durante il ciclo vitale degli stessi, ma anche di concentrare decorrenza e scadenza in un' unica data con conseguente calcolo degli importi

Visione on-line: le esigenze del gruppo vengono decise con la piena collaborazione deliberativa di tutti i partecipanti al processo di acquisizione e gestione per i piani di marketing basati sull'informazione, nei confronti della rete di vendita e dei clienti, attraverso il WEB e costruita sul prodotto per acquisire la fiducia dei clienti e della forza-vendita.

I servizi di post vendita la certificazione della corretta istallazione dei certificati SSL I servizi di riposizionamento

Il ciclo vitale di un certificato ssl deve seguire l'azienda e il dominio che va a certificare che per i più svariati motivi può essere di breve o lungo periodo, fornire il certificato e non controllare poi la corretta istallazione è non solo poco professionale ma può essere dannoso per che vende lo stesso e per chi lo utilizza.

Un esame accurato della corretta istallazione di uno o più certificati SSL deve

essere eseguito ci sono una combinazione piuttosto vasta di errori che possono vanificare se non addirittura compromettere l'uso del certificato stesso. I Browser sempre più sofisticati ed accorti nel rilevare alcune di queste problematiche segnalano all'utente in modo diretto ed impietoso istallazioni errate dei certificati e loro rispondenza alla esatta configurazione del sito web ed oltre, il tipo del messaggio che il Browser manda all'utente è purtroppo diverso ne ho esaminato solo uno ma il risultato con altri Browser è lo stesso vediamone alcuni tra le più significativi cercando di spiegarne le cause.CHROME ad esempio, da tutta una serie d'indicazioni e relative spiegazioni dei simboli e messaggi di allerta che espone nel proprio browser abbastanza significativi, questo rappresenta per Gogle un maggior onere e in in alcuni casi una maggiore responsabilità e evidente quindi che la loro posizione accumunata da altro Browser sia prudente e tendente al risparmio pur tuttavia bisogna dare atto che ultimamente hanno investito abbastanza ma non sufficientemente nella sicurezza, bisogna altresì dire che la loro visione è globale e quindi debbono seguire la problematica tenendo conto del mondo intero.

Indicatori di sicurezza dei siti web

Quando ti connetti a un sito web, Il Browser mostra i dettagli relativi alla connessione e avvisarti nel caso non sia possibile stabilire connessioni protette con il sito, esaminiamo in dettaglio uno dei browser più recenti Google Chrome.

Controllare se il sito sta utilizzando una connessione protetta (SSL)

Se stai inserendo informazioni personali importanti in una pagina, controlla che vi sia l'icona a forma di lucchetto alla sinistra dell'URL del sito nella barra degli indirizzi per sapere e se viene usato il protocollo SSL. Il protocollo SSL è un protocollo che fornisce un tunnel crittografato tra il computer e il sito che stai visualizzando. I siti web possono usare il protocollo SSL per evitare che terze parti interferiscano con le informazioni inviate attraverso il tunnel di sicurezza protetto il browser segnala con varie icone lo status della connessione l'unica comune a tutti è il lucchetto come comune a tutti è l'aggiungere la lettera s al protocollo http che diviene https.

ICONA	SIGNIFICATO, CHIARIMENTI E COMMENTI
	**Il sito non sta usando il protocollo SSL.** La maggior parte dei siti non sono obbligati a usare il protocollo SSL perché non gestiscono informazioni personali importanti o transazioni in denaro, pur tuttavia per le ragioni anzidette in questo libro sarebbe consigliabile passare tutti a connessioni SSL. Evitare di inserire informazioni personali importanti, quali nome utente e password od altro di strettamente personale
	**Google Chrome ha stabilito correttamente una connessione protetta con il sito che stai visitando.** Controlla che vi sia quest'icona e verifica che l'URL abbia il dominio corretto, cioè quello che cercavi, particolarmente se devi eseguire l'accesso sul sito o inserire informazioni personali importanti nella pagina. Se un sito utilizza un certificato EV SSL (Extended Validation SSL), accanto all'icona in verde viene visualizzato anche il nome dell'organizzazione. Controlla che il browser sia impostato su Verifica revoca certificato server per identificare i siti con certificati EV-SSL.
	**Il sito utilizza SSL, ma Google Chrome ha rilevato del contenuto non sicuro nella pagina.** Stai attento se ti viene richiesto di inserire informazioni personali importanti in questa pagina. I contenuti non sicuri possono fornire a qualcuno la via d'accesso per modificare l'aspetto della pagina. Questo era considerato fino a poco tempo fa un "peccato veniale" oggi non lo è più, molti hacker hanno affinato tecniche per intervenire in situazioni come queste e credetemi riescono a fare di tutto.
	**Il sito utilizza SSL, ma Google Chrome ha rilevato contenuto molto rischioso nella pagina oppure problemi con il certificato del sito.** Non inserire informazioni personali importanti in questa pagina. I certificati non validi o altri gravi problemi con https potrebbero essere un indizio che qualcuno stia tentando di intervenire attraverso la tua connessione al sito. È la condizione più critica che può scaturire da vari elementi ecco la finestra di allarme di CHROME che mi sembra sia chiara! E' in-

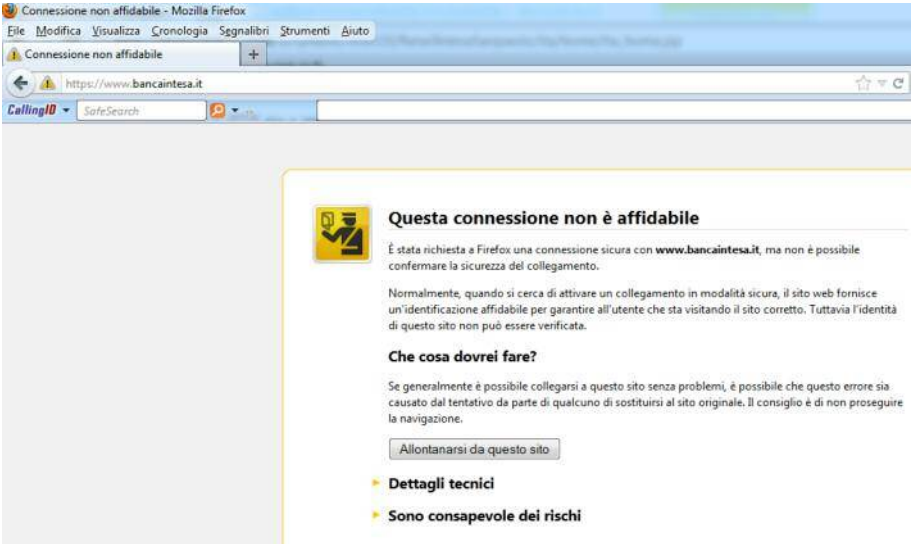
teressante notare come CHROME e del resto tutti gli altri Browser lascino il libero arbitrio di entrare o meno nel sito web all'utente con la significativa frase ***" Procedi Comunque"*** o ***"Sono consapevole dei rischi"***

Molto più esplicito Mozzilla Firefox, è bene far vedere la differenza sullo stesso sito web esaminato con CHROME che non lascia alcun dubbio, direi che assomiglia all''inferno di Dante "*lasciate ogni speranza voi che entrate"*. E' molto importante ribadire il concetto che ognuno è responsabile della propria sicurezza una sorta di libero arbitrio molto significativo nella rete.

Messaggi di avviso SSL

Anche i messaggi di avviso sulla sicurezza dei browser sono diversi anche se alla fine il significato e lo scopo è sempre quello di allertare l'utente, ad esempio quando Google Chrome rileva che il sito visitato potrebbe essere dannoso per il computer.

- **È possibile che questo sito non sia quello che stavi cercando.**
  Questo messaggio viene visualizzato quando l'URL elencato nel certificato del sito non corrisponde all'effettivo URL del sito. Il sito che stai tentando di visitare potrebbe spacciarsi per un altro sito o peggio essere il clone di quello vero. Quando ti colleghi a un sito web che utilizza il protocollo SSL per



trasmettere i dati, il server che lo ospita presenta a Google Chrome e ad altri browser un certificato per verificarne l'identità. Il certificato contiene informazioni, come l'indirizzo del sito web, che sono confermate da un'organizzazione di terze parti riconosciuta. Se l'indirizzo riportato nel certificato corrisponde all'indirizzo del sito web, avrai la certezza di comunicare con il sito web indicato nel certificato e non con una terza parte che ne simula l'identità.

Possibili motivi per cui tale avviso viene visualizzato

Le comunicazioni del server sono intercettate da qualcuno che sta presentando un certificato per un sito web diverso. Ciò potrebbe provocare un'errata corrispondenza. Il server potrebbe essere impostato per restituire lo stesso certificato per più siti web correlati, compreso quello che stai cercando di aprire, anche se tale certificato non è valido per tutti. Ad esempio, il certificato potrebbe indicarci che l'indirizzo web deve essere http://www.cucumbers.com, ma noi non possiamo verificare che corrisponda al sito web http://cucumbers.com. Se sei assolutamente sicuro che il sito al quale stai accedendo è affidabile, puoi decidere di aprirlo facendo clic su Procedi comunque. In

genere, è preferibile cautelarsi e fare clic su Torna nell'area protetta, che riporta all'ultima pagina visitata.

- **Il certificato di sicurezza del sito non è affidabile.**
  Questo messaggio viene visualizzato se il certificato non è stato rilasciato da un'organizzazione di terze parti affidabile. Poiché tutti possono creare un certificato, Google Chrome controlla se il certificato del sito è stato rilasciato da un'organizzazione affidabile. Quando ti colleghi a un sito web che utilizza il protocollo SSL per trasmettere i dati, il server che lo ospita presenta a Google Chrome e ad altri browser un certificato per verificarne l'identità. Questo certificato contiene informazioni, come l'indirizzo del sito web, che sono confermate da un'organizzazione di terze parti ritenuta affidabile dal browser. Se l'indirizzo riportato nel certificato corrisponde all'indirizzo del sito web, avrai la certezza di comunicare con il sito web indicato nel certificato e non con una terza parte che ne simula l'identità.
  Motivi per cui tale avviso viene visualizzato
  L'organizzazione di terze parti che ha emesso il certificato del sito web di destinazione non è compresa tra quelle riconosciute dal browser. Chiunque può creare un certificato e spacciarsi per un sito web. Google Chrome darà la conferma che ti stai collegando al sito web originale solo se il certificato del sito è stato emesso da un'organizzazione affidabile.
  Se sei assolutamente sicuro che il sito al quale stai accedendo sia affidabile, potrai decidere di aprirlo facendo clic su Procedi comunque. In genere è preferibile cautelarsi e fare clic su torna nell'area protetta, che riporta all'ultima pagina web visitata. Per organizzazione affidabile s'intende quella elencata dai browser è qui infatti che si conservano i certificati mondialmente riconosciuti da tutti i browser gli stessi da tempo regolano le loro attività in modo trasparente e pubblico, con la costituzione di CAB Forum , il forum tra tutte le Certification Authority mondialmente riconosciute in Internet e i maggiori Browser www.cabforum.org . In appendice troverete l'ultimo regolamento riguardante le attività degli stessi con il sistema con cui vengono esaminati i siti web (Autenticazione e Validazione) prima di rilasciare un certificato SSL.
- **Il certificato di sicurezza del sito è scaduto.**
  o
  Il certificato di sicurezza del server non è ancora valido. Questi mes-

saggi vengono visualizzati se il certificato del sito non è aggiornato. Di conseguenza Google Chrome non può verificare la sicurezza del sito. Le CA emettono liste di revoca è buona norma cliccare sul lucchetto  per verificare la validità del certificato potrà apparire la seguente immagine:

L'avviso di Mozilla FireFox è ancora più esplicito:

- **Il certificato di sicurezza del server è stato revocato.**
  Questo messaggio viene visualizzato se l'organizzazione di terze parti che ha rilasciato il certificato del sito lo ha contrassegnato come non valido. Di conseguenza Google Chrome/ Firefox non possono verificare la sicurezza del sito. Se si vuole approfondire la problematica operare come al punto precedente e visionare la lista di revoca della CA che ha emesso il certificato.
- **Il sito usa una certificazione**
  A livello di dominio DV non autenticata e validata a livello di organizzazione/Azienda
  Praticamente nessun Browser invia questo tipo di avviso ad eccezione di DRAGON di COMODO, ovviamente questo non vuol dire che il sito non abbia la dovuta protezione ma avverte il cliente che l'autenticazione e validazione del sito è avvenuta solo a livello di dominio e non a livello organizzativo. E' un tipo di certificato a basso costo come detto in precedenza che può essere usato solo per alcune applicazioni. A mio avviso è un tipo di certificazione "non certificata" il costo dei certificati SSL è così basso che un risparmio su questi mi sembra assurdo ma soprattutto non ripaga.

Visualizza ulteriori dettagli del sito

Fai clic sull'icona del o sull'icona a forma di lucchetto per visualizzare ancora più dettagli sull'identità del sito, sulla connessione e sulla tua cronologia

di navigazione relativa al sito questo menù dara la possibilità di avere ulteriori informazioni.

Identità del sito

Per verificare l'identità, i siti che utilizzano il protocollo SSL presentano al browser certificati di sicurezza di tipo SSL. Chiunque può creare un sito web e simulare con questo un altro sito, ma solo il sito autentico possiede un certificato di sicurezza valido per l'URL della pagina che tenti di aprire. I certificati non validi possono rivelare che qualcuno sta tentando di intromettersi nella connessione al sito.

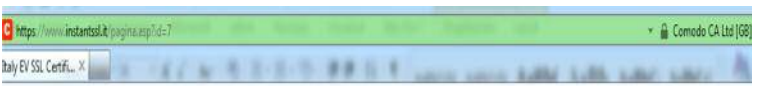
ICONA	SIGNIFICATO CHIARIMENTI E COMMENTI
	Il certificato di sicurezza del sito è valido e l'identità è stata verificata da un'autorità di terze parti attendibile.
	Il sito non ha fornito un certificato al browser. Questo è normale per comuni siti HTTP (cerca l'icona del nella barra degli indirizzi), perché i certificati di solito vengono forniti solo se il sito utilizza SSL. Un ulteriore accortezza per verificare la presenza anche in forma non esplicita della copertura SSL è quella di provare a ricaricare il sito con avanti all'url HTTPS invece di http.
	Google Chrome ha rilevato problemi con il certificato del sito. Sii prudente, perché il sito potrebbe simulare un altro sito al fine di indurti con l'inganno a spartire informazioni personali o altro tipo di informazioni sensibili.

La connessione al sito

Google Chrome ti informa se la connessione è crittografata o meno. Se la connessione non è protetta, terze parti potrebbero essere in grado di visualizzare,copiare o manomettere le informazioni che fornisci al sito.

ICONA **SIGNIFICATO CHIARIMENTI E COMMENTI**

Google Chrome ha stabilito correttamente una connessione protetta con il sito che stai visitando.
Interessante è vedere come il Browser IE identifica una classe superiore di certificati gli EV Extended Validation con un intera barra verde rendendo così molto più facile la protezione SSL del sito:



La tua connessione al sito non è crittografata. Questo è normale per comuni siti HTTP ,nel cliccare sull'icona del nella barra degli indirizzi si avrà il seguente risultato:

Cliccando sul menù qui accanto si potranno avere altre informazioni sul sito che s'intende visitare.

La tua connessione al sito è crittografata ma Google Chrome ha rilevato del contenuto misto sulla pagina esaminata. Stai attento se inserisci informazioni personali in questa pagina. I contenuti misti possono fornire a qualcuno la via d'accesso per manipolare la pagina che stai visitando. Questi contenuti potrebbero essere immagini o annunci di terze parti incorporati nella pagina ma non protetti da connessione SSL. Purtroppo per verificare questa

condizione ci si deve accorgere del piccolo triangolino sito a lato del lucchetto e cliccare sullo stesso solo così si avrà il menù affianco che segnalerà la problematica.

La tua connessione al sito è crittografata, ma Google Chrome ha rilevato scripting misto nella pagina. Attenzione, nell' inserire informazioni personali in questa pagina. Lo scripting misto può fornire a qualcuno la via d'accesso per assumere il controllo della pagina. Questi contenuti potrebbero essere script o video di terze parti incorporati nella pagina.
Se sei connesso a Internet tramite una rete wireless pubblica, lo scripting misto è particolarmente rischioso perché è più facile intromettersi in una rete wireless che in una rete cablata.

Cronologia visite

In questa sezione puoi controllare se hai già visitato il sito in passato. Tuttavia, se hai cancellato la cache e i cookie, anche la cronologia visite viene cancellata, non potrai quindi conoscere se sei già stato in questo sito web.

ICONA **SIGNIFICATO**

Hai visitato questo sito in precedenza, quindi è probabile che tu consideri questo sito attendibile.

Non hai mai visitato questo sito prima. Questo messaggio è normale se sai che il sito è attendibile. Tuttavia, se il sito ha un aspetto familiare e non hai cancellato la cronologia di navigazione di recente, è possibile che il sito simuli un altro sito. Procedi con prudenza.

Certificati SSL pluriennali, ri-posizionamento

In passato, difficilmente venivano acquistati certificati SSL pluriennali qualsiasi variazione nei propri sistemi comportava la perdita degli stessi e conseguentemente se ne doveva acquistare uno nuovo, attualmente molte CA tra cui GlobalTrust e Comodo consentono il riposizionamento dei certificati per tutto il ciclo vitale degli stessi.
L'acquisto può oggi essere fatto per più di un anno in molti casi fino a cinque.

In tal modo, oltre ad avere notevoli risparmi, si evitano problematiche come quelle appena descritte. Le moderne CA danno la possibilità, non solo di ri-posizionare i certificati in server diversi durante il ciclo vitale degli stessi ma anche altre possibili sostituzione ed operazioni che seguono il cliente nella sua evoluzione nel web non vanificando gli investimenti fatti.
In ogni caso un sistema automatico avverte il cliente nell'approssimarsi la scadenza del certificato evitando così una mancanza di copertura delle pagine web e d'interi siti, qualora ci si dimentichi di rinnovare un solo certificato, esponendo, così, a gravi rischi l'azienda ed i propri clienti.

La Certificazione della corretta istallazione SSL

Normalmente una Ca si limita a fornire sulla base della richiesta del cliente un certificato SSL non entrando nel merito di cosa veramente il cliente abbia bisogno. Al giorno d'oggi la certificazione SSL è divenuta molto più complessa di 10 anni fa assieme la certificato standard SSL si sono aggiunti tutta una serie di altri certificati atti a coprire tutte le esigenze del cliente che hanno diverse specifiche utilizzazioni. La prima grande suddivisione dei certificati SSLcome detto precedentemente e data dal tipo di Autenticazione e validazione che viene eseguita per il rilascio degli stessi sono suddivisi quindi in DV dove viene effettuata solo la validazione del dominio in OV dove viene effettuata la validazione anche della organizzazione proprietaria del dominio EV extended Validation la validazione è estremamente severe ed il Brovser restituisce una Banda VERDE sulla riga dove c'è l'URL. Multe CA chiamano i certificati SSL in modo diverso nomi come Rapid, Instant, Platinum Gold, Diamond e chi più ne ha più ne metta in sostanza però si tratta dello stesso vecchio Certificato SSL della RSA[5] a cui vengono aggiunti alcuni add-on come una copertura assicu-

---

[5] Nel 1976 Whitfield Diffie e Martin Hellman, crittologi americani, hanno ipotizzato la creazione di un cifrario "asimmetrico" composto da "chiavi pubbliche". Il sistema di crittografia si basa sull'esistenza di due chiavi distinte, che vengono usate per cifrare e decifrare. Se la prima chiave viene usata per la cifratura, la seconda deve necessariamente essere utilizzata per la decifratura e viceversa. La questione fondamentale è che nonostante le due chiavi siano fra loro dipendenti, non sia possibile risalire dall'una all'altra, in modo che se anche si è a conoscenza di una delle due chiavi, non si possa risalire all'altra, garantendo in questo modo l'integrità della crittografia.

rativa più alta ecc., eccone alcuni:

TIPO CERT.	DESCRIZIONE
SSL	Si possono avere diverse denominazioni per lo più scelte dalle CA ma è la base della certificazione nel web diverse possono essere gli “optional” come la copertura assicurativa, la durata max. 5 anni può essere di tipo DV o EV.
SAN SSL	SAN sta per Subject Alternative Name è un normale certificato SSL con la peculiarità di poter essere esteso a più domini a patto che siano di proprietà della stessa organizzazione o gruppo, il suo corretto rilascio può essere solo a livello OV. In sostanza un solo certificato per più domini web di una stessa organizzazione o gruppo finanziario anche correlato.
UCC	Unified Communication Certificate Creato e voluto in un primo momento da Microsoft per applicazioni su server Exchange è ora normalmente esteso in applicazioni anche Open Source Linux ecc. Ha le stesse feature del SAN come domini multipli per applicazioni per la comunicazione unificata. Il suo corretto rilascio può essere solo a livello OV. Il numero dei domini permessi e dei server in cui può essere istallato dipende molto dalla CA che lo rilascia, anche la durata e limitata dalla CA stessa.
WILDCARD	Particolare menzione questo tipo di certificato creato per chi ha più sottodomini da amministrare e vuole che tutti siano certificati, molto semplice da istallare in sostanza si può aggiungere qualsiasi tipo di sottodominio al post della wildcard * del tipo *miodominio.it dove al posto della + si potrà inserire quello che si desidera. Anche questo tipo di certificato, a mio avviso deve essere di tipo OV, seppure alcune CA lo rilasciano anche come DV, estremamente sconsigliabile. il suo corretto rilascio può essere solo a livello OV.
EV	Sta per Extended Validation è il certificato SSL che differisce dagli altri solo ed esclusivamente per l’accurata Autenticazione e validazione che viene fatta, può essere quindi di tutti i tipi su esposti. La durata non supera i due anni è la tipicità unica del suo genere è il fatto che mostra una intera barra verde sul

Browser il suo corretto rilascio può essere solo a livello OV come da immagine qui sotto:

CODE SIGN Anche se non propriamente un certificato SSL ha utilizzi molto vicini al web. L'utilizzo è quello di rendere un codice software sicuro a livello di provenienza. Sempre più spesso scarichiamo applicativi online questi certificati garantiscono l'affidabilità del proprietario del software.

Vedete quindi quanto sia importante avere un adeguato supporto di PRE-SALES che vi segua in tutte le fasi dell'acquisto per trovare quello che occorra alle vostre esigenze oltre ad aiutarvi nell'istallazione del tipo di certificati SSL adatti alla vostra organizzazione indicandovi quanto occorre realmente per la sicurezza vostra Azienda nel web arrivando a far risparmiare importi notevoli. Anche il servizio di AFTER SALES è importante c'è un buon margine d'errore nell'istallazione di un certificato SSL che può vanificare quanto investito in sicurezza che invia ad istallazione avvenuta del vostro certificato **un check completo del vostro sito web** indicando eventuali lacune e suggerimenti per porvi immediato rimedio. Un'ulteriore certificazione della corretta istallazione e operatività del nostro prodotto sul vostro sito web, in sostanza una vera propria certificazione dell'istallazione dei certificati SSL del nostro Quality Controll Labs. Non vi lasceremo mai soli e nessuno dei nostri certificati SSL arriverà a

scadenza senza che siate avvertiti per tempo.
Un'interrogazione della porta 443 standard per l'uso di SSL se eseguita in modo esaustivo porta al risultato che si vede nella certificazione qui di seguito

Sicurezza della certificazione digitale

CERTIFICATE OF INSTALLATION FOR SSL CERTIFICATE

According to the information gathering from web at date and time of this certificate. We certify the results of SSL installation of:

www.globaltrust.it

The relevant comment and recommendation are on the next section in original language.

SSL LAB TEST

NOTE AND RECOMMENDATION

ATTENZIONE: **Il bordo verde della certificazione indica che non ci sono problemi con l'istallazione del certificato/i SSL relativi al sito preso in esame.**

Il certificato è installato correttamente.

Digitally signed by Massimo Penco
DN: cn=Massimo Penco e=mpenco@globaltrust.it
Reason: GlobalTrus Labs SSL Test
Location:
Date: 2012-05-17 15:17+02:00

APPENDICE 1

Forse non tutti sanno che…

Quando sono collegato ad Internet altri possono intercettare quello che scrivo?

In linea di massima no, a meno che non abbiamo già preso un Virus o un Keylogger (un programma che registra quanto viene digitato sulla tastiera). Fino a quando non faccio click sul tasto "Invia" (o "Submit" in inglese) dopo aver compilato il Form, nulla viene inviato nella rete. Come funziona un comune Keylogger? In pratica registra ogni digitazione che viene fatta sulla tastiera e, i più sofisticati, riescono ad inserire quanto digitato su uno spazio nel vostro PC e, al momento dell'invio dell'informazione on-line, essa viene deviata dove l'hacker ha deciso che venga inviata. Si tratta, praticamente, di una sorta di spia digitale della vostra tastiera.

Quando ricevo una mail che mi invita a cliccare sul link di "Poste.it" o di qualche banca on-line, posso ritenere che si tratti di una mail vera?

Attenzione perché le mail possono essere abilmente contraffatte. Sembrano arrivare da "poste.it" o da qualche banca di nostra fiducia, mentre sono state scritte da altre organizzazioni criminali. Non solo… Il link "https" che viene spesso riportato in queste e-mail può corrispondere ad un altro link "http" di un altro sito, ovvero del sito pirata. Questo lo si può verificare abbastanza facilmente passando il cursore del mouse sul link riportato nella e-mail. Si potrà vedere come lo stesso link (nella parte inferiore del browser o del client di posta utilizzato) riconduca ad un altro sito. Questo è sicuramente un caso di *phishing*. Evitate di cliccarci sopra e di entrare nel sito che, anche se, molto probabilmente, apparirà molto simile a quello che conosciamo, in realtà ha lo scopo di raccogliere i dati dell'utente e di trasmetterli a qualche criminale che ne potrà fare uso in futuro. Inoltre potrebbe essere

un modo per fare entrare nel pc quello che viene definito “Cavallo di Troia” che metterebbe a repentaglio la sicurezza di tutti i dati. Un ottimo metodo preventivo è quello di usare GlobalTrust CallingID, un sistema gratuito che vi segnala la sicurezza e le proprietà del sito web.

Come faccio ad essere sicuro che il mio computer sia protetto da rischi ed infezioni?

Spesso la sensazione di essere al sicuro è più rischiosa rispetto a quella di ritenersi potenzialmente vulnerabili. La sicurezza deriva dal fatto che si possiede il personal firewall, l’antivirus e anche l’ antispyware ma, spesso, molte azioni illecite vengono fatte dall’esterno (o dall’interno) sfruttando proprio i canali che vengono lasciati aperti sui firewall per permettere le attività lecite. Sembra un paradosso ma si dovrebbe scegliere se usare il computer per attività ludiche o per lavorare o per fare Internet Banking, shopping on line e così via.

Se non si può operare questa scelta si dovrebbero usare impostazioni un po’ più “restrittive” per il proprio Browser e non permettere in modo incondizionato l’accettazione di tutti i “Cookies”, né l’esecuzione di tutte le “ActiveX” o “Javascript” che vengono ripetutamente iniettati sul PC. Ma non si dovrebbe nemmeno scegliere di far “ricordare” le password al Browser, perché le stesse potrebbero poi essere utilizzate, a totale insaputa dell’utente, da un codice maligno eventualmente eseguito sulla macchina.

Insomma, occorre un po’ di consapevolezza nell’uso dello strumento poiché non esiste ancora un pc che possa definirsi “sicuro”. Sarebbe più corretto dire “A ciascuno il suo PC”. Chi non è un esperto non deve correre rischi inutili, che possono fargli perdere soldi, credibilità o causare problemi legali. Chi è un esperto, invece, sa come proteggersi e quindi già usa il proprio computer già nel modo giusto.

Mi hanno detto che Internet Explorer è più vulnerabile di Mozilla Firefox. È vero?

Non ci sono delle assolute “verità” a tal proposito. Era vero, fino a qualche anno fa, che Internet Explorer era il browser più diffuso nel pianeta. Ora non è più così ed altri browsers, (tipo Mozilla Firefox o altri), manifestano le loro vulner-

abilità. Semplicemente perché “maggiore è la diffusione di uno strumento, tanto più cresce l’interesse a cercarne le possibilità di violazione”.
Ritengo che, nelle loro attuali versioni, siano entrambi parimenti funzionali e, allo stesso tempo, sicuri. Inoltre, ultimamente, tutti i Browser avvisano in modo molto efficace quando si sta per accedere ad un sito che presenta dei problemi.

Basta avere un buon AntiVirus per essere sicuri e non avere problemi?

L’AntiVirus è solo una delle punte dell’iceberg. È bene averne uno valido e conosciuto, non necessariamente “commerciale”, che sia in grado di aggiornarsi automaticamente e con una buona periodicità. Sono, però, sempre necessarie delle buone abitudini di comportamento nell’uso del proprio computer.
È bene anche prestare attenzione ai messaggi che ci arrivano tramite la posta elettronica. Ricordiamoci che se riceviamo un messaggio “non atteso”, non abbiamo certo l’obbligo di fare click su uno dei links che vengono evidenziati. Questi potrebbero farci aprire delle pagine sul Web che mettono a repentaglio la sicurezza del PC (e magari anche il contenuto del nostro conto corrente…).

Le applicazioni che ciascuno di noi utilizza possono essere a loro volta sfruttate in modo malevolo per utilizzare in modo improprio il nostro pc. È bene avere anche un buon Personal Firewall, che sia in grado di comprendere quando qualche applicazione sul pc sta “tentando” di svolgere delle operazioni non previste, o comunque anomale, permettendone o negandone l’esecuzione. (Ad esempio può essere normale che, all’apertura del nostro ambiente di posta elettronica, MS-Outlook il Personal Firewall ci segnali che l’applicazione Outlook sta tentando di accedere ad Internet, mentre è sicuramente meno “normale” che, all’apertura di un file Word, il Personal Firewall ci segnali che l’applicazione MS-Word sta tentando di spedire una e-mail).
La combinazione delle due difese è, oggi, quella più comune e ci sono molteplici sistemi, definiti “Internet Security suite”, che svolgono insieme tutte le attività di protezione, alcune delle quali gratuite.

Mentre vado su un sito https, il programma Internet Explorer mi dice che il Certificato del sito che sto visitando non appartiene all’elenco dei Certificati attendibili: cosa vuol dire?

Non tutte le aziende che mettono in linea il proprio sito decidono di affidarsi ad una Autorità di Certificazione Accreditata. Ce ne sono molte, è vero, basta aprire Internet Explorer, e fare *"Strumenti/OpzioniInternet/Contenuto/Certificati/Autorità di Certificazione Fonti Attendibili",* per vedere la lista delle Autorità "riconosciute" in modo standard dal nostro browser.
È anche vero, però, che i Sistemi Operativi delle macchine Server consentono, in maniera gratuita, di poter realizzare la funzione di Autorità di Certificazione con una certa immediatezza e con dei risultati spesso molto soddisfacenti. Fino a quando l'azienda citata opera questo tipo di scelta per mettere i propri Intranet Servers in condizioni di eseguire traffico protetto e cifrato a livello "uso interno" non ci sono problemi ma nel momento in cui la stessa azienda vuole rendere disponibili i propri servizi anche verso Internet la cosa si complica.

Infatti i Certificati digitali emessi dall' Autorità di Certificazione interna all'azienda non sono quasi mai riconosciuti all'interno dei browsers di cui dispongono gli utenti finali, generando quel fastidioso messaggio di "certificato non attendibile" che spesso ci costringe, per andare avanti, ad accettare che esso venga "inserito" tra le fonti attendibili, in modo tale che, nelle visite successive, questa domanda non ci venga più fatta.
Nella maggior parte dei casi ciò non comporta alcun rischio grave ma è la prova che l'Azienda ha dato dimostrazione di buona volontà facendo il possibile per non mettere a repentaglio i dati di scambio tra il visitatore e il sito; tuttavia l'azienda dovrebbe avvertire i propri potenziali visitatori del modo in cui avviene la procedura di accesso, dando informazione del messaggio di richiesta di caricamento del Certificato.
Diverso è il caso in cui l'utente capita in modo del tutto involontario su un sito https che non conosce e sul quale non ha deciso di recarsi. In questa situazione si dovrebbe evitare di accettare il caricamento di tale Certificato rifiutandolo in modo esplicito, poiché nel caso in cui lo si accettasse esso andrebbe a caricarsi tra i "Certificati Attendibili", anche se il sito di destinazione fosse, invece, illegale.

Se un Certificato è eguale all'altro perché debbo pagare una Certification Authority quando io stesso posso generarne una?

È un po' come chiedersi per quale motivo occorre andare da un notaio e a cosa

serve. Nella rete è ancora peggio poichè la fiducia deve essere riposta su qualcosa d'impalpabile, come un sito web, dove tutto è virtuale. Lo sforzo da parte del proprietario e del gestore di un sito è quello di favorire l'ingresso nello stesso e renderlo, non solo accattivante e confortevole, ma anche sicuro. La sicurezza non è data dal certificato, bensì dalla *Certification Authority* che deve essere "terza parte" e garantire, tramite il certificato, che quel sito è affidabile, che garantisce la sicurezza dello scambio d'informazioni e che sia a prova di hackers.

Allora con un certificato SSL si arriva a proteggere il proprio sito web da ogni tipo di attacco?

No. La protezione SSL è specifica per la creazione di un "tunnel" sicuro di comunicazione tra il sito ed un utente. Attacchi come *DDoS Distributed denial-of-service* non possono, per la loro stessa natura, essere protetti da SSL. Un attacco *DDoS* è un sistema che, simultaneamente, accede ad un server "target",

dove è presente il sito interessato all'attacco, da un numero consistente di utenti; in questo modo si riesce a bloccare il sito per un sovraccarico di richieste. Ciò accade normalmente anche per la popolarità di un sito web in un particolare momento ed è quindi difficile discernere quale sia un attacco malevolo o un sovraccarico dovuto a motivi legittimi.

La certificazione digitale e la Pubblica Amministrazione nel WEB

Una delle domande che mi hanno rivolto spesso è " esiste una regola/disposizione di legge in merito ai siti web della pubblica amministrazione per la sicurezza nel WEB" ? In un paese dove ci si muove solo ed esclusivamente in base a leggi, regolamenti, circolari ecc. la mia risposta purtroppo è no ! Eppure la PA quale tenutaria di enormi banche dati personali dei Cittadini Italiani dovrebbe essere la prima a curare in modo meticoloso la sicurezza dei propri cittadini nella rete. Non credo ci sia bisogno di afre esempi anche l'anagrafe di un piccolo Comune conserva tutti ma proprio tutti i dati dei propri Cittadini, per non parlare poi di una ASL un Ospedale e quanto altro, non penso che almeno su questo ci sia da discutere. Si sta assistendo ad circolo non virtuoso come dovrebbe essere ma vizioso . Da un lato si spingono i cittadini è la PA ad usare mezzi sempre più informatizzati basati sulla rete da un altro non ci rende conto che allo stato è come dare una pistola carica ad un bambino sperando che non si faccia male o non faccia male agli altri. Lo chiamata Torre di Babele ed in effetti questo mia profezia si sta puntualmente avverando. Se da un lato c'è stato un lodevole aumento della presenza nel WEB della PA centrale e locale da un altro la interoperabilità dei vari sistemi a volte messi su artigianalmente senza una regola minima (Chi mi conosce sa che non amo le regole) ma soprattutto senza una minima considerazione sulla sicurezza e sulla riservatezza dei dati dei Cittadini ed anche degli stessi dipendenti della PA che hanno il più delle volte i loro indirizzi email in data base facilmente accessibili.

Lo stato dell'arte della certificazione digitale della PA nel web

L'ultima disposizione di legge in materia il decreto sulle semplificazioni emanato quest'anno impone che dal 2014 si comunicherà con la PA solo attraverso il WEB, tutte una serie di notizie sono apparse nei media negli ultimi mesi. Questa lodevole iniziativa non è accompagnata da nessun minimo di norme di come questo possa avvenire, conseguentemente ognuno farà come crede.

ALCUNI DATI

Direi che la base del nostro sistema pone il Comune come aggregatore principale ed essenziale d'informazioni da quest'antico organismo si traggono le basi di tutto lo scibile della popolazione Italiana ma la base di tutto l'apparato

produttivo Imprese professionisti ecc. Rappresenta altresì il modello da cui trarre un minimo d'informazione al fine di verificare il grado di sensibilità alla sicurezza nelle applicazioni web nella PA. I dati tratti dall'ANCITEL sono assolutamente confortanti si può parlare di una presenza nel web vicina al 100% dei Comuni Italiani.

Regione	Totale Comuni	Comuni con sito web	%
Sicilia	390	390	100,00
Umbria	92	92	100,00
Veneto	581	581	100,00
Valle d'Aosta	74	74	100,00
Emilia-Romagna	348	348	100,00
Toscana	287	287	100,00
Lombardia	1.544	1.541	99,81
Sardegna	377	376	99,73
Puglia	258	257	99,61
Basilicata	131	130	99,24
Friuli-Venezia Giulia	218	216	99,08
Piemonte	1.206	1.193	98,92
Marche	239	236	98,74
Abruzzo	305	301	98,69
Molise	136	134	98,53
Campania	551	542	98,37
Lazio	378	371	98,15
Calabria	409	401	98,04
Liguria	235	230	97,87
Trentino-Alto Adige	333	312	93,69
Italia	**8.092**	**8.012**	**99,01**

A fronte di questo interessante fenomeno che è un enorme passo, avanti fanno da contrasto:

1) Nessuna schematizzazione comune per alcuni servizi essenziali come ad esempio l'anagrafe ognuno fa come crede, in tema che sta tanto a cuore il governo "lo spending Review" almeno i servizi di base potrebbero essere realizzati con un modello unico e soprattutto interoperabili.
2) Fruibilità del sito non è indispensabile ma uno schema di base sarebbe utile.
3) Sicurezza, da un esame effettuato con il nostro sistema di controllo SSL solo

alcune decine, di Comuni hanno provveduto a mettere in sicurezza gli accessi ad applicazioni web.

Discorso analogo per gli altri enti pubblici locali, Regioni, provincie, per non parlare delle ASL e Ospedali ecc., dove sembra ci sia una gara a realizzare siti web con la prerogativa che ognuno fa come gli pare, un esempio per tutti venuto alla cronaca proprio in questi giorni la Provincia di Cuneo che fa scuola nel modo in cui viene interpretata la sicurezza nel web dagli enti pubblici dove in sintesi si fa esattamente quanto già visto nel caso Anagrafe Tributaria citato e riportato in appendice 3 salvo rientrare subito non appena il caso viene segnalato (vedi frase evidenziata in Giallo) questo è quello che viene fuori nel sito della Provincia di Cuneo mentre sto scrivendo.

Ci digitali SSL/TLS

Si informa l'utenza che tutti i certificati digitali SSL/TLS presenti sulle aree sicure del portale (dominio provincia.cuneo.it), sono emessi direttamente della Provincia di Cuneo.

Quando un browser incontra un certificato digitale non firmato da una Certification Authority, informa l'utente e chiede se procedere o meno sul sito.

Per accedere ai vari servizi SSL/TLS occorre dunque procedere, confermando l'eccezione.

Accedi ai servizi SSL/TLS della Provincia di Cuneo

- **Portale appalti**: https://appalti.provincia.cuneo.it/
- Webmail: https://www.provincia.cuneo.it/webmail
- Gestione presenze: https://www.provincia.cuneo.it/dol
- Servizi on line: https://servizi.provincia.cuneo.it/
- Servizi per i comuni: https://www.provincia.cuneo.it/area_protetta/comuni/gare_appalto/
- Atti del Consiglio: https://www.provincia.cuneo.it/area_protetta/consiglio/

E' in fase di acquisizione un certificato digitale emesso da una Certification Authority.

Realizzare un indagine completa sulla PA on-line richiederebbe anni, salvo poi iniziare da capo, difatti la *progressione* se così la si può chiamare è continua nel senso che non esiste una organicità ed un disegno quadro su come la PA debba fornire tutta una serie di servizi on-line al cittadino ed anche a se stessa

visto che i vari settori della PA debbono pur usare il web per comunicare più velocemente, facilmente ed in sicurezza fra loro. Tutto questo però è fantascienza in quanto semplicemente l'incomunicabilità della PA con se stessa è un fatto reale, Interoperabilità, compatibilità standard di comunicazione ed accesso hai dati sono parole senza senso per la PA in Italia.

La Posizione del garante dei dati personali

In assenza di una normativa specifica il garante si è mosso fino ad oggi in base a segnalazioni e denunce come quella relativa all'Anagrafe Tributaria ed enti ad essa collegati dove il garante ha effettivamente tracciato dei paletti importanti che possono, purtroppo, essere usati solo per analogia in altri casi simili l'esame compiuto dallo stesso è però completo e significativo ed è stato riportato per intero nell'appendice 3 di questo libro, gli aspetti più importanti tratti integralmente sono i seguenti:

CONTROLLO A LARGO RAGGIO

Gli accertamenti ispettivi hanno avuto luogo presso l'Agenzia delle entrate, Sogei S.p.A. (Società generale d'informatica, responsabile del trattamento dei dati contenuti nell'anagrafe tributaria), regioni, province, comuni e altri enti che accedono a tale anagrafe, con la piena collaborazione degli enti coinvolti. Le verifiche hanno consentito di evidenziare criticità, in ambito sia informatico, sia organizzativo, documentate nei verbali in atti.

Dalle risultanze emerge che i sistemi di collegamento all'anagrafe tributaria utilizzati dai soggetti esterni all'amministrazione finanziaria sono i seguenti:

- *"Siatel", applicazione web utilizzata principalmente da comuni, province, regioni, università, asl e consorzi di bonifica, per un totale di circa 9.400 enti e 60.000 utenze, che consente di visualizzare dati anagrafici completi, dati fiscali e atti del registro relativi alla totalità dei contribuenti;*
- *"Puntofisco", applicazione web di recente realizzazione e attualmente in dotazione a enti previdenziali, tribunali, camere di commercio e società varie, per un totale di circa 180 enti e 18.000 utenze. Puntofisco consente di visualizzare dati anagrafici, fiscali e atti del registro relativi alla totalità dei contribuenti, più aggiornati e con maggiore segmentazione delle informazioni rispetto a Siatel (ad es., differenziando tra dati anagrafici attuali o completi dello storico), ma permette anche di accedere a dati sensibili (presenti nel det-*

taglio degli oneri deducibili);

- *"3270 enti esterni", collegamento diretto, tramite terminali fisici o emulatori di terminale, ai sistemi centrali dell'anagrafe tributaria, in corso di dismissione per esigenze di aggiornamento tecnologico, che tuttora consente a soggetti anche privati (Telecom Italia S.p.A., Enel, Inail, Inps, camere di commercio, Ministero delle politiche agricole, "interforze") di collegarsi a informazioni anagrafiche e fiscali relative alla totalità dei contribuenti; la struttura dell'applicativo non consente all'Agenzia delle entrate di conoscere il numero di utenti;*
- *"Entratel", applicativo utilizzato dagli enti principalmente ai fini della trasmissione delle dichiarazioni, con flussi di dati solo in entrata verso l'Agenzia delle entrate; le credenziali di autenticazione fornite dall'Agenzia permettono altresì all'operatore di visualizzare la posizione fiscale dell'ente attraverso l'apposita web application ("Fisconline"/"Cassetto fiscale");*
- *"web services", strumenti realizzati sulla base di specifiche tecniche definite caso per caso dall'Agenzia delle entrate, che consentono di accedere a dati anagrafici anche completi relativi alla totalità dei contribuenti. Tali collegamenti sono utilizzati da 21 enti, ma la configurazione del collegamento non consente all'Agenzia di conoscere il numero di utenti;*
- *"file transfer", collegamenti per la gestione di flussi di dati per la gran parte in entrata (principalmente provenienti da banche), ma alcuni anche in uscita (ad es., verso concessionari della riscossione), utilizzati da circa 200 enti.*

Mi sembra evidente che l'indagine abbia coinvolto seppur indirettamente più di un ente a cascata, il lungo elenco riguarda non solo l'Agenzia delle Entrate e sue appaltanti (SOGEI) ma come è ovvia anche tutti gli enti e privati cittadini che hanno la possibilità di accedere alle relative banche dati, in sostanza un numero indefinito di utenti come si evince chiaramente che usano principalmente un interfaccia (sito-web) per connettersi. L'attività del Garante seppur molto scrupolosa non è riuscita ad ottenere tutta una serie d'informazioni essenziali ai fini della valutazione del rischio da parte degli utenti, del resto non era compito dello stesso entrare nel merito. Ritengo però utile a tutti leggere l'intero provvedimento, sarebbe addirittura molto utile avere il rapporto originale redatto dagli Ispettori del Garante, è comunque un documento guida da additare

come esempio di corretto intervento.
In finale cercando di rimanere nel tema della certificazione digitale nel web da parte della PA si è arrivati ad alcune importanti conclusioni che riporto:
*"**2.1.1. Sicurezza dei sistemi di autenticazione***
Criticità
Per le web application è stato utilizzato un certificato Ssl di tipo self signed (non firmato da una Ca, Certification authority, ufficiale) non attendibile che, in mancanza di una Ca affidabile, non offre le garanzie di certezza dell'identità dell'erogatore del servizio tipiche della certificazione digitale tramite Pki (public key infrastructure): risultano pertanto facilitate azioni di phishing in danno di utenti del sistema e la possibile acquisizione indebita di credenziali di autenticazione, idonea a consentire utilizzi impropri dell'applicazione.
Dalle risultanze agli atti emerge inoltre che, rispetto a taluni collegamenti, l'identificazione dell'utente finale dell'applicazione è in molti casi in capo all'ente esterno. L'Agenzia non ha pertanto alcuna conoscenza dell'effettiva identità e del numero degli utenti che accedono, con tali modalità di connessione, da sistemi informativi esterni collegati direttamente all'anagrafe tributaria (ad es., 3270 enti esterni e web services).
È risultato, poi, possibile accedere alle web application Siatel e Puntofisco attraverso l'utilizzo delle medesime credenziali contemporaneamente da postazioni diverse, anche con indirizzo Ip diverso (perfino da rete esterna all'ente), nonostante, per quanto riguarda il Siatel, all'atto dell'accesso tale possibilità venga esclusa da un apposito avviso."
Da queste rilevazioni per la parte WEB si è quindi arrivati all'assoluta proibizione dell'uso di Certificati digitali emessi dallo stesso ente "self signed" Prescrivendo:
Prescrizioni
L'Agenzia deve prevedere che tutte le applicazioni accessibili da rete pubblica in forma di web application siano implementate con protocolli https/ssl provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una Certification Authority ufficiale, evitando il ricorso a certificati di tipo self-signed.
Allo scopo di identificare le postazioni da cui vengono effettuati gli accessi, occorre inoltre che l'Agenzia implementi un sistema di certificazione digitale e di censimento delle postazioni terminali, in modo da realizzare procedure di au-

tenticazione che, basandosi sul mutuo riconoscimento tra i server che erogano il servizio e le postazioni che accedono a esso, consentano di definire condizioni di accesso più complesse e sicure per determinate classi di incaricati o profili di autorizzazione.

Risulta evidente la precisa ed ovvia indicazione del Garante in materia di Certificazione digitale:

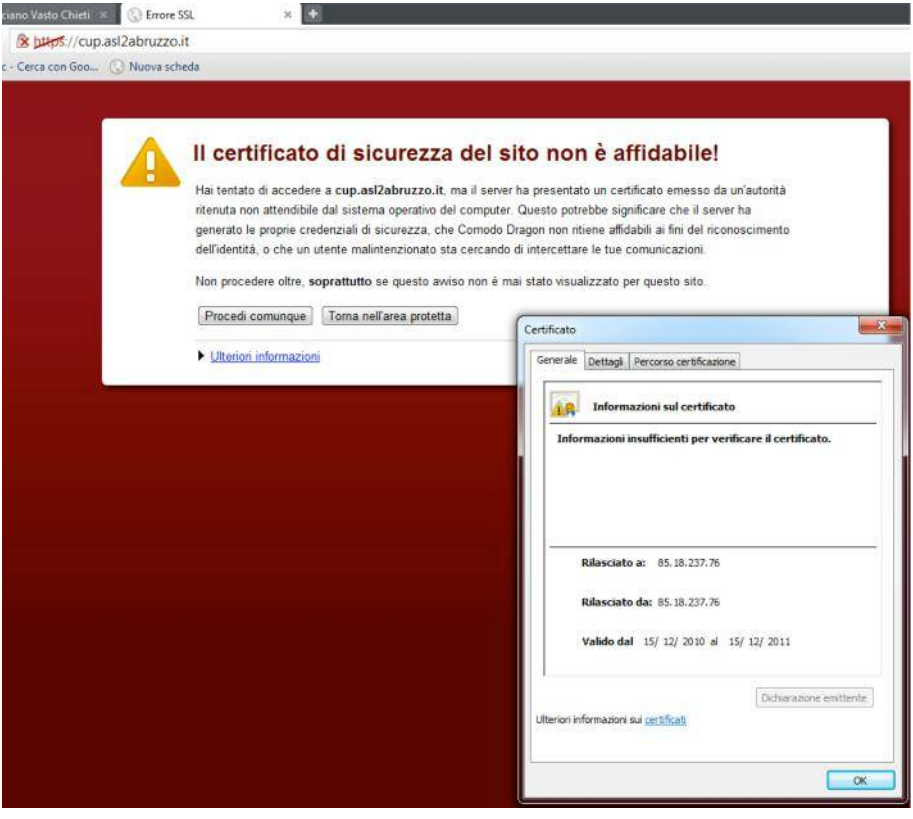
1) Non può essere valida una certificazione "fatta in casa" anche se chi la fa è un ente pubblico
2) Il certificatore deve essere terza parte
3) L'identità digitale deve essere accertata anche per i siti web, direi special modo, della PA. Quest'ultima affermazione in piena preveggenza di quanto l' *"electronic identification and trust services for electronic transactions in the internal market"* emanato proprio in questi giorni dalla UE.

Ovviamente la logica avrebbe consigliato al Garante di proseguire nell'accertamento andando a visitare le centinaia di enti collegati con le banche dati dell'Agenzia delle entrate, sicuramente ciò avrebbe significato un impegno enorme, conseguentemente si assiste ancora oggi ad episodi come quello segnalato dall'associazione Cittadini di internet della Provincia di Cuneo, o dell' ASL di Chieti vedi immagine qui sotto tanto per citare un paio di esempi ma c'è ne sono centinaia.

In sede di Spending Review fatta come vedo dal decreto omonimo ritengo *ironicamente* che cose come la certificazione dei siti web sia da abolire visto che costa l'enorme cifra di circa 500 Euro per Comune o ASL ad esempio, mentre si spendono migliaia di Euro per siti web dove forse solo gli autori degli stessi riescono a districarsi e navigare veri e propri guazzabugli d'informazione messi li a casaccio.. Evidentemente frasi come razionalizzazione dei sistemi informativi ed uso corretto e intelligente delle nuove tecnologie sono senza senso per coloro che dovrebbero razionalizzare la PA Italiana spendendo meno ovviamente qualora si usi un minimo di discernimento.

Asl Chieti: pagare ticket online non è sicuro.

Il certificato di sicurezza dell'Asl è scaduto dal 15 dicembre 2011


Errore SSL
https://cup.asl2abruzzo.it
Nuova scheda
Il certificato di sicurezza del sito non è affidabile!
Hai tentato di accedere a cup.asl2abruzzo.it, ma il server ha presentato un certificato emesso da un'autorità ritenuta non attendibile dal sistema operativo del computer. Questo potrebbe significare che il server ha generato le proprie credenziali di sicurezza, che Comodo Dragon non ritiene affidabili ai fini del riconoscimento dell'identità, o che un utente malintenzionato sta cercando di intercettare le tue comunicazioni.
Non procedere oltre, soprattutto se questo avviso non è mai stato visualizzato per questo sito.
Procedi comunque
Torna nell'area protetta
Ulteriori informazioni
Certificato
Generale
Dettagli
Percorso certificazione
Informazioni sul certificato
Informazioni insufficienti per verificare il certificato.
Rilasciato a: 85.18.237.76
Rilasciato da: 85.18.237.76
Valido dal 15/ 12/ 2010 al 15/ 12/ 2011
Dichiarazione emittente
Ulteriori informazioni sui certificati
OK

APPENDICE 2

II CAB FORUM

Un club esclusivo che raccogli praticamente tutte la Certification Authority al Mondo e tutti i browser oltre alla Microsoft fondato nel 2001.
The Certification Authority Browser Forum, conosciuto anche come CA/Browser Forum, è un consorzio volontario senza fine di lucro compost tra I leader che hanno creato e sviluppato la tecnologia del l certificato digitale SSL ed applicazioni relative. Nel Febrbaio, 2009, si sono unite alter importanti organizzazioni che hanno collaborato nella redazione delle nuove regole sia sulle CA e Browser ed anche per la emission e gestione di tutti I tipi di certificate SSL. Information Security Committee of the American Bar Association Section of Science & Technology, Law and the Canadian Institute of Chartered Accountants .
Gli attuali membri sono:
A-Trust GmbH
AC Camerfirma SA
Buypass AS
Certum
Chunghwa Telecom Co., Ltd.
Comodo CA Ltd
Cybertrust
D-TRUST GmbH
DanID A/S
DigiCert, Inc.
Digidentity
E-TUGRA Inc.
Echoworx Corporation
Entrust, Inc.
GeoTrust, Inc.
Getronics PinkRoccade
GlobalSign
GoDaddy.com, Inc.
IdenTrust, Inc.

ipsCA, IPS Certification Authority s.l.
Izenpe S.A.
Japan Certification Services, Inc.
Kamu Sertifikasyon Merkezi
KEYNECTIS
Logius PKIoverheid
Network Solutions, LLC
QuoVadis Ltd.
RSA Security, Inc.
SECOM Trust Systems CO., Ltd.
Skaitmeninio sertifikavimo centras (SSC)
StartCom Certification Authority
SwissSign AG
Symantec Corporation
T-Systems International GmbH.
TC TrustCenter GmbH
Trustwave
Thawte, Inc.
Trustis Limited
TURKTRUST
TAIWAN-CA Inc.
Wells Fargo Bank, N.A.

Internet Browser Software Vendors

Apple
Google Inc.
KDE
Microsoft Corporation
Opera Software ASA
The Mozilla Foundation
Research in Motion Limited

A questi sino aggiunti come partecipanti esterni alla redazione delle regole:

Access
Check Point Software
Cisco

Electronic Frontier Foundation
Federated Business
Kyle Hamilton
Internet Society
Messaging, Malware, and Mobile Anti-Abuse Working Group
National Institute of Standards and Technology
Opera
PayPal
Qualys
Chris Richardson
Red Hound Software
Safelayer
SiteTruth
Stephen Schultze
World Wide Web Consortium

Oltre a: Information SecurityCommittee of the American Bar Association, Canadian Institute of Chartered Accountants

Come risultato della collaborazione tra I player del mercato nel 2007, il CA/Browser Forum ha pubblicato la prima guida per l'emissione e gestione dei certificati SSL di tipo EV,. lo scopo era quello di creare uno standard "de facto" sul ciclo vitale dei certificati SSL partendo dalla guida per il più avanzato degli stessi. La regola principale era quella per le CA di poter emettere certificate di tipo EV solo ed esclusivamente in rispetto della norme contenute nella guida. Dopo questo primo importante passo come ovvia conseguenza fu di estendere le regole a tutti i Certificati SSL emessi dalle CA cosa fatta in aprile 2011 che entrerà in vigore dall'1 Giugno 2012 e riguarderà sia Certificati SSL del tipo DV, Domain-validated che OV/IV Organisation-validation. Questa è una svolta epocale nel controllo della emissione dei certificati di tipo SSL TLS e delle stesse Ca e dei Browser, ritengo quindi importante che si abbia una conoscenza approfondita su queste nuove regole che riguardano tutti i navigatori Internet che riporto per intero qui di seguito.

APPENDICE 3

CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0

Adopted on 22 Nov. 2011 with an Effective Date of 1 July 2012

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v. 1.0

Version 1.0, as adopted by the CA/Browser Forum on 22 Nov. 2011 with an Effective Date of 1 July 2012.

These Baseline Requirements describe an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements that are necessary (but not sufficient) for the issuance and management of Publicly-Trusted Certificates; Certificates that are trusted by virtue of the fact that their corresponding Root Certificate is distributed in widely-available application software. The Requirements are not mandatory for Certification Authorities unless

and until they become adopted and enforced by relying–party Application Software Suppliers.

Notice to Readers
This version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates present criteria established by the CA/Browser Forum for use by Certification Authorities when issuing, maintaining, and revoking publicly-trusted Certificates. The Requirements may be revised from time to time, as appropriate, in accordance with procedures adopted by the CA/Browser Forum. Because one of the primary beneficiaries of these Requirements is the end user, the Forum openly invites anyone to make recommendations and suggestions by email to the CA/Browser Forum at . The Forum members value all input, regardless of source, and will seriously consider all such input.

The CA/Browser Forum
The CA/Browser Forum is a voluntary organization of Certification Authorities and suppliers of Internet browser and other relying-party software applications. Membership as of November 2011 is as follows:

Certification Authorities
- A-Trust GmbH
- AC Camerfirma SA
- Buypass AS
- Certum
- Comodo CA Ltd
- Cybertrust
- D-TRUST GmbH
- DanID A/S
- DigiCert, Inc.
- Digidentity BV
- Echoworx Corporation
- Entrust, Inc.
- GeoTrust, Inc.
- Getronics PinkRoccade
- GlobalSign

- GoDaddy.com, Inc.
- IdenTrust, Inc.
- ipsCA, IPS Certification Authority s.l.
- Izenpe S.A.
- Japan Certification Services, Inc.
- Kamu Sertifikasyon Merkezi
- Keynectis
- Logius PKIoverheid
- Network Solutions, LLC
- QuoVadis Ltd.
- RSA Security, Inc.
- SECOM Trust Systems CO., Ltd.
- Skaitmeninio sertifikavimo centras (SSC)
- StartCom Certification Authority
- SwissSign AG
- Symantec Corporation
- T-Systems Enterprise Services GmbH.
- TC TrustCenter GmbH
- Thawte, Inc.
- TÜRKTRUST
- Trustis Limited
- Trustwave
- TWCA
- Verizon
- Wells Fargo Bank, N.A.

Relying-Party Application Software Suppliers

- Apple
- Google Inc.
- KDE
- Microsoft Corporation
- Opera Software ASA
- Research in Motion Limited
- The Mozilla Foundation

Other groups that have participated in the development of these Requirements

include the AICPA/CICA WebTrust for Certification Authorities task force and ETSI ESI. Participation by such groups does not imply their endorsement, recommendation, or approval of the final product.

1. Scope

The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates describe a subset of the requirements that a Certification Authority must meet in order to issue Publicly Trusted Certificates. Except where explicitly stated otherwise, these requirements apply only to relevant events that occur on or after the Effective Date.

These Requirements do not address all of the issues relevant to the issuance and management of Publicly-Trusted Certificates. The CA/Browser Forum may update the Requirements from time to time, in order to address both existing and emerging threats to online security. In particular, it is expected that a future version will contain more formal and comprehensive audit requirements for delegated functions.

This version of the Requirements only addresses Certificates intended to be used for authenticating servers accessible through the Internet. Similar requirements for code signing, S/MIME, time-stamping, VoIP, IM, Web services, etc. may be covered in future versions.

These Requirements do not address the issuance, or management of Certificates by enterprises that operate their own Public Key Infrastructure for internal purposes only, and for which the Root Certificate is not distributed by any Application Software Supplier.

2. Purpose

The primary goal of these Requirements is to enable efficient and secure electronic communication, while addressing user concerns about the trustworthiness of Certificates. The Requirements also serve to inform users and help them to make informed decisions when relying on Certificates.

3. References

ETSI TS 102 042 V2.1.1, Electronic Signatures and Infrastructures (ESI); Pol-

icy requirements for certification authorities issuing public key certificates.
FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.
ISO 21188:2006, Public key infrastructure for financial services — Practices and policy framework.
RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.
RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and certification Practices Framework, Chokhani, et al, March 1999.
RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers, et al, June 1999.
RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.
RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.
RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.
WebTrust, WebTrust Program for Certification Authorities Version 2.0, AICPA/CICA, available at http://www.webtrust.org/homepage-documents/item49945.aspx
X.509v3 , ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

4. Definitions

Affiliate: A corporation, partnership, joint venture or other entity controlling, con-

trolled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise)
in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Cer-

tificate to a particular community and/or PKI implementation with common security requirements.
Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.
Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.
Certification Practice Statement: One of several documents forming the governance framework in which
Certificates are created, issued, managed, and used.
Cross Certificate: A certificate that is used to establish a trust relationship between two Root CAs.
Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
Domain Authorization: Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.
Domain Name: The label assigned to a node in the Domain Name System.
Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain
Name System.
Domain Name Registrant: Sometimes referred to as the “owner” of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the “Registrant” by WHOIS or the Domain Name Registrar.
Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name author-

ity/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).
Effective Date: These Requirements come into force on 1 July 2012.
Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of
Certificates to that organization.
Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.
Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet
Domain Name System.
Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).
Internal Server Name: A Server Name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.
Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root
CA or a Subordinate CA.
Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.
Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair**. Key Pair:** The Private Key and its associated Public Key.
Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.
Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for
Standardization's applicable standard for a specific object or object class.
OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.
Online Certificate Status Protocol: An online Certificate-checking protocol

that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root
Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 17.6 (Auditor
Qualifications).

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when

software distributed by such Supplier merely displays information relating to a Certificate.
Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.
Requirements: This document.
Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:
Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software
Suppliers and that issues Subordinate CA Certificates.
Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of
Certificates issued to its Subordinate CAs.
Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The
Subject is either the Subscriber or a device under the control and operation of the Subscriber.
Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.
Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate
CA.
Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a
Subscriber or Terms of Use Agreement.
Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA.
Trustworthy System: Computer hardware, software, and procedures that

are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.
Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialists: Someone who performs the information verification duties specified by these
Requirements.
Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.
Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully- Qualified Domain Names contained in the Certificate.

5. Abbreviations and Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol

OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VOIP	Voice Over Internet Protocol

6. Conventions

Terms not otherwise defined in these Requirements shall be as defined in applicable agreements, user manuals, Certificate Policies and Certification Practice Statements, of the CA.
The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in these Requirements shall be interpreted in accordance with RFC 2119.

7. Certificate Warranties and Representations

7.1 By the CA

By issuing a Certificate, the CA makes the Certificate Warranties listed in Section 7.1.2 to the Certificate
Beneficiaries listed in 7.1.1.

7.1.1 Certificate Beneficiaries

Certificate Beneficiaries include, but are not limited to, the following:

1. The Subscriber that is a party to the Subscriber or Terms of Use Agreement for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate.

7.1.2 Certificate Warranties

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. **Right to Use Domain Name or IP Address:** That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
2. **Authorization for Certificate:** That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
3. **Accuracy of Information:** That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
4. **No Misleading Information:** That, at the time of issuance, the CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
5. **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Ap-

plicant in accordance with Sections 9.2.4 and 11.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
6. **Subscriber Agreement:** That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use;
7. **Status:** That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
8. **Revocation:** That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

7.2 By the Applicant

The CA SHALL require, as part of the Subscriber or Terms of Use Agreement, that the Applicant make the commitments and warranties set forth in Section 10.3.2 of these Requirements, for the benefit of the CA and the Certificate Beneficiaries.

8. Community and Applicability

8.1 Compliance

The CA SHALL at all times:
1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with these Requirements;
3. Comply with the audit requirements set forth in Section 17; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

If a court or government body with jurisdiction over the activities covered by these Requirements determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies

only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved SHALL notify the CA / Browser Forum of the facts, circumstances, and law(s) involved, so that the CA/Browser Forum may revise these Requirements accordingly.

8.2 Certificate Policies

8.2.1 Implementation

The CA SHALL develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements.

8.2.2 Disclosure

The CA SHALL publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose its CA business practices to the extent required by the CA's selected audit scheme (see Section 17.1). The disclosures MUST include all the material required by RFC 2527 or RFC 3647, and MUST be structured in accordance with either RFC 2527 or RFC 3647.

8.3 Commitment to Comply

The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version. The CA MAY fulfill this requirement by incorporating these Requirements directly into its Certificate Policy and/or Certification Practice Statements or by incorporating them by reference using a clause such as the following (which MUST include a link to the official version of these Requirements):
[Name of CA] conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at g. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

8.4 Trust model

The CA SHALL disclose all Cross Certificates that identify the CA as the Sub-

ject, provided that the CA arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

9. Certificate Content and Profile

9.1 Issuer Information

An Issuing CA SHALL populate the issuer field of each Certificate issued after the adoption of these Requirements in accordance with the following subsections.

9.1.1 Issuer Common Name Field

Certificate Field: issuer:commonName (OID 2.5.4.3)
Required/Optional: Optional
Contents: If present in a Certificate, the Common Name field MUST include a name that accurately identifies the Issuing CA.

9.1.2 Issuer Domain Component Field

Certificate Field: issuer:domainComponent (OID 0.9.2342.19200300.100.1.25)
Required/Optional: Optional.
Contents: If present in a Certificate, the Domain Component field MUST include all components of the Issuing CA's Registered Domain Name in ordered sequence, with the most significant component, closest to the root of the namespace, written last.

9.1.3 Issuer Organization Name Field

Certificate Field: issuer:organizationName (OID 2.5.4.10)
Required/Optional: Required
Contents: This field MUST contain the name (or abbreviation thereof), trademark, or other meaningful identifier for the CA, provided that they accurately identify the CA. The field MUST NOT contain a generic designation such as "Root" or "CA1".

9.1.4 Issuer Country Name Field

Certificate Field: issuer:countryName (OID 2.5.4.6)
Required/Optional: Required

Contents: This field MUST contain the two-letter ISO 3166-1 country code for the country in which the issuer's place of business is located.

9.2 Subject Information

By issuing the Certificate, the CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

9.2.1 Subject Alternative Name Extension

Certificate Field: extensions:subjectAltName
Required/Optional: Required
Contents: This extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate.
Wildcard FQDNs are permitted.
As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name, the CA SHALL notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. Also as of the Effective Date, the CA SHALL NOT issue a certificate with an Expiry Date later than 1 November 2015 with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name. Effective 1 October 2016, CAs SHALL revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Server Name.

9.2.2 Subject Common Name Field

Certificate Field: subject:commonName (OID 2.5.4.3)
Required/Optional: Deprecated (Discouraged, but not prohibited)

Contents: If present, this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see Section 9.2.1).

9.2.3 Subject Domain Component Field
Certificate Field: subject:domainComponent (OID 0.9.2342.19200300.100.1.25)
Required/Optional: Optional.
Contents: If present, this field MUST contain all components of the subject's Registered Domain Name in ordered sequence, with the most significant component, closest to the root of the namespace, written last.

9.2.4 Subject Organization Name Field
Certificate Fields:
Organization name: organizationName (OID 2.5.4.10)
Number and street: subject:streetAddress (OID: 2.5.4.9)
City or town: subject:localityName (OID: 2.5.4.7)
State or province (where applicable): subject:stateOrProvinceName (OID: 2.5.4.8)
Country: subject:countryName (OID: 2.5.4.6)
Postal/Zip code: subject:postalCode (OID: 2.5.4.17)
Required/Optional: The organization name is OPTIONAL. If organization name is present, then localityName, stateOrProvinceName (where applicable), and countryName are REQUIRED and streetAddress and postalCode are OPTIONAL. If organization name is absent, then the Certificate MUST NOT contain a streetAddress, localityName, stateOrProvinceName, or postalCode attribute. The CA MAY include the Subject's countryName field without including other Subject Identity Information pursuant to Section 9.2.5.
Contents: If the organizationName field is present, the field MUST contain the Subject's name or DBA and the required address fields MUST contain a location of the Subject as verified by the CA pursuant to Section 11.2. If the Subject is a natural person, because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, the CA MAY use the organizationName field to convey the

Subject's name or DBA.
If the fields include discrepancies that the CA considers minor, such as common variations and abbreviations, then the CA SHALL document the discrepancy and SHALL use locally accepted abbreviations when abbreviating the organization name, e.g., if the official record shows "Company Name Incorporated", the CA MAY include "Company Name, Inc."
The organizationName field may include a verified DBA or tradename of the Subject.

9.2.5 Subject Country Name Field
Certificate Field: subject:countryName (OID: 2.5.4.6)
Required/Optional: Optional
Contents: If the subject:countryName field is present, then the CA SHALL verify the country associated with the
Subject in accordance with Section 11.2.5 and use its two-letter ISO 3166-1 country code.

9.2.6 Other Subject Attributes
With the exception of the subject:organizationalUnitName (OU) attribute, optional attributes, when present within the subject field, MUST contain information that has been verified by the CA. Metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable, SHALL NOT be used.
CAs SHALL NOT include Fully-Qualified Domain Names in Subject attributes except as specified in Sections 9.2.1 and 9.2.2, above.
The CA SHALL implement a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 11.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 11.2.

9.3 Certificate Policy Identification
This section describes the content requirements for the Root CA, Subordinate

CA, and Subscriber Certificates, as they relate to the identification of Certificate Policy.

9.3.1 Reserved Certificate Policy Identifiers

The following Certificate Policy identifiers are reserved for use by CAs as an optional means of asserting compliance with these Requirements as follows:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline- requirements(2) domain-validated(1)} (2.23.140.1.2.1), if the Certificate complies with these Requirements but lacks Subject Identity Information that is verified in accordance with Section 11.2.

If the Certificate asserts the policy identifier of 2.23.140.1.2.1, then it MUST NOT include organizationName, streetAddress, localityName, stateOrProvinceName, or postalCode in the Subject field.

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline- requirements(2) subject-identity-validated(2)} (2.23.140.1.2.2), if the Certificate complies with these Requirements and includes Subject Identity Information that is verified in accordance with Section 11.2.

If the Certificate asserts the policy identifier of 2.23.140.1.2.2, then it MUST also include organizationName, localityName, stateOrProvinceName (if applicable), and countryName in the Subject field.

9.3.2 Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

9.3.3 Subordinate CA Certificates

A Certificate issued after the Effective Date to a Subordinate CA that is not an Affiliate of the Issuing CA:

1. MUST include one or more explicit policy identifiers that indicates the Subordinate CA's adherence to and compliance with these Requirements (i.e. either the CA/Browser Forum reserved identifiers or identifiers defined by the CA in its Certificate Policy and/or Certification Practice Statement) and
2. MUST NOT contain the "anyPolicy" identifier (2.5.29.32.0).

A Certificate issued after the Effective Date to a Subordinate CA that is an affiliate of the Issuing CA:

1. MAY include the CA/Browser Forum reserved identifiers or an identifier defined by the CA in its Certificate Policy and/or Certification Practice Statement to indicate the Subordinate CA's compliance with these Requirements and
2. MAY contain the "anyPolicy" identifier (2.5.29.32.0) in place of an explicit policy identifier.

A Subordinate CA SHALL represent, in its Certificate Policy and/or Certification Practice Statement, that all Certificates containing a policy identifier indicating compliance with these Requirements are issued and managed in accordance with these Requirements.

9.3.4 Subscriber Certificates

A Certificate issued to a Subscriber MUST contain one or more policy identifier(s), defined by the Issuing CA, in the Certificate's certificatePolicies extension that indicates adherence to and compliance with these Requirements. CAs complying with these Requirements MAY also assert one of the reserved policy OIDs in such Certificates.

The issuing CA SHALL document in its Certificate Policy or Certification Practice Statement that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Requirements.

9.4 Validity Period

Certificates issued after the Effective Date MUST have a Validity Period no greater than 60 months.

Except as provided for below, Certificates issued after 1 April 2015 MUST have a Validity Period no greater than
39 months.

Beyond 1 April 2015, CAs MAY continue to issue Certificates with a Validity Period greater than 39 months but not greater than 60 months provided that the CA documents that the Certificate is for a system or software that:

(a) was in use prior to the Effective Date;

(b) is currently in use by either the Applicant or a substantial number of Relying Parties;

(c) fails to operate if the Validity Period is shorter than 60 months;
(d) does not contain known security risks to Relying Parties; and
(e) is difficult to patch or replace without substantial economic outlay.

9.5 Subscriber Public Key

The CA SHALL reject a certificate request if the requested Public Key does not meet the requirements set forth in
Appendix A or if it has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

9.6 Certificate Serial Number

CAs SHOULD generate non-sequential Certificate serial numbers that exhibit at least 20 bits of entropy.

9.7 Additional Technical Requirements

The CA SHALL meet the technical requirements set forth in Appendix A - Cryptographic Algorithm and Key Requirements, and
Appendix B – Certificate Extensions, and Appendix C – User Agent Verification.

10. Certificate Application

10.1 Documentation Requirements

Prior to the issuance of a Certificate, the CA SHALL obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber or Terms of Use Agreement, which may be electronic.

The CA SHOULD obtain any additional documentation the CA determines necessary to meet these Requirements.

10.2 Certificate Request

10.2.1 General

Prior to the issuance of a Certificate, the CA SHALL obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with these Requirements. One certificate request MAY suffice for multiple Certificates to

be issued to the same Applicant, subject to the aging and updating requirement in Section 11.3, provided that each Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request MAY be made, submitted and/or signed electronically.

10.2.2 Request and Certification

The certificate request MUST contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

10.2.3 Information Requirements

The certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant.

Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's SubjectAltName extension.

10.2.4 Subscriber Private Key

Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key.

If the CA or any of its designated RAs generated the Private Key on behalf of the Subscriber, then the CA SHALL encrypt the Private Key for transport to the Subscriber.

If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

10.3 Subscriber and Terms of Use Agreement

10.3.1 General

Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate
Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's agreement to the Terms of Use agreement.

The CA SHALL implement a process to ensure that each Subscriber or Terms of Use Agreement is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber or Terms of Use Agreement.

10.3.2 Agreement Requirements

The Subscriber or Terms of Use Agreement MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
3. **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate:** An obligation and warranty to install the Certificate only

on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement;

5. **Reporting and Revocation:** An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;
6. **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. **Responsiveness:** An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance:** An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

11. Verification Practices

11.1 Authorization by Domain Name Registrant

The CA SHALL confirm that, as of the date the Certificate was issued, the Applicant either had the right to use, or had control of, the Fully-Qualified Domain Name(s) and IP address(es) listed in the Certificate, or was authorized by a person having such right or control (e.g. under a Principal-Agent or Licensor-Licensee relationship) to obtain a Certificate containing the Fully-Qualified Domain Name(s) and IP address(es).

If the CA relies on a confirmation of the right to use or control the Registered Domain Name(s) from a Domain Name Registrar, and the top-level Domain is a two-letter country code (ccTLD), the CA SHALL obtain the confirmation directly from the Domain Name Registrar for the Domain Name level to which the rules of the ccTLD apply. For example, if the requested FQDN is then the CA SHALL

obtain confirmation from the Domain Name Registrant of the Domain Name example.co.uk, because applications for Domain Names immediately subordinate to .co.uk are governed by the rules of the .uk registry.
If the CA uses the Internet mail system to confirm that the Applicant has authorization from the Domain Name Registrant to obtain a Certificate for the requested Fully-Qualified Domain Name, the CA SHALL use a mail system address formed in one of the following ways:

1. Supplied by the Domain Name Registrar;
2. Taken from the Domain Name Registrant's "registrant", "technical", or "administrative" contact information, as it appears in the Domain's WHOIS record; or;
3. By pre-pending a local part to a Domain Name as follows:
   a. Local part - One of the following: 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster'; and
   b. Domain Name – Formed by pruning zero or more components from the Registered Domain Name or the requested Fully-Qualified Domain Name.

If the Domain Name Registrant has used a private, anonymous, or proxy registration service, and the CA relies upon a Domain Authorization as an alternative to the foregoing, the Domain Authorization MUST be received directly from the private, anonymous, or proxy registration service identified in the WHOIS record for the Registered Domain Name. The document MUST contain the letterhead of the private, anonymous, or proxy registration service, the signature of the General Manager, or equivalent, or an authorized representative of such officer, dated on or after the certificate request date, and the Fully-Qualified Domain Name(s) to be included in the Certificate. If the WHOIS record identifies the private, anonymous, or proxy registration service as the Domain Name Registrant, then the Domain Authorization MUST contain a statement granting the Applicant the right to use the Fully- Qualified Domain Name in a Certificate. The CA SHALL contact the private, anonymous, or proxy registration service directly, using contact information obtained from a reliable, independent, third-party data source, and obtain confirmation from the Domain Name Registrant that the Domain Authorization is authentic.

11.2 Verification of Subject Identity Information

If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then the CA SHALL verify the country associated with the Subject using a verification process meeting the requirements of Section 11.2.5 and that is described in the CA's Certificate Policy and/or Certification Practice Statement. If the Applicant requests a Certificate that will contain the countryName field and other Subject Identity Information, then the CA SHALL verify the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of this Section 11.2 and that is described in the CA's Certificate Policy and/or Certification Practice Statement. The CA SHALL inspect any document relied upon under this Section for alteration or falsification.

11.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated, which the CA has evaluated in accordance with Section 11.6;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

Alternatively, the CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that meets the requirements of Section 11.6.

11.2.2 DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. Documentation or communication provided by a third party source that meets the requirements of Section 11.6;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by documentary support that meets the requirements of Section 11.6; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that meets the requirements of Section 11.6.

11.2.3 Authenticity of Certificate Request

If the Applicant for a Certificate containing Subject Identity Information is an organization, the CA SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

The CA MAY use the sources listed in section 11.2.1 to verify the Reliable Method of Communication. Provided that the CA uses a Reliable Method of Communication, the CA MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

In addition, the CA SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA SHALL NOT accept any certificate requests that are outside this specification. The CA SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

11.2.4 Verification of Individual Applicant

If an Applicant subject to this Section 11.2 is a natural person, then the CA SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

The CA SHALL verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The CA SHALL inspect the copy for any indication of alteration or falsification.

The CA SHALL verify the Applicant's address using a form of identification that meets Section 11.6, such as a government ID, utility bill, or bank or credit card statement. The CA MAY rely on the same government-issued ID that was used to verify the Applicant's name.

The CA SHALL verify the certificate request with the Applicant using a Reliable Method of Communication.

11.2.5 Verification of Country

If the subject:countryName field is present, then the CA SHALL verify the country associated with the Subject using one of the following: (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; (c) information provided by the Domain Name Registrar; or (d) a method identified in Section 11.2.1. The CA SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

11.3 Age of Certificate Data

Section 9.4 limits the validity period of Subscriber Certificates. The CA SHALL NOT use any data or document to validate a certificate request if the data or document was obtained more than thirty-nine (39) months prior to the Certificates' issuance.

11.4 Denied List

In accordance with Section 15.3.2, the CA SHALL maintain an internal database of all previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. The CA SHALL use this information to identify subsequent suspicious certificate requests.

11.5 High Risk Requests

The CA SHALL identify high risk certificate requests, and conduct such additional verification activity, and take such additional precautions, as are reasonably necessary to ensure that such requests are properly verified under these Requirements.

The CA MAY identify high risk requests by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and by automatically flagging certificate requests that match these lists for further scrutiny before issuance. Examples of such lists include: internal databases maintained by the CA that include previously revoked Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage.

The CA SHALL use information identified by the CA's high-risk criteria to flag suspicious certificate requests. The CA SHALL follow a documented procedure for performing additional verification of any certificate request flagged as suspicious or high risk.

11.6 Data Source Accuracy

Before relying on a data source to verify Subject Identity Information, the CA SHALL evaluate the data source's accuracy and reliability. The CA SHALL NOT use a data source to verify Subject Identity Information if the CA's evaluation determines that the data source is not reasonably accurate or reliable.

12. Certificate Issuance by a Root CA

Certificate issuance by the Root CA SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certifi-

cate signing operation.
Root CA Private Keys MUST NOT be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates);
4. Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA; and
5. Subscriber Certificates, provided that:
   a. The Root CA uses a 1024-bit RSA signing key that was created prior to the Effective Date;
   b. The Applicant's application was deployed prior to the Effective Date;
   c. The Applicant's application is in active use by the Applicant or the CA uses a documented process to establish that the Certificate's use is required by a substantial number of Relying Parties;
   d. The CA follows a documented process to determine that the Applicant's application poses no known security risks to Relying Parties; and
   e. The CA documents that the Applicant's application cannot be patched or replaced withoutsubstantial economic outlay.

13. Certificate Revocation and Status Checking

13.1

Revocation

13.1.1 Revocation Request

The CA SHALL provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in the CA's Certificate Policy or Certification Practice Statement. The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

13.1.2 Certificate Problem Reporting

The CA SHALL provide Subscribers, Relying Parties, Application Software Sup-

pliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA SHALL publicly disclose the instructions through a readily accessible online means.

13.1.3 Investigation

The CA SHALL begin investigation of a Certificate Problem Report within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
4. Relevant legislation.

13.1.4 Response

The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

13.1.5 Reasons for Revocation

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA obtains evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has suffered a Key Compromise, or that the Certificate has otherwise been misused (also see Section 10.2.4);

4. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement;
5. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
6. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
7. The CA is made aware of a material change in the information contained in the Certificate;
8. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
9. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
10. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
11. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
12. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
13. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or
14. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

13.2 Certificate Status Checking

13.2.1 Mechanisms

The CA SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with Appendix B.

If the Subscriber Certificate is for a high-traffic FQDN, the CA MAY rely on stapling, in accordance with [RFC4366], to distribute its OCSP responses. In this case, the CA SHALL ensure that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshake. The CA SHALL enforce this requirement on the Subscriber either contractually, through the Subscriber or Terms of Use Agreement, or by technical review measures implement by the CA.

13.2.2 Repository

The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

For the status of Subscriber Certificates:

1. If the CA publishes a CRL, then the CA SHALL update and reissue CRLs at least once every seven days, and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field; and
2. The CA SHALL update information provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.

For the status of Subordinate CA Certificates:

1. The CA SHALL update and reissue CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field MUST NOT be more than twelve months beyond the value of the thisUpdate field; and
2. The CA SHALL update information provided via an Online Certificate Status Protocol at least (i) every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

Effective 1 January 2013, the CA SHALL support an OCSP capability using the GET method for Certificates issued in accordance with these Requirements.

13.2.3 Response Time

The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

13.2.4 Deletion of Entries

Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.

13.2.5 OCSP Signing

OCSP responses MUST conform to RFC2560 and/or RFC5019. OCSP responses MUST either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC2560.

14. Employees and Third Parties

14.1 Trustworthiness and Competence

14.1.1 Identity and Background Verification

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, the CA SHALL verify the identity and trustworthiness of such person.

Pié di pagina della pagina [RTF: }CA / Browser Forum Baseline Requirements, v. 1.0

14.1.2 Training and Skill Level

The CA SHALL provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tac-

tics), and these Requirements.
The CA SHALL maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.
Validation Specialists engaged in Certificate issuance SHALL maintain skill levels consistent with the CA's training and performance programs.
The CA SHALL document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.
The CA SHALL require all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in these Requirements.

14.2 Delegation of Functions

14.2.1 General

The CA MAY delegate the performance of all, or any part, of Section 11 of these Requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 11.
Before the CA authorizes a Delegated Third Party to perform a delegated function, the CA SHALL contractually require the Delegated Third Party to:

1) Meet the qualification requirements of Section 14.1, when applicable to the delegated function;
2) Retain documentation in accordance with Section 15.3.2;
3) Abide by the other provisions of these Requirements that are applicable to the delegated function; and
4) Comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third

Party's practice statement that the CA has verified complies with these Requirements.
The CA SHALL verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 and the document retention and event logging requirements of Section 15.

14.2.2 Compliance Obligation

The CA SHALL internally audit each Delegated Third Party's compliance with

these Requirements on an annual basis.

14.2.3 Allocation of Liability

For delegated tasks, the CA and any Delegated Third Party MAY allocate liability between themselves contractually as they determine, but the CA SHALL remain fully responsible for the performance of all parties in accordance with these Requirements, as if the tasks had not been delegated.

14.2.4 Enterprise RAs

The CA MAY designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization.

The CA SHALL NOT accept certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

1. The CA SHALL confirm that the requested Fully-Qualified Domain Name(s) are within the Enterprise RA's verified Domain Namespace (see Section 7.1.2 para 1).
2. If the certificate request includes a Subject name of a type other than a Fully-Qualified Domain Name, the CA SHALL confirm that the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, the CA SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are affiliated (see Section 11.1) or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested Subject FQDN falls within the Domain Namespace of ABC Co.'s Registered Domain Name.

The CA SHALL impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA.

15. Data Records

15.1 Documentation and Event Logging

The CA and each Delegated Third Party SHALL record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the cer-

tificate request; the time and date; and the personnel involved. The CA SHALL make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

15.2 Events and Actions

The CA SHALL record at least the following events:

1. CA key lifecycle management events, including:
   a. Key generation, backup, storage, recovery, archival, and destruction; and
   b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
   a. Certificate requests, renewal, and re-key requests, and revocation;
   b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
   c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
   d. Acceptance and rejection of certificate requests;
   e. Issuance of Certificates; and
   f. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
   a. Successful and unsuccessful PKI system access attempts;
   b. PKI and security system actions performed;
   c. Security profile changes;
   d. System crashes, hardware failures, and other anomalies;
   e. Firewall and router activities; and
   f. Entries to and exits from the CA facility.

Log entries MUST include the following elements:

1. Date and time of entry;
2. Identity of the person making the journal entry; and
3. Description of the entry.

15.3 Retention

15.3.1 Audit Log Retention

The CA SHALL retain any audit logs generated after the Effective Date for at least seven years. The CA SHALL

make these audit logs available to its Qualified Auditor upon request.

15.3.2 Documentation Retention
The CA SHALL retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

16. Data Security

16.1 Objectives

The CA SHALL develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CA by law.

16.2 Risk Assessment

The CA's security program MUST include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

16.3 Security Plan

Based on the Risk Assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST also take into account then-available technology and the cost of implementing the specific measures, and SHALL implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

16.4 Business Continuity

In addition, the CA SHALL document a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The CA is not required to publicly disclose its business continuity plans but SHALL make the business continuity plan and security plan of Section 15.3 available to the CA's auditors upon request. The CA SHALL annually test, review, and update these procedures. The business continuity plan MUST include:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes

11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

16.5 System Security[1]

The Certificate Management Process MUST include:

1. physical security and environmental controls;
2. system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, separate trusted-role assignments, education, awareness, and training; and
5. logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

16.6 Private Key Protection

The CA SHALL protect its Private Key in a system or device that has been validated as meeting at least FIPS 140 level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats. The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the Private Key outside the validated

---

[1]The CA/Browser Forum will enact additional security requirements after the adoption of v1.0 of the Requirements.

system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. The CA SHALL encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part. The Private Key SHALL be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

17. Audit

17.1 Eligible Audit Schemes

The CA SHALL undergo an audit in accordance with one of the following schemes:

1. WebTrust for Certification Authorities v2.0 or later;
2. A national scheme that audits conformance to ETSI TS 101 456 v1.2.1 or later;
3. A national scheme that audits conformance to ETSI TS 102 042 V1.1.1 or later;
4. A scheme that audits conformance to ISO 21188:2006, completed by a Qualified Auditor; or
5. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it may use such scheme provided that: (a) the audit either (i) encompasses all requirements of one of the above schemes or (ii) consists of comparable criteria that are available for public review, and (b) the audit is performed by a Qualified Auditor, who is separate from the CA and who meets the requirements of Section 17.6.

17.2 Audit Period

The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.

17.3 Audit Report

The CA SHALL make the Audit Report publicly available. The CA is not required

to make publicly available any general audit findings that do not impact the overall audit opinion. For both government and commercial CAs, the CA SHOULD make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, the CA SHALL provide an explanatory letter signed by the Qualified Auditor.

17.4 Pre-Issuance Readiness Audit

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 17.1, then no pre-issuance readiness assessment is necessary.

If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 17.1, then, before issuing Publicly-Trusted Certificates, the CA SHALL successfully complete a point-in- time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 17.1. The point-in-time readiness assessment SHALL be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

17.5 Audit of Delegated Functions

If a Delegated Third Party is not currently audited in accordance with Section 17 and is not an Enterprise RA, then prior to certificate issuance the CA SHALL ensure that the domain control validation process required under Section 11.1 has been properly performed by the Delegated Third Party by either (1) using an out-of-band mechanism involving at least one human who is acting either on behalf of the CA or on behalf of the Delegated Third Party to confirm the authenticity of the certificate request or the information supporting the certificate request or (2) performing the domain control validation process itself. If the CA is not using one of the above procedures and the Delegated Third Party is not an Enterprise RA, then the CA SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in Section 17.1, that provides an opinion whether the Delegated Third Party's

performance complies with either the Delegated Third Party's practice statement or the CA's Certificate Policy and/or Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then the CA SHALL not allow the Delegated Third Party to continue performing delegated functions.
The audit period for the Delegated Third Party SHALL NOT exceed one year (ideally aligned with the CA's audit). However, if the CA or Delegated Third Party is under the operation, control, or supervision of a Government Entity and the audit scheme is completed over multiple years, then the annual audit MUST cover at least the core controls that are required to be audited annually by such scheme plus that portion of all non-core controls that are allowed to be conducted less frequently, but in no case may any non-core control be audited less often than once every three years.

17.6 Auditor Qualifications

The CA's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal
Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme;
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme;
5. Bound by law, government regulation, or professional code of ethics; and
6. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

17.7 Key Generation Ceremony

For Root CA Key Pairs created after the Effective Date that are either (i) used as Root CA Key Pairs or (ii) Key Pairs generated for a subordinate CA that is

not the operator of the Root CA or an Affiliate of the Root CA, the CA SHALL:
1. prepare and follow a Key Generation Script,
2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process, and
3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs created after the Effective Date that are for the operator of the Root CA or an Affiliate of the Root CA, the CA SHOULD:
1. prepare and follow a Key Generation Script and
2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire

Root CA Key Pair generation process.

In all cases, the CA SHALL:
1. generate the keys in a physically secured environment as described in the CA's Certificate Policy and/or Certification Practice Statement;
2. generate the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement;
4. log its CA key generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

17.8 Regular Quality Assessment Self Audits

During the period in which the CA issues Certificates, the CA SHALL monitor adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was

taken. Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 16.3, the CA SHALL strictly control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by the CA perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. The CA SHALL review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant Certificate Policy and/or Certification Practice Statement.

18. Liability and Indemnification

18.1 Liability to Subscribers and Relying Parties

If the CA has issued and managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA MAY disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in the CA's Certificate Policy and/or Certification Practice Statement. If the CA has not issued or managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA MAY seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that the CA desires. If the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement, then the CA SHALL include the limitations on liability in the CA's Certificate Policy and/or Certification Practice Statement.

18.2 Indemnification of Application Software Suppliers

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the

Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, the CA SHALL defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

18.3 Root CA Obligations

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

Appendix A - Cryptographic Algorithm and Key Requirements (Normative)

Certificates MUST meet the following requirements for algorithm type and key size.

(1) Root CA Certificates

	Validity period beginning on or before 31 Dec 2010	Validity period beginning after 31 Dec 2010
Digest algorithm	MD5 (NOT RECOMMENDED), SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048**	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

(2) Subordinate CA Certificates

	Validity period beginning on or before 31 Dec 2010 and ending on or before 31 Dec 2013	Validity period beginning after 31 Dec 2010 or ending after 31 Dec 2013
Digest algorithm	SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

(3) Subscriber Certificates

	Validity period ending on or before 31 Dec 2013	Validity period ending after 31 Dec 2013
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512	SHA1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521

* SHA-1 MAY be used until SHA-256 is supported widely by browsers used by a substantial portion of relying- parties worldwide.
** A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits MAY still serve as a trust anchor for Subscriber Certificates issued in accordance with these Requirements.

Appendix B – Certificate Extensions (Normative)

This appendix specifies the requirements for Certificate extensions for Certificates generated after the Effective
Date.

Root CA Certificate

Root Certificates MUST be of type X.509 v3.

A. basicConstraints

This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

B. keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

C. certificatePolicies

This extension SHOULD NOT be present.

D. extendedKeyUsage

This extension MUST NOT be present.

All other fields and extensions MUST be set in accordance to RFC 5280.

Subordinate CA Certificate

Subordinate CA Certificates MUST be of type X.509 v3.

A. certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical. certificatePolicies:policyIdentifier (Required)

The following fields MAY be present if the Subordinate CA is not an Affiliate of the entity that controls the
Root CA.

certificatePolicies:policyQualifiers:policyQualifierId (Optional)

- id-qt 1 [RFC 5280]. certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)
- HTTP URL for the Root CA's Certificate Policies, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the CA.

B. cRLDistributionPoints

This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.

C. authorityInformationAccess

With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). See Section 13.2.1 for details.

The HTTP URL of the Issuing CA's OCSP responder MAY be omitted, provided that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshakes [RFC4366].

D. basicConstraints

This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.

E. keyUsage

This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

All other fields and extensions MUST be set in accordance to RFC 5280.

Subscriber Certificate

A. certificatePolicies

This extension MUST be present and SHOULD NOT be marked critical. certificatePolicies:policyIdentifier (Required)

- A Policy Identifier, defined by the issuing CA, that indicates a Certificate Policy asserting the issuing CA's adherence to and compliance with these Requirements.

The following extensions MAY be present:

certificatePolicies:policyQualifiers:policyQualifierId (Recommended)

- id-qt 1 [RFC 5280]. certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

- HTTP URL for the Subordinate CA's Certification Practice Statement, Relying Party Agreement or other pointer to online information provided by the CA.

B. cRLDistributionPoints

This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service. See Section 13.2.1 for details.

C. authorityInformationAccess

With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and it MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). See Section 13.2.1 for details.

The HTTP URL of the Issuing CA's OCSP responder MAY be omitted provided that the Subscriber "staples" OCSP responses for the Certificate in its TLS handshakes [RFC4366].

D. basicConstraints (optional)

If present, the cA field MUST be set false.

E. keyUsage (optional)

If present, bit positions for keyCertSign and cRLSign MUST NOT be set.

F. extKeyUsage (required)

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present. id-kp-emailProtection [RFC5280] MAY be present. Other values SHOULD NOT be present.

All other fields and extensions MUST be set in accordance to RFC 5280.

Appendix C - User Agent Verification (Normative)

The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.

APPENDICE 4

Anagrafe tributaria: sicurezza e accessi
18 settembre 2008

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Giovanni Buttarelli, segretario generale;
VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);
VISTA la documentazione in atti;
VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante
n. 1/2000;
RELATORE il prof. Francesco Pizzetti;

PREMESSO

Sulla base di un'analisi preliminare del sistema informativo della fiscalità, il 14 dicembre 2007 il Garante ha deliberato l'avvio di accertamenti volti a verificare, in più fasi, i trattamenti di dati personali effettuati presso l'anagrafe tributaria, rilevando che elementi di maggior criticità e urgenza erano da ravvisarsi nelle misure di sicurezza adottate per gli accessi da parte di enti esterni, pubblici e privati, all'amministrazione finanziaria.
La prima fase di accertamenti attinente a tali accessi è stata completata. Il Garante svolgerà nel prosieguo le altre verifiche programmate sul trattamento dei dati effettuato dalle articolazioni dell'amministrazione finanziaria, con par-

ticolare riguardo alla struttura degli archivi, alle modalità di accesso, alle applicazioni utilizzate, alle tipologie di informazioni, alle misure di sicurezza, alle abilitazioni e alle autorizzazioni degli utenti.
Le attività ispettive completate hanno invece riguardato, in particolare:
1) il controllo degli applicativi che consentono l'accesso all'anagrafe tributaria a soggetti esterni all'amministrazione finanziaria (loro funzionalità; tipologie di dati visualizzabili con i differenti profili di autorizzazione previsti);
2) la designazione di responsabili e di incaricati, i sistemi di autenticazione (ad es., modalità di formazione e gestione delle *password*; controlli degli accessi ai sistemi applicativi) e i sistemi di autorizzazione;
3) le procedure di *audit* interno ed esterno sull'accesso alle informazioni contenute nell'anagrafe tributaria (ad es., controlli sulle abilitazioni e sulle autorizzazioni degli utenti abilitati all'utilizzo degli applicativi, modalità di raccolta dei *logfile* e loro analisi automatizzata).

Gli accertamenti ispettivi hanno avuto luogo presso l'Agenzia delle entrate, Sogei S.p.A. (Società generale d'informatica, responsabile del trattamento dei dati contenuti nell'anagrafe tributaria), regioni, province, comuni e altri enti che accedono a tale anagrafe, con la piena collaborazione degli enti coinvolti. Le verifiche hanno consentito di evidenziare criticità, in ambito sia informatico, sia organizzativo, documentate nei verbali in atti.
Dalle risultanze emerge che i sistemi di collegamento all'anagrafe tributaria utilizzati dai soggetti esterni all'amministrazione finanziaria sono i seguenti:
- "Siatel", applicazione *web* utilizzata principalmente da comuni, province, regioni, università, asl e consorzi di bonifica, per un totale di circa 9.400 enti e 60.000 utenze, che consente di visualizzare dati anagrafici completi, dati fiscali e atti del registro relativi alla totalità dei contribuenti;
- "Puntofisco", applicazione *web* di recente realizzazione e attualmente in dotazione a enti previdenziali, tribunali, camere di commercio e società varie, per un totale di circa 180 enti e 18.000 utenze. Puntofisco consente di visualizzare dati anagrafici, fiscali e atti del registro relativi alla totalità dei contribuenti, più aggiornati e con maggiore segmentazione delle informazioni rispetto a Siatel (ad es., differenziando tra dati anagrafici attuali o completi dello storico), ma permette anche di accedere a dati sensibili (presenti nel dettaglio degli oneri deducibili);

- "3270 enti esterni", collegamento diretto, tramite terminali fisici o emulatori di terminale, ai sistemi centrali dell'anagrafe tributaria, in corso di dismissione per esigenze di aggiornamento tecnologico, che tuttora consente a soggetti anche privati (Telecom Italia S.p.A., Enel, Inail, Inps, camere di commercio, Ministero delle politiche agricole, *"interforze"*) di collegarsi a informazioni anagrafiche e fiscali relative alla totalità dei contribuenti; la struttura dell'applicativo non consente all'Agenzia delle entrate di conoscere il numero di utenti;
- "Entratel", applicativo utilizzato dagli enti principalmente ai fini della trasmissione delle dichiarazioni, con flussi di dati solo in entrata verso l'Agenzia delle entrate; le credenziali di autenticazione fornite dall'Agenzia permettono altresì all'operatore di visualizzare la posizione fiscale dell'ente attraverso l'apposita *web application* ("Fisconline"/"Cassetto fiscale");
- *"web services"*, strumenti realizzati sulla base di specifiche tecniche definite caso per caso dall'Agenzia delle entrate, che consentono di accedere a dati anagrafici anche completi relativi alla totalità dei contribuenti. Tali collegamenti sono utilizzati da 21 enti, ma la configurazione del collegamento non consente all'Agenzia di conoscere il numero di utenti;
- *"file transfer"*, collegamenti per la gestione di flussi di dati per la gran parte in entrata (principalmente provenienti da banche), ma alcuni anche in uscita (ad es., verso concessionari della riscossione), utilizzati da circa 200 enti.

OSSERVA

Nel corso dei menzionati accertamenti ispettivi, sulla base della documentazione in atti, sono state riscontrate alcune criticità di seguito descritte, già in parte riconosciute dall'Agenzia, relative agli accessi all'anagrafe tributaria da parte degli enti esterni all'amministrazione finanziaria, riferibili in particolare alle autenticazioni e alle autorizzazioni degli utenti, ai controlli da parte dell'Agenzia e alle estese possibilità di accesso alle banche dati. Accanto a diverse problematiche attinenti alla sicurezza, sono emersi e vengono affrontati connessi profili concernenti aspetti sostanziali del trattamento.

Il Garante, ai sensi dell'art. 154, comma 1, lett. c) del Codice, ritiene necessario prescrivere una serie di misure e accorgimenti che devono essere adottati dall'Agenzia delle entrate, anche in riferimento ai soggetti esterni che accedono

all'anagrafe tributaria, di seguito indicati. Tali misure e accorgimenti, principalmente di carattere tecnico e organizzativo, sono necessari al fine di porre rimedio alle carenze riscontrate e a incrementare, in particolare, i livelli di sicurezza degli accessi all'anagrafe tributaria, rendendo il trattamento conforme alle disposizioni vigenti.

1. Accessi all'anagrafe tributaria da parte di soggetti esterni all'amministrazione finanziaria: profili generali

Criticità

Alcuni accertamenti in proposito sono risultati meno agevoli in considerazione del fatto che l'Agenzia non aveva immediatamente disponibile, come richiesto dall'Autorità, una completa documentazione relativa sia ai soggetti esterni collegati, sia ai sistemi di accesso utilizzati da questi ultimi (numero e categorie di soggetti, finalità degli accessi e tipologie di collegamenti e di dati comunicati). Dagli atti emerge ora che l'Agenzia autorizza gli accessi all'anagrafe tributaria solo in seguito alla stipula di apposite convenzioni, anche *standard*, a livello centrale e regionale. Tuttavia, l'assenza di una documentazione di insieme sui collegamenti in essere non agevola un monitoraggio costante sulla sussistenza dei presupposti che hanno consentito l'attivazione del canale informativo, nonché i dovuti controlli sulla correttezza della gestione degli accessi e della consultazione delle informazioni. La periodica ricognizione degli enti che accedono all'anagrafe tributaria, e dei rispettivi utenti, costituisce infatti la premessa per prevenire usi impropri e illeciti delle informazioni in essa contenute.

È stato inoltre riscontrato in atti che in alcune convenzioni stipulate per l'accesso all'anagrafe tributaria non risultano delimitate chiaramente le finalità per cui gli accessi vengono autorizzati; sotto tale aspetto, è stato rilevato che alcuni enti, attraverso gli amministratori locali (soggetti deputati all'abilitazione degli utenti), hanno abilitato di propria iniziativa alcuni utenti al fine di attivare nuovi flussi di dati per finalità ulteriori rispetto a quelle consentite.

Non risulta altresì dagli atti che gli operatori che effettuano gli accessi abbiano l'onere (o la possibilità) di registrare, anche al fine di successivi controlli, le ragioni a supporto delle interrogazioni eseguite.

È stato inoltre verificato che i dati visualizzabili attraverso gli applicativi non sono segmentabili in relazione al bacino di utenza dell'ente che chiede il collegamento (ad es., territorio comunale), e sono relativi a tutto il territorio nazionale.

Infine, le informazioni consultabili non risultano, talvolta, sufficientemente aggiornate per lo svolgimento delle funzioni istituzionali cui gli accessi sono finalizzati (ad es., in Siatel, ai fini della verifica dell'Isee non sono visualizzabili i dati dell'ultima dichiarazione presentata e vengono invece visualizzati dati reddituali riferiti ad annualità pregresse, eccedenti e non pertinenti rispetto alle finalità perseguite, che non consentono di effettuare i puntuali controlli sulle autocertificazioni reddituali ai sensi del d.P.R. n. 445/2000).
Da ultimo, sulla base delle risultanze in atti, è stato rilevato che gli accessi all'anagrafe tributaria vengono effettuati talvolta per conoscere informazioni (ad es., la residenza) che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti (ad es., amministrazioni certificanti ai sensi dell'art. 71 del d.P.R. n. 445/2000).

Prescrizioni
L'Agenzia deve disporre di informazioni complete e strutturate sulla molteplicità di soggetti che, a vario titolo, accedono alla banca dati dell'anagrafe tributaria. Occorre pertanto che la stessa rediga un documento, con formalità descrittive *standard*, che riporti tutti i flussi di trasferimento di dati da e verso l'anagrafe tributaria e tutti gli accessi di tipo interattivo, *batch* o di altro genere, specificando per ciascun flusso o accesso l'identità dei soggetti legittimati a realizzarlo, la base normativa (anche ai sensi dell'art. 19, comma 2 del Codice, previa comunicazione al Garante), la finalità istituzionale, la natura e la qualità dei dati trasferiti o a cui si è avuto accesso, la frequenza e il volume dei trasferimenti o degli accessi e il numero di soggetti che utilizzano la procedura. Tale documento dovrà essere mantenuto costantemente aggiornato, nonché reso disponibile nel caso di controlli.
L'Agenzia deve altresì verificare, con cadenza periodica annuale, l'attualità delle finalità per cui ha concesso l'accesso agli enti esterni, anche con riferimento al numero di utenze attive, inibendo gli accessi (autorizzazioni o singole utenze) effettuati al di fuori dei presupposti riconducibili all'art. 19 del Codice (norme di legge o regolamento, nonché eventuali comunicazioni al Garante ai sensi dell'art. 19 del Codice) e quelli non conformi a quanto stabilito nelle convenzioni. All'esito di tali verifiche, in particolare, devono essere eliminati gli accessi effettuati per conoscere informazioni che, ai sensi della normativa vigente,

dovrebbero essere invece controllate presso altri soggetti.
Per vincolare effettivamente gli accessi alle finalità consentite, l'Agenzia deve introdurre nelle applicazioni volte all'uso interattivo da parte di incaricati un campo per l'indicazione obbligatoria del numero di riferimento della pratica (ad es. numero del protocollo o del verbale) nell'ambito della quale viene effettuata la consultazione.
L'Agenzia deve poi far sì che gli applicativi consentano, per quanto più possibile, la segmentazione dei dati visualizzabili in particolare in modo cronologico (attuale o storico, per periodi di imposta), geografico (comune, provincia, regione) e per tipologia di dati (ad es. di sintesi)al fine di rendere consultabili dall'utente, anche in base al proprio profilo e in relazione al bacino di utenza dell'ente che chiede il collegamento, esclusivamente i dati necessari rispetto alle finalità perseguite (ad es. l'ultimo domicilio fiscale o l'ultimo periodo di imposta).

2. I sistemi utilizzati per il collegamento all'anagrafe tributaria

2.1. Profili comuni

Le principali criticità di carattere generale relative all'utilizzo degli applicativi riscontrate nel corso degli accertamenti ispettivi sugli accessi da parte dei soggetti esterni sono di seguito individuate.

2.1.1. Sicurezza dei sistemi di autenticazione
Criticità
Per le *web application* è stato utilizzato un certificato *Ssl* di tipo *self signed* (non firmato da una *Ca, Certification authority*, ufficiale) non attendibile che, in mancanza di una *Ca* affidabile, non offre le garanzie di certezza dell'identità dell'erogatore del servizio tipiche della certificazione digitale tramite *Pki (public key infrastructure)*: risultano pertanto facilitate azioni di *phishing* in danno di utenti del sistema e la possibile acquisizione indebita di credenziali di autenticazione, idonea a consentire utilizzi impropri dell'applicazione.
Dalle risultanze agli atti emerge inoltre che, rispetto a taluni collegamenti, l'identificazione dell'utente finale dell'applicazione è in molti casi in capo all'ente esterno. L'Agenzia non ha pertanto alcuna conoscenza dell'effettiva identità e del numero degli utenti che accedono, con tali modalità di connessione, da sistemi informativi esterni collegati direttamente all'anagrafe tributaria (ad es.,

3270 enti esterni e *web services*).
È risultato, poi, possibile accedere alle *web application* Siatel e Puntofisco attraverso l'utilizzo delle medesime credenziali contemporaneamente da postazioni diverse, anche con indirizzo *Ip* diverso (perfino da rete esterna all'ente), nonostante, per quanto riguarda il Siatel, all'atto dell'accesso tale possibilità venga esclusa da un apposito avviso.

Prescrizioni
L'Agenzia deve prevedere che tutte le applicazioni accessibili da rete pubblica in forma di *web application* siano implementate con protocolli *https/ssl* provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una *Certification Authority* ufficiale, evitando il ricorso a certificati di tipo *selfsigned*.
Allo scopo di identificare le postazioni da cui vengono effettuati gli accessi, occorre inoltre che l'Agenzia implementi un sistema di certificazione digitale e di censimento delle postazioni terminali, in modo da realizzare procedure di autenticazione che, basandosi sul mutuo riconoscimento tra i *server* che erogano il servizio e le postazioni che accedono a esso, consentano di definire condizioni di accesso più complesse e sicure per determinate classi di incaricati o profili di autorizzazione.
A fronte dell'accertata possibilità per taluni applicativi di effettuare più accessi contemporanei con le medesime credenziali, al fine di consentire a ciascun utente di controllare l'utilizzo del proprio *account*, l'Agenzia deve poi prevedere in considerazione della specificità dell'anagrafe tributariala visualizzazione, nella prima schermata successiva al collegamento, di informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui è stata effettuata la precedente connessione). Per accrescere la consapevolezza del controllo, le stesse informazioni devono essere riportate anche relativamente alla sessione corrente.
Infine, l'Agenzia deve disciplinare la possibilità di effettuare accessi contemporanei con le medesime credenziali (sessioni multiple), limitandone l'utilizzo ai soli casi necessari per esigenze di servizio (ad es., per le connessioni originate da una stessa postazione di lavoro). In ogni caso, tale possibilità deve

essere consentita esclusivamente laddove il certificato digitale o l'indirizzo Ip siano sufficienti a discriminare l'identità digitale delle postazioni accedenti, come sopra descritto. Nel caso in cui non sia possibile individuare la postazione di lavoro, nelle more dell'attuazione delle prescrizioni sopra individuate, deve essere inibita la possibilità di accessi contemporanei.

2.1.2. Amministratori locali, abilitazioni e autorizzazioni
Criticità
È stato verificato negli accertamenti ispettivi che gli enti esterni hanno spesso affidato il compito di amministratore locale (il soggetto deputato alla gestione delle utenze) a personale non in grado né di valutare la pertinenza delle richieste di abilitazione delle utenze, né di monitorarne gli eventuali utilizzi impropri. In taluni enti è stata riscontrata la presenza di più amministratori locali con funzionalità che non consentivano di gestire gli utenti in modo tra loro coordinato.
Dalle risultanze agli atti è emerso, inoltre, che non è stato predeterminato un adeguato flusso informativo tra l'amministratore locale e l'unità organizzativa deputata alla gestione del personale al fine di consentire l'immediata disabilitazione o revisione del profilo di autorizzazione dei soggetti indirizzati ad altre mansioni o il cui rapporto con l'ente sia cessato.
Sono stati riscontrati poi casi di cessioni e condivisioni di credenziali di accesso, profili di autorizzazione inadeguati e/o eccessivi rispetto alle finalità perseguite, nonché mancate designazioni di incaricati al trattamento.
È stato verificato altresì che alcuni enti hanno utilizzato strumenti automatizzati di interrogazione che hanno consentito la duplicazione anche massiva di dati contenuti nell'anagrafe tributaria, con la creazione di autonome basi di dati, non conforme alle finalità per le quali è stato autorizzato l'accesso all'anagrafe tributaria.
Dalla documentazione in atti emerge che l'Agenzia, anche a seguito delle prime risultanze dell'attività ispettiva sopra illustrate, ha manifestato l'intenzione di voler gestire direttamente l'abilitazione di tutte le utenze, eliminando gli amministratori di sistema degli enti esterni.
Al riguardo, nonostante le predette criticità concernenti l'attività svolta dagli amministratori esterni, il modello decentrato di gestione delle utenze incentrato su

tali figure, opportunamente integrato con le misure di seguito descritte, costituisce comunque il perno per un corretto sistema di accesso all'anagrafe tributaria. L'amministratore locale, infatti, è il soggetto più idoneo a controllare l'attività quotidiana dei propri utenti senza limitarne l'operatività, anche a fronte dell'ingente numero di enti, e quindi di utenti, abilitati ad accedere all'anagrafe tributaria, ognuno per il proprio specifico fabbisogno informativo.

Prescrizioni

L'Agenzia, nelle convenzioni che disciplinano l'accesso all'anagrafe tributaria, deve prevedere che gli "amministratori locali" (soggetti deputati alla gestione delle utenze) scelti dagli enti esterni siano individuati sulla base di elevati requisiti di idoneità soggettiva, preferibilmente tra soggetti che abbiano un rapporto stabile con essi. Questi soggetti, prima di intraprendere la loro attività, devono essere formati dall'Agenzia delle entrate in ordine alle funzionalità dell'applicativo e all'attività di autorizzazione degli utenti. L'amministratore locale dell'ente esterno che accede all'anagrafe tributaria deve rimanere il punto di riferimento per le richieste di abilitazione e autorizzazione con la possibilità di gestire direttamente le utenze; deve essere altresì dotato degli adeguati strumenti di controllo sugli accessi (cfr. punto 3).

Nelle convenzioni deve essere poi previsto che gli enti esterni, anche per mezzo degli amministratori locali, debbano istruire adeguatamente il personale addetto all'utilizzo dei vari applicativi in ordine al corretto utilizzo delle funzionalità dei *software*. Le convenzioni, entro i medesimi termini, devono inoltre imporre periodici controlli sugli accessi agli enti esterni anche attraverso gli appositi strumenti di monitoraggio e *alert* in dotazione all'amministratore locale che saranno attivati dall'Agenzia (cfr. punto 3)i cui esiti devono essere documentati secondo le modalità definite nelle convenzioni stesse.

Le convenzioni devono anche predefinire una procedura per le autenticazioni e le autorizzazioni che coinvolga attivamente le figure apicali degli uffici interessati e un unico supervisore (soggetto giuridicamente preposto all'individuazione degli utenti e dei profili). Il supervisore può anche non coincidere con l'amministratore tecnicamente deputato alla materiale gestione delle abilitazioni (e del relativo profilo), ma deve rispondere del controllo sullo stesso. Occorre inoltre che venga assicurato un flusso di comunicazione tra l'ammini-

stratore locale e l'articolazione che si occupa della gestione delle risorse umane, al fine di procedere alla tempestiva revisione del profilo di abilitazione o alla disabilitazione dei soggetti preposti ad altre mansioni o che abbiano cessato il rapporto con l'ente (soprattutto con riguardo ad enti di rilevanti dimensioni), anche con apposite verifiche a cadenza almeno trimestrale.
Per quanto riguarda la possibilità di individuare più amministratori locali per ciascun ente, l'Agenzia deve valutare e coordinare attentamente i profili di autorizzazione da attribuire, garantendo in capo a un'unica figura la possibilità, ove occorra, di intervenire su tutti gli utenti anche amministratori, monitorandone l'operato (amministratore con ruolo di supervisore).
É necessario che l'Agenzia predefinisca anche soglie relative al numero di utenti abilitabili da ciascun ente in relazione alle sue dimensioni e alle finalità per le quale viene richiesto il collegamento. Le richieste di superamento di tali soglie devono essere valutate caso per caso dall'Agenzia stessa.
Le *web application* predisposte dall'Agenzia per l'utilizzo da parte di enti esterni vanno integrate con procedure di "autenticazione forte" (*strong authentication*) per ridurre la possibilità di usi impropri delle credenziali, la loro cessione o la loro sottrazione ai legittimi assegnatari. Tali procedure devono essere prefigurate nei confronti delle classi di utenti cui corrispondono profili di autorizzazione più critici in relazione alle funzioni o ai dati accessibili e, comunque, almeno per tutti i profili di autorizzazione corrispondenti alle funzioni di amministrazione locale delle applicazioni. Tali procedure potranno essere basate sull'utilizzo di dispositivi standard quali *smart card* o *token* per la generazione di *onetimepassword*.
L'Agenzia deve infine prevedere limitazioni orarie per gli accessi, mantenendo la possibilità di specifiche deroghe adeguatamente motivate.
Le convenzioni stipulate con ciascun ente devono prevedere espressamente i vincoli necessari ad assicurare un corretto trattamento dei dati e devono stabilire le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione.

2.2. I singoli sistemi
2.2.1. Siatel
Criticità

Con particolare riferimento all'applicativo Siatel, nel corso degli accertamenti sono state rilevate le seguenti criticità:

- l'area di gestione dei file da scaricare nella funzione "fornitura dati" disponibile per i comuni e le regioni riporta soltanto la data di primo *download* del file, che rimane da quel momento disponibile per ulteriori e illimitati *download* non censiti e, pertanto, non controllabili;
- le funzionalità di *file transfer*, predisposte per i comuni ai fini dell'allineamento dell'anagrafe tributaria con le anagrafi della popolazione, sono state talvolta utilizzate per finalità diverse, potendo determinare l'introduzione di informazioni errate nei sistemi;
- i dati anagrafici visualizzabili sono completi (ad es., forniscono sempre lo "storico" delle residenze) e non è possibile limitare la consultazione alle sole informazioni anagrafiche attuali.

Prescrizioni

L'Agenzia deve introdurre misure di controllo per la funzionalità di "fornitura dati" visualizzabile nell'apposita schermata dell'applicativo (ad es., rimuovendo il *file* messo a disposizione in rete dopo un certo tempo dalla richiesta, ovvero indicando il numero di operazioni di *download* già effettuate per ciascun *file*, l'utenza, la data e l'orario del *download*, nonché limitandoli alla sola utenza richiedente).

Con riferimento alle funzionalità di Siatel utilizzabili da parte degli operatori comunali a soli fini anagrafici, devono essere inserite nell'applicativo da parte dell'Agenzia specifiche indicazioni all'amministratore locale affinché vengano autorizzati solo utenti che agiscono presso l'ufficio anagrafe del comune.

2.2.2. Puntofisco

Criticità

In relazione al sistema Puntofisco è stato verificato dalle risultanze in atti che l'applicativo permette di visualizzare i dati sensibili relativi agli oneri deducibili contenuti nelle dichiarazioni dei redditi.

L'amministratore locale ("gestore") non è in grado di visualizzare lo stato delle utenze (attiva/disattiva) e la lista utenti a lui disponibile comprende anche gli utenti già disabilitati. Il sistema di gestione delle utenze, inoltre, non permette

regolarmente al gestore (amministratore), visualizzando il profilo dell'utente, di conoscere l'effettiva possibilità di accesso dello stesso al sistema.

Prescrizioni
Occorre aggiornare il profilo di autorizzazione assegnato agli enti esterni abilitati, escludendo a priori la consultabilità di dati sensibili laddove non sussista un'idonea base normativa che consenta la comunicazione di tale categoria di dati.
L'Agenzia deve inserire all'interno della procedura informatica di gestione degli utenti in uso all'amministratore locale indicazioni che gli consentano di visualizzare lo *status* di tutte le utenze con i profili abilitativi correnti, comprese quelle già cancellate. Deve essere corretta altresì l'anomalia, relativa al sistema di gestione, che non permette regolarmente all'amministratore locale, visualizzando il profilo del singolo utente, di conoscerne l'effettiva possibilità di accesso dello stesso al sistema.

2.2.3. 3270 enti esterni, web services e file transfer
Criticità
Con riferimento alle risultanze ispettive, è stato rilevato che il collegamento denominato 3270 enti esterni, l'accesso tramite *web service* e lo scambio dati mediante *file transfer* non consentono attualmente di limitare e controllare gli accessi in relazione alla loro provenienza, e non garantiscono misure idonee a verificare il rispetto delle regole di sicurezza di cui all'Allegato B del Codice. In particolare, è risultato che:
- l'Agenzia non è in grado di quantificare i soggetti che accedono ai dati, di attribuire agli stessi le operazioni tracciate dal sistema e di verificare il rispetto delle misure di sicurezza poiché l'identificazione degli *enduser* degli applicativi è affidata all'ente esterno che chiede il collegamento, come anche l'attribuzione certa a ogni incaricato di una o più credenziali per l'autenticazione, nonché la periodica scadenza della parola chiave;
- è impossibile per l'Agenzia individuare la postazione che effettua gli accessi, risultando assenti idonei sistemi che la consentirebbero quali, ad esempio, la certificazione digitale sulle postazioni e sugli emulatori di terminale utilizzati.

Prescrizioni

Devono essere garantite condizioni adeguate di protezione dei dati personali, di controllo e di verifica delle attività compiute (funzioni di *audit*) sugli applicativi utilizzati per accedere all'anagrafe tributaria, nonché strumenti che permettano all'Agenzia di verificare il rispetto delle misure di sicurezza.

Per quanto riguarda gli accessi all'anagrafe tributaria effettuati mediante l'applicativo 3270 enti esterni gli enti ad oggi abilitati devono migrare verso applicativi che offrono maggiori garanzie (ad es., Puntofisco o Siatel).

Con riferimento ai *web service*, l'Agenzia deve effettuare una ricognizione dei servizi al momento esposti e sospenderne l'attività in attesa della revisione delle attuali modalità di implementazione con le adeguate misure e gli accorgimenti di seguito descritti.

Laddove, infatti, l'Agenzia intenda impiegare *web service* esposti anche in una rete pubblica per l'utilizzo da parte di enti esterni, questi, in considerazione della delicatezza delle informazioni contenute nell'anagrafe tributaria, anche al fine di evitare duplicazioni delle banche dati e rischi di disallineamento, devono essere configurati offrendo un livello minimo di accesso ai dati e limitando i risultati delle interrogazioni a valori di tipo *booleano* (ad es., *web service* che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un determinato codice fiscale). Le convenzioni per l'utilizzo di tali servizi, inoltre, devono prevedere stringenti condizioni d'uso tali da consentire anche un'effettiva capacità di controllo da parte dell'Agenzia. Dal punto di vista tecnico, tali condizioni d'uso dei *web service* devono essere trasposte in appositi "accordi di servizio", redatti secondo il modello della cooperazione applicativa impiegata all'interno del sistema pubblico di connettività istituito dal Codice dell'amministrazione digitale. Gli "accordi di servizio" devono individuare idonee garanzie per il trattamento dei dati personali, prevedendo, in particolare, il tracciamento delle operazioni compiute in cooperazione applicativa, con possibilità di identificazione dell'utente che accede ai dati, il *timestamp*, l'indirizzo Ip di provenienza dell'utente e del *server* interconnesso, l'operazione effettuata e i dati trattati.

I collegamenti per la gestione di flussi di dati mediante *file transfer* devono essere realizzati su canali di connessione sicuri e l'Agenzia deve garantire, anche attraverso la configurazione dei sistemi, che le credenziali di abilitazione

utilizzate dagli operatori dell'ente esterno rispettino le prescrizioni indicate nell'Allegato B al Codice, in particolare identificando il soggetto che effettua lo scambio dei dati e prevedendo che la parola chiave prevista sia soggetta a scadenza periodica secondo i termini ivi indicati.

2.2.4. Entratel
Criticità
Dagli accertamenti ispettivi è emerso che le caratteristiche tecniche di Entratel, in uso dal 1998, sono state realizzate al fine di consentire al tempo la massima fruibilità dell'applicativo anche a soggetti con limitate risorse tecnologiche. Allo stato degli atti, le credenziali attribuite dall'Agenzia (anche le chiavi asimmetriche) identificano però solo l'ente richiedente, anziché l'operatore finale. Per quanto riguarda l'accesso all'applicativo Fisconline/Cassetto fiscale, le *password* non sono soggette a scadenza periodica.

Prescrizioni
L'Agenzia deve configurare Entratel e Fisconline/Cassetto fiscale in modo da poter verificare il rispetto delle prescrizioni indicate nell'Allegato B al Codice relative, in particolare, al sistema di scadenza delle *password* e all'attribuzione di credenziali idonee ad identificare direttamente, oltre all'ente abilitato, anche il singolo incaricato che fisicamente effettua l'accesso, autentica e trasmette i *file*.

3. Le procedure di audit sull'accesso alle informazioni contenute nell'anagrafe tributaria da parte di soggetti esterni

Criticità
Gli accertamenti hanno permesso di verificare che tutti i *file* di *log* relativi alle transazioni effettuate nell'anagrafe tributaria sono conservati a tempo indeterminato da Sogei S.p.a., quelli relativi agli ultimi sette giorni sono mantenuti in linea, mentre quelli precedenti sono conservati su nastri magnetici. Talvolta Sogei S.p.a., di propria iniziativa, al fine di monitorare anomalie e funzionalità del sistema, ha eseguito alcuni rilievi quantitativi sulle transazioni effettuate provvedendo a segnalare all'Agenzia le attività difformi riscontrate.
Secondo quanto si evince dalla documentazione in atti, l'Agenzia dispone di uno

strumento di *business intelligence* denominato Vermont che, per quanto riguarda gli enti esterni, consente di controllare gli accessi effettuati dagli utenti con Siatel (e non quindi, in particolare, con Puntofisco e *web services*) dal 1° gennaio 2005 alle informazioni loro disponibili. Tale strumento permette poi monitoraggi statistici degli accessi e la predisposizione di sistemi di *alert*. Vermont utilizza *database* multidimensionali e consente di visualizzare i *log* relativi a un'interrogazione delle c.d. "informazioni generalizzate at" (principalmente, dati anagrafici e fiscali contenuti in anagrafe tributaria), mentre quelli relativi alle variazioni delle utenze o agli accessi a dati diversi, pur essendo registrati, non vengono rilevati da tale sistema. Analogo strumento è in dotazione anche a Sogei S.p.a.

Sulla base delle risultanze ispettive, è possibile rilevare tuttavia che l'Agenzia delle entrate non ha predisposto idonee procedure di *audit* anche periodiche sugli enti esterni.

Con particolare riferimento alle *web application* (Siatel e Puntofisco), non risultano monitorati l'attività degli amministratori locali, il numero di utenze abilitate da questi ultimi, i profili di autorizzazione e gli accessi; ciò, sebbene, per quanto riguarda Siatel, siano disponibili gli strumenti applicativi di gestione delle utenze (in uso alla Direzione centrale e alle direzioni regionali competenti) e il predetto sistema Vermont.

L'applicativo di *business intelligence* Vermont utilizzato dall'Agenzia non registra, in particolare, le interrogazioni effettuate dagli utenti attraverso Puntofisco e i *web service.*

Non risultano allo stato strumenti di controllo idonei a monitorare gli accessi effettuati attraverso l'applicativo *3270 enti esterni, web service e file transfer.*

Dagli atti emerge che gli amministratori locali degli enti esterni che accedono all'anagrafe tributaria non hanno effettuato i necessari controlli, anche periodici, sugli accessi e sulla sussistenza dei requisiti per le abilitazioni e le autorizzazioni degli utenti, anche per l'assenza di idonei strumenti a ciò finalizzati; tali soggetti, oltre alle anomalie relative alla gestione degli utenti riscontrate nei punti precedenti, non sono dotati di un sistema di *alert* o di un "cruscotto" che consenta loro di monitorare a livello statistico gli accessi all'anagrafe tributaria da parte degli utenti dell'ente. Peraltro, in taluni enti sono presenti più

amministratori la cui attività non è risultata essere coordinata.

Prescrizioni

L'Agenzia deve predisporre idonee e concrete procedure di *audit* anche periodiche sugli enti esterni e anche sull'attività svolta da Sogei S.p.a. in qualità di responsabile del trattamento. In particolare, per quanto riguarda gli enti esterni, oltre ad attività di *audit* basate sul monitoraggio delle transazioni e su sistemi di *alert*, tali procedure devono prevedere la verifica periodica, anche a campione, del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso.

Negli strumenti di *business intelligence* (applicativo Vermont o altri analoghi) utilizzati dall'Agenzia per monitorare gli accessi all'anagrafe tributaria dovranno confluire i *log* relativi a tutti gli attuali e futuri applicativi utilizzati per gli accessi da parte degli enti esterni.

Deve essere prefigurata da parte dell'Agenzia l'attivazione di specifici *alert* che individuino comportamenti anomali o a rischio, anche attraverso il monitoraggio e l'analisi periodica, a livello statistico, dei dati relativi alle transazioni eseguite dagli enti esterni.

Gli amministratori locali presso gli enti esterni devono essere dotati di strumenti di gestione delle utenze più efficaci e intuitivi che prevedano anche la possibilità di monitoraggi statistici degli accessi con l'attivazione di sistemi di *alert.*

Gli strumenti in dotazione agli amministratori locali devono essere idonei a supportare i controlli che gli enti sono tenuti ad effettuare ai sensi delle convenzioni che autorizzano l'accesso all'anagrafe tributaria. Tali controlli devono riguardare in particolare, anche a campione, la rispondenza delle interrogazioni a una precisa finalità amministrativa (cfr. l'inserimento del numero di pratica nell'applicativo), e essere effettuati con cadenze periodiche e documentati con le modalità stabilite con l'Agenzia.

***

Le prescrizioni sopra illustrate devono essere predisposte al più presto. Anche sulla base del confronto con l'Agenzia curato da ultimo dall'Ufficiorispetto all'impiego delle risorse necessarie per la loro idonea attuazione e tenuto conto del rispetto dei diritti degli interessati, si ritiene necessario che le misure e gli ac-

corgimenti sopra indicati, valutati singolarmente e nel loro complesso, siano accorpati in due distinti gruppi di adempimenti che dovranno essere posti in essere dall'Agenzia entro i termini, rispettivamente, di tre e di sei mesi. Limitatamente a taluni specifici e limitati profili, considerata la particolare complessità organizzativa richiesta, alcune delle misure e degli accorgimenti indicati devono essere invece completati entro il temine di dodici mesi. L'adempimento di tutte le prescrizioni del Garante dovrà essere, di volta in volta, puntualmente documentato a questa Autorità nei termini indicati decorrenti dalla data di ricezione del presente provvedimento.

TUTTO CIÒ PREMESSO IL GARANTE

ai sensi dell'art. 154, comma 1, lett. c) del Codice prescrive all'Agenzia delle entrate, con particolare riferimento alle attività dei soggetti esterni che accedono all'anagrafe tributaria, di adottare al più presto le misure e gli accorgimenti seguenti al fine di porre rimedio alle carenze indicate in motivazione, riferibili in particolare alle autenticazioni e alle autorizzazioni degli utenti, ai controlli da parte dell'Agenzia e alle estese possibilità di accesso alle banche dati, rendendo il trattamento conforme alle disposizioni vigenti e provvedendo comunque entro, e non oltre, i distinti termini di volta in volta indicati. L'adempimento delle prescrizioni dovrà essere, di volta in volta, documentato puntualmente a questa Autorità nei medesimi termini indicati decorrenti dalla data di ricezione del presente provvedimento.

a) Con riferimento ai profili generali relativi agli accessi all'anagrafe tributaria da parte di soggetti esterni all'amministrazione finanziaria:
   1) entro 6 mesi:
      • l'Agenzia deve redigere con formalità descrittive *standard* un documento, costantemente aggiornato, che riporti tutti i flussi di trasferimento di dati da e verso l'anagrafe tributaria e tutti gli accessi di tipo interattivo, *batch* o di altro genere, specificando per ciascun flusso o accesso l'identità dei soggetti legittimati a realizzarlo, la base normativa, la finalità istituzionale, la natura e la qualità dei dati trasferiti o a cui si è avuto accesso, la frequenza e il volume dei trasferimenti o degli accessi e il numero di soggetti che utilizzano la procedura. Tale documento deve essere mantenuto costantemente aggiornato, e reso disponibile nel caso

di controlli;

- con cadenza periodica annuale, l'Agenzia deve verificare l'attualità delle finalità per cui ha concesso l'accesso agli enti esterni, anche con riferimento al numero di utenze attive, inibendo gli accessi effettuati al di fuori dei presupposti riconducibili all'art. 19 del Codice e quelli non conformi a quanto stabilito nelle convenzioni. All'esito di tali verifiche, in particolare, devono essere eliminati gli accessi effettuati per conoscere informazioni che, ai sensi della normativa vigente, dovrebbero essere invece controllate presso altri soggetti;

2) entro 12 mesi:

- l'Agenzia deve introdurre nelle applicazioni volte all'uso interattivo da parte di incaricati un campo per l'indicazione obbligatoria del numero di riferimento della pratica nell'ambito della quale viene effettuata la consultazione;
- devono essere segmentati per quanto più possibile i dati visualizzabili attraverso gli applicativi (in modo cronologico, geografico e per tipologia di dati).

b) In relazione alla sicurezza dei sistemi di autenticazione degli applicativi utilizzati, l'Agenzia delle entrate deve:

1) entro 3 mesi:

- prevedere che tutte le applicazioni accessibili da rete pubblica in forma di *web application* siano implementate con protocolli *https/ssl* provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una *Certification Authority* ufficiale;
- permettere la visualizzazione, nella prima schermata successiva al collegamento, di informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui è stata effettuata la precedente connessione). Le stesse informazioni devono essere riportate anche relativamente alla sessione corrente;
- disciplinare la possibilità di effettuare accessi contemporanei con le medesime credenziali, limitandone l'utilizzo ai soli casi necessari per esi-

genze di servizio. In ogni caso, tale possibilità deve essere consentita esclusivamente laddove il certificato digitale o l'indirizzo Ip siano sufficienti a discriminare l'identità digitale delle postazioni accedenti. Nel caso in cui non sia possibile individuare la postazione di lavoro, la possibilità di accessi contemporanei deve essere inibita;

2) entro 6 mesi:
   - provvedere all'implementazione di un sistema di certificazione digitale e di censimento delle postazioni terminali, in modo da realizzare procedure di autenticazione che consentano di definire condizioni di accesso più complesse e sicure per determinate classi di incaricati o profili di autorizzazione.

c) Per quanto riguarda gli amministratori locali, le abilitazioni e le autorizzazioni degli utenti occorre che:
   1) entro 3 mesi:
      - nelle convenzioni che disciplinano l'accesso all'anagrafe tributaria sia previsto che gli enti esterni individuino gli "amministratori locali" sulla base di elevati requisiti di idoneità soggettiva, preferibilmente tra soggetti che abbiano un rapporto stabile con essi. Questi soggetti, prima di intraprendere la loro attività, devono essere formati dall'Agenzia delle entrate in ordine alle funzionalità dell'applicativo e all'attività di autorizzazione degli utenti. L'amministratore locale dell'ente esterno che accede all'anagrafe tributaria deve rimanere il punto di riferimento per le richieste di abilitazione e autorizzazione con la possibilità di gestire direttamente le utenze;
      - l'Agenzia stabilisca nelle convenzioni che gli enti esterni debbano istruire adeguatamente il personale addetto all'utilizzo dei vari applicativi in ordine al corretto utilizzo delle funzionalità dei *software*. Le convenzioni, entro i medesimi termini, devono imporre agli enti, anche attraverso gli strumenti di *audit* in uso all'amministratore locale, controlli periodici i cui esiti devono essere documentati secondo le modalità definite nella stessa convenzione;
      - le convenzioni stipulate dall'Agenzia predefiniscano una procedura per le autenticazioni e le autorizzazioni che coinvolga attivamente le figure

apicali degli uffici interessati e un supervisore unico (soggetto giuridicamente preposto all'individuazione degli utenti e dei profili). Il supervisore può anche non coincidere con l'amministratore tecnicamente deputato alla materiale gestione delle abilitazioni (e del relativo profilo), ma deve rispondere del controllo sullo stesso. Occorre inoltre che venga assicurato un flusso di comunicazione tra l'amministratore locale e l'articolazione che si occupa della gestione delle risorse umane al fine di procedere alla tempestiva revisione del profilo di abilitazione o alla disabilitazione dei soggetti preposti ad altre mansioni o che abbiano cessato il rapporto con l'ente, anche con apposite verifiche a cadenza almeno trimestrale;

- in presenza di più amministratori locali per ciascun ente, l'Agenzia valuti e coordini i profili di autorizzazione da attribuire, garantendo in capo a un'unica figura la possibilità di intervenire su tutti gli utenti anche amministratori, monitorandone l'operato;
- l'Agenzia predefinisca, soglie relative al numero di utenti abilitabili da ciascun ente. Le richieste di superamento di tali soglie devono essere valutate caso per caso dall'Agenzia;
- siano previste limitazioni orarie per gli accessi, mantenendo comunque la possibilità di specifiche deroghe adeguatamente motivate;

2) entro 6 mesi:

- le *web application* predisposte dall'Agenzia per l'utilizzo da parte di enti esterni siano integrate, con procedure di "autenticazione forte" per ridurre la possibilità di usi impropri delle credenziali. Tali procedure devono essere prefigurate nei confronti di quelle classi di utenti cui corrispondano profili di autorizzazione che risultano più critici e, comunque, almeno per tutti i profili di autorizzazione corrispondenti alle funzioni di amministrazione locale;
- le convenzioni stipulate con ciascun ente prevedano espressamente i vincoli necessari ad assicurare un corretto trattamento dei dati e stabiliscano anche le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione.

d) Con riguardo ai singoli sistemi l'Agenzia deve:
1) entro 3 mesi:
- rispetto all'applicativo Siatel, introdurre misure di controllo per la funzionalità di "fornitura dati" visualizzabile nell'apposita schermata dell'applicativo e, con riferimento alle funzionalità utilizzabili da parte degli operatori comunali a soli fini anagrafici, inserire nell'applicativo medesimo specifiche indicazioni all'amministratore locale affinché vengano autorizzati solo utenti che agiscono presso l'ufficio anagrafe del comune;
- per quanto riguarda l'applicativo Puntofisco, aggiornare il profilo di autorizzazione assegnato agli enti esterni abilitati, escludendo a priori la consultabilità di dati sensibili laddove non sussista un'idonea base normativa. All'interno della procedura informatica di gestione degli utenti in uso all'amministratore locale devono essere inserite indicazioni che consentano all'Agenzia di visualizzare lo *status* di tutte le utenze con i profili abilitativi correnti, comprese quelle già cancellate. Entro il medesimo termine, deve essere corretta l'anomalia, relativa al sistema di gestione, che non permette regolarmente all'amministratore locale, visualizzando il profilo del singolo utente, di conoscerne l'effettiva possibilità di accesso dello stesso al sistema;
- per quanto riguarda gli applicativi Entratel e Fisconline/Cassetto fiscale, configurare i sistemi in modo da poter verificare il rispetto delle prescrizioni indicate nell'Allegato B al Codice relative, con particolare riferimento al sistema di scadenza delle *password* e all'attribuzione di credenziali idonee a identificare direttamente, oltre all'ente abilitato, anche il singolo incaricato che fisicamente effettua l'accesso, autentica e trasmette i file;

2) entro 6 mesi:
- realizzare la migrazione degli enti a oggi abilitati ad accedere all'anagrafe tributaria mediante 3270 enti esterni verso applicativi che offrono maggiori garanzie;
- con riferimento ai *web service*, effettuare una ricognizione dei servizi attualmente esposti e sospenderne l'attività in attesa della revisione delle attuali modalità di implementazione con le misure e gli

accorgimenti di seguito descritti. Laddove l'Agenzia intenda impiegare *web service* esposti anche in rete pubblica per l'utilizzo da parte di enti esterni, questi devono essere configurati offrendo un livello minimo di accesso ai dati e limitando i risultati delle interrogazioni a valori di tipo *booleano*. Le convenzioni per l'utilizzo di tali servizi, inoltre, devono prevedere stringenti condizioni d'uso tali da consentire anche un'effettiva capacità di controllo da parte dell'Agenzia. Dal punto di vista tecnico, tali condizioni d'uso dei *web service* devono essere trasposte in appositi "accordi di servizio", redatti secondo il modello della cooperazione applicativa impiegata all'interno del sistema pubblico di connettività istituito dal Codice dell'amministrazione digitale. Gli "accordi di servizio" devono individuare idonee garanzie per il trattamento dei dati personali, prevedendo, in particolare, il tracciamento delle operazioni compiute in cooperazione applicativa, con possibilità di identificazione dell'utente che accede ai dati, il *timestamp*, l'indirizzo Ip di provenienza dell'utente e del server interconnesso, l'operazione effettuata e i dati trattati;

3) entro 12 mesi:
   - realizzare i collegamenti per la gestione di flussi di dati mediante *file transfer* su canali di connessione sicuri e garantire, anche attraverso la configurazione dei sistemi, che le credenziali di abilitazione utilizzate dagli operatori dell'ente esterno rispettino le prescrizioni indicate nell'Allegato B al Codice, in particolare identificando il soggetto che effettua lo scambio dei dati e prevedendo che la parola chiave prevista sia soggetta a scadenza periodica secondo i termini ivi indicati.

e) In relazione alle procedure di *audit* sull'accesso alle informazioni contenute nell'anagrafe tributaria da parte di soggetti esterni:

1) entro 3 mesi:
   - l'Agenzia deve predisporre idonee e concrete procedure di *audit* anche periodiche sugli enti esterni e anche sull'attività svolta da Sogei S.p.a. In particolare, per quanto riguarda gli enti esterni, oltre ad attività di audit basate sul monitoraggio delle transazioni e su sistemi di *alert*, tali procedure devono prevedere la verifica periodica, anche a campione,

del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso;

2) entro 6 mesi:
   - negli strumenti di *business intelligence* utilizzati dall'Agenzia per monitorare gli accessi all'anagrafe tributaria devono confluire i *log* relativi a tutti gli attuali e futuri applicativi utilizzati per gli accessi da parte degli enti esterni;
   - deve essere prefigurata da parte dell'Agenzia l'attivazione di specifici *alert* che individuino comportamenti anomali o a rischio, anche attraverso il monitoraggio e l'analisi periodica, a livello statistico, dei dati relativi alle transazioni eseguite dagli enti esterni;
   - gli amministratori locali presso gli enti esterni devono essere dotati di strumenti di gestione delle utenze più efficaci e intuitivi che prevedano anche la possibilità di monitoraggi statistici degli accessi con l'attivazione di sistemi di *alert*. Gli strumenti in dotazione agli amministratori locali devono essere idonei a supportare i controlli che gli enti sono tenuti ad effettuare ai sensi delle convenzioni che autorizzano l'accesso all'anagrafe tributaria. Tali controlli devono riguardare, in particolare, anche a campione la rispondenza delle interrogazioni ad una precisa finalità amministrativa e essere effettuati con cadenze periodiche e documentati con le modalità stabilite con l'Agenzia.

Roma, 18 settembre 2008

IL PRESIDENTE
Pizzetti
IL RELATORE
Pizzetti
IL SEGRETARIO GENERALE
Buttarelli

Roma, 01 Settembre 2009
Raccomandata AR
Spett.le
Autorità Garante per la
protezione dei dati personali
Piazza di Montecitorio, 121
00181 – Roma

Oggetto: segnalazione ex art. 141, comma 1, lett. b), D.lgs 196/2003 – Agenzia delle Entrate, servizi telematici.

PREMESSO CHE

- sulla base di un'analisi preliminare del sistema informativo della fiscalità, il 14 dicembre 2007, era stato deliberato l'avvio di accertamenti volti a verificare, in più fasi, i trattamenti di dati personali effettuati presso l'anagrafe tributaria, rilevando che elementi di maggior criticità e urgenza erano da ravvisarsi nelle misure di sicurezza adottate per gli accessi da parte di enti esterni, pubblici e privati, all'amministrazione finanziaria;
- Successivi accertamenti ispettivi avevano avuto luogo presso l'Agenzia delle entrate, Sogei S.p.A. (Società generale d'informatica, responsabile del trattamento dei dati contenuti nell'anagrafe tributaria), regioni, province, comuni e altri enti, consentendo di riscontrare criticità relative agli accessi da parte degli enti esterni all'amministrazione finanziaria riferibili in particolare alle autenticazioni e alle autorizzazioni degli utenti, ai controlli da parte dell'Agenzia e alle estese possibilità di accesso alle banche dati.
- Tra le altre cose, era stato evidenziato come per le *web application* fosse stato utilizzato un certificato *Ssl* di tipo *self signed* (non firmato da una *Ca, Certification authority*, ufficiale) non attendibile che, in mancanza di una *Ca* affidabile, non era in grado di offrire le garanzie di certezza dell'identità dell'erogatore del servizio tipiche della certificazione digitale tramite *Pki (public key infrastructure*): risultavano, pertanto, facilitate azioni di *phishing* in danno di utenti del sistema e la possibile acquisizione indebita di credenziali di autenticazione, idonea a consentire utilizzi impropri dell'applicazione.

- Conseguentemente, il 18 settembre 2008 codesta spettabile Autorità, ai sensi dell'art. 154, comma 1, lett. c) del Codice, aveva ritenuto necessario prescrivere una serie di misure e accorgimenti che avrebbero dovuto essere adottati dall'Agenzia delle Entrate, anche in riferimento ai soggetti esterni in grado di accedere all'anagrafe tributaria;
- In particolare, veniva richiesto all'Agenzia delle Entrate, nei successivi tre mesi (ovverosia entro il 18 dicembre 2008), di fare in modo che tutte le applicazioni accessibili da rete pubblica in forma di *web application* fossero implementate con protocolli *https/ssl* provvedendo ad asseverare l'identità digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali emessi da una *Certification Authority* ufficiale, evitando il ricorso a certificati di tipo *self-signed*;
- Il 10 giugno 2009 veniva pubblicato sul sito dell'Agenzia dell'Entrate (cfr. All. 1) un documento recante *"Adeguamento dei servizi telematici dell'Agenzia delle entrate alle prescrizioni del Garante per la protezione dei dati personali (Provvedimento del Direttore)"* nel quale si dava atto di quanto era stato fatto per ottemperare alle indicazioni fornite dall'Autorità;
- Nel documento di cui sopra non veniva fatto cenno alcuno all'adozione di un certificato digitale emesso da una *Certification Authority* ufficiale in luogo di quello self-signed fino a quel momento utilizzato, così come prescritto dall'Autorità.

Tutto ciò premesso,

SI SEGNALA CHE

Ad oggi, 31 agosto 2009, l'accesso ai servizi telematici offerti dall'Agenzia delle Entrate avviene sulla base di una connessione protetta senza, tuttavia, che l'identità digitale dei server erogatori dei servizi sia assicurata tramite l'utilizzo di certificati digitali emessi da una *Certification Authority* ufficiale. Al contrario, ***si continua ad utilizzare un certificato self-signed rilasciato dalla stessa Agenzia delle Entrate, in qualità di ente certificatore di se stesso***[1]. A parere della scrivente Associazione risulta palese l'inadempimento delle prescrizioni imposte dall'Autorità nel suo provvedimento del 18 settembre 2008. Si segnala, inoltre, che **analoga situazione è avvisabile con riferimento al ser-**

[1]Cfr. http://telematici.agenziaentrate.gov.it/doc/ca.der

vizio "*estratto conto*" di Equitalia S.p.A.[2], che consente di consultare online la propria posizione debitoria nei confronti dell'erario. Anche in questo caso per accedere al servizio viene richiesto di installare un certificato non rilasciato da una CA ufficiale, ma, ancora una volta, dall'Agenzia delle Entrate. Stante la delicatezza dei dati trattati e del rischio di *phishing* in danno degli utenti del sistema, fatto peraltro apparso nella cronaca di questi giorni traendo proprio dal marchio della Agenzia la fiducia necessaria per ingannare gli utenti, si confida in un pronto intervento di codesta spettabile Autorità.

Distinti Saluti
Associazione Cittadini di Internet

[2]http://www.equitaliaspa.it/equitalia/opencms/focuson/34653455465.html

PROT. N. 79952/2009

Adeguamento dei servizi telematici dell'Agenzia delle entrate alle prescrizioni del Garante per la protezione dei dati personali di cui al Provvedimento 18 settembre 2008

IL DIRETTORE DELL'AGENZIA

In base alle attribuzioni conferitegli dalle norme riportate nel seguito del presente provvedimento

Dispone:

1.Definizioni.

1.1 Ai fini del presente provvedimento si intende:

a) per "servizio Entratel", il servizio telematico di cui al Capo II del decreto 31 luglio 1998, utilizzabile dai soggetti di cui ai all'art. 3, commi 2, 2-bis e 3 del decreto del Presidente della Repubblica 22 luglio 1998, n. 322;

b) per "servizio Fisconline", il servizio telematico Internet di cui al Capo IV del decreto 31 luglio 1998, utilizzabile dai soggetti individuati dall'art. 3, ultimo periodo del comma 2, del decreto del Presidente della Repubblica 22 luglio 1998, n. 322, e dai soggetti di cui al comma 2-ter del medesimo articolo;

c) per "sito dei servizi telematici" dell'Agenzia delle entrate, il sito Internet dei servizi Entratel e Fisconline, raggiungibile all'indirizzo http://telematici.agenziaentrate.gov.it;

d) per "gestori incaricati", le persone fisiche, autonomamente abilitate ai servizi telematici dell'Agenzia delle entrate, designate dagli utenti diversi dalle persone fisiche abilitati a Entratel o a Fisconline, o dagli utenti per-

sone fisiche abilitati al servizio Entratel che ne ravvisino l'esigenza, per interagire con i servizi telematici in nome e per conto dei suddetti utenti, nonché per creare ed aggiornare l'elenco degli operatori incaricati all'utilizzo dei servizi telematici in nome e per conto degli utenti medesimi;

e) per "operatori incaricati", le persone fisiche, autonomamente abilitate ai servizi telematici, che sono designate, dagli utenti diversi dalle persone fisiche abilitati a Entratel o a Fisconline, o dagli utenti persone fisiche abilitati al servizio Entratel che ne ravvisino l'esigenza, ad operare in nome e per conto dei suddetti utenti sui predetti servizi.

2. Abilitazione al servizio Entratel

2.1. I soggetti che hanno i requisiti per essere abilitati al servizio Entratel, ai sensi e per gli effetti del decreto del Presidente della Repubblica 22 luglio 1998, n. 322, e successive modificazioni, richiedono l'abilitazione in base a quanto stabilito nei seguenti punti.

2.2. L'utente richiede via web, sul sito dei servizi telematici, il codice di pre-iscrizione; quest'ultimo viene attribuito dal sistema in tempo reale, previo inserimento, da parte dell'utente medesimo, delle informazioni ivi richieste.

2.3. L'utente presenta, entro trenta giorni dalla ricezione del codice di pre-iscrizione, la domanda di abilitazione e la documentazione allegata a un qualsiasi ufficio dell'Agenzia delle entrate della regione in cui ricade il proprio domicilio fiscale.

2.4. Ai fini della puntuale individuazione degli autori delle transazioni telematiche, i soggetti diversi da persona fisica sono tenuti a presentare all'Agenzia delle entrate, unitamente alla domanda di cui al punto 2.3 e in relazione a ciascuna eventuale sede secondaria da attivare, una lista contenente i dati relativi ai gestori incaricati, tenuti a loro volta ad amministrare, mediante il sito dei servizi telematici, gli operatori incaricati che sono autorizzati dai predetti soggetti diversi da persone fisiche ad utilizzare il servizio Entratel in nome e per conto di questi ultimi.

2.5 L'utente diverso da persona fisica, già in possesso dell'abilitazione al servizio Entratel al momento dell'entrata in vigore del presente provvedimento, comunica all'Agenzia delle entrate, per ciascuna sede telematica attiva, l'elenco dei gestori incaricati secondo una delle seguenti modalità: a)

attraverso una funzione disponibile sul sito dei servizi telematici, dedicata ai rappresentanti legali o negoziali, persone fisiche, registrati in anagrafe tributaria; b) presentando un apposito modulo, disponibile presso gli uffici dell'Agenzia o sul sito dei servizi telematici, all'ufficio che ha precedentemente rilasciato l'abilitazione.

2.6. I rappresentanti legali o negoziali, qualora sprovvisti, richiedono, ai fini della comunicazione dei nominativi dei gestori incaricati, l'abilitazione al servizio Entratel o Fisconline in base alle caratteristiche che li qualificano ai sensi dell'art 3 del decreto del Presidente della Repubblica 22 luglio 1998, n. 322 .

2.7. Le persone fisiche abilitate al servizio Entratel hanno la facoltà di effettuare la comunicazione dei gestori incaricati con le medesime modalità illustrate nei punti precedenti.

2.8. La domanda per richiedere l'abilitazione e la relativa documentazione sono presentate in tempo utile per ottemperare agli obblighi previsti dalla normativa vigente; le modalità e i tempi di rilascio delle abilitazioni al servizio Entratel, nonché di perfezionamento, da parte dell'utente, delle operazioni necessarie a rendere operativa l'utenza ottenuta sulla base delle avvertenze consegnate dall'ufficio, non legittimano in alcun caso il differimento dei termini previsti per l'assolvimento degli adempimenti in materia fiscale.

2.9. L'ufficio, dopo aver verificato l'identità del richiedente e la corretta compilazione della domanda di abilitazione e della documentazione allegata, rilascia al richiedente medesimo l'attestazione di abilitazione al servizio Entratel, recante un codice da utilizzare per prelevare le proprie credenziali dal sito dei servizi telematici.

2.10. L'utente controfirma l'attestazione, contenente l'impegno ad assicurare il corretto utilizzo del servizio Entratel e a mantenere riservate le informazioni desunte dalla documentazione rilasciata, dichiarando di accettare le condizioni di funzionamento del servizio che gli vengono contestualmente comunicate dall'ufficio, il quale trattiene copia dell'attestazione controfirmata.

2.11. È cura dell'utente conservare il codice di pre-iscrizione ottenuto con le modalità di cui al precedente punto 2.2 e la documentazione ricevuta dal-

l'ufficio.

2.12. All'ufficio presso il quale è stata presentata la domanda di abilitazione al servizio Entratel devono essere inoltrate le istanze volte a richiedere le variazioni dell'utenza ottenuta, ivi comprese quelle relative ai gestori incaricati qualora l'utente o gli stessi gestori incaricati si trovino impossibilitati ad operare direttamente dal sito dei servizi telematici.

2.13. I soggetti abilitati al servizio Entratel non possono essere, in nessun caso, contemporaneamente titolari dell'abilitazione al servizio Fisconline. Gli utenti abilitati al servizio Entratel che siano, alla data di pubblicazione del presente provvedimento, abilitati anche al servizio Fisconline sono tenuti a chiedere la revoca di quest'ultima abilitazione rivolgendosi ad un ufficio dell'Agenzia delle entrate. In ogni caso, a partire dal trentesimo giorno successivo alla pubblicazione del presente provvedimento, verranno automaticamente disabilitati da Fisconline i soggetti che risultino titolari anche di abilitazione al servizio Entratel.

3. Gestori incaricati ed operatori incaricati

3.1 Gli utenti diversi dalle persone fisiche abilitati ai servizi Entratel o Fisconline comunicano, mediante un'apposita funzione del sito dei servizi telematici riservata ai rappresentanti legali o negoziali registrati in anagrafe tributaria, oppure al competente Ufficio dell'Agenzia delle entrate, con apposito modello, i dati identificativi dei gestori incaricati da un minimo di uno ad un massimo di quattro. Tale comunicazione deve essere effettuata, da parte degli utenti Entratel, per ciascuna sede telematica. Le persone fisiche abilitate al servizio Entratel, che esercitino la facoltà di individuare i gestori incaricati, procedono come sopra stabilito per gli utenti diversi dalle persone fisiche.

3.2. I gestori incaricati amministrano, mediante apposite funzionalità disponibili sul sito dei servizi telematici, l'elenco dei gestori e degli operatori incaricati all'utilizzo dei predetti servizi dell'Agenzia delle entrate in nome e per conto degli utenti deleganti, provvedendo ad eventuali inserimenti e cancellazioni.

3.3 I gestori incaricati e gli operatori incaricati devono essere in possesso dell'abilitazione ai servizi Entratel o Fisconline, a seconda dei requisiti pos-

seduti per la trasmissione telematica delle dichiarazioni fiscali.

3.4. I gestori incaricati e gli operatori incaricati possono utilizzare i servizi telematici in nome e per conto di più utenti; dopo aver effettuato l'accesso al sistema con le proprie credenziali, potranno indicare l'utente per conto del quale intendono effettuare le transazioni telematiche.

3.5. I gestori incaricati e gli operatori incaricati, dopo aver indicato l'utente per conto del quale intendono effettuare le transazioni telematiche, interagiscono con i servizi telematici con i medesimi privilegi dell'utente che li ha incaricati.

3.6. A seguito della comunicazione di cui ai punti 2.4, 2.5 e 3.1, i gestori incaricati acquisiscono immediatamente la possibilità di operare telematicamente in nome e per conto del soggetto che li ha incaricati.

3.7 A seguito dell'inserimento nell'elenco di cui al punto 3.2 gli operatori incaricati acquisiscono immediatamente la possibilità di operare telematicamente in nome e per conto del soggetto che li ha incaricati.

3.8 A decorrere dal 1° settembre 2009, agli utenti diversi dalle persone fisiche è inibito l'utilizzo delle attuali credenziali generiche di accesso ai servizi telematici attribuite precedentemente all'entrata in vigore del presente provvedimento. A decorrere dal 1° novembre 2009 sono revocate le abilitazioni ai servizi telematici degli utenti diversi dalle persone fisiche che non hanno perfezionato gli adempimenti previsti dal presente provvedimento.

4. Abilitazione e utilizzo del servizio Fisconline

4.1 Agli utenti diversi dalle persone fisiche abilitati al servizio Fisconline si applicano le norme relative ai gestori incaricati e agli operatori incaricati di cui ai punti 2 e 3 del presente provvedimento.

4.2 Il codice Pin assegnato a ciascun utente del servizio Fisconline scade il 31 dicembre del secondo anno successivo a quello di ultima utilizzazione ovvero, nel caso in cui rimanga del tutto inutilizzato dopo l'assegnazione, scade il 31 dicembre del secondo anno successivo a quello del rilascio. La disposizione di cui al periodo precedente si applica anche ai codici Pin attivi alla data della pubblicazione del presente provvedimento. Il codice Pin perde la sua validità in caso di decesso del titolare.

4.3 In caso di perdita del codice Pin e nel caso in cui l'utente ritenga che lo

stesso venga indebitamente utilizzato da altri, é presentata apposita comunicazione ad un ufficio dell'Agenzia delle entrate, il quale provvede alla revoca dell'abilitazione già in possesso dell'utente e, se richiesta, all'attribuzione di una nuova abilitazione a Fisconline.

4.4 Ai soggetti abilitati al servizio Fisconline che siano, alla data di pubblicazione del presente provvedimento, contemporaneamente titolari dell'abilitazione al servizio Entratel si applicano le disposizioni di cui al punto 2.13.

5. Obbligo di riservatezza

5.1. Gli utenti dei servizi Entratel e Fisconline possono trattare i dati contenuti nei documenti per le sole finalità del servizio di trasmissione telematica e per il tempo a ciò necessario, secondo quanto previsto dall'art. 12-bis del decreto del Presidente della Repubblica, n. 600 del 1973, con le modalità definite dal decreto 31 luglio 1998, dal presente provvedimento e dalle convenzioni con Poste italiane S.p.a.

5.2. Gli utenti dei servizi telematici si configurano quali autonomi titolari del trattamento dei dati personali ai sensi dell'art 4, comma 1, lett. f) del decreto legislativo 30 giugno 2003, n. 196.

5.3. Il trattamento dei dati personali contenuti nei documenti da trasmettere per via telematica è consentito solo ai soggetti, anche esterni, designati come responsabili dagli utenti dei servizi telematici, nel rispetto di quanto previsto dagli articoli 4 e 29 del decreto legislativo 30 giugno 2003, n. 196.

5.4. Le persone fisiche incaricate del trattamento sono individuate dagli utenti dei servizi telematici, o dal soggetto da questi designato quale responsabile, ed operano sulla base dell'autorizzazione ricevuta, attenendosi alle istruzioni impartite e garantendo la riservatezza e sicurezza delle informazioni trattate.

5.5. Gli utenti dei servizi telematici, ad eccezione delle persone fisiche non intermediari che effettuano telematicamente i propri adempimenti fiscali, e i soggetti designati come responsabili adottano le misure organizzative, fisiche e logistiche di cui al decreto legislativo 30 giugno 2003, n. 196, al fine di assicurare la riservatezza e la sicurezza dei dati, anche attraverso l'individuazione di appositi spazi per la conservazione dei medesimi.

5.6. Gli utenti dei servizi telematici si impegnano a ottemperare le attività de-

scritte nell'allegato tecnico al decreto 31 luglio 1998 e a mantenere riservate le informazioni che consentono l'accesso ai predetti servizi.

5.7. Al momento del rilascio dell'attestazione di cui al punto 2, ciascun utente abilitato al servizio Entratel si impegna, con la sottoscrizione, al rispetto delle disposizioni contenute nel presente provvedimento, anche per conto dei soggetti designati come responsabili.

5.8 L'Agenzia delle entrate verifica periodicamente, anche con controlli a campione, il rispetto delle disposizioni contenute nel presente provvedimento.

6. Tutela dei dati personali degli utenti.

6.1. L'informativa ai sensi dell'art. 13 del Decreto Legislativo 30 giugno 2003, n. 196, si intende resa mediante le avvertenze fornite agli utenti sia al momento della presentazione della domanda di abilitazione, cartacea o telematica, sia al momento del rilascio dell'abilitazione ai servizi telematici.

MOTIVAZIONI

Al fine di ottemperare alle prescrizioni adottate dal Garante per la protezione dei dati personali con Provvedimento del 18 settembre 2008, le modalità di abilitazione e di accesso ai servizi telematici sono state riviste al fine di assicurare i migliori standard in materia. In primo luogo, l'Agenzia delle entrate ha rafforzato la password policy relativa alle utenze dei servizi telematici, stabilendo la scadenza periodica delle password ogni novanta giorni. Si è reso inoltre necessario apportare modifiche al sistema in uso per le credenziali d'accesso attribuite agli utenti dei servizi telematici diversi da persona fisica. Pertanto, a partire dall'1 settembre 2009, tutte le credenziali di accesso ai servizi telematici attribuite a soggetti diversi dalla persone fisiche saranno inutilizzabili; i soggetti diversi da persona fisica abilitati ai canali Entratel e Fisconline sono tenuti a comunicare, entro il 31 agosto 2009, all'Agenzia delle entrate i dati identificativi dei cosiddetti "gestori incaricati" e degli "operatori incaricati", cioè di persone fisiche che effettuano transazioni telematiche con credenziali proprie, autorizzati dalle società, enti o organizzazioni cui appartengono ad operare in nome e per conto di questi ultimi I "gestori incaricati" e gli "operatori incaricati" sono, quindi, tenuti a possedere autonoma abilitazione ai servizi telematici. Con il presente provvedimento sono disciplinate le modalità di individuazione e comu-

nicazione dei dati dei “gestori incaricati” e degli “operatori incaricati”. A decorrere dall’1 novembre 2009 sono revocate d’ufficio le abilitazioni ai servizi telematici degli utenti diversi dalle persone fisiche che non hanno perfezionato gli adempimenti previsti dal presente provvedimento. Inoltre, il piano di riforma dei servizi telematici ha comportato l’introduzione di modifiche alla procedura di rilascio delle abilitazioni al servizio telematico Entratel, con il superamento dell’attribuzione delle credenziali mediante buste cartacee, sostituite dalla comunicazione sicura online delle predette credenziali.

Riferimenti normativi

a) Attribuzioni del Direttore dell’Agenzia delle Entrate

- Decreto legislativo 30 luglio 1999, n. 300, recante la riforma dell’organizzazione del Governo, a norma dell’art. 11 della legge 15 marzo 1997, n. 59 comma 1; art. 71, comma 3, lettera a); art. 73, comma 4.
- Statuto dell’Agenzia delle Entrate (art. 5, comma 1; art. 6, comma 1).
- Regolamento di amministrazione dell’Agenzia delle Entrate (art. 2, comma 1).
- Decreto del Ministro delle Finanze 28 dicembre 2000, concernente disposizioni recanti le modalità di avvio delle Agenzie fiscali e l’istituzione del ruolo speciale provvisorio del personale dell’Amministrazione finanziaria a norma degli artt. 73 e 74 del Decreto legislativo 30 luglio 1999, n. 300.

b) Disciplina normativa di riferimento

- Decreto del Presidente della Repubblica del 29 settembre 1973, n. 600, recante disposizioni comuni in materia di accertamento delle imposte sui redditi, e successive modificazioni e integrazioni.
- Decreto legislativo 9 luglio 1997, n. 241, concernente norme di semplificazione degli adempimenti dei contribuenti in sede di dichiarazione dei redditi e dell’imposta sul valore aggiunto, nonché di modernizzazione del sistema di gestione delle dichiarazioni, e successive modificazioni e integrazioni.
- Decreto del Presidente della Repubblica 22 luglio 1998, n. 322, e successive modificazioni: regolamento recante modalità per la presentazione delle dichiarazioni relative alle imposte sui redditi, all’imposta regionale sulle

attività produttive e all'imposta sul valore aggiunto.
- Decreto dirigenziale 31 luglio 1998, e successive modificazioni, recante modalità tecniche di trasmissione telematica delle dichiarazioni e dei contratti di locazione e di affitto da sottoporre a registrazione, nonché di esecuzione telematica dei pagamenti.
- Decreto legislativo 30 giugno 2003, n. 196. Codice in materia di protezione dei dati personali.

La pubblicazione del presente provvedimento sul sito Internet dell'Agenzia delle entrate tiene luogo della pubblicazione nella Gazzetta Ufficiale, ai sensi dell'articolo 1, comma 361, della legge 24 dicembre 2007, n. 244.

Roma, 10 giugno 2009

IL DIRETTORE DELL'AGENZIA
Attilio Befera *

* Firma autografa sostituita da indicazione a mezzo stampa, ai sensi dell'art. 3, comma 2, D.Lgs. N° 39/93

I consigli pratici dell'Agenzia per evitare le trappole della rete

In giro per il web false email riguardanti l'erogazione di rimborsi fiscali e l'attività di accertamento

La truffa viaggia via email. E' questo adesso lo strumento privilegiato dei casi di frode che sfruttano impropriamente il nome e il logo dell'agenzia delle Entrate per raggirare ignari contribuenti. L'ultimo tentativo riguarda messaggi di posta elettronica sull'accertamento provenienti dall'indirizzo inesistenteufficio.accertamenti@agenziaentrate.it e che invitano il destinatario a collegarsi al seguente sito web: http: / /bancadati2009.altervista.org. Inoltre, nelle scorse settimane numerosi utenti hanno ricevuto email che richiedevano coordinate bancarie per ricevere l'accredito di fantomatici rimborsi fiscali. L'Agenzia, attraverso un'attività di informazione ramificata sul territorio nazionale, mette in guardia i contribuenti ricordando che l'Amministrazione non chiede via email dati bancari o sensibili né notifica con questo strumento avvisi di accertamento, garantendo sempre la massima sicurezza delle operazioni effettuate. I dati necessari per ottenere l'accredito di rimborsi fiscali vanno indicati o presentando apposito modello all'ufficio delle Entrate o collegandosi al sito istituzionale **www.agenziaentrate.gov.it.** L'elenco degli uffici locali delle Entrate, invece, è disponibile, per ogni regione, sul relativo sito web.

Per difendersi dalla truffa, si invitano gli utenti a cestinare il messaggio, a non collegarsi ai siti indicati e a segnalare il caso alla Polizia Postale.

Continua così l'impegno dell'Agenzia nel difendere la propria identità istituzionale e i contribuenti dai tentativi di frode. Utilizzare il marchio "Agenzia" per compiere inganni di vario genere, infatti, non è una novità. Già in passato si sono verificati numerosi esempi di raggiri come, ad esempio, proposte di abbonamenti a pubblicazioni fiscali da parte di falsi funzionari e invio di pacchi e materiale informativo con il logo delle Entrate contenenti, invece, proposte commerciali totalmente estranee all'attività dell'Amministrazione Finanziaria.

Alessandra Gambadoro
pubblicato il 28/08/2009

SICUREZZA DELLA CERTIFICAZIONE DIGITALE: *vuole essere una guida per tutti coloro che si occupano della sicurezza e certificazione digitale dei siti web evogliono approfondire ed impiegare in modo esaustivo le risorse di questo sistema di protezione. È una pubblicazione di tipo divulgativo, ma ricca di approfondimenti tecnici e pratici.*

Massimo F. Penco Da sempre impegnato direttamente o indirettamente nella sicurezza informatica, delle reti, comunicazioni e sistemi. Ha viaggiatoin tutto il Mondo ricoprendo cariche direttive, anche come consulente, per importanti istituzioni finanziarie, industrie e governi di vari paesi, StatiUniti, Regno Unito. Forse uno dei maggiori esperti nel mondo in questo campo. Consulente e ricercatore di computer crime, sicurezza dei sistemi di comunicazione e reti informatiche, giornalista internazionale e scrittore di questa materia; animatore di congressi a livello mondiale, autore di numerosi articoli sul tema. Già consulente dei Lloyd's di Londra, dell'associazione bancaria italiana, membro del comitato di automazione bancariaABI, consulente dell'FBI, membro dell'Institute of Electronic Engineers USA, del Computer Security Institute della National Computer Security Association, dell'American Chamber of Commerce in Italy, ed altre associazioni internazionali, Presidente e fondatore di Cittadini di Internet.PHD Dr. In ingegneria elettronica all'università di Stanford, master in security technology and risk management presso lo Stanford Research Institute.Una lunga carriera professionale , associativa e didattica con ultimi incarichi in aziende leader del settore, già direttore per l'Europa di Verisign, oggi Vice Presidente Emea del Gruppo Comodo, Docente e titolare di master in università, in Italia ed all'estero.

Sicurezza della Certificazione digitale

Per la versione e-book questa è la revisione : 1.10.00