



COMUNICATO STAMPA SIT del 13 dicembre 2010

SIT: NESSUN RISCHIO DI BLOCCO DELLA CERTIFICAZIONE ON-LINE DI MALATTIA A CAUSA DELL'USO DEI CODICI FISCALI DEI MEDICI COME USER ID.

Roma, 13 dicembre 2010 – Una recente puntata della rubrica “Percorsi in sanità”, trasmessa da Gold TV e ripresa dal sito FIMMG Roma, ha denunciato la presunta vulnerabilità dell'80% degli account dei medici abilitati alla certificazione on-line di malattia ad un attacco di tipo “diniego di servizio”. Tale rischio viene fatto discendere dalla scelta di utilizzare, come identificativo utente del medico, il suo codice fiscale, il quale è un dato facilmente reperibile on-line, da qualsiasi cittadino, consultando gli albi professionali degli Ordini provinciali dei medici chirurghi e degli odontoiatri.

I medici paventano che qualche malintenzionato, acquisiti i codici fiscali dei medici certificatori, possa collegarsi al sistema con tali credenziali inserendo deliberatamente per tre volte una password fasulla: in questo modo attiverebbe il blocco del sistema, previsto per motivi di sicurezza, costringendo il sanitario a recarsi nuovamente alla ASL per ritirare una nuova busta con le sue credenziali di accesso al sistema. Ciò creerebbe, in definitiva, non solo un grave disagio al medico, ma un inaccettabile disservizio al cittadino nel rilascio della certificazione on-line di malattia.

La SIT, **Società Italiana Telemedicina e sanità elettronica**, ritiene doveroso precisare a tale proposito che **il problema non sussiste** in quanto la procedura di accesso al servizio, rispettando espressamente le normative di legge previste in materia di accesso ai siti web della PA, garantisce al medico la possibilità di ripristinare immediatamente e personalmente, con una semplice operazione on-line, la propria password eventualmente bloccata, senza così creare disservizi ai cittadini o costringere il medico stesso a recarsi alla ASL per farsi rilasciare una nuova password. Un eventuale “disturbatore” può dunque dare noia per i pochi secondi necessari al ripristino della password di accesso al sistema, ma parlare di “a rischio blocco l'80% degli account dei medici di famiglia italiani” appare eccessivo e fuori luogo.

La SIT pertanto, pur ritenendo certamente perfettibile il sistema di certificazione on-line di malattia proposto, lo ritiene sostanzialmente in linea con la normativa vigente ed adeguato, in questa fase iniziale di prima applicazione, alle esigenze per le quali è stato sviluppato; considera dunque ingiustificato l'allarme sociale provocato dalle affermazioni sopra riportate, e continua a dichiararsi disponibile a collaborare, con le istituzioni e con le organizzazioni dei medici, per suggerire i percorsi più adeguati verso quella sanità elettronica, armonica e sostenibile, come ci piace definirla, a misura di medico e di cittadino.

Ufficio stampa SIT

Società Italiana Telemedicina @ sanità elettronica
Via Giovanni Squarcina, 3 – 00143 ROMA
Tel.: +39 06 51 951 1 – Fax: +39 06 50 330 71
E-mail: info@sanitaelettronica.it
Web: www.sanitaelettronica.it

Nella pagina seguente l'approfondimento tecnico

In termini più generali la SIT nota, innanzitutto, come nessun servizio on-line che utilizzi per l'autenticazione una credenziale costituita da un identificativo utente ed una password, possa essere reso completamente immune da un attacco come quello descritto: l'identificativo utente infatti, al contrario della password, non può che essere un'informazione conosciuta o conoscibile da parte di tutti gli utenti effettivi o anche solo potenziali del sistema. E' quindi sempre possibile a chiunque bloccare l'accesso di un altro utente al sistema mediante un attacco mirato. L'importante è che il sistema sia dotato di accorgimenti atti a mitigare efficacemente l'impatto di questa vulnerabilità.

Nel caso specifico il portale prevede che ogni utente medico abbia una "credenziale di emergenza" da utilizzare in caso di blocco dell'accesso principale. Ciò è analogo a quanto avviene nei telefoni cellulari, dove mediante il codice PUK si può ripristinare l'operatività di un telefonino bloccato in seguito al ripetuto inserimento di un PIN errato. Sfruttando questa credenziale di emergenza il medico che abbia l'accesso principale bloccato può ugualmente accedere al sistema e ripristinarne la corretta operatività rimuovendo il blocco in modo facile e veloce, senza conseguenze pratiche sulla propria attività o sulla comunità dei propri assistiti.

Per quanto riguarda le presunte vulnerabilità del sistema, occorre innanzitutto ricordare che l'art. 64 del Codice dell'amministrazione digitale vigente prevede l'accesso ai siti web della PA sia con dispositivi di autenticazione forte (carta di identità elettronica e carta nazionale dei servizi) sia, in via transitoria, con dispositivi deboli (user ID e password, purché rispettino alcune misure di sicurezza come l'identità certa degli utilizzatori). Inoltre le linee guida per i siti web della PA, emanate in ottemperanza a quanto previsto dall'art. 4 della direttiva del Ministro per la pubblica amministrazione e l'innovazione n. 8/2009, con riferimento all'accesso ai servizi on-line prevedono espressamente l'utilizzo, come User ID, del codice fiscale degli utenti, nonché il blocco obbligatorio del sistema dopo diversi tentativi errati d'inserimento della password.

Il portale SistemaTS è tuttavia dotato di un'apposita procedura on-line di ripristino della password del medico certificatore eventualmente bloccata, la quale si basa su di un sistema di rilevazione di due domande-risposte segrete inserite dal medico stesso in fase di registrazione. Tramite tale verifica egli può autonomamente, ed in pochi secondi, ripristinare on-line la propria password in caso di errato inserimento, dimenticanza od uso fraudolento della stessa, senza alcuna necessità di recarsi alla ASL per ottenere una nuova busta con le sue credenziali d'accesso al sistema. Tale procedura è esaustivamente descritta al punto 5, pagina 7, del manuale operativo (versione 25/11/2009) per l'autenticazione al portale del SistemaTS.

Analogamente per la certificazione d'invalidità civile INPS, che utilizza sempre i codici fiscali dei medici come user ID, il pronto ripristino della password è garantito dall'inserimento, in fase di registrazione, del numero di cellulare e dell'indirizzo e-mail del medico certificatore.

A parere degli esperti della Società Italiana di Telemedicina e sanità elettronica, quindi, il presunto problema non è specifico del sistema di certificazione on-line di malattia o di invalidità civile ed è per certi versi solo teorico. Del medesimo problema soffrono infatti, ad esempio, tutti i servizi on-line che utilizzano come identificativo utente il suo indirizzo di posta elettronica, il quale è noto per definizione almeno a tutti coloro con cui egli è entrato, anche solo una volta, in contatto.

La criticità evidenziata non è dunque da riferirsi alla scelta di un determinato identificativo utente o nella presenza del blocco automatico per troppi tentativi di accesso errati, ma nella effettiva disponibilità di una modalità mediante la quale poter ripristinare facilmente e rapidamente un accesso bloccato a seguito di errore o di dolo. Essendo tale possibilità a disposizione del medico utente sia del portale SOGEI che quello INPS, ed attivabile facilmente on-line, il problema evidenziato è comunque marginale. Naturalmente la sua effettiva funzionalità dipende dalla cura con cui il singolo medico ha effettuato la registrazione al portale: se egli non ha provveduto ad inserire i dati necessari al ripristino in caso di blocco, sebbene chiaramente richiesti, non potrà avvalersi della procedura di emergenza in caso di blocco ma dovrà effettivamente recarsi di persona presso la ASL o presso l'INPS per richiedere nuove credenziali, vanificando così completamente l'utilità e l'efficacia del sistema on-line.