Certificati di sicurezza dei servizi telematici: nuova scadenza

Con l'Informativa n. 90/2022, il CNDCEC ha reso nota la proroga al **31 gennaio 2023** del termine entro il quale gli intermediari Entratel o gli utenti Fisconline che non hanno ancora rinnovato i certificati digitali per la firma e cifratura dei documenti informatici da scambiare mediante i canali telematici e l'infrastruttura SID sono tenuti a rinnovare il proprio ambiente di sicurezza.
In caso contrario, successivamente a tale data, **non** sarà **più garantita** l'acquisizione delle trasmissioni telematiche effettuate con certificati non adeguati ai nuovi standard di sicurezza.

La scadenza, originariamente fissata al 30 aprile 2022, era già stata rinviata una prima volta al 31 dicembre 2022 dal comunicato dell'Agenzia delle Entrate del 29 aprile 2022.

In particolare, secondo quanto si legge nella **comunicazione** dell'Agenzia delle Entrate allegata all'Informativa in commento, i **nuovi requisiti** minimi di sicurezza da recepire sono:

- algoritmo di hash: SHA-256;
- algoritmo di cifratura: AES-256;
- lunghezza delle chiavi RSA: 4096 bit (cifratura) e 4096 o 2048 bit (firma).

Gli utenti interessati sono invitati a **rinnovare** i propri certificati utilizzando, in alternativa, le applicazioni:

- "Desktop Telematico – Entratel";
- "Generazione certificati".

Tramite tali applicazioni, è possibile anche verificare

l’aggiornamento dei certificati, come di seguito descritto. Innanzitutto, indipendentemente dalla tipologia di applicazione utilizzata, è opportuno inserire preventivamente nel proprio pc la chiavetta USB sulla quale sono memorizzate le credenziali di sicurezza necessarie per controllare se i certificati sono già aggiornati e, in caso contrario, procedere alla relativa rigenerazione.

Poi, nel caso di utilizzo del **Desktop Telematico**, occorre utilizzare la funzione “Sicurezza – Visualizza certificati” del menù “Entratel”, selezionare il bottone “Dettaglio”, dopo aver specificato il certificato da verificare, e controllare che nella cartella “Generale – Certificato selezionato” appaia la dicitura “Chiave Pubblica: Sun RSA public key, 4096 bits”. Nel caso in cui la dicitura riporti un valore diverso, il certificato dovrà essere aggiornato procedendo alla revoca dell’ambiente di sicurezza e alla generazione di uno nuovo (per approfondimenti, si rimanda alla Procedura pratica 4 ottobre 2022 n. 57).

Per quanto riguarda, invece, l’applicazione **Generazione certificati**, bisogna utilizzare la funzione “Gestisci ambiente – Visualizza certificati”, selezionare il bottone “Dettaglio” dopo aver specificato il certificato da verificare e controllare che nella cartella “Generale – Certificato selezionato” appaia la dicitura “Chiave Pubblica: Sun RSA public key, 4096 bits”. Qualora la dicitura descriva un valore diverso, il certificato dovrà essere aggiornato procedendo alla revoca dell’ambiente di sicurezza e alla generazione di uno nuovo.

Eventuali richieste di generazione dei certificati effettuate con una versione non aggiornata delle applicazioni **saranno scartate** dal sistema con il seguente messaggio: “Formato della richiesta di iscrizione al registro utenti non valido (K1024). Verificare la versione del software di generazione dell’ambiente di sicurezza”.

Ove necessario, appare consigliabile provvedere **per tempo** all’eventuale rigenerazione degli ambienti di sicurezza, onde evitare interruzioni della connessione internet durante la procedura di rinnovo, causate da una presumibile “congestione” del traffico dati in prossimità della scadenza.

(MF/ms)