

## **Rinnovo certificati per adeguamento ai nuovi standard di sicurezza**

L'Agenzia delle entrate, ha reso più sicuri i certificati digitali per la firma e cifratura dei documenti informatici da scambiare mediante i canali telematici e l'infrastruttura SID. In particolare, i nuovi requisiti minimi di sicurezza da recepire entro il 30/04/2022 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 potranno rinnovare i propri certificati utilizzando le applicazioni "**Desktop Telematico - Entratel**" oppure "**Generazione certificati**", mediante le quali è possibile anche verificare l'aggiornamento dei certificati, come di seguito descritto.

- **Desktop Telematico:** utilizzare la funzione "Sicurezza - Visualizza certificati" del menù "Entratel", selezionare il bottone "Dettaglio" dopo aver specificato il certificato da verificare, e verificare che nella cartella "Generale - Certificato selezionato" appaia la dicitura "Chiave Pubblica: Sun RSA public key, 4096 bits"; nel caso la dicitura elenchi un valore diverso, il certificato dovrà essere aggiornato procedendo alla revoca dell'ambiente di sicurezza e alla generazione di un nuovo ambiente di sicurezza;
- **Gestione certificati:** utilizzare la funzione "Gestisci ambiente - Visualizza certificati", selezionare il bottone "Dettaglio" dopo aver specificato il certificato da verificare, e "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 un nuovo ambiente di sicurezza.

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