

***EVOLUZIONE DEI SISTEMI DI SICUREZZA PER LA FIRMA E LA CIFRATURA DEI
DATI DELL'AGENZIA DELLE ENTRATE***

***NOTA INFORMATIVA SDI – FATTURE E CORRISPETTIVI - SERVIZI SDI SFTP
MASSIVI***

INFORMATIVA

L'Agenzia delle Entrate nell'ambito dell'adeguamento continuo delle misure di sicurezza del proprio servizio SDI – Fatture e Corrispettivi ha definito nuove regole relative agli algoritmi di hashing e di cifratura e ai parametri dei certificati di firma e cifratura dei documenti in ingresso ed in uscita relativi ai servizi SDI SFTP Massivi.

È previsto un intervento sui requisiti minimi sull'algoritmo di cifratura, sulla lunghezza delle chiavi RSA e sull'algoritmo hash che viene utilizzato nell'ambito della firma digitale dei supporti scambiati nel suddetto canale di trasmissione, per calcolare:

- l'impronta dei documenti;
- la firma digitale vera e propria dei documenti.

I nuovi requisiti minimi sono:

- Algoritmo di hash: SHA-256;
- Lunghezza delle chiavi RSA: 4096 bit (cifratura) e 4096/2048 bit (firma);
- Algoritmo di cifratura: AES-256.

Tali requisiti minimi saranno obbligatori per tutti i sistemi che scambiano dati con l'Agenzia a partire dal 31 maggio 2021.

Le tempistiche e le modalità dell'intervento saranno gestite dal gruppo servizicrittograficftp di Sogei, che, secondo una predefinita calendarizzazione, contatterà il referente tecnico di ogni nodo, concordando:

- la consegna di nuove chiavi RSA a lunghezza 4096 bit;
- la data di switch in produzione dei nuovi standard collaudati.

Al completamento delle attività per l'utilizzo dei nuovi standard di cifratura il gruppo servizicrittograficftp avvierà una fase di monitoraggio per accertare il buon funzionamento e sarà disponibile qualora si rendesse necessaria una assistenza di carattere tecnico.