



AgID-CA1 - Procedura per la richiesta di emissione certificato

Per ciascun certificato da emettere, l'organizzazione Richiedente deve inviare all'Agenzia per l'Italia Digitale una "Richiesta di emissione certificato" applicando la seguente procedura:

1. Il Responsabile dell'Organizzazione utilizza il modulo elettronico "Richiesta di Registrazione", e lo compila¹. Il nome del file .doc generato **deve** avere la seguente struttura: <Nome Organizzazione>-<tipo certificato>-<progressivo>-<data>-RR; il <tipo certificato> può assumere i seguenti valori: "firma", "autenticazione", "ssl server"; la <data> **deve** avere il seguente formato: AAAAMMGG.
2. Il Responsabile dell'Organizzazione **firma digitalmente** il documento ottenuto al punto 1, ottenendo un file con estensione **p7m**. Il certificato di firma deve aver valorizzato l'attributo "**organizationName**" (O) nel campo Subject, il cui valore deve coincidere con la denominazione dell'Organizzazione richiedente.
3. Il Responsabile del Server (indicato nel modulo di cui al punto 1), genera la richiesta di certificazione CSR per il server da certificare, in formato PKCS#10. Il nome del file CSR **deve** avere la seguente struttura: <nome Organizzazione>-<tipo certificato>-<progressivo>-<data>.CSR; il <tipo certificato> può assumere i valori indicati al punto 1; la <data> deve avere il formato AAAAMMGG. Per generare la propria coppia di chiavi, deve essere utilizzato l'algoritmo RSA, con lunghezza delle chiavi di 2048bit.
4. Il Responsabile dell'Organizzazione genera un file archivio di nome <Nome Organizzazione>-<tipo certificato>-<progressivo>-<data>-**Richiesta Certificato.zip**" contenente il file **p7m** generato al punto 1 ed il file CSR generato al punto 3.
5. Tutte le Richieste di emissione certificato (ossia i file .zip ottenuti al punto 4) vengono inviate in allegato ad un messaggio di posta elettronica certificata, indirizzato a: Richiesta-Certificati@pec-ic.agid.gov.it che **deve** avere come oggetto: **AgID-CA1-Richiesta Certificato** <Nome Organizzazione>.

Eventuali anomalie riscontrate durante il processo di emissione del certificato saranno notificate al Responsabile del Server, all'indirizzo di posta elettronica indicato nella Richiesta di registrazione.

Al termine delle operazioni di certificazione il certificato prodotto verrà spedito all'indirizzo di PEC dal quale è pervenuta la richiesta del certificato e, per conoscenza, al Responsabile del Server, all'indirizzo di posta elettronica indicato nella Richiesta di registrazione.

¹ La compilazione del modulo elettronico (.dot) deve essere effettuata con MS Word utilizzando il tasto TAB (o PagUp e PagDwn) per passare da campo a campo.