|  |
| --- |
|  |
| Rilascio nuovi certificati AAMS |
| Guida Operativa |

|  |
| --- |
|  |

Sommario

[1. Intento del documento 3](#_Toc484514032)

[2. Introduzione 3](#_Toc484514033)

[3. Credenziali per l’area riservata 3](#_Toc484514034)

[4. Rilascio certificati 3](#_Toc484514035)

[5. Creazione richiesta di certificato e chiave privata 3](#_Toc484514036)

[6. Configurazione Servizi 4](#_Toc484514037)

[6.1. PGAD Anagrafica dei conti di gioco 4](#_Toc484514038)

[6.1.1. Installazione del certificato sul/sui server di Backend 4](#_Toc484514039)

[6.1.2. Aggiornamento della configurazione sul database 5](#_Toc484514040)

[6.1.3. Riavvio del servizio PGADService. 5](#_Toc484514041)

[6.2. Installazione del certificato sul servizio PGDAv2 5](#_Toc484514042)

[7. Aggiornamento in AAMS 6](#_Toc484514043)

[8. Aggiornamento certificati servizi dei partner 6](#_Toc484514044)

[8.1. Aggiornamento certificato ActiveGames 7](#_Toc484514045)

[9. Ottenere l’elenco dei conti gioco della licenza 7](#_Toc484514046)

[10. Allegati 9](#_Toc484514047)

# Intento del documento

Il documento descrive i passi per il rilascio di nuovi certificati e le configurazioni da cambiare per fare acquisire i nuovi certificati dalla piattaforma di gioco.

# Introduzione

Per poter comunicare con i server AAMS è necessario richiedere appositi certificati all’interno della sezione privata del sito di AAMS (<https://www.aams.gov.it>). Per ottenere accesso a tale area è necessario inviare il modulo in [allegato](#_Allegati) appositamente compilato all’indirizzo mail [assistenza-giochi@sogei.it](mailto:assistenza-giochi@sogei.it). I certificati rilasciati all’interno dell’area riservata di AAMS sono utilizzati per i seguenti protocolli:

* PGAD (Anagrafica conti di gioco)
* PGDA (Giochi di abilità e di sorte a quota fissa: Poker, Casino, Skillgames)
* PBAD (Bingo)

# Credenziali per l’area riservata

Di seguito le credenziali utilizzare dal gruppo web per accedere all’area riservata AAMS.

|  |  |
| --- | --- |
| **Credenziali area riservata AAMS** | |
| **Nome Utente** | VSCVCN77T14L259G |
| **Password** | Intralot2016! |
| **Domanda recupero password** | Nome società |
| **Risposta** | Intralot |

In caso in cui la password risulti scaduta è necessario seguire il link “cambia password” per procedere all’aggiornamento della stessa.

# Rilascio certificati

Una volta ottenuto l’accesso all’area riservata di AAMS è necessario recarsi nella sezione *“Rilascio Certificati->Nuova Richiesta”* e selezionare la voce “*Anagrafe Conti*”. Qualora non sia possibile richiedere nuovi certificati è necessario richiedere il ripristino di un certificato già rilasciato selezionando la voce *“Rilascio Certificati->Visualizza Certificati”* e cliccare il tasto “*Chiedi Ripristino*”. Sia per le nuove richieste che per il ripristino di un certificato già rilasciato è necessario creare una richiesta di certificato tramite il tool *openssl.* Per ulteriori informazioni fare riferimento al documento allegato “[PGAD documento tecnico](#_Allegati)”.

# Creazione richiesta di certificato e chiave privata

Prerequisito per la creazione di una richiesta di certificato è l’installazione del tool [openssl](https://www.openssl.org/). Una volta installato il programma sul pc è consigliabile modificare la variabile *PATH* della workstation che si sta utilizzando al fine di rendere visibile l’eseguibile *openssl.exe* da qualsiasi directory di lavoro. Per la generazione dei certificati fare riferimento alla guida in [allegato](#_Allegati). Una volta ottenuto il certificato è necessario esportarlo in formato PKCS#12 come descritto nella guida in [allegato](#_Allegati).

# Configurazione Servizi

# PGAD Anagrafica dei conti di gioco

La configurazione del servizio è suddivisa nei seguenti tre step:

1. Installazione del certificato sul/sui server di Backend
2. Aggiornamento della configurazione sul database
3. Riavvio del servizio PGADService al fine di rileggere la nuova configurazione

# Installazione del certificato sul/sui server di Backend

Il servizio PGAD è pubblicato sui server dei Backend (backend.intralot.it) ed è raggiungibile alla seguente URL: <http://backend.intralot.it/PGADService/PGADService.svc>.

Il certificato esportato in formato PKCS#12 deve essere installato sui server di backend all’interno della directory “Certificati (computer locale) -> Personale“.

Dopo l’installazione del certificato è necessario assicurarsi che l’utente utilizzato dall’application pool del servizio PGDAService abbia il controllo completo sulla chiave privata del certificato. Per verificare/impostare tali permessi è necessario selezionare il certificato all’interno della snapin certificati, cliccare sulla label “*Altre azioni->Tutte le attività->Gestisci chiavi private*” .

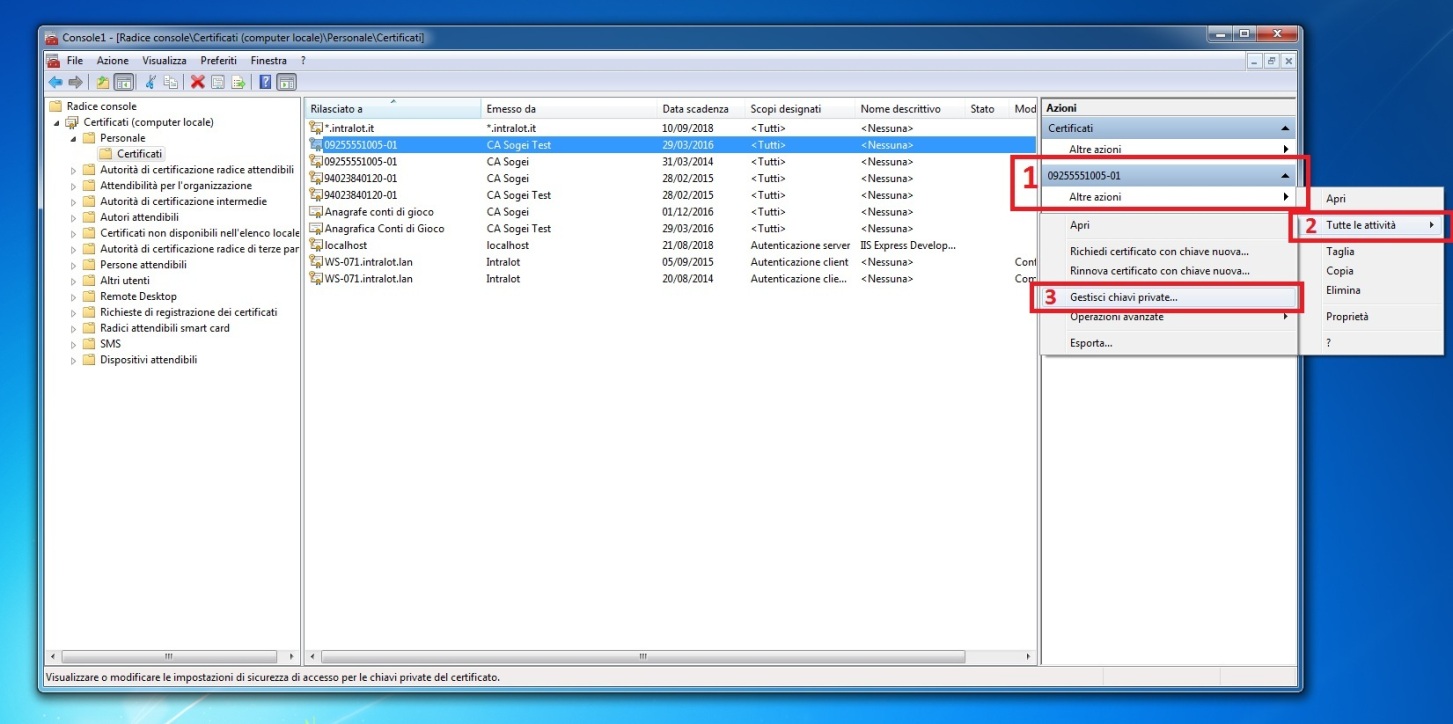


figura 1 - mmc - snap-in certificati

# Aggiornamento della configurazione sul database

Per terminare la configurazione del nuovo certificato è necessario aggiornare la tabella *Dati].[Concessionario]* del database *AnagraficaContiGioco*. In particolare deve essere aggiornata la colonna *chiavePrivata* con il thumbprint del nuovo certificato di **firma**.

Di seguito un update sql che può essere usato per aggiornare la configurazione del certificato di firma per il concessionario 15115. Il thumbprint utilizzato è quello del certificato di firma con seriale 1165047671.

UPDATE [AnagraficaContiGioco].[Dati].[Concessionario] SET chiavePrivata='78b85b75b959db12c2c94741f11f0285d2379783'

WHERE codice=15115

**La modifica della chiave pubblica è relativa al certificato di cifratura rilasciato da AAMS**

# Riavvio del servizio PGADService.

Una volta installato il nuovo certificato e riportata la nuova configurazione sul database è necessario eseguire il riavvio del/dei server di backend (***cmd > issreset***) al fine di aggiornare la nuova configurazione.

# Installazione del certificato sul servizio PGDAv2

Il servizio del PGDAv2 utilizza il certificato di **firma** rilasciato all’interno della sezione riservata di AAMS. Il certificato è contenuto nella cartella **Certificati** posizionata sul server al seguente percorso:

* C:\inetpub\wwwroot\PGDA\_v2.1\Certificati

La cartella al suo interno contiene ulteriori sotto cartelle, ognuna per ogni concessionario:

* Intralot
* Betsson

In ogni cartella sono riportati i certificati di firma del concessionario (chiave privata) e la chiave pubblica di AAMS necessaria per verificare l’autenticità del mittente del messaggio. Il nome del certificato e la posizione sul server del certificato deve corrispondere a quanto riportato sul web.cofing del servizio. Inoltre è necessario che l’utente utilizzato dall’Application Pool del servizio abbia i permessi di lettura su tale cartella. Di seguito la sezione custom del web.config:

<configuration>

……

<intralot.cripto xmlns="Intralot.Cripto.Configuration">

<providers>

<provider license="15115" path="C:\inetpub\wwwroot\PGDA\_v2.1\Certificati\Intralot" state="true">

<certificates>

<certificate type="public" name="CertificatoADM\_test.crt"/>

<certificate type="private" name="09255551005-01\_firma-TEST.pfx" password="intralot"/>

</certificates>

</provider>

<provider>

……..

</provider>

</providers>

</intralot.cripto>

…..

</configuration>

In alternativa, si possono fare leggere i certificati tra quelli installati sulla macchina. Per fare questo, lasciare vuoto il campo path nella sezione provider inserire il thumbprint nel campo name del certificato. Di seguito un esempio di web.config

<configuration>

……

<intralot.cripto xmlns="Intralot.Cripto.Configuration">

<providers>

<provider license="15116" path=" " state="true">

<certificates>

<certificate type="public" name="5b935436f4dde97a486290aef4c4a557001d27c3"/>

<certificate type="private" name="78b85b75b959db12c2c94741f11f0285d2379783" password="intralot"/>

</certificates>

</provider>

<provider>

……..

</provider>

</providers>

</intralot.cripto>

…..

</configuration>

Per ogni concessionario è necessario inserire una nuova configurazione **provider** con una propria sezione **certificates** contenente la lista di certificati utilizzati.

|  |  |
| --- | --- |
| **Nome** | **Descrizione** |
| **Provider** | |
| **license** | Codice concessionario |
| **path** | Path locale della cartella contenente i certificati |
| **Certificate** | |
| **type** | Tipo del certificato (chiave pubblica=”public”, chiave privata =”private”) |
| **name** | Nome del file del certificato |
| **password** | Password della chiave privata |

**Descrizione attributi configurazione**

# Aggiornamento in AAMS

Al fine di far accettare ai servizi di AAMS PGDA e Bingo il nuovo certificato, è necessario inviare comunicazione a [gioconline@sogei.it](mailto:gioconline@sogei.it) contente la partita IVA del concessionario, il seriale del certificato che da utilizzare e i protocolli su cui va utilizzato ( PGDA, Bingo) . Per quanto riguarda il protocollo PGAD, il certificato dovrebbe essere accettato immediatamente dopo il rilascio. In caso negativo deve essere inviata opportuna comunicazione a [assistenza-giochi@sogei.it](mailto:assistenza-giochi@sogei.it).

# Aggiornamento certificati servizi dei partner

In caso in cui il certificato di firma sia stato distribuito ai nostri partner, è necessario inviare opportuna comunicazione in modo tale da far aggiornare il certificato anche nella loro piattaforma. Di seguito i passi necessari per l’aggiornamento dei certificati sulla piattaforma di Active Games ad oggi utilizzata per le verticali di gioco Bingo e Poker. Active Games è l’unico fra i nostri partner ad avere una comunicazione diretta con AAMS ad oggi per conto nostro.

# Aggiornamento certificato ActiveGames

Una volta ottenuto il nuovo certificato dall’area riservata è necessario esportare il certificato in formato pkcs12 aggiungendo come l’alias il numero concessione. Di seguito il comando openssl da lanciare

* ***openssl*** **pkcs12** **-export** **-in** certificato.crt **-inkey** chiave.pem **–certfile** CA.crt **-name** alias **-out** certificato.pfx

|  |  |
| --- | --- |
| **Nome opzione** | **Descrizione** |
| **Openssl** | Programma openssl.exe |
| **pkcs12** | Opzione da settare per esportare/importare certificati in formato pkcs12 |
| **-export** | Il certificato verrà convertito nel formato pkcs12 |
| **-in** | Segue il certificato da convertire |
| **-inkey** | Segue la chiave privata del certificato |
| **-certFile** | Segue la CA del certificato da esportare (nel nostro caso la CA di sogei) |
| **-name** | Segue il nome dell’alias che si vuole dare al certificato (nel nostro caso il codice concessione, 15115) |
| **-out** | Segue il nome del certificato convertito nel formato pkcs12. |

**Descrizione opzioni openssl pkcs12**

Una volta ottenuto il certificato con il nuovo formato è necessario inviarlo al partner tenendo presente le seguenti considerazioni:

* Il certificato deve essere consegnato almeno una settimana prima del rilascio
* L’aggiornamento dei certificati comporta un riavvio dei servizi del partner. Tale riavvio viene eseguito solamente il marterdì.
* Per quanto riguarda il Bingo è necessario uno stop del servizio di un giorno, che va dal giorno precedente al rilascio fino alle ore 10.00 del giorno del rilascio.

# ­­­­­­­Ottenere l’elenco dei conti gioco della licenza

Per eseguire l’operazione è necessario disporre di una utenza adatta ad eseguire l’operazione. Se l’utenza a disposizione non è adatta, contattare il responsabile aziendale per i rapporti con AAMS, o AAMS stessa.

Nell’area riservata, effettuare una richiesta dello scarico dei conti di gioco, facendo riferimento alla Figura 1

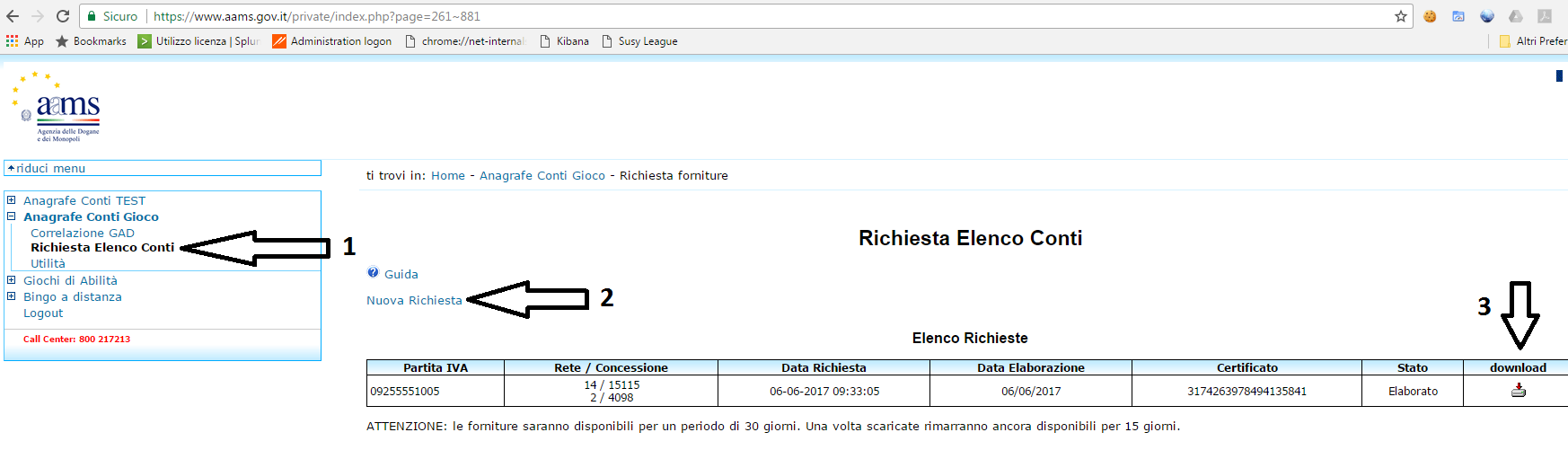


Figura 1 - come richiedere l'elenco dei conti gioco nell'area riservata

La richiesta va prima inserita, e, una volta che AAMS avrà fatto gli opportuni controlli ( l’utente può ricevere una telefonata in cui gli viene richiesta conferma dell’operazione) sarà elaborata. A questo punto l’elenco dei conti di gioco è disponibile per il download.

Si ottiene quindi un file con estensione \*.tar.gz, che va scompattato due volte per ottenere un file con estensione \*.encrypted e un certificato pubblico \*.cer.

Il certificato pubblico è la chiave pubblica del certificato di cifratura creato attraverso il paragrafo 5

Tramite il tool open ssl eseguire il comando:

openssl smime -decrypt -inform DER -in file.encrypted -recip cifra.cer -inkey key.pem -out file.decrypted

dove:

* file.encrypted è il file ottenuto scompattando.
* cifra.cer è il certificato di cifratura creato da Intralot (anche questo viene dato scompattando il file dell’area riservata).
* key.pem è la chiave utilizzata per creare il certificato di cifratura (fare riferimento al paragrafo 5).
* file.decrypted è il file decriptato contenente l’elenco dei conti di gioco (per leggere il file è necessario un ulteriore passaggio, descritto di seguito).

La procedura per essere eseguita richiede la password del certificato (inserita in fase di creazione del certificato stesso).

Il file ottenuto non è ancora leggibile. Va decriptato utilizzando la chiave pubblica di aams e la ca di aams in formato PEM. Entrambi i certificati, se non sono già disponibili, possono essere ottenuti dall’area riservata.

Il certificato di CA viene fornito in formato \*.cer . Per convertirlo in formato \*.pem eseguire il comando

openssl x509 -inform der -in certificate.cer -out certificate.pem

dove:

* certificate.cer è il certificato in format cer
* certificate.pem è il certificato convertito in formato pem

Per ottenere quindi l’elenco XML dei conti di gioco, eseguire il commando

openssl smime -verify -inform DER -in file.decrypted -signer aams.cer -CAfile ca.pem m -noverify -out file.tar.gz

dove:

* file.decrypted è ottenuto dalla procedura descritta in precedenza
* aams.cer è la chiave pubblica di aams
* ca.pem è la CA di aams in formato pem
* file.tar.gz è il file contanente le informazioni richieste.

Scompattando due volta il file file.tar.gz, si ottiene l’elenco dei conti di gioco in formato XML.

# Allegati

|  |  |
| --- | --- |
| Allegato | File |
| Modulo Abilitazione area riservata |  |
| PGAD documento tecnico |  |
| Guida generazione certificati PGAD |  |
| Piccola Guida openssl |  |