amministrazione autonoma
dei monopoli di stato

Allegato tecnico

per il

gioco a distanza

INDICE

1. RILASCIO CERTIFICATI DIGITALI

1.1 NUOVA RICHIESTA

Il Concessionario chiede ad AAMS di accedere all'Area Riservata del sito aams.gov.it (https://www.aams.gov.it) per poter usufruire della funzionalità di rilascio dei certificati digitali necessari per il protocollo di comunicazione dell'Anagrafe dei Conti di Gioco (PGAD); a tal fine comunica la propria Partita I.V.A., i propri dati anagrafici, il codice fiscale e l'indirizzo e-mail di una o più persone abilitate all'accesso al sito per conto delle sue concessioni.

Accedendo alla sezione "Rilascio Certificati" dell'area riservata del sito AAMS è possibile scegliere il tipo di certificato da richiedere; nel caso di certificato per l'Anagrafe dei Conti di Gioco, nella schermata successiva, se l'utente possiede più di una Partita Iva, gli sarà chiesto di specificare per quale di queste intende fare richiesta, altrimenti passerà direttamente alla schermata di caricamento in cui vengono visualizzati due campi di testo dove devono essere inserire le richieste (nello standard PKCS#10 in formato PEM) una per il certificato di firma e l'altra per quello di cifratura; il primo necessario al Concessionario per firmare le richieste verso il Sistema Centrale AAMS, l'altro per permettere ad AAMS di rispondere in modo in cifrato alle comunicazioni che contengono dati sensibili.

Un esempio di come possono essere generate tali richieste usando Openssl è il seguente:

```
openssl req -new -newkey rsa:1024 -keyout private_key.pem
-out richiesta.pem
```

Verranno generati due file, uno con nome “private_key.pem”, che contiene la chiave privata in formato testuale, e l’altro con nome “richiesta.pem” che è la richiesta da inviare tramite il sito AAMS.

Durante questa operazione con Openssl vengono richieste alcune informazioni che verranno incorporate nel certificato rilasciato, tra cui:

- `COUNTRY NAME`: Indicare la sigla dello stato in cui ha sede legale la società richiedente
- `STATE OR PROVINCE NAME:` Indicare per esteso il nome dello stato in cui ha sede legale la società richiedente
- `LOCALITY NAME:` Indicare il nome della città in cui ha sede legale la società richiedente
- `ORGANIZATION NAME:` Nome della società richiedente
- `ORGANIZATION UNIT:` Nome dell’unità organizzativa richiedente
- `COMMON NAME:` Indicare la Partiva I.V.A. per la quale si vorrà firmare o cifrare le comunicazioni, seguito da -01 (esempio: 01234567890-01)

ATTENZIONE: il comando Openssl deve essere eseguito due volte, una volta per la richiesta del certificato di firma e la seconda per il certificato di cifratura.

Una volta caricate le due richieste, comprensive del "----- BEGIN CERTIFICATE REQUEST -----" e "----- END CERTIFICATE REQUEST -----", si deve attendere che vengano processate e al termine dell'operazione di elaborazione i certificati saranno VALIDI e disponibili nella sezione "Visualizza Certificati".

Per l'Anagrafe dei Conti di Gioco viene data la possibilità di richiedere due certificati (due di firma e due di cifra) che possono essere usati contemporaneamente (entrambi validi);

questo permette di chiedere il ripristino di un certificato mentre l'altro è ancora valido e consente di non dover fermare le attività in corso.

1.2 VISUALIZZA CERTIFICATI

Tramite la sezione "Visualizza Certificati" la persona abilitata alla gestione delle richieste dei certificati per conto di un Concessionario visualizza l'elenco completo dei certificati richiesti; da qui, cliccando sul link "DETTAGLIO", è possibile visualizzare il dettaglio del certificato selezionato ed è possibile effettuare alcune operazioni a seconda dello status del certificato. In particolare è possibile:

- Visualizzare il certificato;
- Visualizzare le scadenze e il serial number;
- Visualizzare lo status del certificato;
- Chiedere il ripristino del certificato.

L'operazione di ripristino consiste nella rigenerazione del certificato, sia di firma che di cifratura. Questa operazione può essere molto utile nel caso di perdita delle chiavi e/o passphrase, sia per compromissione delle stesse o per l'avvicinarsi della scadenza.
I certificati di firma e di cifratura vengono gestiti in coppia: il ripristino di quello di firma prevede il ripristino anche di quello di cifratura e viceversa.

2. FORNITURE CONTI DI GIOCO

2.1 INVIO FORNITURE

Il Concessionario chiede ad AAMS di accedere all'Area Riservata del sito aams.gov.it (https://www.aams.gov.it) per poter trasmettere le informazioni relative ai conti di gioco a distanza stipulati con i propri giocatori; a tal fine comunica la propria Partita I.V.A., i propri dati anagrafici, il codice fiscale e l'indirizzo e-mail di una o più persone abilitate all'accesso al sito per conto delle sue concessioni.

La funzionalità "Invio forniture", disponibile nell'Area Riservata del sito AAMS, consente alle persone abilitate di inviare al sistema centrale di AAMS le informazioni relative ai conti di gioco tramite appositi file in formato XML, denominati in seguito "forniture".

Le forniture devono essere create rispettando alcune regole sintattiche definite nello schema (XSD), disponibile nella sezione "Invio forniture", e alcune regole strutturali, definite nella stessa sezione.

Per garantire la riservatezza dei dati trasmessi e l'autenticità del mittente, le forniture dovranno essere firmate e codificate con standard basati su chiavi asimmetriche; in particolare ogni file xml, che potrà essere compresso con winzip su sistemi windows oppure con tar –cz su sistemi linux, dovrà essere firmato con il certificato rilasciato da AAMS al Concessionario e successivamente cifrate con la chiave pubblica di AAMS, disponibile sempre nella sezione "Invio forniture", garantendo così che i dati trasmessi siano leggibili solo dal sistema centrale di AAMS.

Sono previste tre differenti tipologie di forniture:

- Anagrafe dei conti di gioco: per comunicare i dati richiesti per i conti di gioco e i relativi intestatari;
- Chiusura dei conti : per comunicare la chiusura dei conti di gioco;
- Variazione della provincia di residenza : per comunicare il cambio di residenza degli intestatari dei conti di gioco.

Una volta predisposto, il file XML può essere compresso o meno, in base alla dimensione dello stesso, e successivamente firmato utilizzando, ad esempio, OPENSSL con l'istruzione:

```
openssl smime -sign -in file_da_firmare -outform DER
–binary -nodetach -signer pkcs12.pem
-passin pass:passphrase_del_concessionario
-out file_firmato
```

Una volta ottenuto il file firmato si può procedere alla sua cifratura utilizzando la chiave pubblica di AAMS come nell'esempio (OPENSSL):

```
openssl smime -encrypt -inkey aams_public_key.pem
-in file_firmato -outform DER -des3 -binary
-out fornitura_pronta aams_certificate.pem
```

a questo punto accedendo alla funzionalità "Invio forniture", disponibile sempre nel sito AAMS, si potrà procedere al caricamento della fornitura.

2.2 VERIFICHE

Nell' Area Riservata del sito AAMS sono disponibili 3 funzionalità:

- Forniture inviate
- Verifica conto
- Visualizza errori

La funzionalità "Forniture inviate" consente all'utente autorizzato di visualizzare, verificare, e stampare l'esito dell'elaborazione delle forniture inviate. Grazie alla funzionalità di ricerca l'utente può interrogare le forniture per data di caricamento o per identificativo fornitura (campo "<id_fornitura>" dell'XML).
Selezionando la voce "Dettaglio" è possibile visualizzare le informazioni di riepilogo sull'esito del caricamento dei record presenti all'interno di una fornitura e, in caso di presenza di errori, selezionando la voce "Riepilogo errori", sarà possibile visualizzare la tipologia di errore riscontrato nel caricamento di ogni singolo record, individuandolo dal campo univoco nella fornitura denominato "<prog>" (progressivo).

La funzionalità "Verifica conto" consente ai soli utenti autorizzati, di verificare la corretta registrazione di un singolo conto di gioco nel sistema centralizzato di AAMS. Per l'interrogazione è necessario specificare l'identificativo del conto, il codice della concessione titolare del conto e la tipologia di concessione (Rete).

La funzionalità "Visualizza errori" consente ai soli utenti autorizzati di ricercare e visualizzare tutti gli errori rilevati dal sistema per i singoli record trasmessi con le forniture inviate nel periodo selezionato.

2.3 UTILITÀ

Nell' Area Riservata del sito AAMS è disponibile la funzionalità Utilità che consente all'utente autorizzato di scaricare i seguenti documenti relativi al protocollo di colloquio dell'anagrafe dei conti di gioco (PGAD):

- WSDL e Schema XSD del PGAD
- Certificato della CA Sogei con cui i Concessionari verificano la firma apposta da AAMS ai messaggi
- Certificato di cifratura del sistema centrale AMMS tramite il quale i Concessionari inviano richieste cifrate ad AAMS

In questa sezione sono pubblicati anche i seguenti documenti relativi all'invio delle forniture:

- Schema XSD delle forniture XML
- Chiave pubblica di AAMS per la cifratura delle forniture

3. SPECIFICHE DI SICUREZZA PER IL RICHIAMO DEI WEBSERVICES

3.1 PREMESSA - INTRODUZIONE

Il sistema centrale di AAMS espone dei webservices che consentono il trasferimento delle informazioni sui conti di gioco a distanza gestiti dai singoli concessionari.
L'interazione con il sistema di AAMS è basato su webservices con protocollo SOAP su HTTPS.
Per rispondere alle esigenze di sicurezza viene utilizzato lo standard WS Security sia per l'autenticazione del soggetto chiamante sia per garantire l'autenticità, la riservatezza e l'inalterabilità dei dati trasmessi.
Di seguito viene specificato il profilo di WS Security adottato dal sistema.

3.2 CRITERI DI SICUREZZA ADOTTATI

Nel colloquio il concessionario si autentica sul sistema centrale di AAMS utilizzando lo standard Username Token Profile della WS-Security con il valore del campo Username coincidente con la Partita I.V.A. del concessionario stesso. Inoltre il concessionario firma lo Username Token contenuto nell'header ed anche il body della richiesta SOAP.

I certificati necessari ai concessionari per le firme, rilasciati secondo la procedura già descritta nel capitolo 1, conterranno nel campo Common Name (CN) il valore della Partita I.V.A. del concessionario stesso seguita da un trattino ed un codice numerico di due cifre.

Viene controllato che il valore della Partita I.V.A. del concessionario contenuta nel campo Username dello Username Token coincida con il valore della Partita I.V.A. contenuto nel CN del certificato di firma.

Il concessionario dovrà cifrare, secondo le specifiche tecniche di seguito indicate, il body del messaggio di input al metodo "aperturaContoPersonaFisica"; quindi nel caso di richiamo di questo metodo andrà applicata anche la cifratura all'intero body del messaggio SOAP.

La risposta emessa dal sistema centrale di AAMS sarà anch'essa firmata e tale firma deve essere verificata dai sistemi dei Concessionari.

3.3 SPECIFICHE DI SICUREZZA DEL COLLOQUIO

Vengono di seguito specificate in dettaglio le modalità di interazione con il sistema centrale di AAMS in relazione allo UsernameToken Profile, alla tipologia di firma e di cifratura da adottare.

3.3.1 USERNAMETOKEN PROFILE

Per tale standard dovrà essere valorizzato solo il campo Username non includendo il campo Password. Tale campo dovrà essere firmato e dovrà corrispondere alla Partita I.V.A. del soggetto e coincidere con il valore della Partita I.V.A. contenuto nel Common Name del certificato di firma.

3.3.2 FIRMA

Per quanto riguarda la firma devono essere utilizzate le seguenti impostazioni:

- **Key Identifier Type** = Binary Security Token
- **Signature Algorithm** = http://www.w3.org/2000/09/xmldsig#rsa-sha1
- **Signature Canonocalization** = http://www.w3.org/2001/10/xml-exc-c14n#

Le stesse modalità verranno applicate alla firma della risposta realizzata dal sistema centrale di AAMS.

3.3.3 CIFRATURA

Nel caso di richiamo del metodo “aperturaContoPersonaFisica” l’intero body SOAP dovrà essere cifrato seguendo le seguenti impostazioni:

- **Key Identifier Type** = Subject Key Identifier
- **Symmetric Encoding Algorithm** = http://www.w3.org/2001/04/xmlenc#aes128-cbc
- **Key Encryption Algorithm** = http://www.w3.org/2001/04/xmlenc#rsa-1_5
- **Encryption Canonicalization** = http://www.w3.org/2001/10/xml-exc-c14n#