FAQ - SIOPE PLUS

Registrazione e Autenticazione

1. Cos'è la CNS?

La Carta Nazionale dei Servizi (CNS) è uno strumento di identificazione in rete che consente la fruizione dei servizi erogati dalle amministrazioni pubbliche. Altri tipi di carte denominate Carta Regionale dei Servizi (CRS) e Tessera Sanitaria CNS (TS-CNS) sono equivalenti, dal punto di vista tecnico e normativo, alla CNS e possono quindi essere utilizzate per gli stessi scopi. Tali carte possono essere emesse solo dalle Pubbliche Amministrazioni (solitamente dalle Regioni, ma può trattarsi anche di Comuni o altri enti pubblici).

2. Cosa significa autenticarsi con la CNS?

Per potersi autenticare (identificare) con la CNS è necessario disporre di un dispositivo di tipo Smart Card o Chiavetta USB , rilasciato da un Ente certificatore accreditato a livello nazionale, contenente l'apposito certificato di autenticazione. Solitamente lo stesso dispositivo è anche abilitato alla funzione di firma digitale e per questo contiene al suo interno due certificati, uno da utilizzarsi per la firma e l'altro per l'autenticazione. Se il dispositivo è abilitato alla funzione di autenticazione (CNS), dovrebbe riportare all'esterno la dicitura "Carta Nazionale dei Servizi". Sul sito Agenzia per l'Italia Digitale (http://www.agid.gov.it) è disponibile l'elenco pubblico dei certificatori accreditati che emettono certificati CNS e certificati di firma digitale.

3. La CNS può essere di tipologia *LIKE* od obbligatoriamente *FULL*?

Non è consentito l'utilizzo di "CNS LIKE", è previsto il solo utilizzo di CNS (o "CNS Full") rilasciate da CA presenti sull'elenco pubblico dei certificatori che emettono certificati CNS (Trusted LIST ITALIANA). Tale lista include tutti i certificati afferenti le autorità di certificazione che rilasciano certificati anche per le Carte Nazionali dei Servizi.

Per i dettagli tecnici e normativi si rimanda al sito AGID:

http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/carta-nazionale-servizi

http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche/certificati

4. Ho una CNS, come la installo e come configuro il *browser*?

Bisogna essere in possesso di una CNS e di un lettore oppure di una chiavetta USB che contiene i certificati e il software necessario. L'installazione e la configurazione potrà essere portata a termine seguendo le istruzioni del fornitore.

A titolo di esempio si segnalano i siti dei principali fornitori:

https://www.firma.infocert.it/installazione/certificato4.php

https://www.firma.infocert.it/installazione/certificato3.php

https://www.card.infocamere.it/infocard/pub/

https://www.card.infocamere.it/infocard/pub/guide-installazione_5390

https://www.card.infocamere.it/infocard/pub/assistenza_5442

5. Ho inserito la CNS ma non mi chiede il PIN.

Accertarsi di seguire la guida di installazione del software a corredo della CNS. Accertarsi altresì di aver disabilitato in Internet Explorer (o sul browser utilizzato) i protocolli "SSL 2.0" e "SSL 3.0". L'autenticazione con CNS è supportata solo dai protocolli TLS 1.0 o superiore.

6. Ho inserito la CNS, il browser funziona su altri siti ma non chiede il PIN.

Provare altri browser come ad esempio Mozilla Firefox. Su quest'ultimo in particolare potrebbe essere necessario importare il dispositivo (SMARTCARD o token USB). Sulla Rete esistono diverse guide fornite dai certificatori accreditati che possono aiutare in questa operazione. Per qualsiasi ulteriore informazione, per la risoluzione di eventuali malfunzionamenti e per reperire il software necessario (driver), si rimanda, come già segnalato, ai siti degli Enti Certificatori.

7. Non riesco a confermare la registrazione iniziale.

È possibile che siano trascorse più di 72 ore e quindi è necessario ripetere la procedura di registrazione. In alcuni casi particolari, pur non essendo trascorse le 72 ore, è possibile che l'attivazione non vada a buon fine a causa del comportamento di alcuni client e-mail che modificano il link inviato dall'applicazione rendendolo invalido. In questo caso, il processo di registrazione può essere completato copiando il testo dell'indirizzo mediante la funzionalità di copia e quindi incollandolo direttamente nella barra indirizzi del browser.

8. Non ho ricevuto la e-mail di conferma registrazione.

Accertarsi che la propria casella postale non abbia superato i limiti di utilizzo consentiti, ovvero che l'e-mail non sia stata intercettata da sistemi automatici di anti-spam o anti-phishing. In tal caso, controllare nella cartella posta indesiderata della vostra casella. Accertarsi di non aver utilizzato un indirizzo di posta elettronica certificata (PEC).

9. Non sono sicuro di aver inserito l'indirizzo e-mail corretto.

Attendere 72 ore e ripetere la registrazione con l'indirizzo corretto.

Abilitazione e Gestione dell'Utenza Applicativa A2A - Credenziali

10. Cos'è una credenziale applicativa (A2A)?

La credenziale A2A è un codice alfanumerico nella forma A2A-<123456789>, a tale codice identificativo è possibile far corrispondere una serie di informazioni:

- certificato x509 di autenticazione;
- certificato x509 di cifratura;
- uno o più manager della credenziale (i manager si distinguono per codice fiscale e sono persone fisiche identificate con la CNS);
- uno o più contesti applicativi, ogni credenziale può essere utilizzata su una o più applicazioni esposte sul canale Internet.

11. L'utenza A2A deve essere rilasciata a una persona fisica?

Si. Una persona fisica incaricata dall'Operatore si registra al sito della Banca d'Italia utilizzando credenziali SPID almeno di secondo livello, ovvero, solo per la fase di avvio del progetto, altri strumenti di identificazione digitale aventi livelli di sicurezza equipollenti.

12. Credenziali di collaudo (alias certificazione) e produzione, come si distinguono?

Le controparti otterranno credenziali A2A (applicative) che il sistema assegnerà attraverso l'interfaccia di gestione, la forma delle credenziali sarà del tipo A2A-1234567. Esiste un'interfaccia distinta per l'ambiente di TEST e di ESERCIZIO, con assegnazione separata quindi delle utenze di autenticazione tra i due ambienti. Sarà cura della controparte utilizzare la credenziale corretta sull'ambiente corrispondente.

13. **Nel caso in cui un soggetto faccia da Tramite PA (partner tecnologico) per più Enti, questi ultimi sono singolarmente tenuti a comunicare alla RGS l'identificativo dell'Utenza A2A utilizzando il sistema PCC?**

Si. Il rappresentante della PA accreditato sulla Piattaforma Web per la certificazione dei crediti commerciali comunica l'identificativo dell'utenza A2A alla RGS utilizzando i servizi offerti dalla PCC. Il Tramite si fa invece carico dei primi due step della procedura di registrazione (ottenere un'utenza applicativa A2A e associarvi un certificato digitale per l'autenticazione).

14. **Qualora la persona fisica registrata alla piattaforma SIOPE+, manager delle credenziali A2A, cessi dalle sue funzioni cosa ne è delle credenziali associate e della relativa utenza?**

Il manager delle credenziali A2A può delegare la gestione delle credenziali a uno o più manager, che potranno operare singolarmente. La cancellazione di uno dei manager non inficia la validità delle credenziali e dunque la possibilità di continuare a utilizzare l'utenza.

15. **Il Tramite può operare come tale per più enti utilizzando le stesse credenziali?**

Si. L'IdA2A, ottenuto dal Tramite con la procedura di *self-registration*, consente allo stesso di colloquiare con SIOPE+ per conto di più enti.

16. **Un manager può richiedere più utenze A2A?**

Si. Si ricordi che ogni credenziale deve disporre di almeno un certificato digitale (x509).

17. **Nel caso in cui un soggetto faccia da Tramite sia per conto di enti che per quello di tesorieri deve utilizzare due utenze applicative A2A?**

Si, sebbene sia tecnicamente possibile utilizzare un'unica utenza A2A per fare da tramite sia agli enti che ai tesorieri, si raccomanda l'utilizzazione di due distinte utenze applicative.

Abilitazione e Gestione dell'Utenza Applicativa A2A - Certificati

18. **Che requisiti deve avere il certificato x509 da associare all'utenza A2A?**

Il certificato di autenticazione deve essere rilasciato da un'Autorità di Certificazione (AC) da individuarsi tra quelle disponibili nel bundle Mozilla (https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/). Il certificato (usato per autenticazione client SSL) deve avere l'attributo "X509v3 Extended Key Usage: TLS Web Client Authentication".

19. **Qualora si disponga già di un certificato x509, utilizzato per la gestione di un'utenza applicativa diversa da quella afferente la piattaforma SIOPE PLUS (es. procedura ABACO) può ricorrersi al medesimo certificato?**

Si. Si badi che il certificato può essere utilizzato nuovamente, ma le credenziali devono essere attivate ex novo, non potendosi utilizzare quelle già in essere per la gestione di altra procedura.

20. **È ammessa la gestione via software dei certificati per la protezione del canale, oppure risulta obbligatorio l'utilizzo di apparati HW (i cosiddetti HSM)?**

Solo i certificati di firma devono essere conservati su dispositivi sicuri per l'apposizione della firma del tipo SmartCard (CNS). I certificati utilizzati per l'autenticazione del canale sono di norma oggetti su file protetti da opportuni SW (Keystore). La responsabilità della gestione della sicurezza ricade interamente sul possessore del certificato associato alla credenziale.

21. È possibile per un centro servizi utilizzare un unico certificato per "cifrare " (via crittografia e firma del file trasmesso) le informazioni degli intermediari serviti nello scambio di informazioni con il sistema o è necessario utilizzare un certificato per ogni intermediario per la "*securizzazione*" del dato?

Vanno distinti i due casi dipendenti dal *"verso"* dei messaggi:

- per i messaggi trasmessi da un intermediario il cui destinatario è il sistema la cifratura dei messaggi dovrà essere eseguita con il certificato X509 fornito dal sistema stesso e reso disponibile su Internet attraverso il portale informativo;
- per i messaggi trasmessi dal sistema il cui destinatario è un intermediario esisterà un certificato di cifratura caricato sulla credenziale A2A associato all'intermediario.

22. Che tipo di certificati sono i file con estensione ".pem"? Si fa sempre riferimento al certificato di cifratura e di autenticazione?

Il formato PEM è il formato più comunemente utilizzato dalle Certification Authorities per emettere i certificati. Altre estensioni convenzionali possono essere .crt e .cer. I PEM sono file ASCII con codifica Base64 e contengono "-----BEGIN CERTIFICATE-----" all'inizio e "-----END CERTIFICATE-----" alla fine. Possono essere in formato PEM sia certificati server, che certificati intermedi e chiavi private.

(cfr. https://it.wikipedia.org/wiki/X.509, https://www.ietf.org/rfc/rfc5280.txt)

23. Quali sono le tipologie di certificato associabili all'utenza A2A?

- certificato X509 di autenticazione: necessario per mutua autenticazione SSL tra gli applicativi delle controparti e i sistemi applicativi. COMMON NAME= <campo libero, si consiglia di utilizzare un nome descrittivo dell'ente/controparte/intermediario/tramite>; X509v3 Key Usage critical: Digital Signature, Key Encipherment; X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication;

- certificato di cifratura: utilizzato dall'sistema per cifrare i flussi di risposta verso le controparti. Può essere riutilizzato lo stesso certificato utilizzato per l'autenticazione.

24. Quanti certificati digitali sono necessari?

Le controparti (segnalanti) possono gestire le credenziali A2A con un solo manager identificato con CNS. Eventualmente, potrebbero richiedere due diversi certificati x509 di autenticazione per finalità applicativa (A2A), come anche due diversi certificati di firma e due diversi certificati di crittografia; distinti cioè per gli ambienti di TEST (alias certificazione) e ambienti di PRODUZIONE. Nulla osta ai segnalanti l'utilizzo di solo tre certificati (identificazione, firma e crittografia) sia per TEST che per PRODUZIONE.

25. L'acquisizione dei certificati per l'autenticazione e cifratura dei dati vanno richiesti presso un'azienda accreditata dall'Agenzia per l'Italia Digitale AGID sia per le informazioni da segnalante al sistema che viceversa? L'AGID è l'ente certificatore sia per i segnalanti che per il sistema?

No, la normativa vigente (EIDAS-AGID) impone vincoli solo sui certificati digitali utilizzabili per Firma Digitale Qualificata, Marca Temporale e CNS (identificazione persona fisica). I certificati di autenticazione e cifratura applicativa (flussi A2A) possono essere rilasciati da una qualunque CA di cui al bundle mozilla (vedi infra, faq n. 20).

26. Il certificato di cifratura dovrebbe contenere una chiave AES generata dal segnalante e protetta con una chiave pubblica, questa chiave pubblica è del sistema?

No, l'eventuale utilizzo di CSR (certificate signing request) per la generazione di certificati X509 fa parte del metodo scelto dalla CA di riferimento della controparte, ciò detto non si entra nel merito di come sono generati/approvvigionati i certificati di autenticazione e cifratura.

27. Se il sistema deve utilizzare la chiave AES per cifrare i dati che inoltra al segnalante, sarebbe possibile aprire quella cifratura solo con la chiave privata del sistema. Non è chiaro se il processo preveda la cifratura della chiave AES con la chiave pubblica del sistema o no.

Lo standard di riferimento per la cifratura è la RFC3852. Si segnala che la chiave simmetrica di cifratura AES viene cifrata con la chiave pubblica del destinatario in modo che il solo il destinatario la possa aprire usando la sua chiave privata.

28. Come si usa il certificato X509 di autenticazione?

La mutua autenticazione tra applicazioni avviene con lo scambio di certificati digitali di tipo X509. Lo standard di riferimento per l'autenticazione è la RFC5246.

29. La connessione SSL dell'applicazione fallisce. Il certificato del SERVER non sembra valido.

L'applicazione client deve avere nel suo archivio delle autorità attendibili (TRUSTSTORE) il certificato della CA_root che ha firmato il certificato della CA intermedia, che a sua volta ha firmato il certificato SSL del SERVER che eroga le funzionalità applicative.

30. Abbiamo incluso la CA_root nell'archivio delle autorità attendibili ma la connessione fallisce ancora, Il certificato del CLIENT non sembra accettato.

Durante l'handshake TLS il client deve fornire anche il certificato della CA intermedia (CHAIN). Tale modalità è espressamente prevista dallo standard RFC5246: The Transport Layer Security (TLS) Protocol Version 1.2.

Cfr. https://tools.ietf.org/html/rfc5246#section-7.4.2:

certificate_list: this is a sequence (chain) of certificates. The sender's certificate MUST come first in the list. Each following certificate MUST directly certify the one preceding it. Because certificate validation requires that root keys be distributed independently, the self-signed certificate that specifies the root certificate authority MAY be omitted from the chain, under the assumption that the remote end must already possess it in order to validate it in any case. The same message type and structure will be used for the client's response to a certificate request message. Note that a client MAY send no certificates if it does not have an appropriate certificate to send in response to the server's authentication request.